Alfred R. Fabricant
afabricant@fabricantllp.com
Peter Lambrianakos
plambrianakos@fabricantllp.com
Vincent J. Rubino, III
vrubino@fabricantllp.com
Joseph Mercadante
jmercadante@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue, Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Benjamin T. Wang (CA SBN 228712)
bwang@raklaw.com
Minna Y. Chan (CA SBN 305941)
mchan@raklaw.com
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, California 90025
Telephone: (310) 826-7474
Facsimile: (310) 826-9226

Attorneys for Plaintiff
Taasera Licensing LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TAASERA LICENSING LLC, Plaintiff, v. SONICWALL, INC., Defendant.	Case No. 5:24-cv-00749 **TAASERA LICENSING LLC'S COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Taasera Licensing LLC ("Taasera" or "Plaintiff") files this Complaint for Patent Infringement and Demand for Jury Trial against SonicWall, Inc. ("SonicWall" or "Defendant") and alleges:

THE PARTIES

1. Taasera is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located in Plano, Texas.

2. Upon information and belief, SonicWall is a Delaware corporation with its headquarters and principal place of business at 1033 McCarthy Blvd., Milpitas, CA 95035.

JURISDICTION AND VENUE

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) and (c) and 28 U.S.C. § 1400(b).

5. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant is headquartered and has its principal place of business in this District. Defendant also regularly and continuously does business in this District and has infringed or induced infringement, and continues to do so, in this District. In addition, the Court has personal jurisdiction over Defendant because minimum contacts have been established with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district-wide basis.

PATENTS-IN-SUIT

7. On March 2, 2010, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,673,137 (the "'137 Patent") entitled "System and Method for the Managed Security Control of Processes on a Computer System." The '137 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '137 Patent was developed by Thomas James Satterlee and William Frank Hackenberger of IBM. A true and correct copy of the '137 Patent is attached hereto as Exhibit 1.

8. On February 28, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,127,356 (the "'356 Patent") entitled "System, Method and Program Product for Detecting Unknown Computer Attacks." The '356 Patent generally relates to technology that determines whether a packet is a new, exploit candidate. The technology described in the '356 Patent was developed by Frederic G. Thiele and Michael A. Walter of IBM. A true and correct copy of the '356 Patent is attached hereto as Exhibit 2.

9. On December 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,327,441 (the "'441 Patent") entitled "System and Method for Application Attestation." The '441 Patent generally relates to technology for application attestation. The technology described in the '441 Patent was developed by Srinivas Kumar and Gurudatt Shashikumar of TaaSera, Inc. A true and correct copy of the '441 Patent is attached hereto as Exhibit 3.

10. On September 30, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,850,517 (the "'517 Patent") entitled "Runtime Risk Detection Based on User, Application, and System Action Sequence Correlation." The '517 Patent generally relates to runtime risk detection based on user, application, and/or system actions. The technology

described in the ’517 Patent was developed by Srinivas Kumar of TaaSera, Inc. A true and correct copy of the ’517 Patent is attached hereto as Exhibit 4.

11. On March 24, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,990,948 (the "’948 Patent") entitled "Systems and Methods for Orchestrating Runtime Operational Integrity." The ’948 Patent generally relates to technology that provides runtime operational integrity profiles identifying a threat level of subjects or applications. The technology described in the ’948 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc. A true and correct copy of the ’948 Patent is attached hereto as Exhibit 5.

12. On July 28, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,092,616 (the "’616 Patent") entitled "Systems and Methods for Threat Identification and Remediation." The ’616 Patent generally relates to technology that provides integrity profiles identifying a threat level of a system. The technology described in the ’616 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc. A true and correct copy of the ’616 Patent is attached hereto as Exhibit 6.

13. On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the "’038 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." The ’038 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’038 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM. A true and correct copy of the ’038 Patent is attached hereto as Exhibit 7.

14. On March 20, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,923,918 (the "’918 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." The ’918 Patent

generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the ’918 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM. A true and correct copy of the ’918 Patent is attached hereto as Exhibit 8.

15. On March 28, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,608,997 (the “’997 Patent”) entitled “Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities.” The ’997 Patent generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the ’997 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM. A true and correct copy of the ’997 Patent is attached hereto as Exhibit 9.

16. Four of the Patents-in-Suit were developed by TaaSera, Inc. TaaSera, Inc. was a leader in preemptive breach detection systems, and comprised of security architects and subject matter experts with decades of experience in firewalls, intrusion detection, security event management, malware analysis, and endpoint security. The TaaSera, Inc. patents identify patterns of malicious coordinated network and endpoint behaviors. TaaSera, Inc. manufactured commercial and academic versions of its NetTrust Security Appliance. NetTrust combined breach detection with security analytics to identify hidden threatening network behaviors. The analytics engine analyzed behavioral profiles, threat patterns, and contextual evidence to rank systems by their risk of breach.

17. Five of the Patents-in-Suit were invented by International Business Machines (“IBM”). IBM pioneered the field of network security. Every year, IBM spends billions of dollars on research and development to invent, market, and sell new technology, and IBM obtains patents on many of the novel inventions that come out of that work, including the Patents-in-Suit. The five

patents invented by IBM are the result of the work from 6 different researchers, spanning over a decade.

18. Taasera is the sole and exclusive owner of all right, title, and interest in the ’137 Patent, the ’356 Patent, the ’441 Patent, the ’517 Patent, the ’948 Patent, the ’616 Patent, the ’038 Patent, the ’918 Patent, and the ’997 Patent (collectively, the “Patents-in-Suit”), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Taasera also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

THE ACCUSED PRODUCTS

19. Defendant has infringed and continues to infringe the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or import the Accused Products that implement the inventions claimed in the Patents-in Suit. The Accused Products are described below.

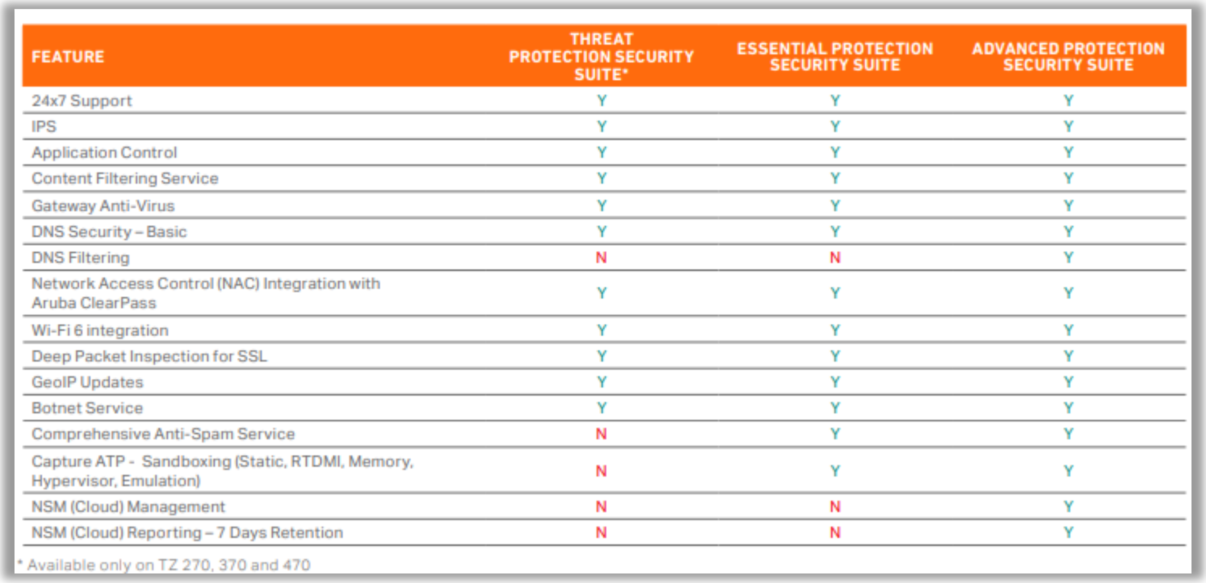
SonicWall Network Security Products and Network Security Services

20. SonicWall makes, uses, sells, offers to sell, and/or imports, and actively induces others to make, use, sell, offer to sell, and/or import its various firewall products, including SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W)[1], NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450,

[1] https://www.sonicwall.com/products/firewalls/entry-level/; https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-tz-series-gen-7.pdf; https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-tz-series-gen-6.pdf.

NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650)[2], NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400)[3], NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270)[4].

21. SonicWall "integrates a wide range of network security services into convenient, affordable packages: Threat Protection Service Suite, Essential Protection Service Suite, and Advanced Protection Service Suite."[5]



FEATURE	THREAT PROTECTION SECURITY SUITE*	ESSENTIAL PROTECTION SECURITY SUITE	ADVANCED PROTECTION SECURITY SUITE
24x7 Support	Y	Y	Y
IPS	Y	Y	Y
Application Control	Y	Y	Y
Content Filtering Service	Y	Y	Y
Gateway Anti-Virus	Y	Y	Y
DNS Security – Basic	Y	Y	Y
DNS Filtering	N	N	Y
Network Access Control (NAC) Integration with Aruba ClearPass	Y	Y	Y
Wi-Fi 6 integration	Y	Y	Y
Deep Packet Inspection for SSL	Y	Y	Y
GeoIP Updates	Y	Y	Y
Botnet Service	Y	Y	Y
Comprehensive Anti-Spam Service	N	Y	Y
Capture ATP - Sandboxing (Static, RTDMI, Memory, Hypervisor, Emulation)	N	Y	Y
NSM (Cloud) Management	N	N	Y
NSM (Cloud) Reporting – 7 Days Retention	N	N	Y

* Available only on TZ 270, 370 and 470

[6]

[2] https://www.sonicwall.com/products/firewalls/mid-range/; https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-gen-7-nsa-series.pdf; https://www.sonicwall.com/medialibrary/en/datasheet/datasheet-sonicwall-network-security-appliance-nsa-series.pdf.

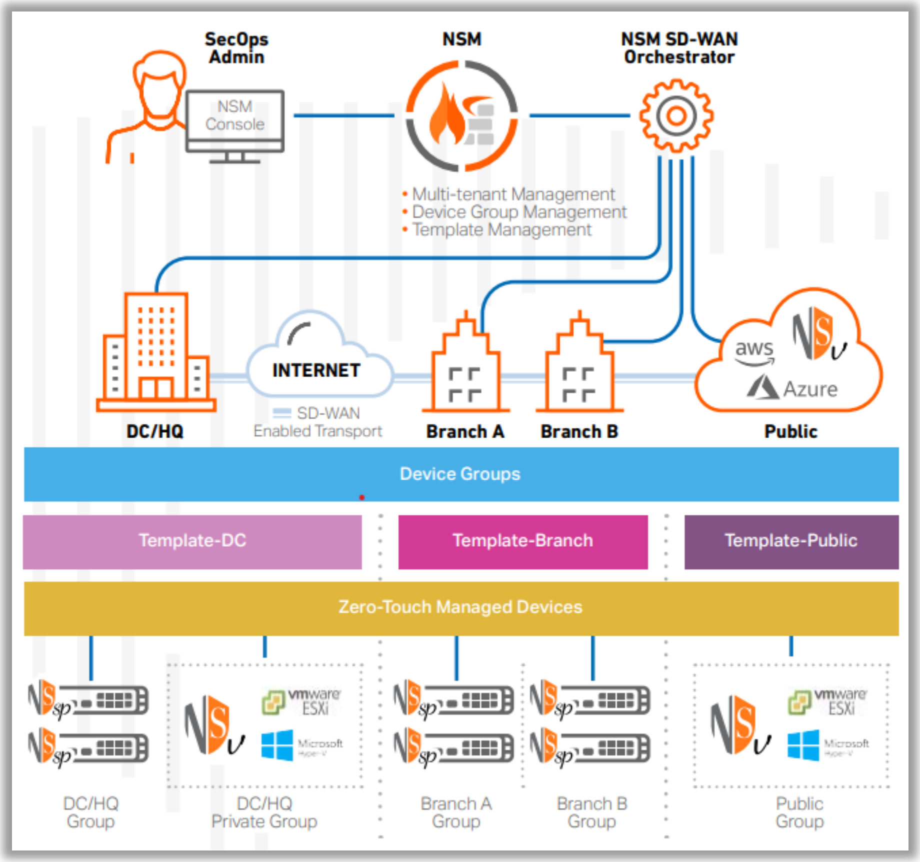
[3] https://www.sonicwall.com/products/firewalls/high-end/; https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-gen-7-nssp-series.pdf; https://www.sonicwall.com/medialibrary/en/datasheet/datasheet-sonicwall-network-security-services-platform-nssp-12000-series.pdf; https://www.sonicwall.com/medialibrary/en/datasheet/datasheet-sonicwall-supermassive-series.pdf.

[4] https://www.sonicwall.com/products/firewalls/nsv-series/; https://www.sonicwall.com/medialibrary/en/datasheet/datasheet-nsv-270-470-870.pdf.

[5] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-protection-service-suites.pdf, at 1.

[6] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-protection-service-suites.pdf, at 3.

22. SonicWall Network Security Manager (NSM) allows an administrator, "[f]rom a single console, [to] orchestrate all firewall operations, see hidden risks, discover misconfigured policies, and make compliance easier with a full audit trail."[7]



[8]

23. Intrusion Prevention Service (IPS) "integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic."[9]

24. "SonicOS and SonicOSX (SonicOS/X) 7 runs on SonicWall network security appliances (firewalls) and provides the web management interface for configuring the features, policies, and security services, updating the firmware, managing connected devices such as switches

[7] https://www.sonicwall.com/products/management-and-reporting/network-security-manager/

[8] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

[9] https://www.sonicwall.com/support/knowledge-base/intrusion-prevention-service-frequently-asked-questions-faqs/170505669856588/

and access points, monitoring traffic/users/threats, investigating events, and much more. SonicOS/X runs on top of SonicCore, SonicWall's secure underlying operating system."[10] "SonicOSX 7 is supported on SonicWall NSv and NSsp series firewalls. SonicOS 7 is supported on SonicWall TZ series, NSa series, NSsp 13700 and NSv series firewalls."[11]

25. "Capture ATP helps SonicWall firewall identify whether a file is a virus or not by transmitting the file to the Cloud where the SonicWall Capture ATP cloud service analyzes the file to determine if it is a virus and it then sends the results to the SonicWall firewall. This process is done in real time while the file is being processed by the SonicWall firewall."[12] "SonicWall Capture ATP scans a broad range of file types to prevent zero-day attacks, targeted malware, advanced ransomware and more. Capture ATP analyzes behavior in a multi-engine sandbox platform that includes full system emulation, hypervisor-level analysis, virtualized sandboxing and RTDMI™, which uses real-time, memory-based inspection techniques to force malware to reveal its weaponry into memory. By giving admins the ability to block until verdict, create customized policies and scan select files in the cloud, SonicWall Capture ATP combines the efficiency of automation with greater flexibility and control."[13]

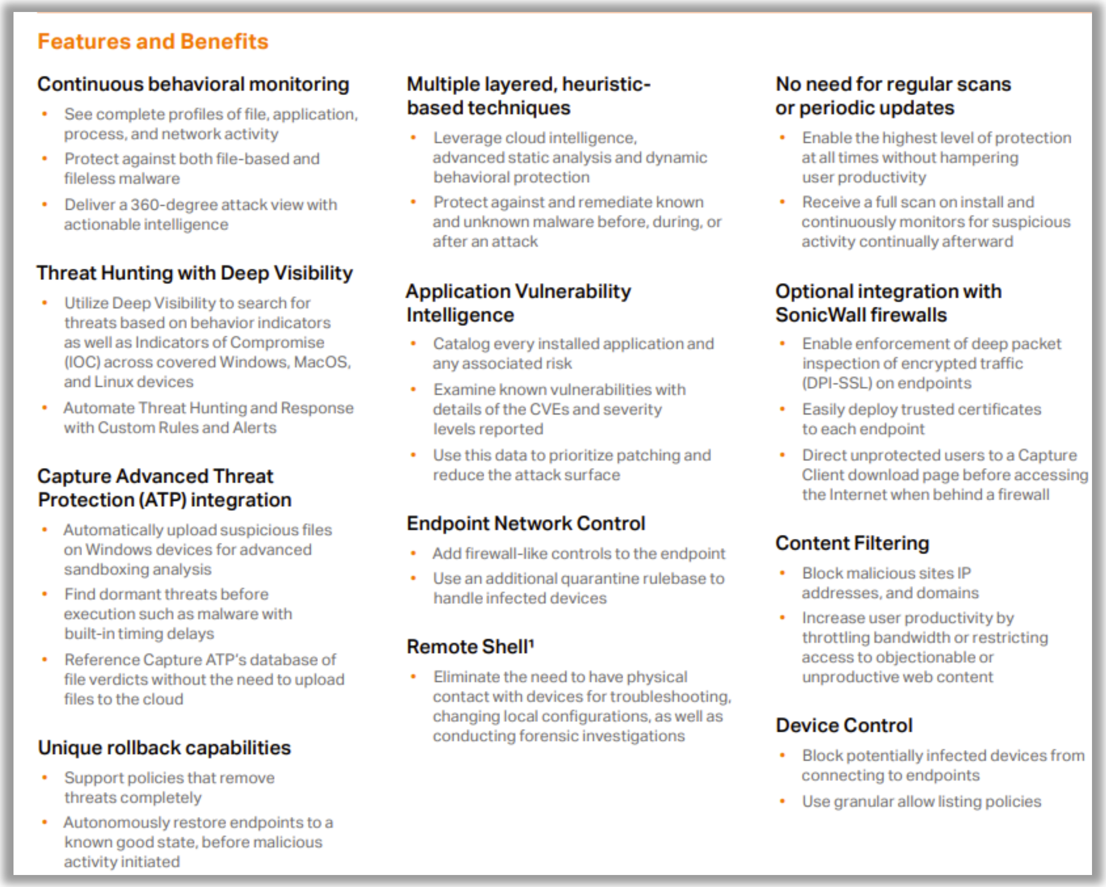
26. "Capture Threat Assessment (also known as CTA) is a SonicWall service that provides network traffic and threat report generation. The service is provided directly from the SonicOS firewall interface. You can navigate to the Capture Threat Assessment page to generate the report. The output is generated in PDF format, and previous reports are saved in the cloud and displayed in a table so you can access them later."[14] "The Capture Threat Assessment service

[10] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 4.
[11] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 5.
[12] https://www.sonicwall.com/support/knowledge-base/capture-advanced-threat-protection-feature-overview/170504863294345/
[13] https://www.sonicwall.com/products/capture-advanced-threat-protection/
[14] https://www.sonicwall.com/techdocs/pdf/cta-user_guide.pdf, at 3.

accurately identifies real-time vulnerabilities, exploits, intrusions and other network-based threats. With it, you can see security gaps in the organization and better understand the risks."[15]

SonicWall Capture Client and Integrations

27. SonicWall makes, uses, sells, offers to sell, and/or imports, and actively induces others to make, use, sell, offer to sell, and/or import SonicWall Capture Client, which "is a unified client platform that delivers multiple Endpoint Detection & Response (EDR) capabilities, including behavior-based malware protection, advanced threat hunting and visibility into application vulnerabilities."[16] Capture Client is capable of the following features and benefits:



Features and Benefits

Continuous behavioral monitoring

- See complete profiles of file, application, process, and network activity
- Protect against both file-based and fileless malware
- Deliver a 360-degree attack view with actionable intelligence

Threat Hunting with Deep Visibility

- Utilize Deep Visibility to search for threats based on behavior indicators as well as Indicators of Compromise (IOC) across covered Windows, MacOS, and Linux devices
- Automate Threat Hunting and Response with Custom Rules and Alerts

Capture Advanced Threat Protection (ATP) integration

- Automatically upload suspicious files on Windows devices for advanced sandboxing analysis
- Find dormant threats before execution such as malware with built-in timing delays
- Reference Capture ATP's database of file verdicts without the need to upload files to the cloud

Unique rollback capabilities

- Support policies that remove threats completely
- Autonomously restore endpoints to a known good state, before malicious activity initiated

Multiple layered, heuristic-based techniques

- Leverage cloud intelligence, advanced static analysis and dynamic behavioral protection
- Protect against and remediate known and unknown malware before, during, or after an attack

Application Vulnerability Intelligence

- Catalog every installed application and any associated risk
- Examine known vulnerabilities with details of the CVEs and severity levels reported
- Use this data to prioritize patching and reduce the attack surface

Endpoint Network Control

- Add firewall-like controls to the endpoint
- Use an additional quarantine rulebase to handle infected devices

Remote Shell[1]

- Eliminate the need to have physical contact with devices for troubleshooting, changing local configurations, as well as conducting forensic investigations

No need for regular scans or periodic updates

- Enable the highest level of protection at all times without hampering user productivity
- Receive a full scan on install and continuously monitors for suspicious activity continually afterward

Optional integration with SonicWall firewalls

- Enable enforcement of deep packet inspection of encrypted traffic (DPI-SSL) on endpoints
- Easily deploy trusted certificates to each endpoint
- Direct unprotected users to a Capture Client download page before accessing the Internet when behind a firewall

Content Filtering

- Block malicious sites IP addresses, and domains
- Increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content

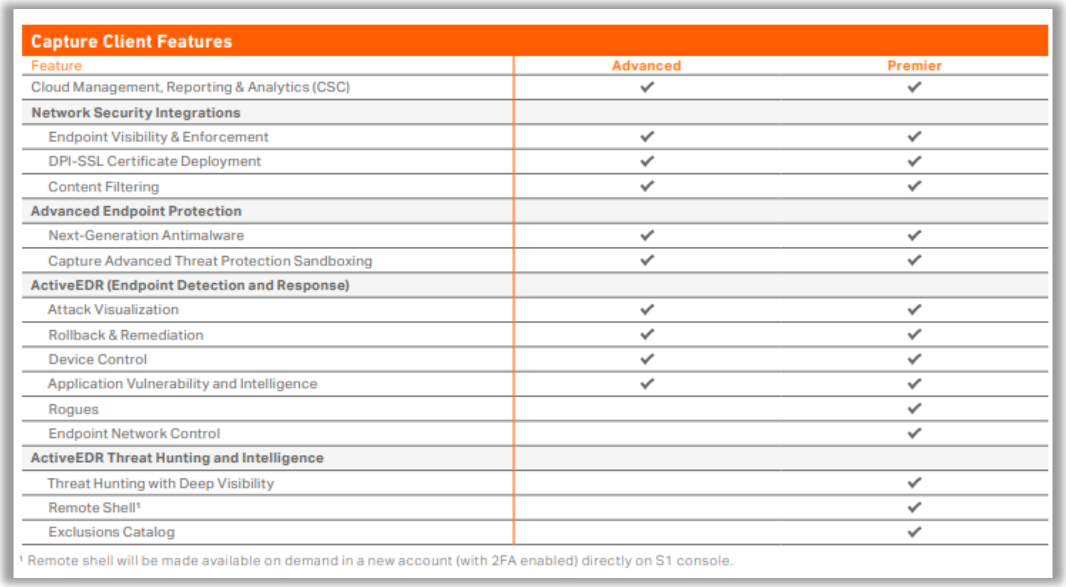
Device Control

- Block potentially infected devices from connecting to endpoints
- Use granular allow listing policies

[17]

[15] *Id.*
[16] https://www.sonicwall.com/products/firewalls/security-services/capture-client/.
[17] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.

28. Upon information and belief, SonicWall offers two packages of Capture Client features: Advanced and Premier:



Capture Client Features

Feature	Advanced	Premier
Cloud Management, Reporting & Analytics (CSC)	✓	✓
Network Security Integrations		
Endpoint Visibility & Enforcement	✓	✓
DPI-SSL Certificate Deployment	✓	✓
Content Filtering	✓	✓
Advanced Endpoint Protection		
Next-Generation Antimalware	✓	✓
Capture Advanced Threat Protection Sandboxing	✓	✓
ActiveEDR (Endpoint Detection and Response)		
Attack Visualization	✓	✓
Rollback & Remediation	✓	✓
Device Control	✓	✓
Application Vulnerability and Intelligence	✓	✓
Rogues		✓
Endpoint Network Control		✓
ActiveEDR Threat Hunting and Intelligence		
Threat Hunting with Deep Visibility		✓
Remote Shell[1]		✓
Exclusions Catalog		✓

[1] Remote shell will be made available on demand in a new account (with 2FA enabled) directly on S1 console.

[18]

29. SonicWall Capture Client "integrat[es] with the Capture Security Center [to] create[] a single pane of glass across network and endpoint security operations for centralized control of attack visualization, rollback and remediation, network control and remote shell troubleshooting abilities."[19]

30. Capture Client also "integrates with SonicWall Capture Advanced Threat Protection (ATP) to take advantage of its ability to manipulate and test files in ways that endpoints can't. Discovering, quarantining, and removing undercover threats before they execute saves time for end users and administrators."[20] Capture Client also features an optional integration with SonicWall firewalls that "direct[s] unprotected users to a Capture Client download page before accessing the Internet when behind a firewall."[21]

COUNT I

[18] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 3.
[19] https://www.sonicwall.com/products/firewalls/security-services/capture-client/
[20] https://www.sonicwall.com/products/firewalls/security-services/capture-client/; https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.
[21] *Id.*

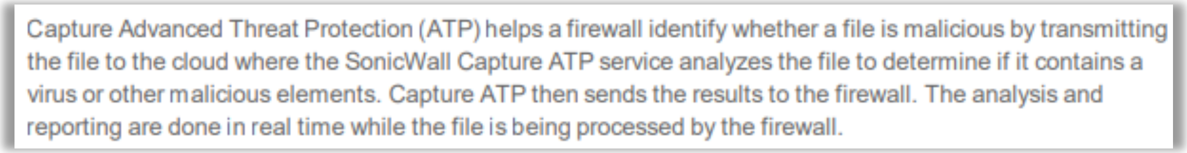
(Infringement of the ‘137 Patent)

31. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

32. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’137 Patent.

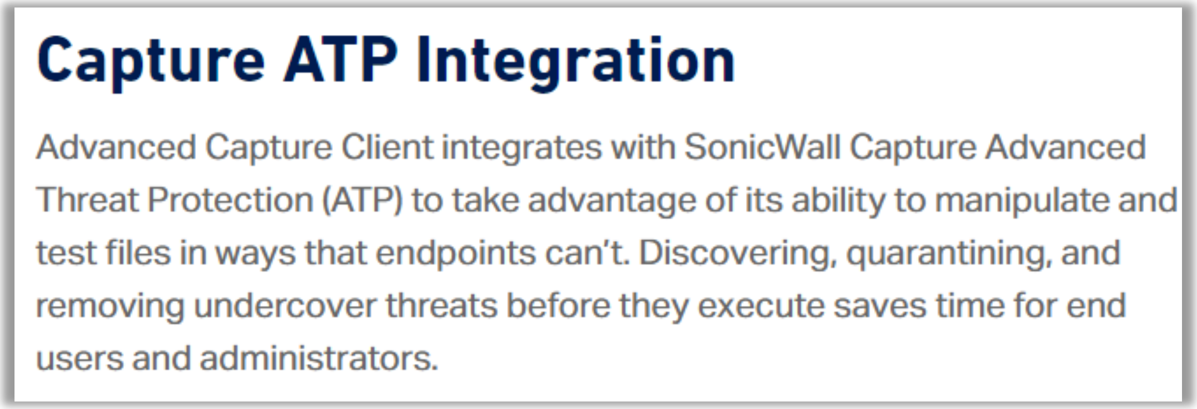
33. Defendant has and continues to directly infringe the ’137 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’137 Patent. Such products include at least SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) integrated with Capture ATP, or SonicWall Capture Client integrated with Capture ATP (the “’137 Accused Products”), which practice a system for managing security of a computing device comprising: a pre-execution module operable for receiving notice from the computing device's operating system that a new program is being loaded onto the computing device; a validation module coupled to the pre-execution module [sic] operable for determining whether the program is valid; a detection module coupled to the pre-execution module [sic] operable for intercepting a trigger from the computing device's operating system; and an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module.

34. Every ’137 Accused Product comprises a pre-execution module operable for receiving notice from the computing device's operating system that a new program is being loaded onto the computing device. For example, when a new program is being loaded, Capture ATP performs an analysis to find dormant threats before execution such as malware with built-in timing delays and determine if the file contains a virus or other malicious elements.



Capture Advanced Threat Protection (ATP) helps a firewall identify whether a file is malicious by transmitting the file to the cloud where the SonicWall Capture ATP service analyzes the file to determine if it contains a virus or other malicious elements. Capture ATP then sends the results to the firewall. The analysis and reporting are done in real time while the file is being processed by the firewall.

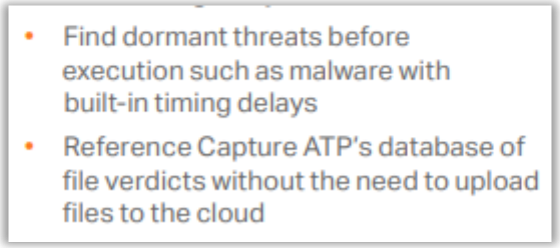
[22]



Capture ATP Integration

Advanced Capture Client integrates with SonicWall Capture Advanced Threat Protection (ATP) to take advantage of its ability to manipulate and test files in ways that endpoints can’t. Discovering, quarantining, and removing undercover threats before they execute saves time for end users and administrators.

[23]



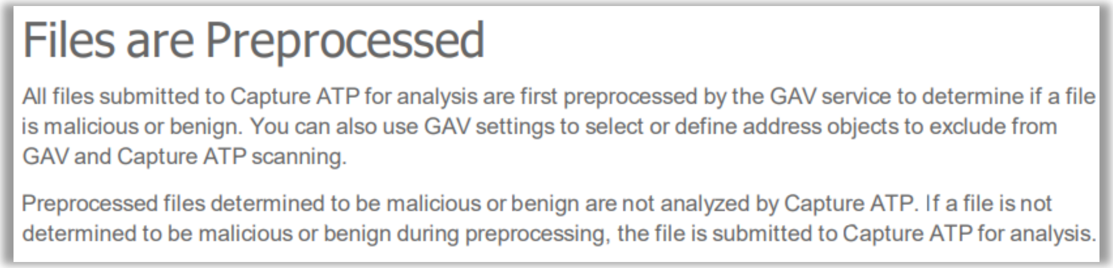
- Find dormant threats before execution such as malware with built-in timing delays
- Reference Capture ATP’s database of file verdicts without the need to upload files to the cloud

[24]

35. Every ’137 Accused Product comprises a validation module coupled to the pre-execution module [sic] operable for determining whether the program is valid. For example, during a pre-processing stage, Capture ATP determines whether program files are malicious or benign (i.e.,

[22] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 3.
[23] https://www.sonicwall.com/products/firewalls/security-services/capture-client/, at 2.
[24] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.

not valid or valid). For further example, Capture Client also performs pre-execution, static AI, techniques including blacklists, whitelists and cloud intelligence, along with complex analysis of pre-execution attributes to determine whether a program is valid.

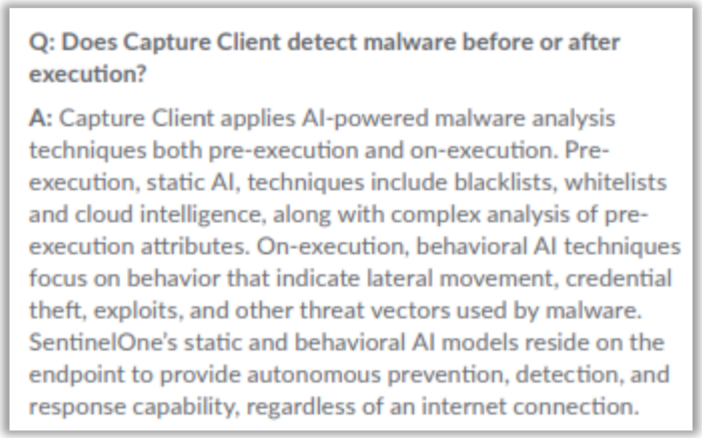


Files are Preprocessed

All files submitted to Capture ATP for analysis are first preprocessed by the GAV service to determine if a file is malicious or benign. You can also use GAV settings to select or define address objects to exclude from GAV and Capture ATP scanning.

Preprocessed files determined to be malicious or benign are not analyzed by Capture ATP. If a file is not determined to be malicious or benign during preprocessing, the file is submitted to Capture ATP for analysis.

[25]



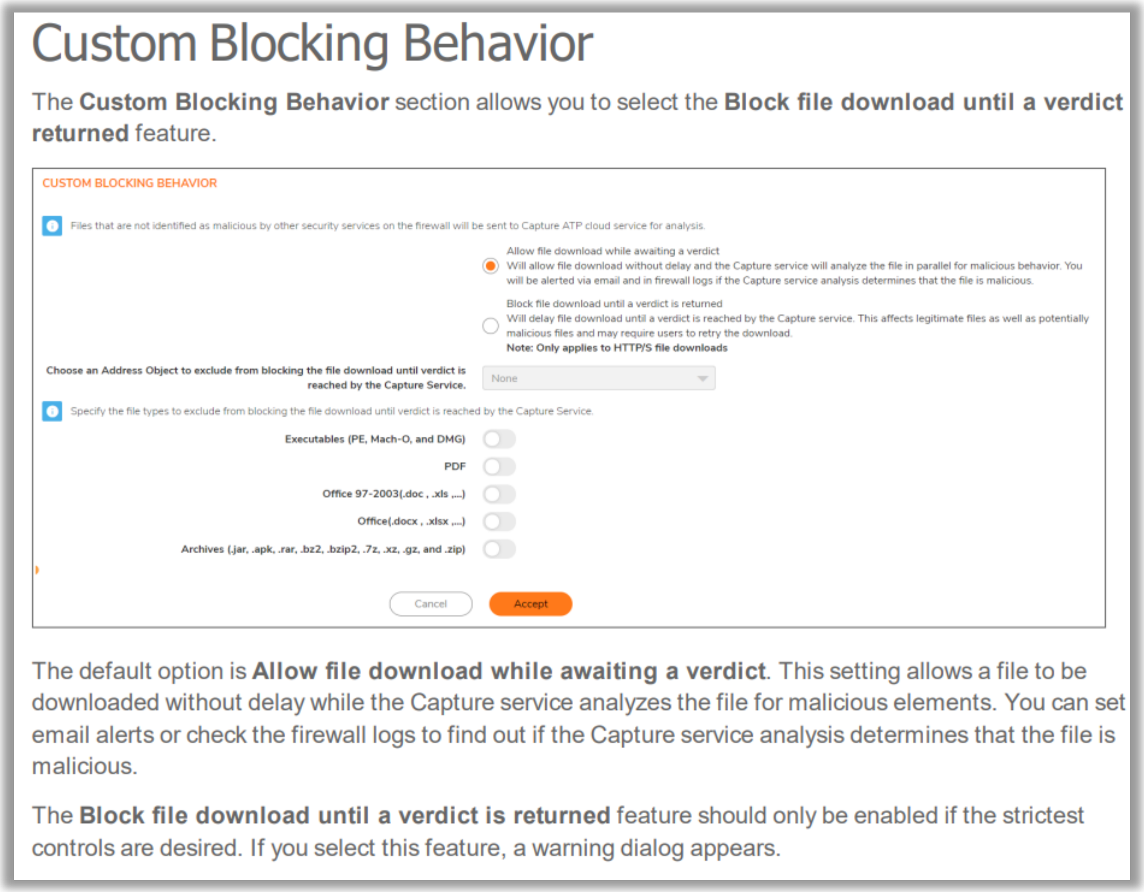
Q: Does Capture Client detect malware before or after execution?

A: Capture Client applies AI-powered malware analysis techniques both pre-execution and on-execution. Pre-execution, static AI, techniques include blacklists, whitelists and cloud intelligence, along with complex analysis of pre-execution attributes. On-execution, behavioral AI techniques focus on behavior that indicate lateral movement, credential theft, exploits, and other threat vectors used by malware. SentinelOne's static and behavioral AI models reside on the endpoint to provide autonomous prevention, detection, and response capability, regardless of an internet connection.

[26]

36. Every ’137 Accused Product comprises a detection module coupled to the pre-execution module [sic] operable for intercepting a trigger from the computing device's operating system. For example, Capture ATP comprises a detection module because opening, executing, or writing to each of the various identified file types are various triggers from the computing device’s operating system, and these triggers are necessary for determining whether a file is blocked until a verdict by Capture ATP is reached. For further example, other such triggers intercepted by Capture Client include the creation/modification of files, execution of processes and scripts on disk and memory, and inter-process communication.

[25] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 4.
[26] https://media.zones.com/images/pdf/sonicwall-capture-client-faqs.pdf, at 2.



Custom Blocking Behavior

The **Custom Blocking Behavior** section allows you to select the **Block file download until a verdict returned** feature.

CUSTOM BLOCKING BEHAVIOR

Files that are not identified as malicious by other security services on the firewall will be sent to Capture ATP cloud service for analysis.

● Allow file download while awaiting a verdict
Will allow file download without delay and the Capture service will analyze the file in parallel for malicious behavior. You will be alerted via email and in firewall logs if the Capture service analysis determines that the file is malicious.

○ Block file download until a verdict is returned
Will delay file download until a verdict is reached by the Capture service. This affects legitimate files as well as potentially malicious files and may require users to retry the download.
Note: Only applies to HTTP/S file downloads

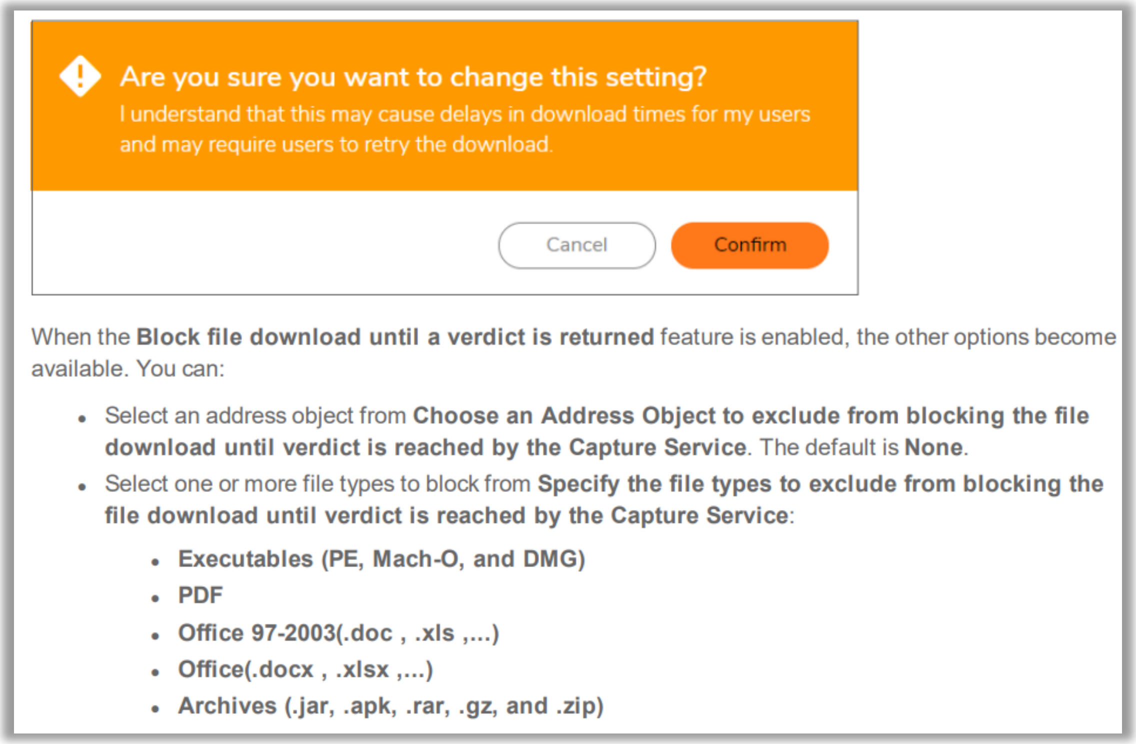
Choose an Address Object to exclude from blocking the file download until verdict is reached by the Capture Service. None

Specify the file types to exclude from blocking the file download until verdict is reached by the Capture Service.

Executables (PE, Mach-O, and DMG) ○
PDF ○
Office 97-2003(.doc , .xls ,...) ○
Office(.docx , .xlsx ,...) ○
Archives (.jar, .apk, .rar, .bz2, .bzip2, .7z, .xz, .gz, and .zip) ○

The default option is **Allow file download while awaiting a verdict**. This setting allows a file to be downloaded without delay while the Capture service analyzes the file for malicious elements. You can set email alerts or check the firewall logs to find out if the Capture service analysis determines that the file is malicious.

The **Block file download until a verdict is returned** feature should only be enabled if the strictest controls are desired. If you select this feature, a warning dialog appears.



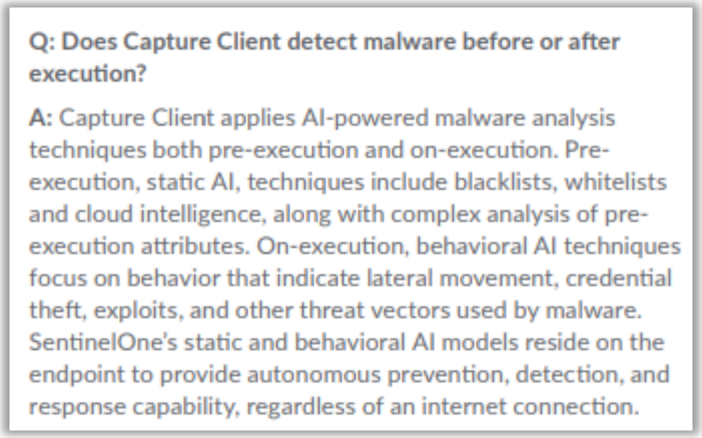
Are you sure you want to change this setting?

I understand that this may cause delays in download times for my users and may require users to retry the download.

When the **Block file download until a verdict is returned** feature is enabled, the other options become available. You can:

- Select an address object from **Choose an Address Object to exclude from blocking the file download until verdict is reached by the Capture Service**. The default is **None**.
- Select one or more file types to block from **Specify the file types to exclude from blocking the file download until verdict is reached by the Capture Service**:
  - **Executables (PE, Mach-O, and DMG)**
  - **PDF**
  - **Office 97-2003(.doc , .xls ,...)**
  - **Office(.docx , .xlsx ,...)**
  - **Archives (.jar, .apk, .rar, .gz, and .zip)**

[27]



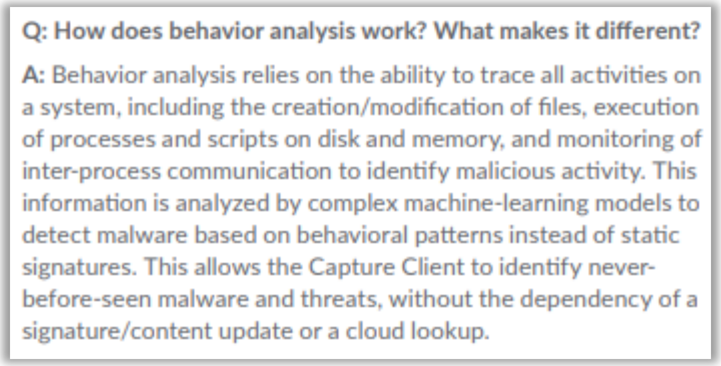
Q: Does Capture Client detect malware before or after execution?

A: Capture Client applies AI-powered malware analysis techniques both pre-execution and on-execution. Pre-execution, static AI, techniques include blacklists, whitelists and cloud intelligence, along with complex analysis of pre-execution attributes. On-execution, behavioral AI techniques focus on behavior that indicate lateral movement, credential theft, exploits, and other threat vectors used by malware. SentinelOne's static and behavioral AI models reside on the endpoint to provide autonomous prevention, detection, and response capability, regardless of an internet connection.

[28]

[27] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 9-10.

[28] https://media.zones.com/images/pdf/sonicwall-capture-client-faqs.pdf, at 2.

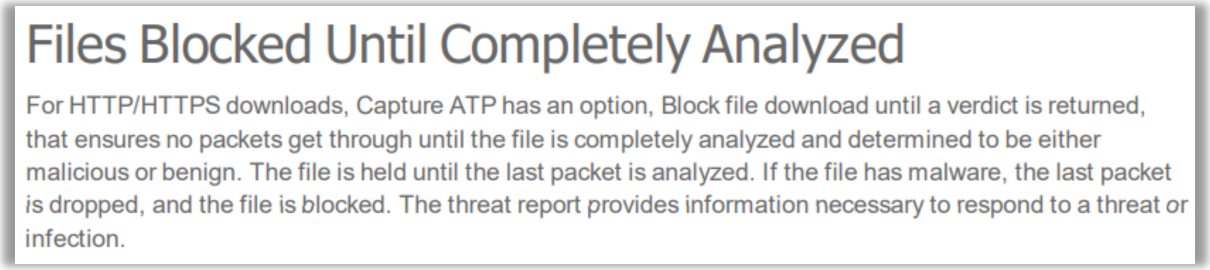


Q: How does behavior analysis work? What makes it different?

A: Behavior analysis relies on the ability to trace all activities on a system, including the creation/modification of files, execution of processes and scripts on disk and memory, and monitoring of inter-process communication to identify malicious activity. This information is analyzed by complex machine-learning models to detect malware based on behavioral patterns instead of static signatures. This allows the Capture Client to identify never-before-seen malware and threats, without the dependency of a signature/content update or a cloud lookup.

[29]

37. Every '137 Accused Product comprises an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module. For example, Capture ATP comprises an execution module for analyzing (i.e., monitoring) programs and files in response to determining whether those files are blocked in response to the file type triggers intercepted.

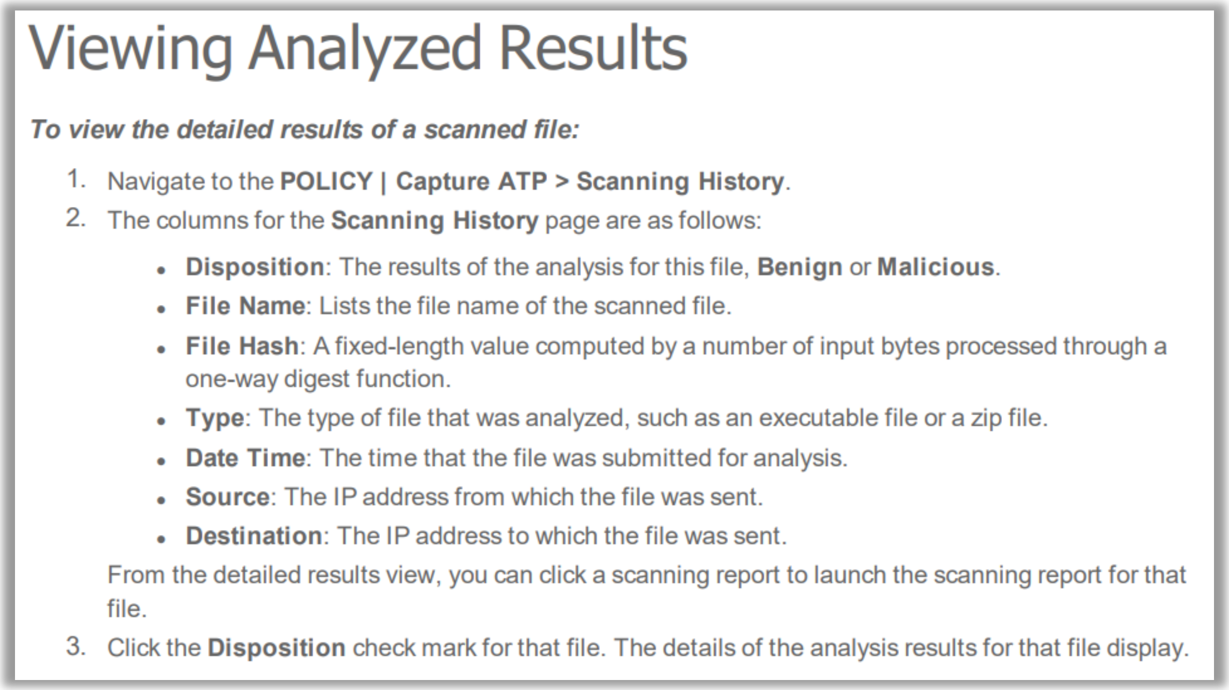


Files Blocked Until Completely Analyzed

For HTTP/HTTPS downloads, Capture ATP has an option, Block file download until a verdict is returned, that ensures no packets get through until the file is completely analyzed and determined to be either malicious or benign. The file is held until the last packet is analyzed. If the file has malware, the last packet is dropped, and the file is blocked. The threat report provides information necessary to respond to a threat or infection.

[30]

[29] https://media.zones.com/images/pdf/sonicwall-capture-client-faqs.pdf, at 1.
[30] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 4.

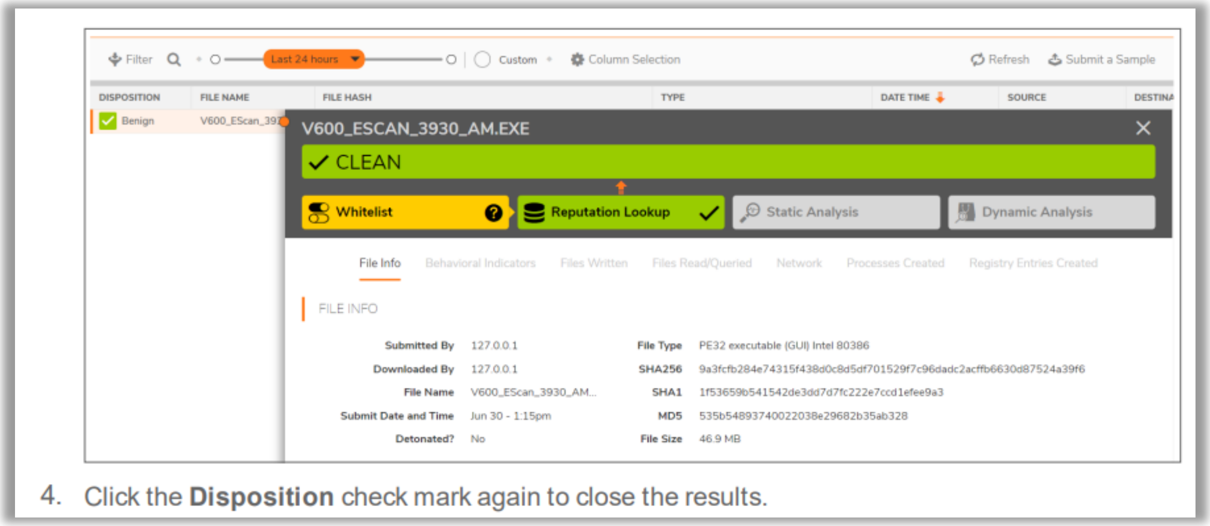


Viewing Analyzed Results

To view the detailed results of a scanned file:

1. Navigate to the **POLICY | Capture ATP > Scanning History**.
2. The columns for the **Scanning History** page are as follows:
   - **Disposition**: The results of the analysis for this file, **Benign** or **Malicious**.
   - **File Name**: Lists the file name of the scanned file.
   - **File Hash**: A fixed-length value computed by a number of input bytes processed through a one-way digest function.
   - **Type**: The type of file that was analyzed, such as an executable file or a zip file.
   - **Date Time**: The time that the file was submitted for analysis.
   - **Source**: The IP address from which the file was sent.
   - **Destination**: The IP address to which the file was sent.

   From the detailed results view, you can click a scanning report to launch the scanning report for that file.
3. Click the **Disposition** check mark for that file. The details of the analysis results for that file display.

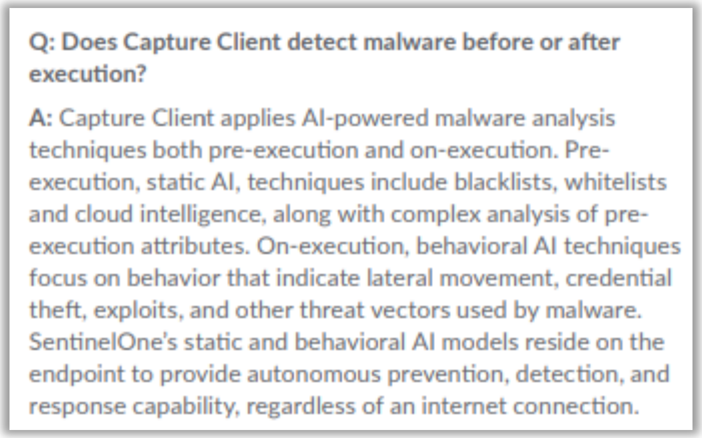


Submitted By	127.0.0.1	File Type	PE32 executable (GUI) Intel 80386
Downloaded By	127.0.0.1	SHA256	9a3fcfb284e74315f438d0c8d5df701529f7c96dadc2acffb6630d87524a39f6
File Name	V600_EScan_3930_AM...	SHA1	1f53659b541542de3dd7d7fc222e7ccd1efee9a3
Submit Date and Time	Jun 30 - 1:15pm	MD5	535b54893740022038e29682b35ab328
Detonated?	No	File Size	46.9 MB

4. Click the **Disposition** check mark again to close the results.

[31]

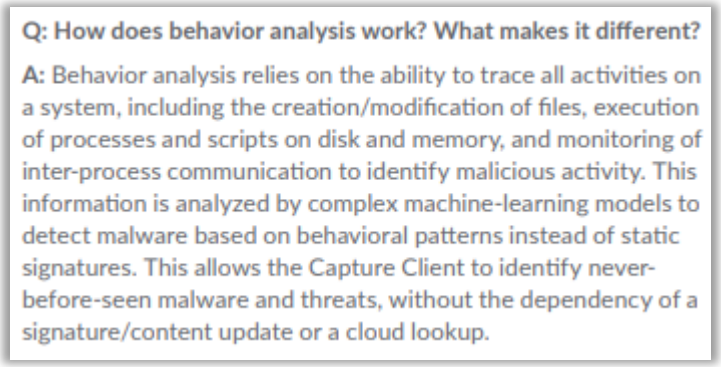
[31] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 14-15.



Q: Does Capture Client detect malware before or after execution?

A: Capture Client applies AI-powered malware analysis techniques both pre-execution and on-execution. Pre-execution, static AI, techniques include blacklists, whitelists and cloud intelligence, along with complex analysis of pre-execution attributes. On-execution, behavioral AI techniques focus on behavior that indicate lateral movement, credential theft, exploits, and other threat vectors used by malware. SentinelOne's static and behavioral AI models reside on the endpoint to provide autonomous prevention, detection, and response capability, regardless of an internet connection.

[32]



Q: How does behavior analysis work? What makes it different?

A: Behavior analysis relies on the ability to trace all activities on a system, including the creation/modification of files, execution of processes and scripts on disk and memory, and monitoring of inter-process communication to identify malicious activity. This information is analyzed by complex machine-learning models to detect malware based on behavioral patterns instead of static signatures. This allows the Capture Client to identify never-before-seen malware and threats, without the dependency of a signature/content update or a cloud lookup.

[33]

38. Defendant has and continues to directly infringe one or more claims of the ’137 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

39. Defendant has and continues to indirectly infringe one or more claims of the ’137 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’137 Accused Products.

[32] https://media.zones.com/images/pdf/sonicwall-capture-client-faqs.pdf, at 2.
[33] https://media.zones.com/images/pdf/sonicwall-capture-client-faqs.pdf, at 1.

40. Defendant has and continues to indirectly infringe one or more claims of the ’137 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’137 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’137 Patent by providing these products to customers and end-users for use in an infringing manner.

41. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’137 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[34] Video Tutorials,[35] SonicWall University,[36] and Customer Service[37] websites.

42. Defendant has and continues to indirectly infringe one or more claims of the ’137 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’137 Patent. Such components include, for example, SonicWall’s network

[34] https://www.sonicwall.com/support/technical-documentation/?language=English

[35] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[36] https://www.sonicwall.com/partners/sonicwall-university/

[37] https://www.sonicwall.com/support/contact-support/customer-service/

security appliances such as firewalls or Capture Client, that integrate with Sonicwall Capture ATP. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’137 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’137 Patent but remained willfully blind to the infringing nature of others’ actions.

43. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’137 Patent in an amount to be proved at trial.

44. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’137 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

45. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’137 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’137 Patent. Upon information and belief, Defendant had actual knowledge of the ’137 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’137 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT II
(Infringement of the ’356 Patent)

46. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

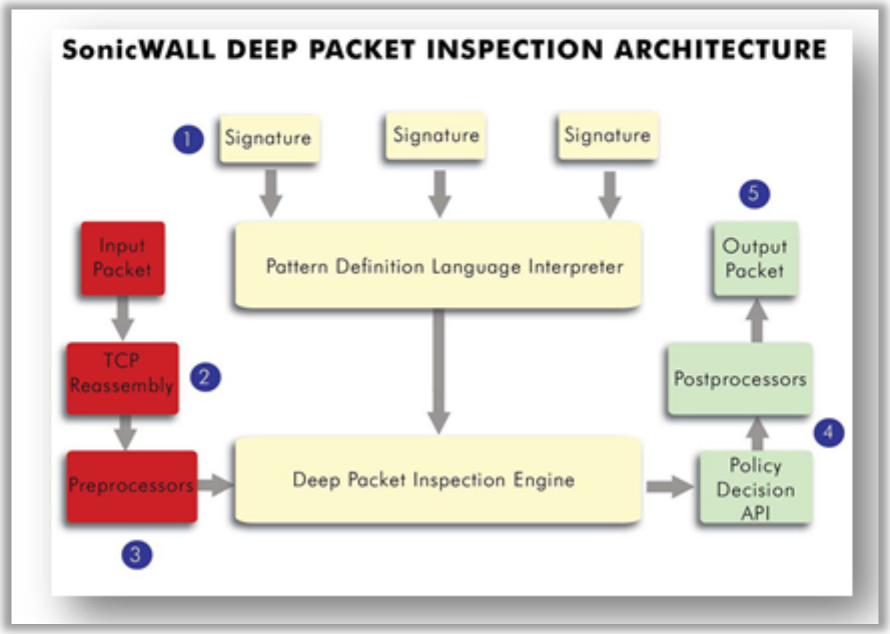
47. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’356 Patent.

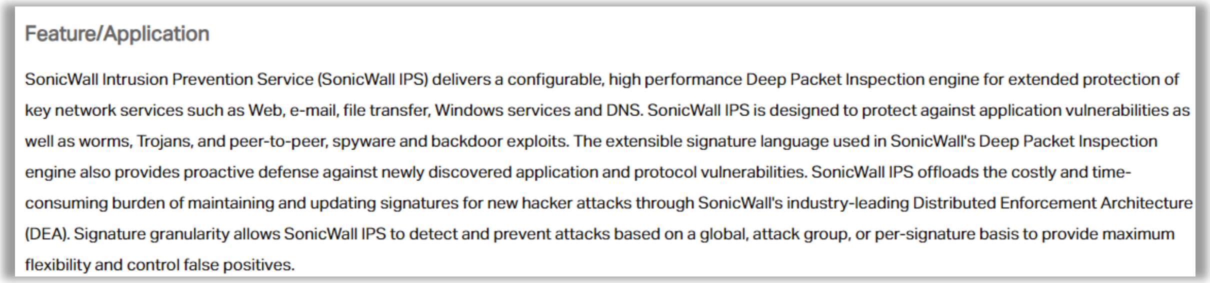
48. Defendant has and continues to directly infringe the ’356 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’356 Patent. Such products include at least SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) integrated with SonicWall IPS (the “’356 Accused Products”)which are computer program products for automatically determining if a packet is a new, exploit candidate comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; third program instructions to determine if the packet is network administration traffic; fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a

broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth, and fifth program instructions are stored on the computer-readable tangible storage device.

49. Every '356 Accused Product comprises a computer-readable tangible storage device that stores the first, second, third, fourth, and fifth program instructions described below. For example, IPS includes stored instructions for "the extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS" and "protect[ion] against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits" by comparing packets to stored signatures and updating signatures for new hacker attacks.

Signature - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.





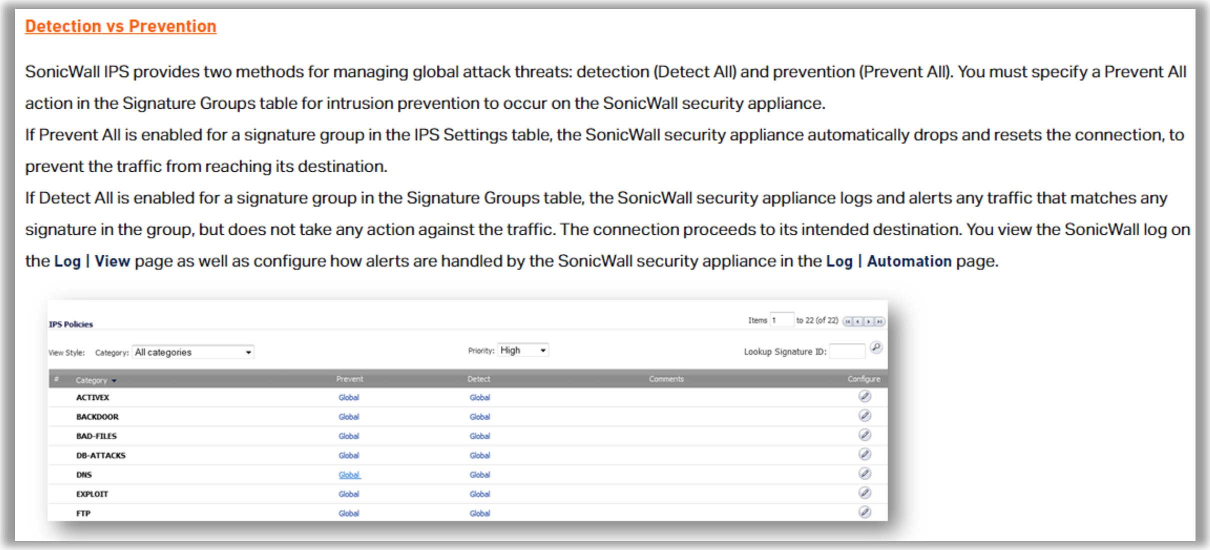
Feature/Application

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

[38]

50. Every ’356 Accused Product comprises first program instructions to determine if the packet is a known exploit. For example, IPS determines that a packet is not a new exploit because it checks stored signature groups. For further example, using “Detect All,” attack threat management, “the SonicWall security appliance logs and alerts any traffic that matches any signature in the group [i.e., is a known exploit], but does not take any action against the traffic.”

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.



Detection vs Prevention

SonicWall IPS provides two methods for managing global attack threats: detection (Detect All) and prevention (Prevent All). You must specify a Prevent All action in the Signature Groups table for intrusion prevention to occur on the SonicWall security appliance.

If Prevent All is enabled for a signature group in the IPS Settings table, the SonicWall security appliance automatically drops and resets the connection, to prevent the traffic from reaching its destination.

If Detect All is enabled for a signature group in the Signature Groups table, the SonicWall security appliance logs and alerts any traffic that matches any signature in the group, but does not take any action against the traffic. The connection proceeds to its intended destination. You view the SonicWall log on the **Log | View** page as well as configure how alerts are handled by the SonicWall security appliance in the **Log | Automation** page.

IPS Policies

Items 1 to 22 (of 22)

View Style: Category: All categories Priority: High Lookup Signature ID:

#	Category	Prevent	Detect	Comments	Configure
	ACTIVEX	Global	Global		✎
	BACKDOOR	Global	Global		✎
	BAD-FILES	Global	Global		✎
	DB-ATTACKS	Global	Global		✎
	DNS	Global	Global		✎
	EXPLOIT	Global	Global		✎
	FTP	Global	Global		✎

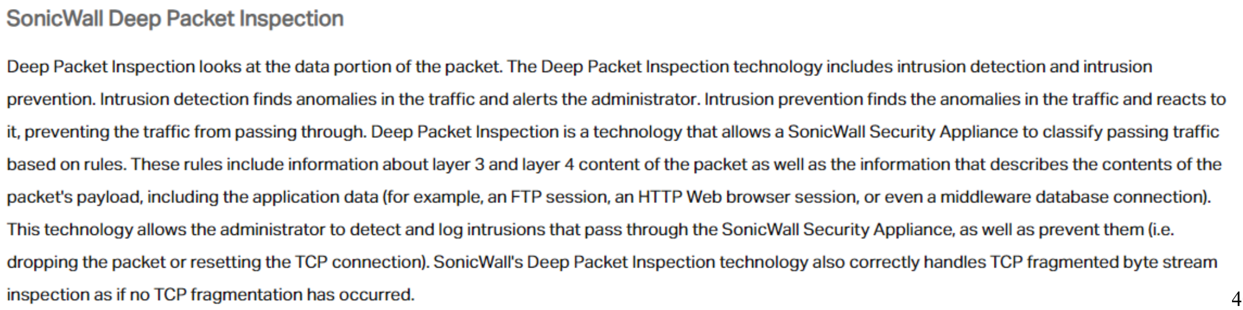
[39]

51. Every ’356 Accused Product comprises second program instructions to determine if the packet is addressed to a broadcast IP address of a network. For example, IPS includes Deep

[38] https://www.sonicwall.com/support/knowledge-base/how-ips-intrusion-prevention-services-works/170504979028241/

[39] https://www.sonicwall.com/support/knowledge-base/how-ips-intrusion-prevention-services-works/170504979028241/

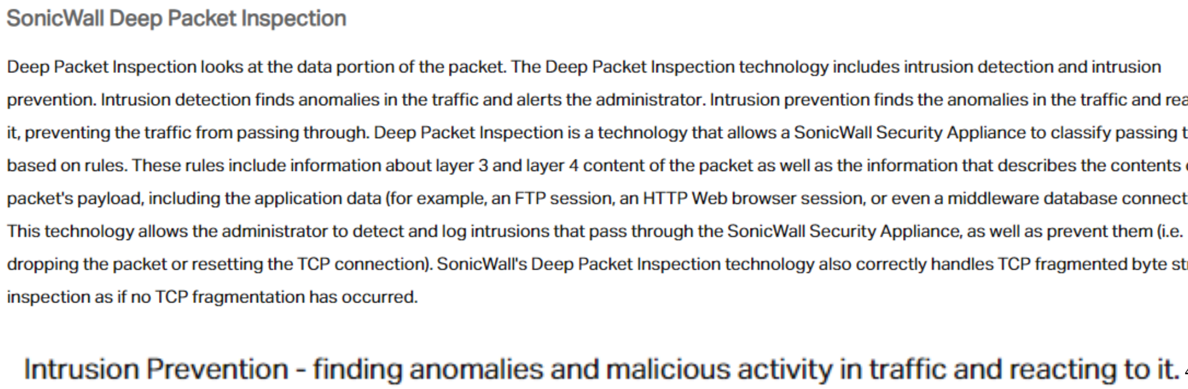
Packet Inspection “that allows a SonicWall Security Appliance to classify passing traffic based on rules” and “rules include information about layer 3 and layer 4 content of the packet.” Layer 3 content includes IP addresses, and particularly a broadcast IP address of a network.



SonicWall Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through. Deep Packet Inspection is a technology that allows a SonicWall Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWall Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWall's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred. [40]

52. Every ’356 Accused Product comprises third program instructions to determine if the packet is network administration traffic. For example, IPS “classif[ies] passing traffic based on rules” and “finds anomalies in the traffic and alerts the administrator,” implying that administrator traffic is permissible.



SonicWall Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through. Deep Packet Inspection is a technology that allows a SonicWall Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWall Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWall's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

Intrusion Prevention - finding anomalies and malicious activity in traffic and reacting to it. [41]

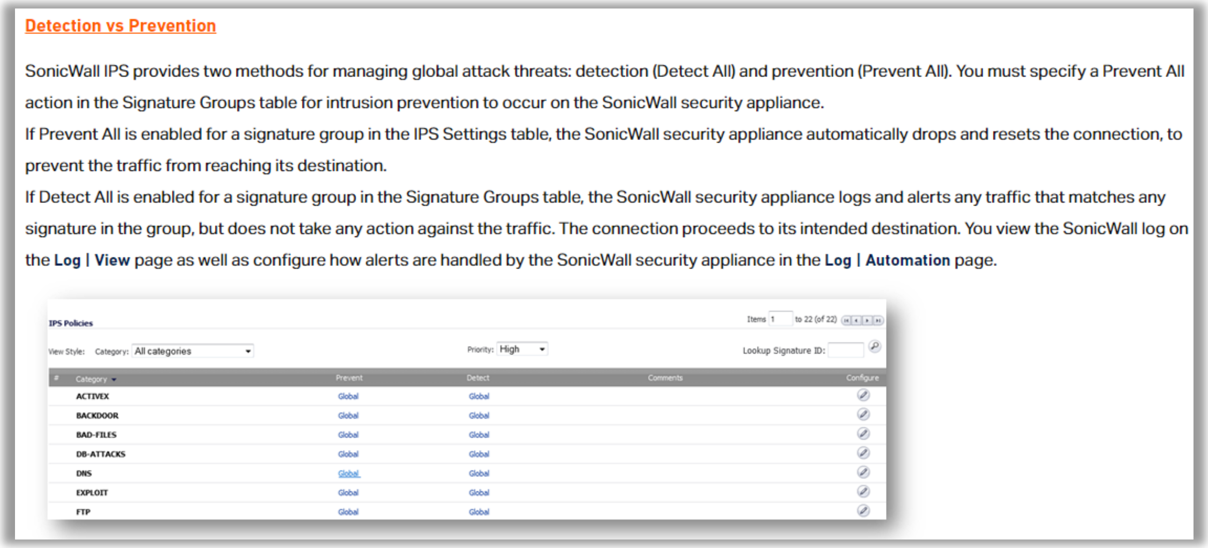
53. Every ’356 Accused Product comprises fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate. For example, IPS determines that a packet is not a new exploit because it

[40] https://www.sonicwall.com/support/knowledge-base/how-ips-intrusion-prevention-services-works/170504979028241/

[41] https://www.sonicwall.com/support/knowledge-base/how-ips-intrusion-prevention-services-works/170504979028241/

checks stored signature groups. For further example, using "Detect All," attack threat management, "the SonicWall security appliance logs and alerts any traffic that matches any signature in the group [i.e., is a known exploit], but does not take any action against the traffic."

1. Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.



Detection vs Prevention

SonicWall IPS provides two methods for managing global attack threats: detection (Detect All) and prevention (Prevent All). You must specify a Prevent All action in the Signature Groups table for intrusion prevention to occur on the SonicWall security appliance.

If Prevent All is enabled for a signature group in the IPS Settings table, the SonicWall security appliance automatically drops and resets the connection, to prevent the traffic from reaching its destination.

If Detect All is enabled for a signature group in the Signature Groups table, the SonicWall security appliance logs and alerts any traffic that matches any signature in the group, but does not take any action against the traffic. The connection proceeds to its intended destination. You view the SonicWall log on the **Log | View** page as well as configure how alerts are handled by the SonicWall security appliance in the **Log | Automation** page.

IPS Policies

Items 1 to 22 (of 22)

View Style: Category: All categories

Priority: High

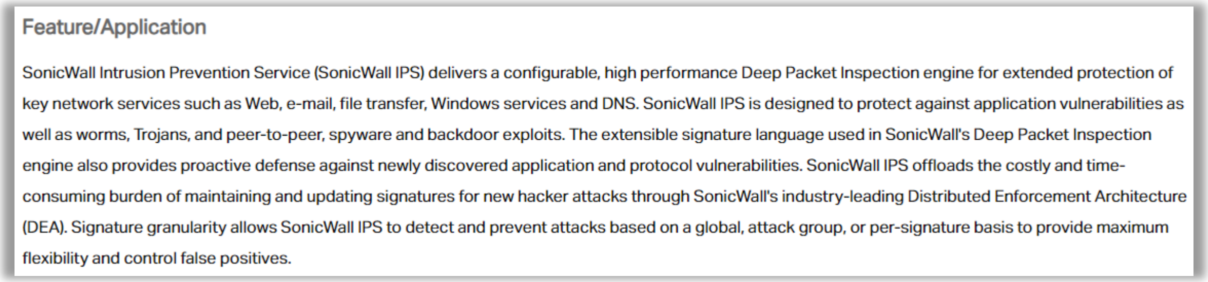
Lookup Signature ID:

#	Category	Prevent	Detect	Comments	Configure
	ACTIVEX	Global	Global		✎
	BACKDOOR	Global	Global		✎
	BAD-FILES	Global	Global		✎
	DB-ATTACKS	Global	Global		✎
	DNS	Global	Global		✎
	EXPLOIT	Global	Global		✎
	FTP	Global	Global		✎

[42]

54. Every '356 Accused Product comprises fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate. For example, IPS "provides proactive defense against newly discovered application and protocol vulnerabilities" and performs "updating signatures for new hacker attacks").

[42] https://www.sonicwall.com/support/knowledge-base/how-ips-intrusion-prevention-services-works/170504979028241/



Feature/Application

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

[43]

55. Defendant has and continues to directly infringe one or more claims of the ’356 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

56. Defendant has and continues to indirectly infringe one or more claims of the ’356 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’356 Accused Products.

57. Defendant has and continues to indirectly infringe one or more claims of the ’356 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’356 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’356 Patent by providing these products to customers and end-users for use in an infringing manner.

[43] https://www.sonicwall.com/support/knowledge-base/how-ips-intrusion-prevention-services-works/170504979028241/

58. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’356 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[44] Video Tutorials,[45] SonicWall University,[46] and Customer Service[47] websites.

59. Defendant has and continues to indirectly infringe one or more claims of the ’356 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’356 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls that integrates with Sonicwall IPS. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’356 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’356 Patent but remained willfully blind to the infringing nature of others’ actions.

60. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’356 Patent in an amount to be proved at trial.

[44] https://www.sonicwall.com/support/technical-documentation/?language=English
[45] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12
[46] https://www.sonicwall.com/partners/sonicwall-university/
[47] https://www.sonicwall.com/support/contact-support/customer-service/

RUSS AUGUST & KABAT

61. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '356 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

62. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the '356 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera's patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the '356 Patent. Upon information and belief, Defendant had actual knowledge of the '356 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant's infringement of the '356 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT III
(Infringement of the '441 Patent)

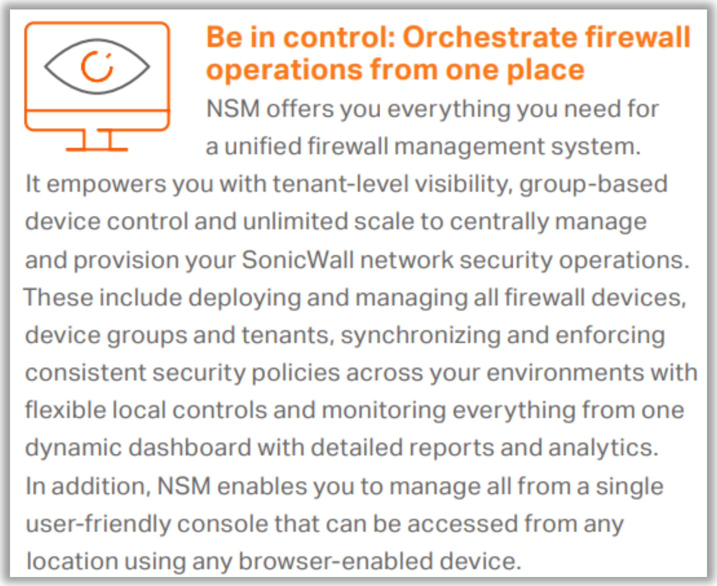
63. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

64. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '441 Patent.

65. Defendant has and continues to directly infringe the '441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '441 Patent. Such products include at least SonicWall's

SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) integrated with Network Security Manager and/or Capture ATP, or SonicWall Capture Client integrated with Capture ATP (the "'441 Accused Products") which practice a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.

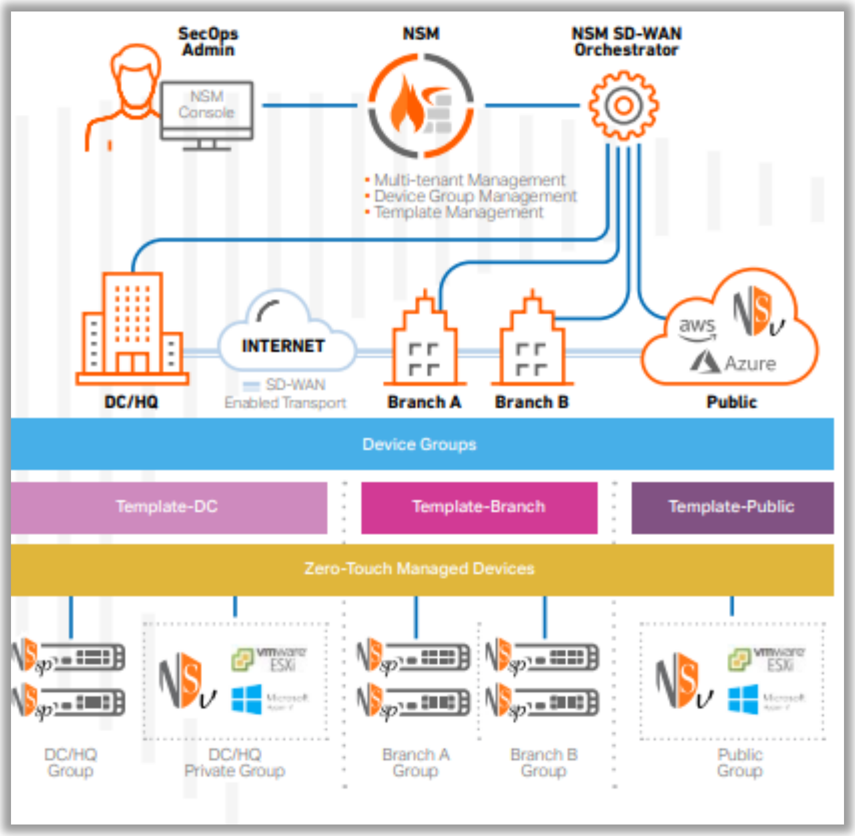
66. Every '441 Accused Product practices receiving, by the attestation server remote from the computing platform. For example, Network Security Manager includes an NSM Console and NSM SD-WAN Orchestrator that is remote from both SonicWall firewalls as well as any endpoint or computing device.



Be in control: Orchestrate firewall operations from one place

NSM offers you everything you need for a unified firewall management system. It empowers you with tenant-level visibility, group-based device control and unlimited scale to centrally manage and provision your SonicWall network security operations. These include deploying and managing all firewall devices, device groups and tenants, synchronizing and enforcing consistent security policies across your environments with flexible local controls and monitoring everything from one dynamic dashboard with detailed reports and analytics. In addition, NSM enables you to manage all from a single user-friendly console that can be accessed from any location using any browser-enabled device.

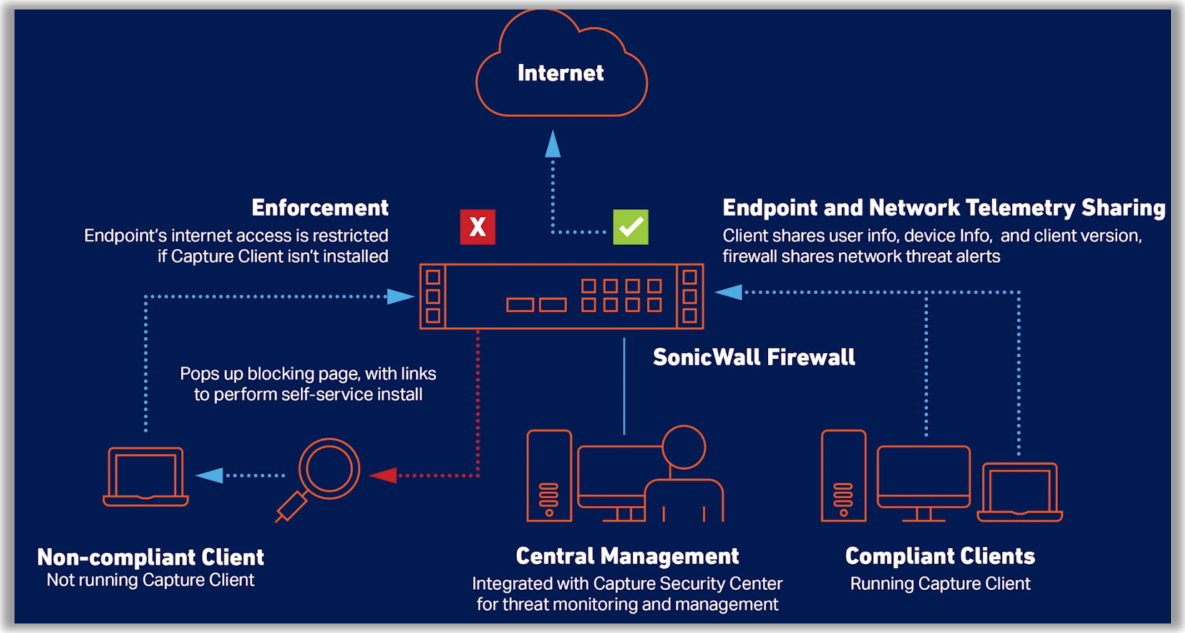
[48]



[49]

[48] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 2.
[49] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 1.

67. For further example, Capture Client performs a method where the Central Management (i.e., attestation server) is remote from the endpoint or computing device.



Internet

Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts

SonicWall Firewall

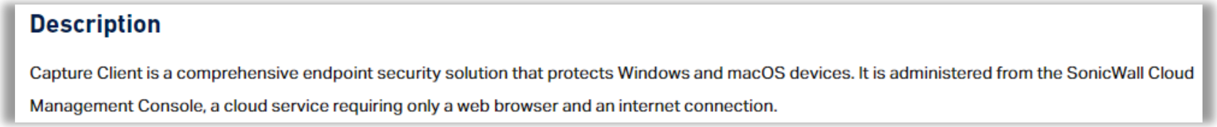
Pops up blocking page, with links to perform self-service install

Non-compliant Client
Not running Capture Client

Central Management
Integrated with Capture Security Center for threat monitoring and management

Compliant Clients
Running Capture Client

[50]



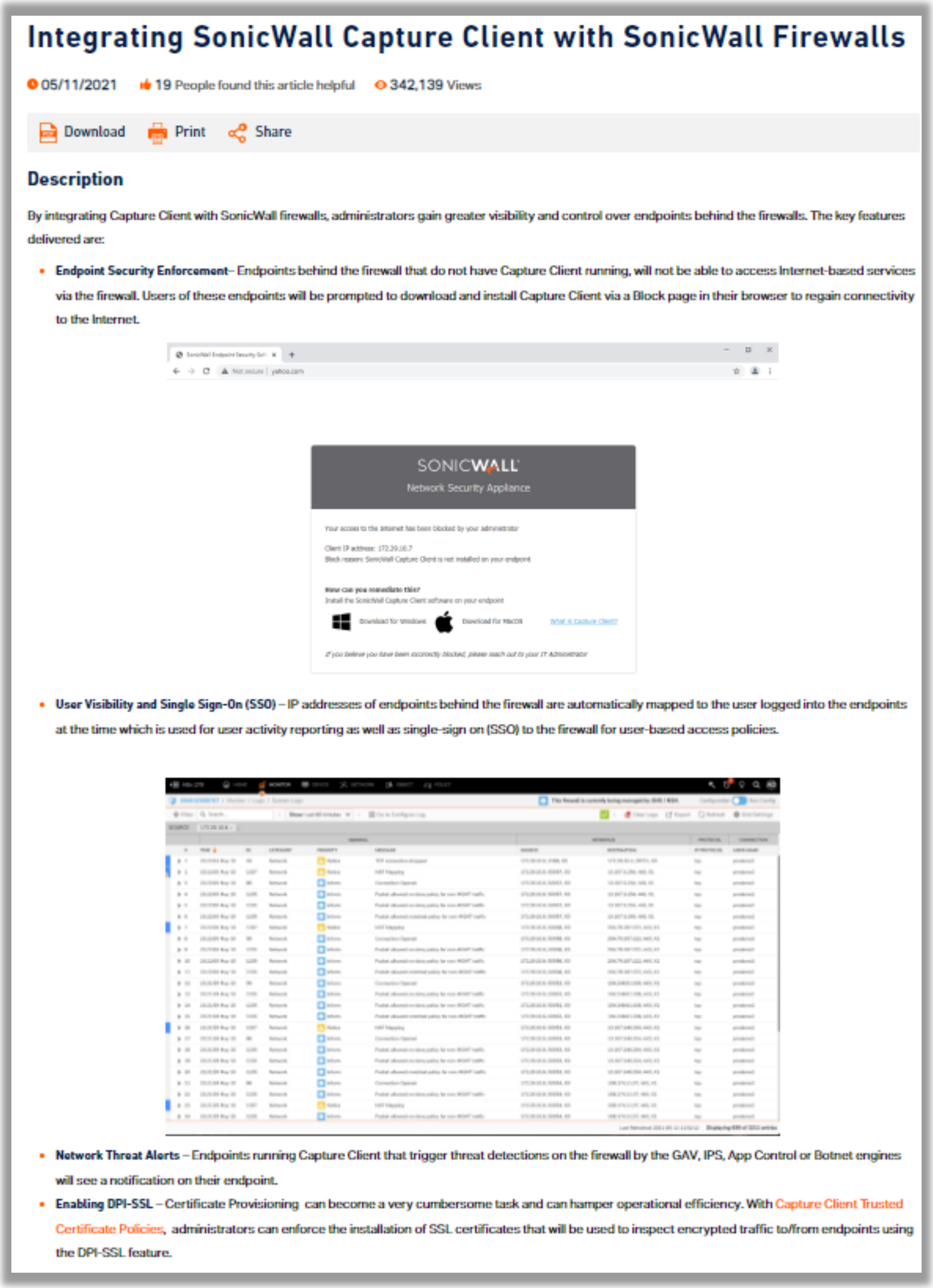
Description

Capture Client is a comprehensive endpoint security solution that protects Windows and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection.

[51]

[50] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[51] https://www.sonicwall.com/support/knowledge-base/capture-client-system-requirements/210512075820480/



Integrating SonicWall Capture Client with SonicWall Firewalls

05/11/2021 19 People found this article helpful 342,139 Views

Description

By integrating Capture Client with SonicWall firewalls, administrators gain greater visibility and control over endpoints behind the firewalls. The key features delivered are:

- **Endpoint Security Enforcement**– Endpoints behind the firewall that do not have Capture Client running, will not be able to access Internet-based services via the firewall. Users of these endpoints will be prompted to download and install Capture Client via a Block page in their browser to regain connectivity to the Internet.

Your access to the Internet has been blocked by your administrator

Client IP address: 172.29.10.7
Block reason: SonicWall Capture Client is not installed on your endpoint

How can you remediate this?
Install the SonicWall Capture Client software on your endpoint

If you believe you have been incorrectly blocked, please reach out to your IT Administrator

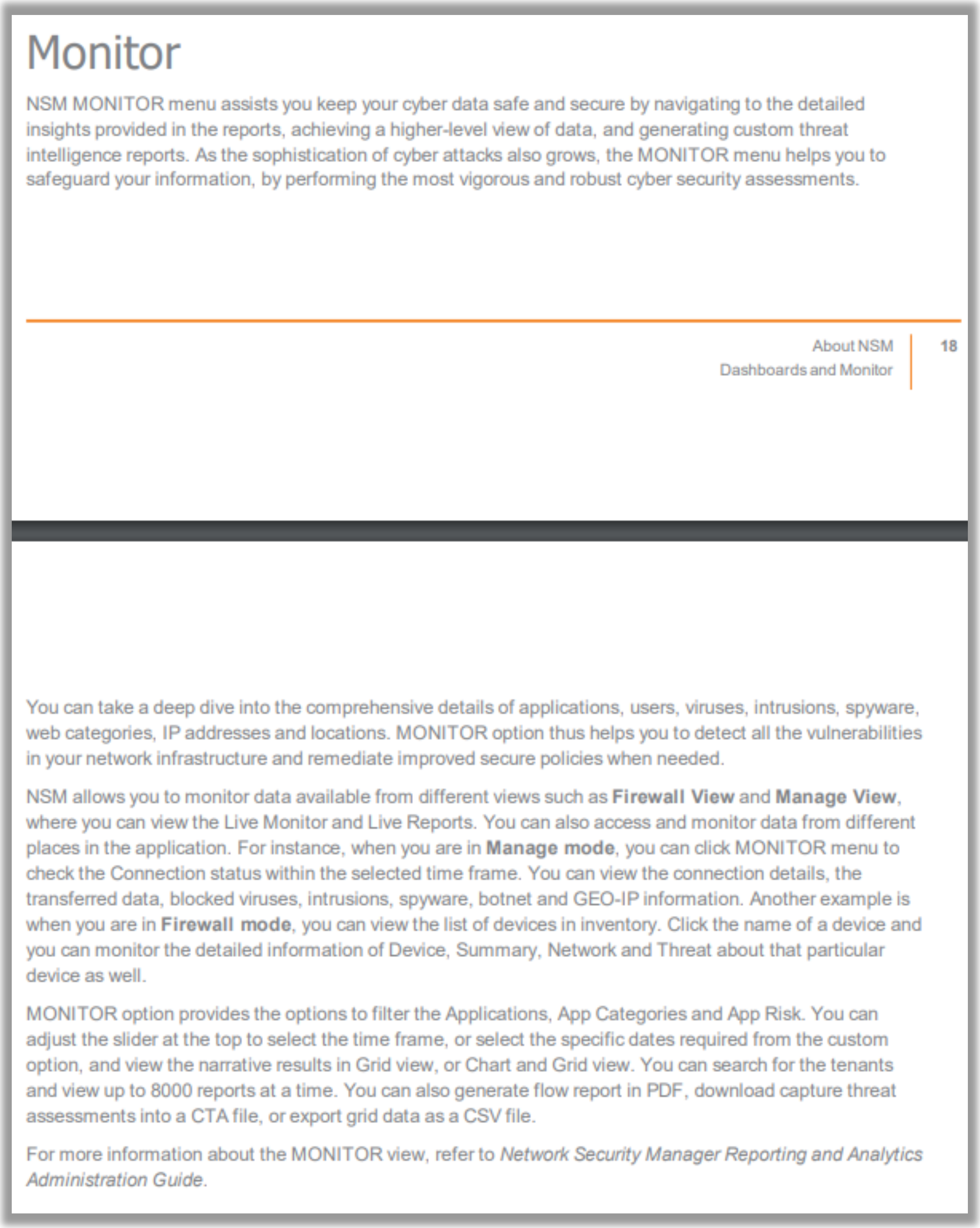
- **User Visibility and Single Sign-On (SSO)** – IP addresses of endpoints behind the firewall are automatically mapped to the user logged into the endpoints at the time which is used for user activity reporting as well as single-sign on (SSO) to the firewall for user-based access policies.

- **Network Threat Alerts** – Endpoints running Capture Client that trigger threat detections on the firewall by the GAV, IPS, App Control or Botnet engines will see a notification on their endpoint.
- **Enabling DPI-SSL** – Certificate Provisioning can become a very cumbersome task and can hamper operational efficiency. With Capture Client Trusted Certificate Policies, administrators can enforce the installation of SSL certificates that will be used to inspect encrypted traffic to/from endpoints using the DPI-SSL feature.

52

68. Every ’441 Accused Product practices receiving …a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application. For example, NSM receives a runtime execution context indicating attributes of the application (“comprehensive details of applications”) and includes “options to filter the Applications, APP Categories and App Risk.” Application files can be executable files.

[52] https://www.sonicwall.com/support/knowledge-base/integrating-sonicwall-capture-client-with-sonicwall-firewalls/210511023450473/



Monitor

NSM MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports. As the sophistication of cyber attacks also grows, the MONITOR menu helps you to safeguard your information, by performing the most vigorous and robust cyber security assessments.

About NSM
Dashboards and Monitor | 18

You can take a deep dive into the comprehensive details of applications, users, viruses, intrusions, spyware, web categories, IP addresses and locations. MONITOR option thus helps you to detect all the vulnerabilities in your network infrastructure and remediate improved secure policies when needed.

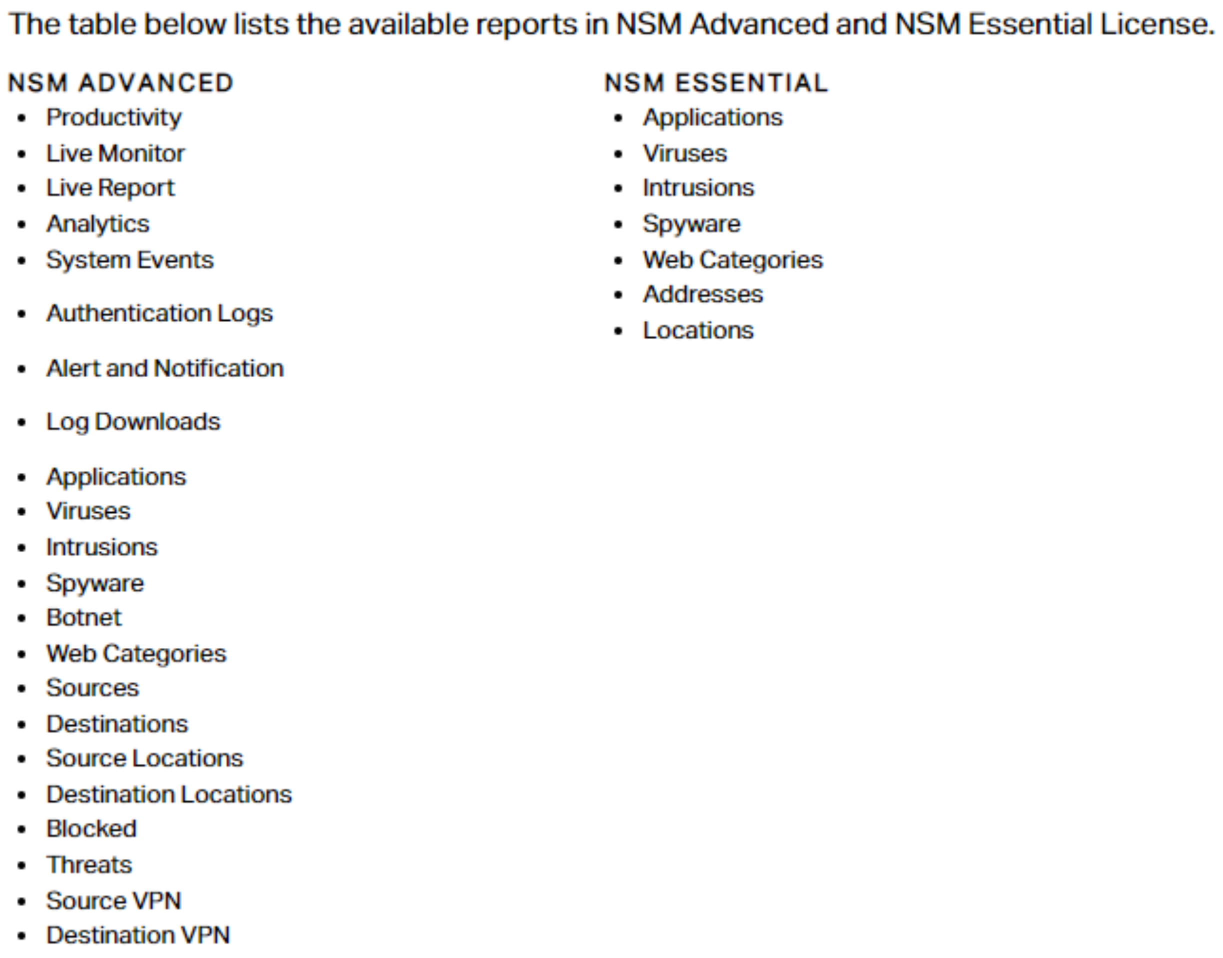
NSM allows you to monitor data available from different views such as **Firewall View** and **Manage View**, where you can view the Live Monitor and Live Reports. You can also access and monitor data from different places in the application. For instance, when you are in **Manage mode**, you can click MONITOR menu to check the Connection status within the selected time frame. You can view the connection details, the transferred data, blocked viruses, intrusions, spyware, botnet and GEO-IP information. Another example is when you are in **Firewall mode**, you can view the list of devices in inventory. Click the name of a device and you can monitor the detailed information of Device, Summary, Network and Threat about that particular device as well.

MONITOR option provides the options to filter the Applications, App Categories and App Risk. You can adjust the slider at the top to select the time frame, or select the specific dates required from the custom option, and view the narrative results in Grid view, or Chart and Grid view. You can search for the tenants and view up to 8000 reports at a time. You can also generate flow report in PDF, download capture threat assessments into a CTA file, or export grid data as a CSV file.

For more information about the MONITOR view, refer to *Network Security Manager Reporting and Analytics Administration Guide*.

[53]

[53] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 18-19.



The table below lists the available reports in NSM Advanced and NSM Essential License.

NSM ADVANCED

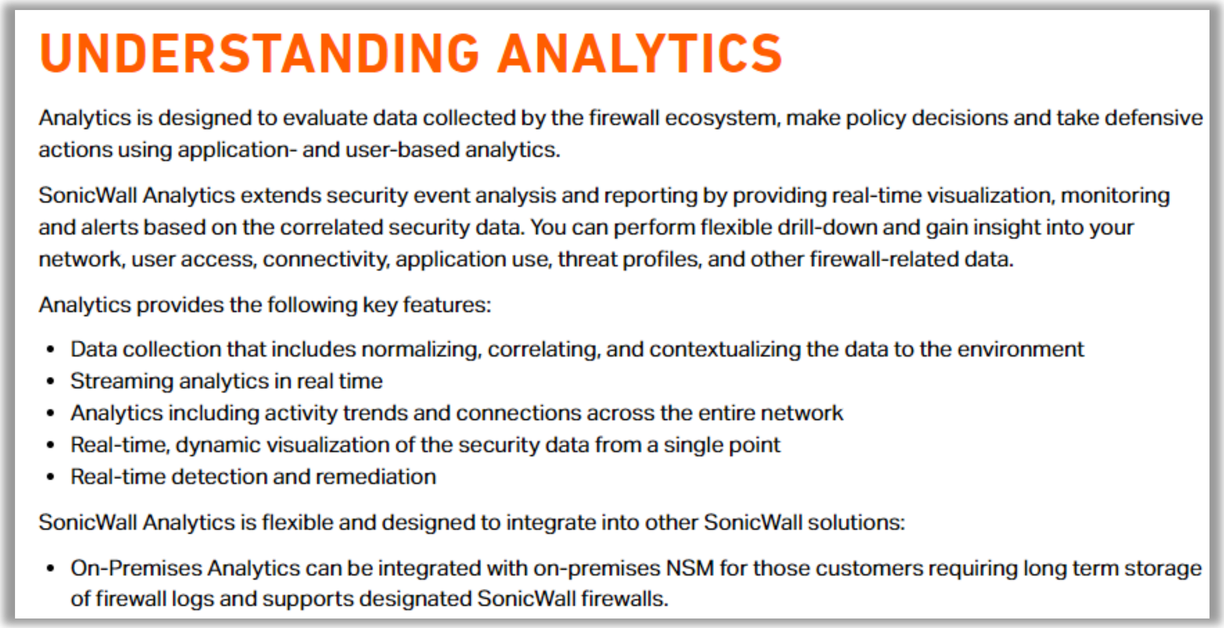
- Productivity
- Live Monitor
- Live Report
- Analytics
- System Events
- Authentication Logs
- Alert and Notification
- Log Downloads
- Applications
- Viruses
- Intrusions
- Spyware
- Botnet
- Web Categories
- Sources
- Destinations
- Source Locations
- Destination Locations
- Blocked
- Threats
- Source VPN
- Destination VPN

NSM ESSENTIAL

- Applications
- Viruses
- Intrusions
- Spyware
- Web Categories
- Addresses
- Locations

[54]

[54] https://www.sonicwall.com/support/technical-documentation/docs/nsm-reporting_and_analytics/Content/allcontent/about-analytics.htm/ ; https://www.sonicwall.com/techdocs/pdf/nsm-reporting_and_analytics.pdf, at 6.



UNDERSTANDING ANALYTICS

Analytics is designed to evaluate data collected by the firewall ecosystem, make policy decisions and take defensive actions using application- and user-based analytics.

SonicWall Analytics extends security event analysis and reporting by providing real-time visualization, monitoring and alerts based on the correlated security data. You can perform flexible drill-down and gain insight into your network, user access, connectivity, application use, threat profiles, and other firewall-related data.

Analytics provides the following key features:

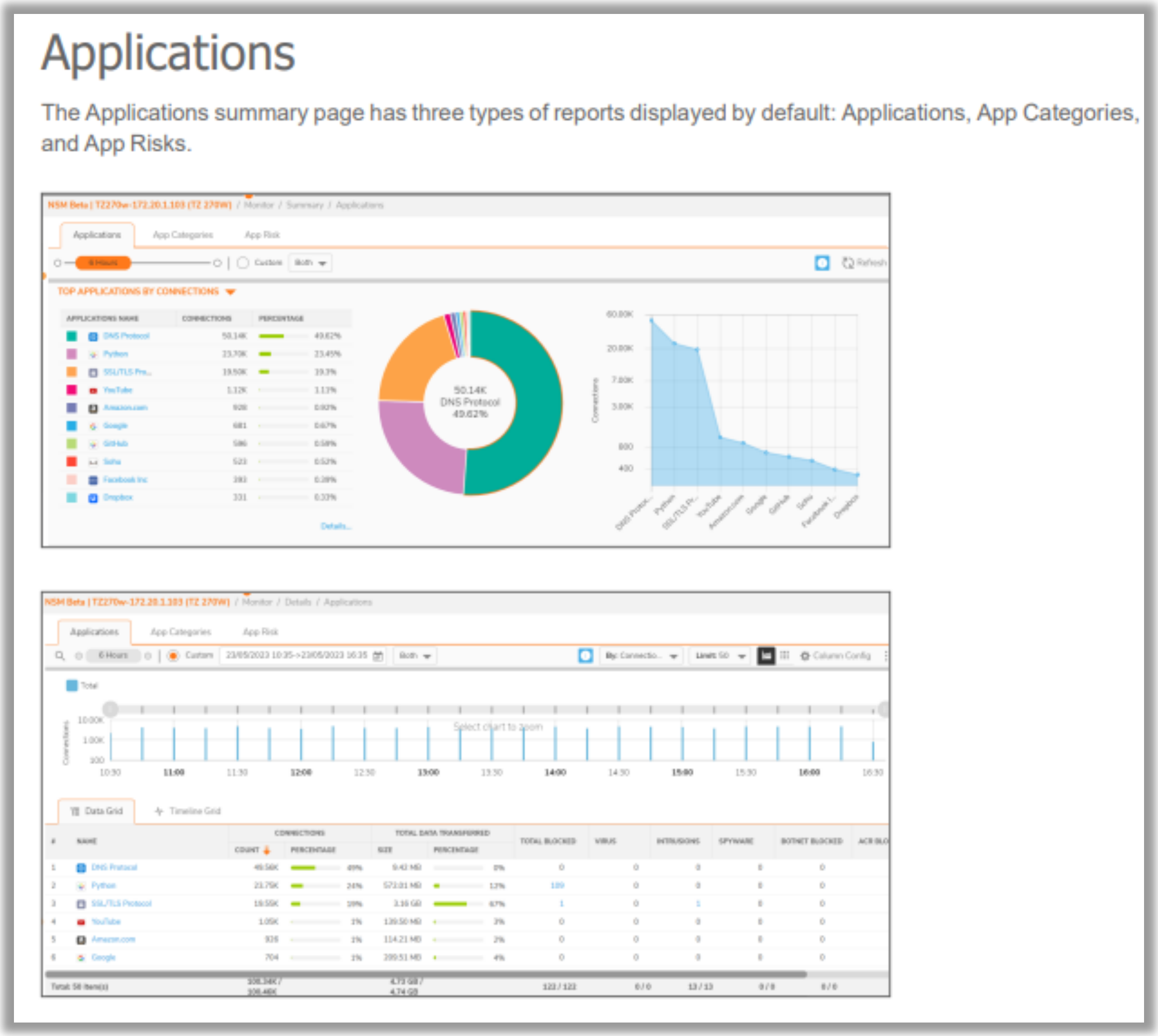
- Data collection that includes normalizing, correlating, and contextualizing the data to the environment
- Streaming analytics in real time
- Analytics including activity trends and connections across the entire network
- Real-time, dynamic visualization of the security data from a single point
- Real-time detection and remediation

SonicWall Analytics is flexible and designed to integrate into other SonicWall solutions:

- On-Premises Analytics can be integrated with on-premises NSM for those customers requiring long term storage of firewall logs and supports designated SonicWall firewalls.

[55]

[55] https://www.sonicwall.com/support/technical-documentation/docs/nsm-reporting_and_analytics/Content/allcontent/about-analytics.htm/ ; https://www.sonicwall.com/techdocs/pdf/nsm-reporting_and_analytics.pdf, at 6-7.



Applications

The Applications summary page has three types of reports displayed by default: Applications, App Categories, and App Risks.

NSM Beta | TZ270w-172.20.1.103 (TZ 270W) / Monitor / Summary / Applications

TOP APPLICATIONS BY CONNECTIONS

APPLICATIONS NAME	CONNECTIONS	PERCENTAGE
🟩 DNS Protocol	50.14K	49.62%
🟪 Python	23.70K	23.45%
🟧 SSL/TLS Pro...	19.50K	19.3%
🟥 YouTube	1.12K	1.11%
🟪 Amazon.com	928	0.92%
🟦 Google	681	0.67%
🟩 GitHub	586	0.58%
🟥 Sohu	523	0.52%
🟥 Facebook Inc	393	0.39%
🟦 Dropbox	331	0.33%

Details...

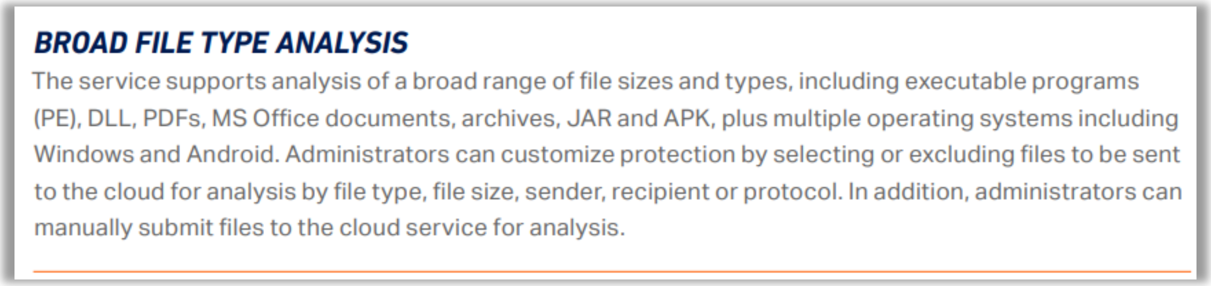
NSM Beta | TZ270w-172.20.1.103 (TZ 270W) / Monitor / Details / Applications

#	NAME	CONNECTIONS		TOTAL DATA TRANSFERRED		TOTAL BLOCKED	VIRUS	INTRUSIONS	SPYWARE	BOTNET BLOCKED	ACR BLO
		COUNT	PERCENTAGE	SIZE	PERCENTAGE						
1	DNS Protocol	49.56K	49%	9.42 MB	0%	0	0	0	0	0	
2	Python	23.75K	24%	573.01 MB	12%	109	0	0	0	0	
3	SSL/TLS Protocol	19.55K	19%	3.16 GB	67%	1	0	1	0	0	
4	YouTube	1.05K	1%	139.50 MB	3%	0	0	0	0	0	
5	Amazon.com	926	1%	114.21 MB	2%	0	0	0	0	0	
6	Google	704	1%	209.51 MB	4%	0	0	0	0	0	
Total: 58 item(s)		108.34K / 108.46K		4.73 GB / 4.74 GB		122 / 122	0 / 0	13 / 13	0 / 0	0 / 0	

[56]

69. For example, Capture ATP receives a runtime execution context indicating attributes of the application to "support[s] analysis of a broad range of file sizes and types, including executable programs."

[56] https://www.sonicwall.com/techdocs/pdf/nsm-reporting_and_analytics.pdf, at 29.

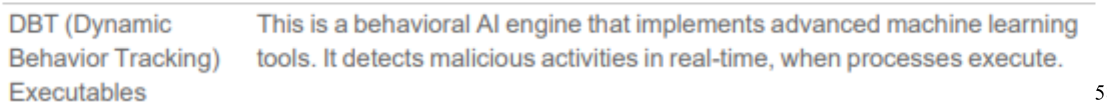


BROAD FILE TYPE ANALYSIS

The service supports analysis of a broad range of file sizes and types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR and APK, plus multiple operating systems including Windows and Android. Administrators can customize protection by selecting or excluding files to be sent to the cloud for analysis by file type, file size, sender, recipient or protocol. In addition, administrators can manually submit files to the cloud service for analysis.

[57]

70. For further example, Capture Client receives a runtime execution context indicating attributes of the application, such as through Dynamic Behavior Tracking Executables, which detects malicious activities in real-time, when processes execute. Capture Client may also use its integration with Capture to receive a runtime execution context, as noted above.

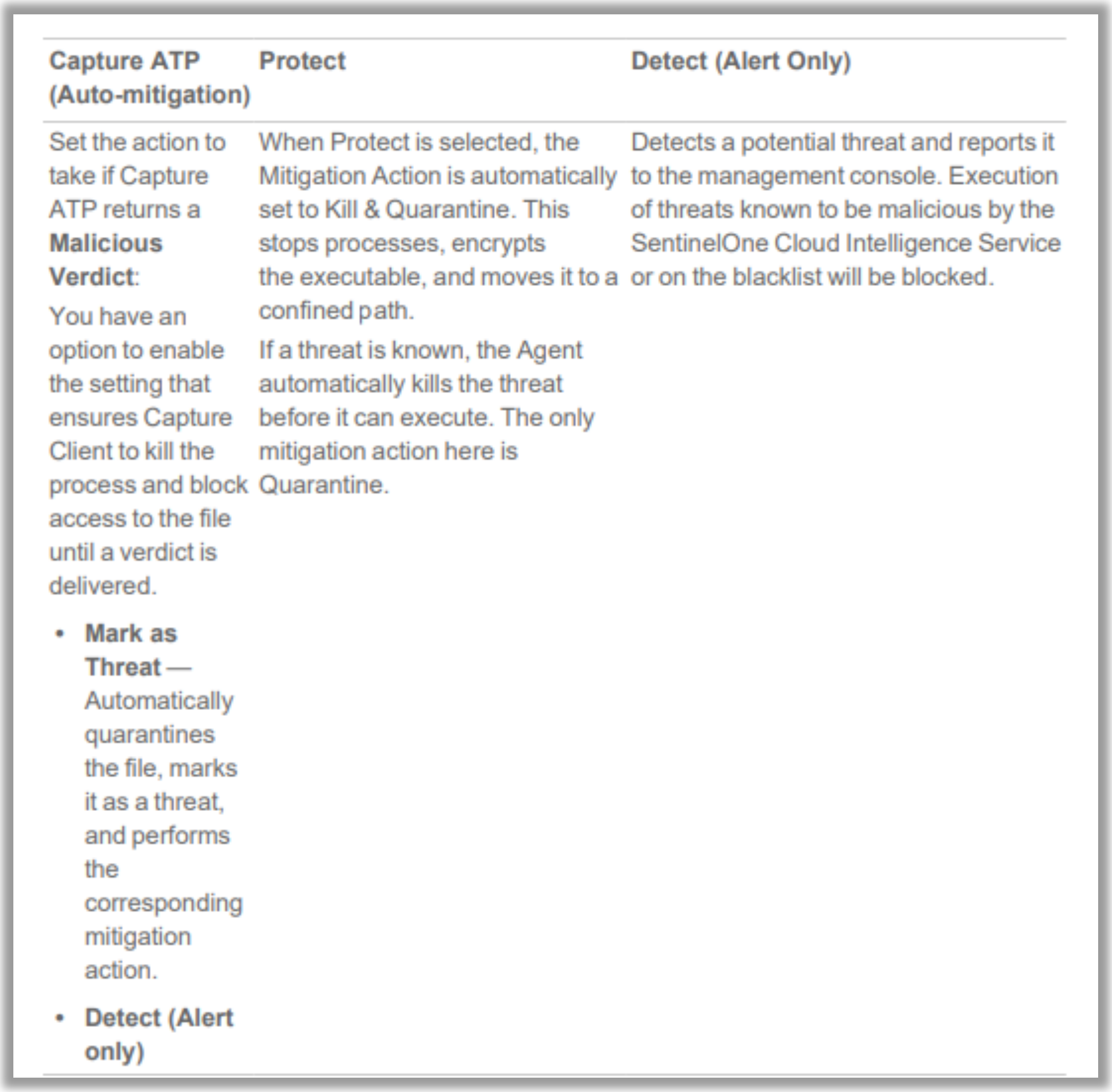


DBT (Dynamic Behavior Tracking) Executables	This is a behavioral AI engine that implements advanced machine learning tools. It detects malicious activities in real-time, when processes execute.

[58]

[57] https://www.sonicwall.com/medialibrary/en/datasheet/datasheet-sonicwall-capture-advanced-threat-protection-service.pdf

[58] https://www.sonicwall.com/techdocs/pdf/capture_client-protecting_assets.pdf, at 14.

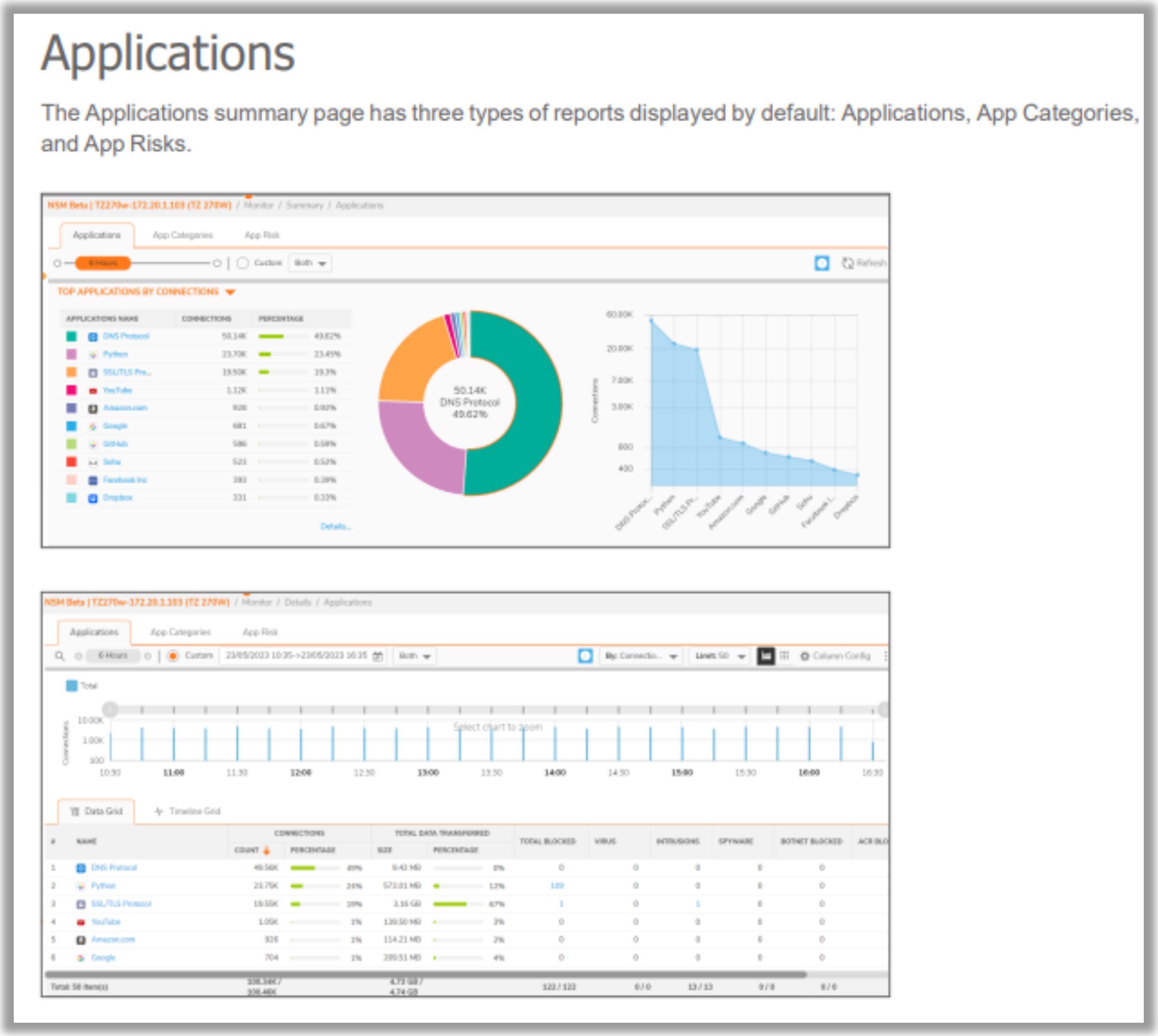


Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a **Malicious Verdict**: You have an option to enable the setting that ensures Capture Client to kill the process and block access to the file until a verdict is delivered. - **Mark as Threat** — Automatically quarantines the file, marks it as a threat, and performs the corresponding mitigation action. - **Detect (Alert only)**	When Protect is selected, the Mitigation Action is automatically set to Kill & Quarantine. This stops processes, encrypts the executable, and moves it to a confined path. If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action here is Quarantine.	Detects a potential threat and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.

[59]

71. Every ’441 Accused Product practices receiving …a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components. For example, NSM receives a security context about the applications it conducts an execution analysis on including each application’s risks.

[59] https://www.sonicwall.com/techdocs/pdf/capture_client-protecting_assets.pdf, at 12.



Applications

The Applications summary page has three types of reports displayed by default: Applications, App Categories, and App Risks.

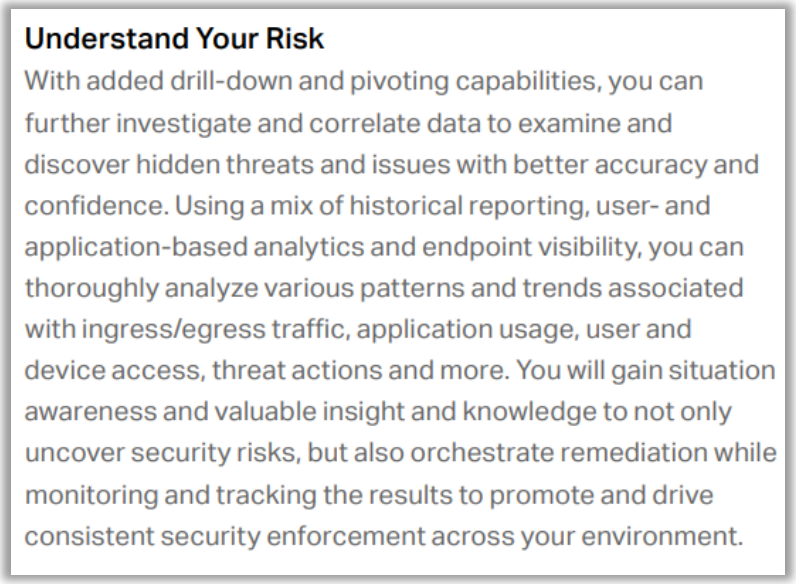
APPLICATIONS NAME	CONNECTIONS	PERCENTAGE
🟩 DNS Protocol	50.14K	49.62%
🟪 Python	23.70K	23.45%
🟧 SSL/TLS Pro...	19.50K	19.3%
🟥 YouTube	1.12K	1.11%
🟦 Amazon.com	928	0.92%
🟦 Google	681	0.67%
🟩 GitHub	586	0.58%
🟥 Sohu	523	0.52%
🟥 Facebook Inc	383	0.28%
🟦 Dropbox	331	0.33%

Details...

#	NAME	CONNECTIONS		TOTAL DATA TRANSFERRED		TOTAL BLOCKED	VIRUS	INTRUSIONS	SPYWARE	BOTNET BLOCKED	ACR BLO
		COUNT	PERCENTAGE	SIZE	PERCENTAGE						
1	DNS Protocol	49.56K	49%	9.43 MB	0%	0	0	0	0	0	
2	Python	23.75K	24%	573.01 MB	13%	109	0	0	0	0	
3	SSL/TLS Protocol	19.55K	19%	3.16 GB	67%	1	0	1	0	0	
4	YouTube	1.05K	1%	139.50 MB	3%	0	0	0	0	0	
5	Amazon.com	926	1%	114.21 MB	2%	0	0	0	0	0	
6	Google	704	1%	199.51 MB	4%	0	0	0	0	0	
Total: 58 item(s)		106.34K / 106.46K		4.73 GB / 4.74 GB		122 / 122	0 / 0	13 / 13	0 / 0	0 / 0	

[60]

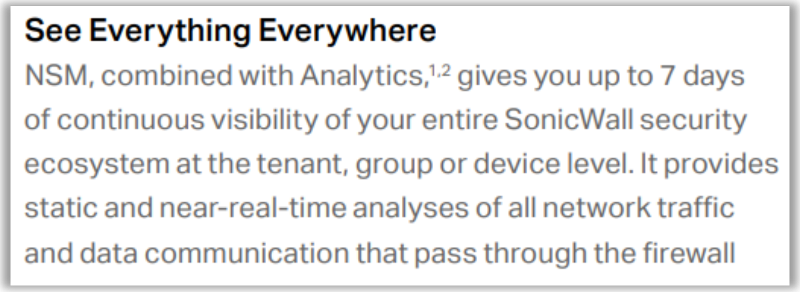
[60] https://www.sonicwall.com/techdocs/pdf/nsm-reporting_and_analytics.pdf, at 29.



Understand Your Risk

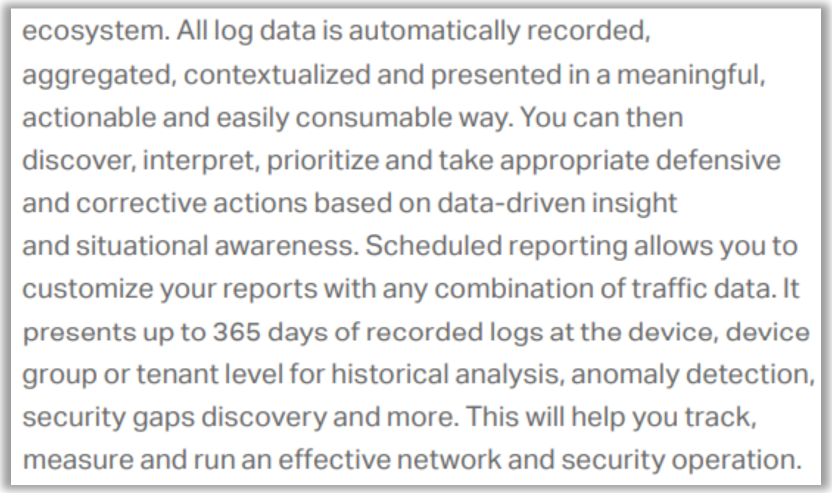
With added drill-down and pivoting capabilities, you can further investigate and correlate data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions and more. You will gain situation awareness and valuable insight and knowledge to not only uncover security risks, but also orchestrate remediation while monitoring and tracking the results to promote and drive consistent security enforcement across your environment.

[61]



See Everything Everywhere

NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall

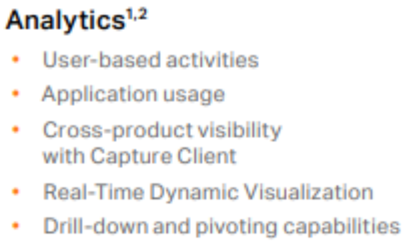


ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way. You can then discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more. This will help you track, measure and run an effective network and security operation.

[62]

[61] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 4.

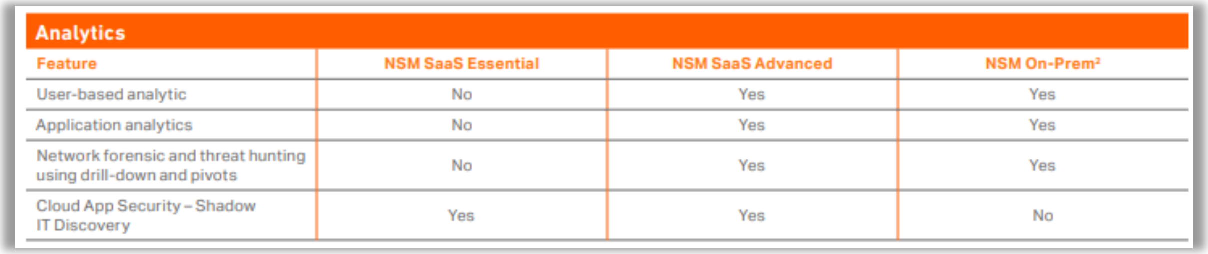
[62] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 3-4.



Analytics[1,2]

- User-based activities
- Application usage
- Cross-product visibility with Capture Client
- Real-Time Dynamic Visualization
- Drill-down and pivoting capabilities

[63]

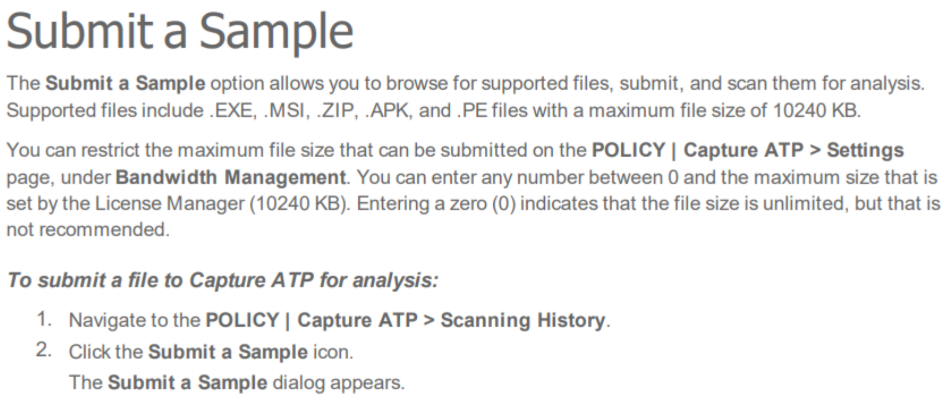


Analytics

Feature	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem[2]
User-based analytic	No	Yes	Yes
Application analytics	No	Yes	Yes
Network forensic and threat hunting using drill-down and pivots	No	Yes	Yes
Cloud App Security – Shadow IT Discovery	Yes	Yes	No

[64]

72. For example, Capture Client receives a security context based on scanning executables for analysis through Capture ATP.



Submit a Sample

The **Submit a Sample** option allows you to browse for supported files, submit, and scan them for analysis. Supported files include .EXE, .MSI, .ZIP, .APK, and .PE files with a maximum file size of 10240 KB.

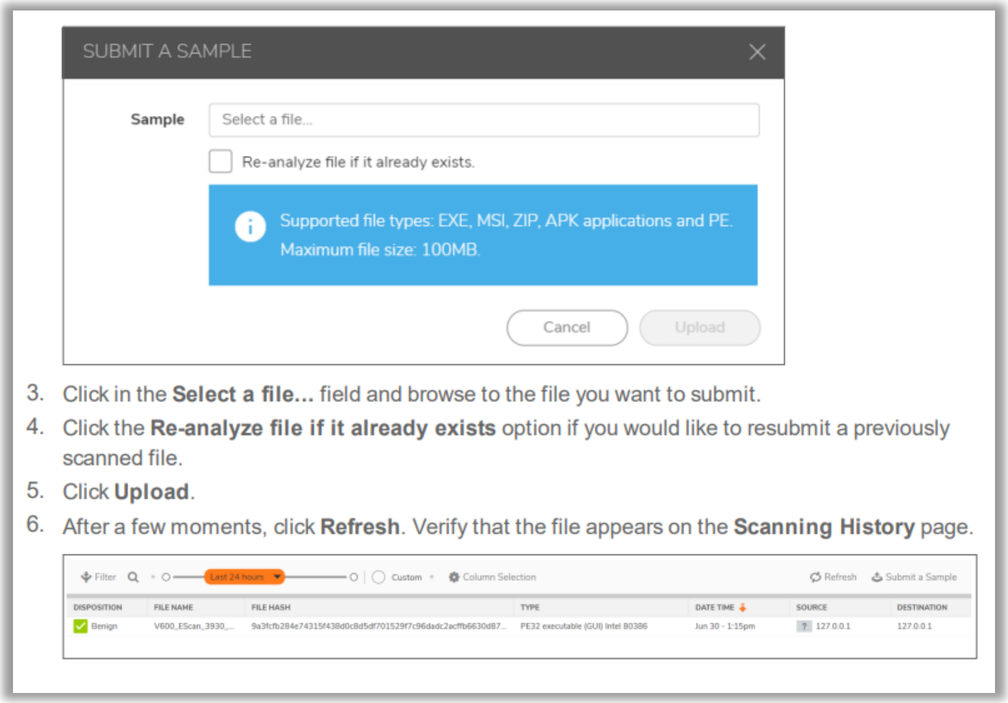
You can restrict the maximum file size that can be submitted on the **POLICY | Capture ATP > Settings** page, under **Bandwidth Management**. You can enter any number between 0 and the maximum size that is set by the License Manager (10240 KB). Entering a zero (0) indicates that the file size is unlimited, but that is not recommended.

To submit a file to Capture ATP for analysis:

1. Navigate to the **POLICY | Capture ATP > Scanning History**.
2. Click the **Submit a Sample** icon.
   The **Submit a Sample** dialog appears.

[63] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 5.

[64] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 6.



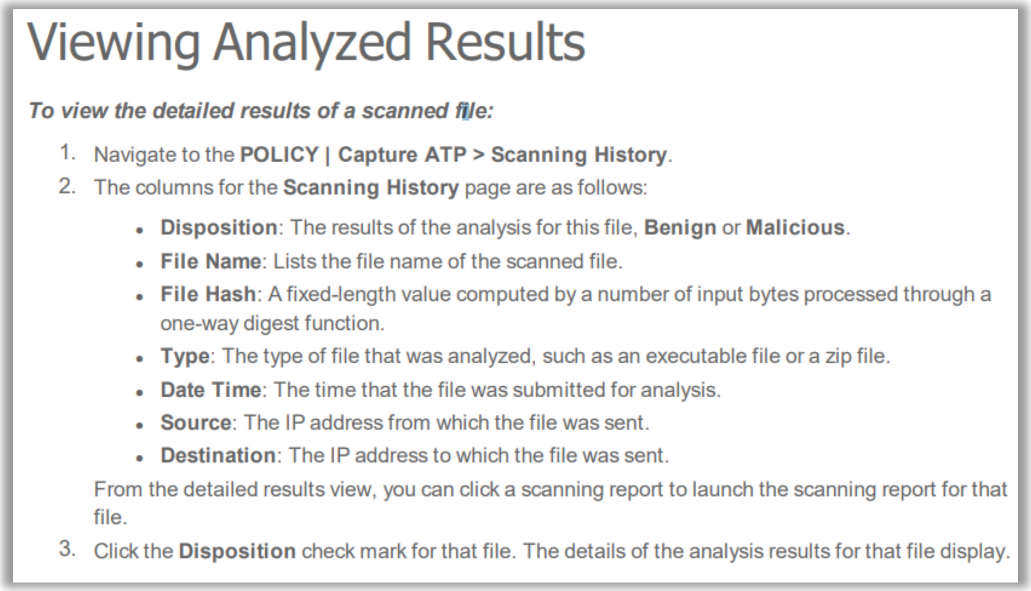
Sample: Select a file...

☐ Re-analyze file if it already exists.

Supported file types: EXE, MSI, ZIP, APK applications and PE.
Maximum file size: 100MB.

3. Click in the **Select a file...** field and browse to the file you want to submit.
4. Click the **Re-analyze file if it already exists** option if you would like to resubmit a previously scanned file.
5. Click **Upload**.
6. After a few moments, click **Refresh**. Verify that the file appears on the **Scanning History** page.

DISPOSITION	FILE NAME	FILE HASH	TYPE	DATE TIME	SOURCE	DESTINATION
✓ Benign	V600_EScan_3930_...	9a3fcfb284e74315f438d0c8d5df701529f7c96dadc2acffb6630d87...	PE32 executable (GUI) Intel 80386	Jun 30 - 1:15pm	? 127.0.0.1	127.0.0.1

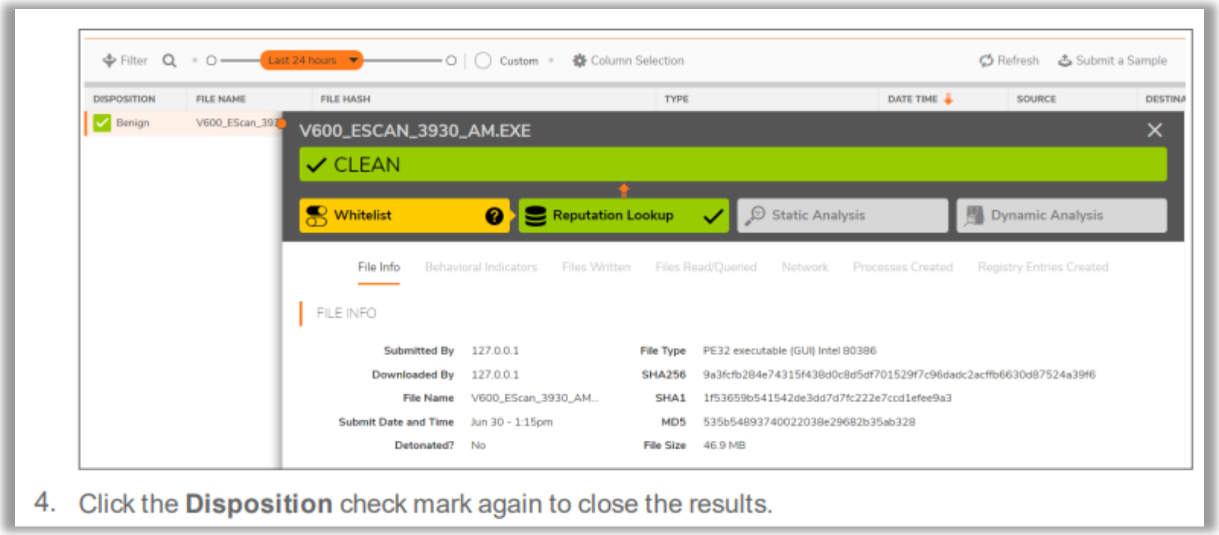


Viewing Analyzed Results

To view the detailed results of a scanned file:

1. Navigate to the **POLICY | Capture ATP > Scanning History**.
2. The columns for the **Scanning History** page are as follows:
   - **Disposition**: The results of the analysis for this file, **Benign** or **Malicious**.
   - **File Name**: Lists the file name of the scanned file.
   - **File Hash**: A fixed-length value computed by a number of input bytes processed through a one-way digest function.
   - **Type**: The type of file that was analyzed, such as an executable file or a zip file.
   - **Date Time**: The time that the file was submitted for analysis.
   - **Source**: The IP address from which the file was sent.
   - **Destination**: The IP address to which the file was sent.

   From the detailed results view, you can click a scanning report to launch the scanning report for that file.
3. Click the **Disposition** check mark for that file. The details of the analysis results for that file display.

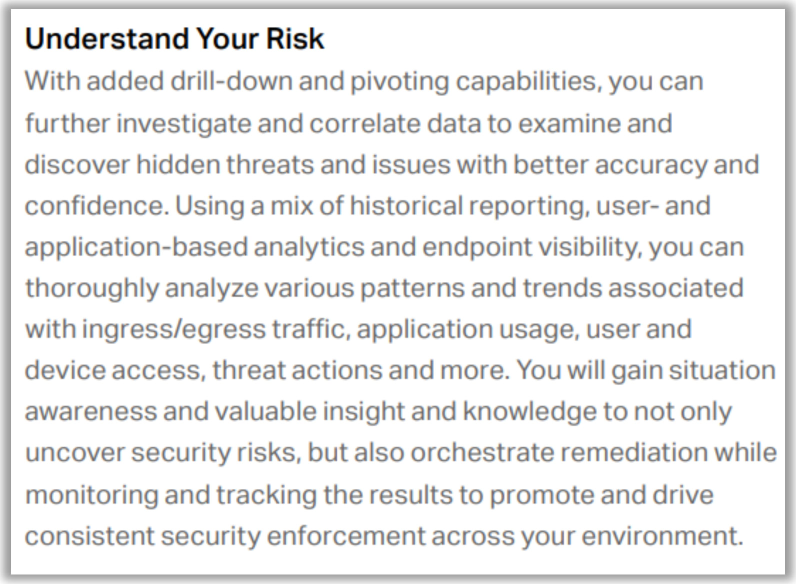


FILE INFO

Submitted By	127.0.0.1	File Type	PE32 executable (GUI) Intel 80386
Downloaded By	127.0.0.1	SHA256	9a3fcfb284e74315f438d0c8d5df701529f7c96dadc2acffb6630d87524a39f6
File Name	V600_EScan_3930_AM...	SHA1	1f53659b541542de3dd7d7fc222e7ccd1efee9a3
Submit Date and Time	Jun 30 - 1:15pm	MD5	535b54893740022038e29682b35ab328
Detonated?	No	File Size	46.9 MB

4. Click the **Disposition** check mark again to close the results. [65]

Every ’441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result and sending, by the attestation server, the attestation result associated with the application. For example, NSM generates a report including “application-based analytics” including security risks associated with the application.

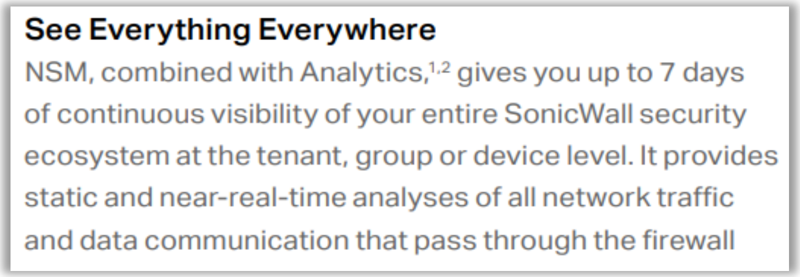


Understand Your Risk

With added drill-down and pivoting capabilities, you can further investigate and correlate data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions and more. You will gain situation awareness and valuable insight and knowledge to not only uncover security risks, but also orchestrate remediation while monitoring and tracking the results to promote and drive consistent security enforcement across your environment. [66]

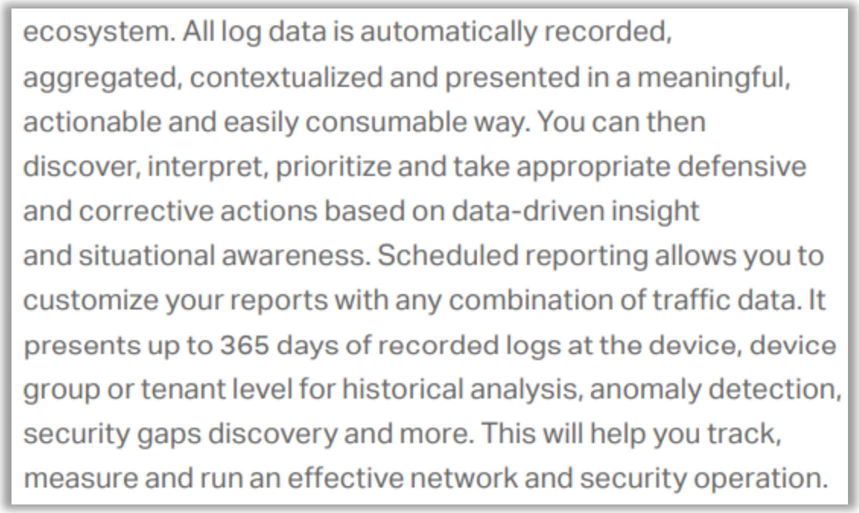
[65] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 13-15.

[66] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf



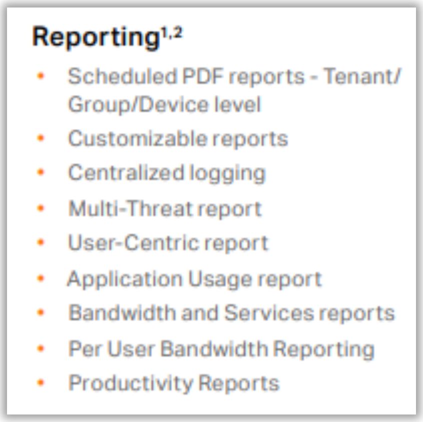
See Everything Everywhere

NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall



ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way. You can then discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more. This will help you track, measure and run an effective network and security operation.

[67]



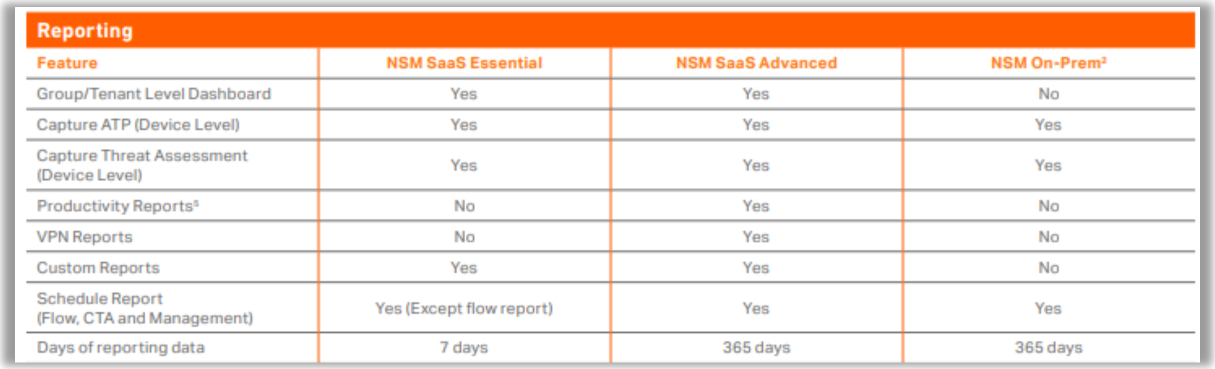
Reporting[1,2]

- Scheduled PDF reports - Tenant/ Group/Device level
- Customizable reports
- Centralized logging
- Multi-Threat report
- User-Centric report
- Application Usage report
- Bandwidth and Services reports
- Per User Bandwidth Reporting
- Productivity Reports

[68]

[67] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

[68] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 5.

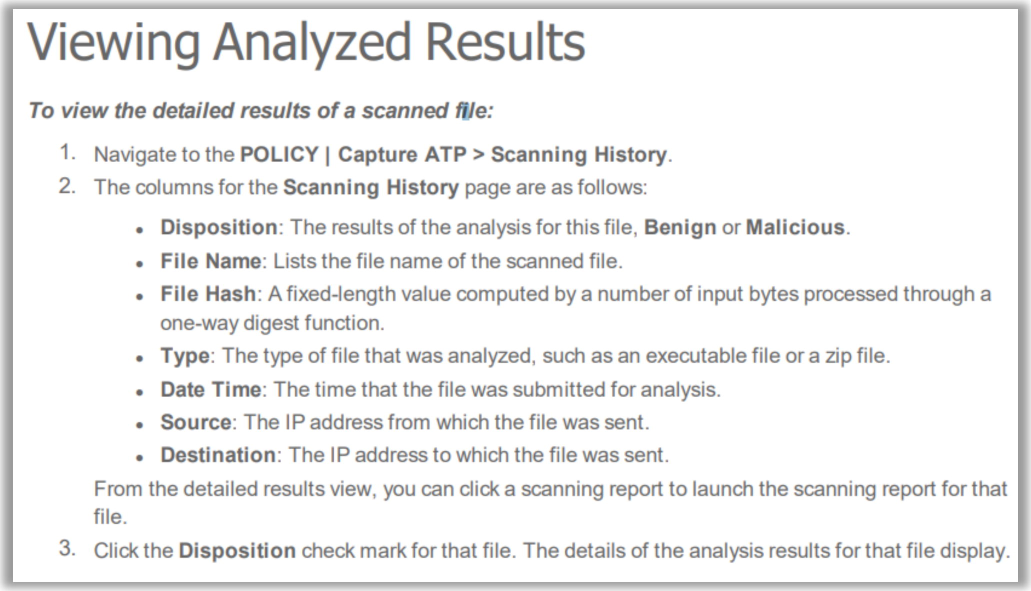


Reporting

Feature	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem[2]
Group/Tenant Level Dashboard	Yes	Yes	No
Capture ATP (Device Level)	Yes	Yes	Yes
Capture Threat Assessment (Device Level)	Yes	Yes	Yes
Productivity Reports[5]	No	Yes	No
VPN Reports	No	Yes	No
Custom Reports	Yes	Yes	No
Schedule Report (Flow, CTA and Management)	Yes (Except flow report)	Yes	Yes
Days of reporting data	7 days	365 days	365 days

[69]

73. For further example, Capture Client can use Capture ATP to generate a report indicating security risks associated with the application, including whether the received executable is "benign" or "malicious" (i.e., attestation result).



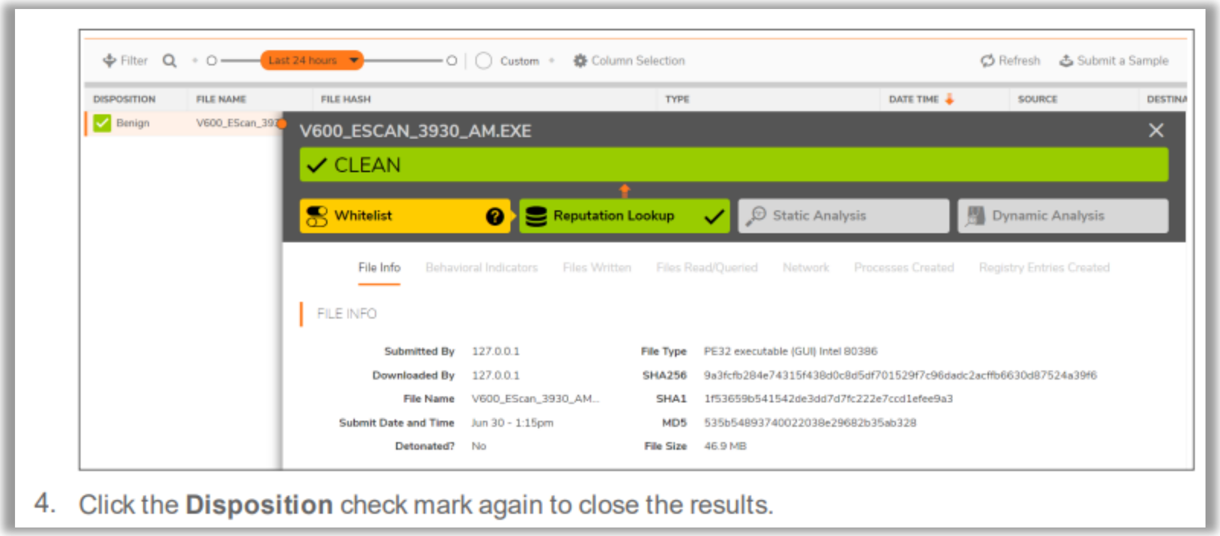
Viewing Analyzed Results

To view the detailed results of a scanned file:

1. Navigate to the **POLICY | Capture ATP > Scanning History**.
2. The columns for the **Scanning History** page are as follows:
    - **Disposition**: The results of the analysis for this file, **Benign** or **Malicious**.
    - **File Name**: Lists the file name of the scanned file.
    - **File Hash**: A fixed-length value computed by a number of input bytes processed through a one-way digest function.
    - **Type**: The type of file that was analyzed, such as an executable file or a zip file.
    - **Date Time**: The time that the file was submitted for analysis.
    - **Source**: The IP address from which the file was sent.
    - **Destination**: The IP address to which the file was sent.

    From the detailed results view, you can click a scanning report to launch the scanning report for that file.
3. Click the **Disposition** check mark for that file. The details of the analysis results for that file display.

[69] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 6.



V600_ESCAN_3930_AM.EXE

✓ CLEAN

FILE INFO

Submitted By	127.0.0.1	File Type	PE32 executable (GUI) Intel 80386
Downloaded By	127.0.0.1	SHA256	9a3fcfb284e74315f438d0c8d5df701529f7c96dadc2acffb6630d87524a39f6
File Name	V600_EScan_3930_AM...	SHA1	1f53659b541542de3dd7d7fc222e7ccd1efee9a3
Submit Date and Time	Jun 30 - 1:15pm	MD5	535b54893740022038e29682b35ab328
Detonated?	No	File Size	46.9 MB

4. Click the **Disposition** check mark again to close the results.

[70]

74. Defendant has and continues to directly infringe one or more claims of the ’441 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

75. Defendant has and continues to indirectly infringe one or more claims of the ’441 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’441 Accused Products.

76. Defendant has and continues to indirectly infringe one or more claims of the ’441 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’441 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly

[70] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-0-0-capture_atp.pdf, at 14-15.

and intentionally induce, direct infringement of the ’441 Patent by providing these products to customers and end-users for use in an infringing manner.

77. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’441 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[71] Video Tutorials,[72] SonicWall University,[73] and Customer Service[74] websites.

78. Defendant has and continues to indirectly infringe one or more claims of the ’441 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’441 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls that integrate with Network Security Manager and/or SonicWall Capture ATP, or Capture Client, that integrates with Sonicwall Capture ATP. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’441 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high

[71] https://www.sonicwall.com/support/technical-documentation/?language=English

[72] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[73] https://www.sonicwall.com/partners/sonicwall-university/

[74] https://www.sonicwall.com/support/contact-support/customer-service/

probability that others would infringe the ’441 Patent but remained willfully blind to the infringing nature of others’ actions.

79. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’441 Patent in an amount to be proved at trial.

80. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’441 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

81. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’441 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’441 Patent. Upon information and belief, Defendant had actual knowledge of the ’441 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’441 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

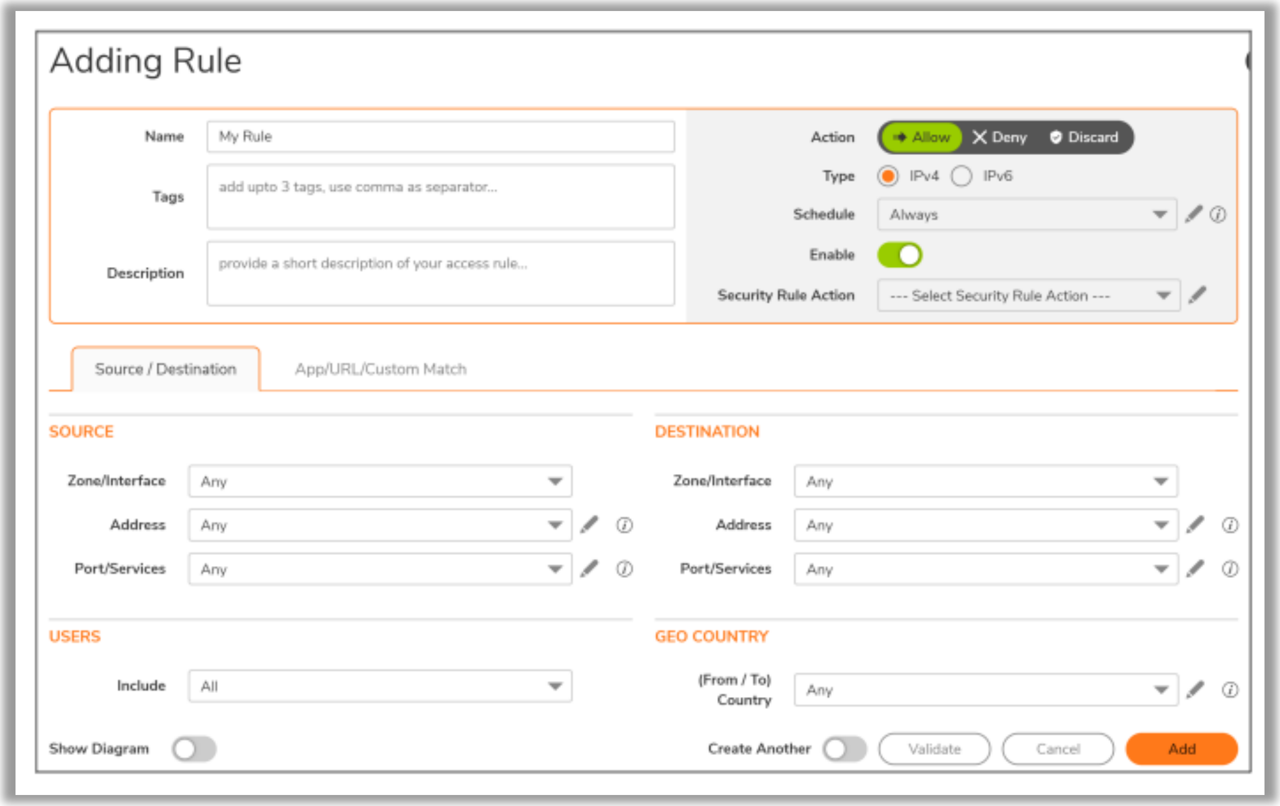
COUNT IV
(Infringement of the ’517 Patent)

82. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

83. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’517 Patent.

84. Defendant has and continues to directly infringe the ’517 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’517 Patent. Such products include at least SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) integrated with Network Security Manager and/or Capture ATP, or SonicWall Capture Client integrated with Capture ATP (the “’517 Accused Products”) which practice a method for assessing runtime risk for an application program that executes on a device, comprising: storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence; storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules; identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application; and identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action.

85. Every ’517 Accused Product practices storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence. For example, Capture ATP is used to add rules in its database that apply to traffic and “[e]ach rule defines the specific criteria to match, and defines an associated action.” “[E]ach rule is defined by match criteria and has an action and/or action profile.”



Adding Rule

Name: My Rule

Tags: add upto 3 tags, use comma as separator...

Description: provide a short description of your access rule...

Action: [✓ Allow] Deny Discard

Type: ● IPv4 ○ IPv6

Schedule: Always

Enable: on

Security Rule Action: --- Select Security Rule Action ---

Source / Destination | App/URL/Custom Match

SOURCE

Zone/Interface: Any

Address: Any

Port/Services: Any

DESTINATION

Zone/Interface: Any

Address: Any

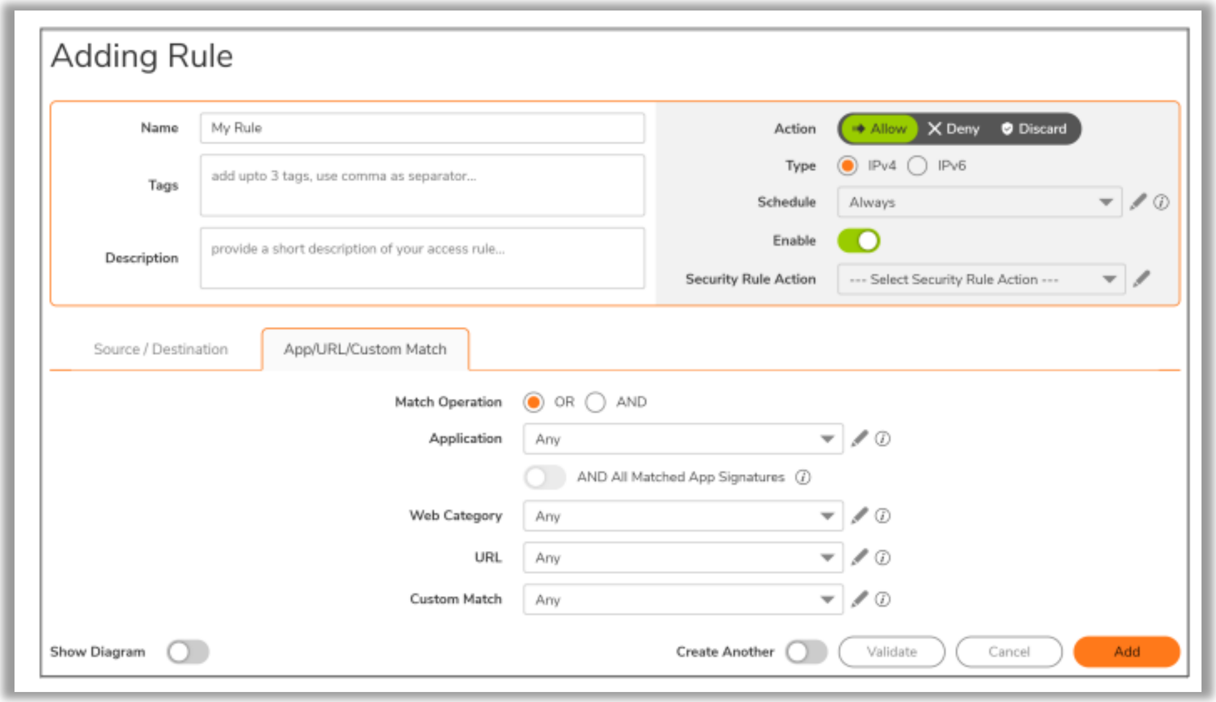
Port/Services: Any

USERS

Include: All

GEO COUNTRY

(From / To) Country: Any



Adding Rule

Name: My Rule

Tags: add upto 3 tags, use comma as separator...

Description: provide a short description of your access rule...

Action: Allow | Deny | Discard

Type: ● IPv4 ○ IPv6

Schedule: Always

Enable: on

Security Rule Action: --- Select Security Rule Action ---

Source / Destination | App/URL/Custom Match

Match Operation: ● OR ○ AND

Application: Any

AND All Matched App Signatures: off

Web Category: Any

URL: Any

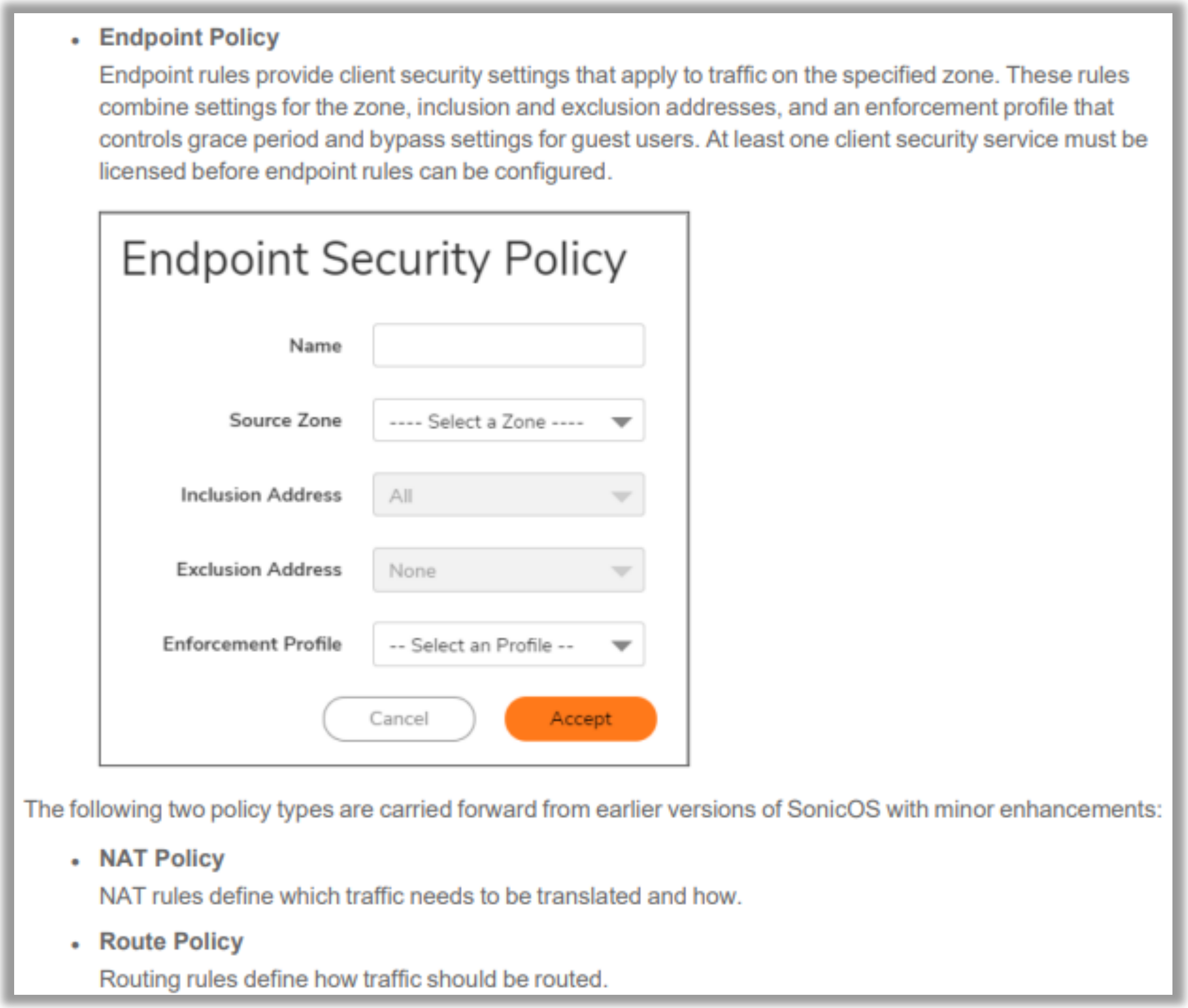
Custom Match: Any

Show Diagram: off

Create Another: off

[75]

[75] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 48-49.



- **Endpoint Policy**
  Endpoint rules provide client security settings that apply to traffic on the specified zone. These rules combine settings for the zone, inclusion and exclusion addresses, and an enforcement profile that controls grace period and bypass settings for guest users. At least one client security service must be licensed before endpoint rules can be configured.

Endpoint Security Policy

Name

Source Zone: ---- Select a Zone ----

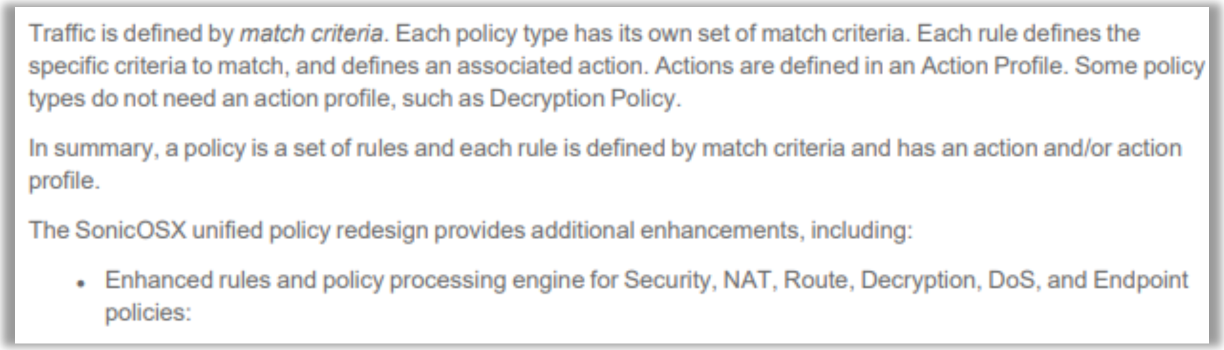
Inclusion Address: All

Exclusion Address: None

Enforcement Profile: -- Select an Profile --

The following two policy types are carried forward from earlier versions of SonicOS with minor enhancements:

- **NAT Policy**
  NAT rules define which traffic needs to be translated and how.
- **Route Policy**
  Routing rules define how traffic should be routed.



Traffic is defined by *match criteria*. Each policy type has its own set of match criteria. Each rule defines the specific criteria to match, and defines an associated action. Actions are defined in an Action Profile. Some policy types do not need an action profile, such as Decryption Policy.

In summary, a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.

The SonicOSX unified policy redesign provides additional enhancements, including:

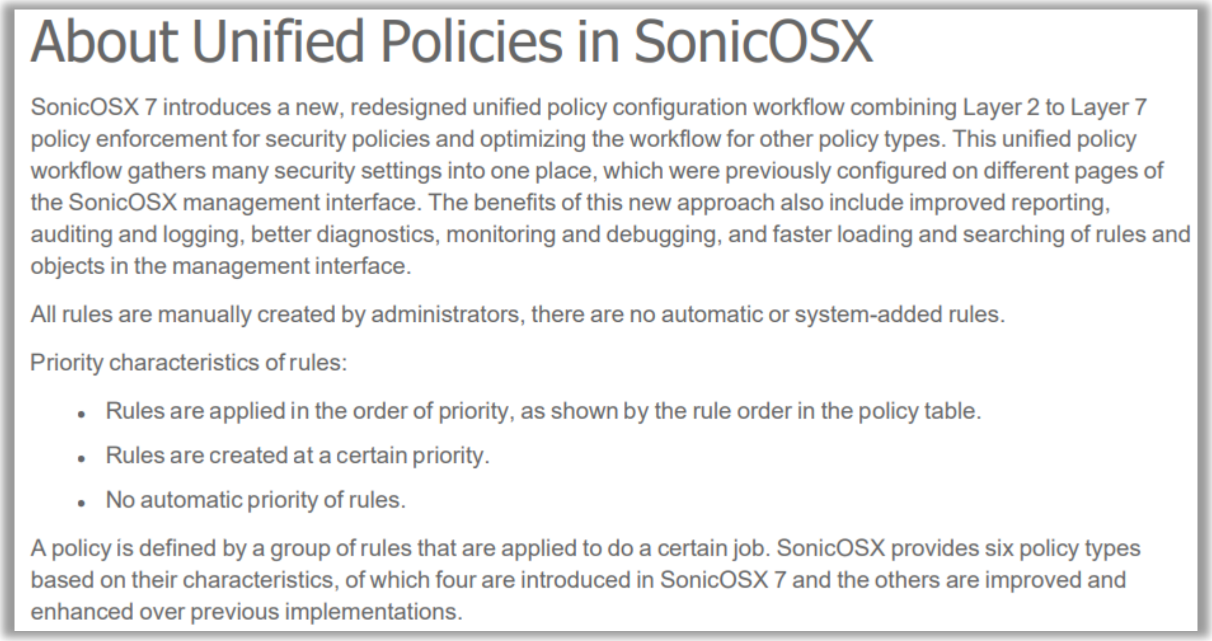
- Enhanced rules and policy processing engine for Security, NAT, Route, Decryption, DoS, and Endpoint policies:

[76]

86. Every ’517 Accused Product practices storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of

[76] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 50-51.

rules. For example, Capture ATP includes a policy database where “a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.”



About Unified Policies in SonicOSX

SonicOSX 7 introduces a new, redesigned unified policy configuration workflow combining Layer 2 to Layer 7 policy enforcement for security policies and optimizing the workflow for other policy types. This unified policy workflow gathers many security settings into one place, which were previously configured on different pages of the SonicOSX management interface. The benefits of this new approach also include improved reporting, auditing and logging, better diagnostics, monitoring and debugging, and faster loading and searching of rules and objects in the management interface.

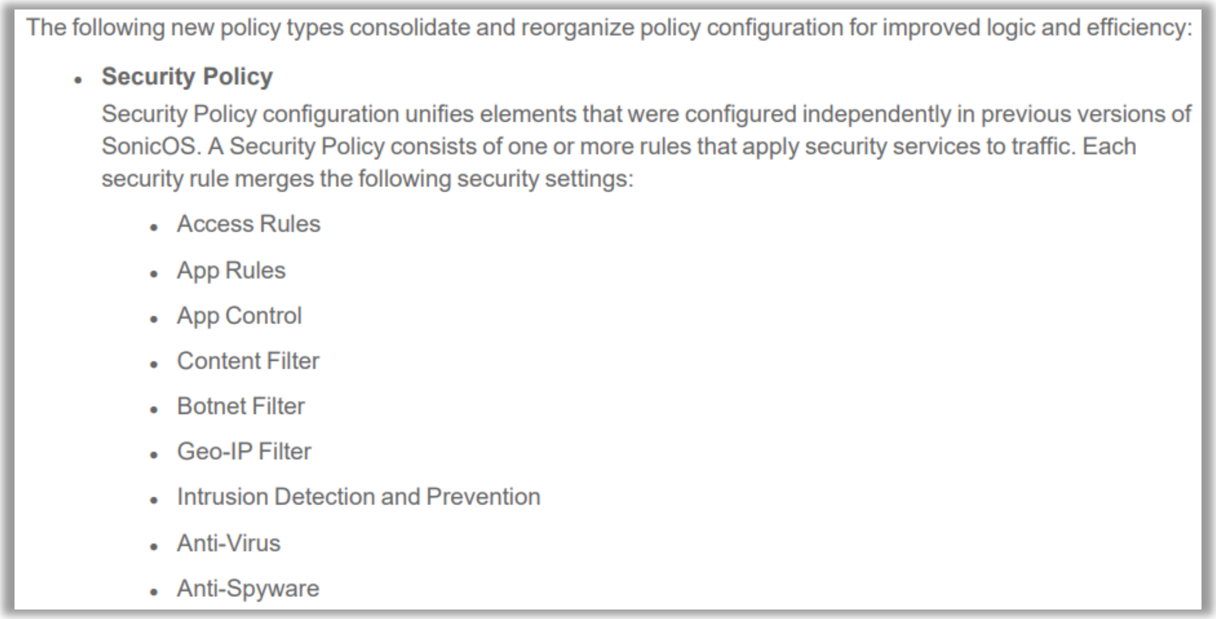
All rules are manually created by administrators, there are no automatic or system-added rules.

Priority characteristics of rules:

- Rules are applied in the order of priority, as shown by the rule order in the policy table.
- Rules are created at a certain priority.
- No automatic priority of rules.

A policy is defined by a group of rules that are applied to do a certain job. SonicOSX provides six policy types based on their characteristics, of which four are introduced in SonicOSX 7 and the others are improved and enhanced over previous implementations.

[77]



The following new policy types consolidate and reorganize policy configuration for improved logic and efficiency:

- **Security Policy**

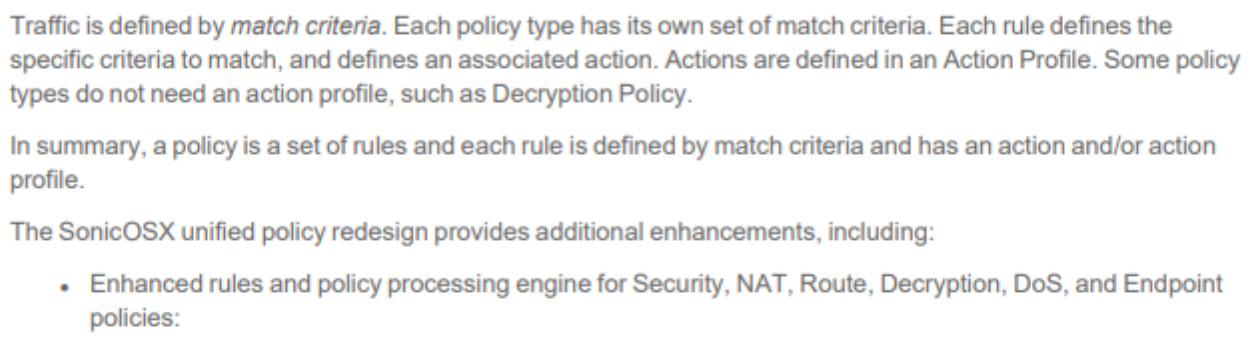
  Security Policy configuration unifies elements that were configured independently in previous versions of SonicOS. A Security Policy consists of one or more rules that apply security services to traffic. Each security rule merges the following security settings:

  - Access Rules
  - App Rules
  - App Control
  - Content Filter
  - Botnet Filter
  - Geo-IP Filter
  - Intrusion Detection and Prevention
  - Anti-Virus
  - Anti-Spyware

[78]

[77] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 47.

[78] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 48.



Traffic is defined by *match criteria*. Each policy type has its own set of match criteria. Each rule defines the specific criteria to match, and defines an associated action. Actions are defined in an Action Profile. Some policy types do not need an action profile, such as Decryption Policy.

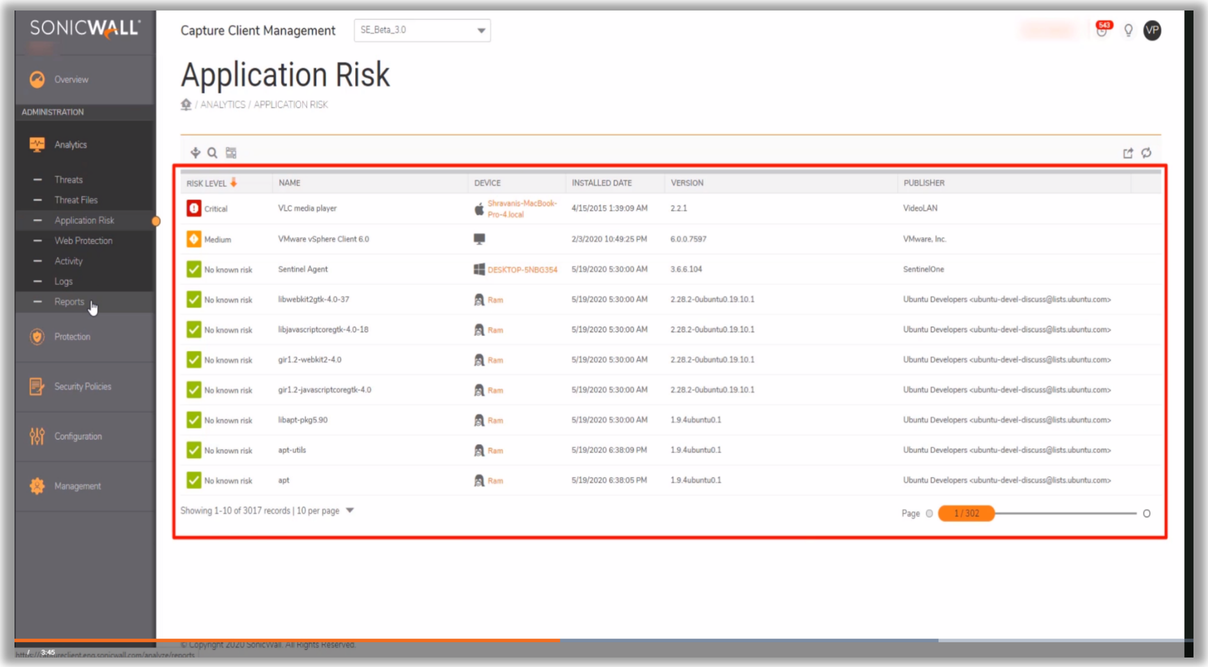
In summary, a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.

The SonicOSX unified policy redesign provides additional enhancements, including:

- Enhanced rules and policy processing engine for Security, NAT, Route, Decryption, DoS, and Endpoint policies:

[79]

87. Every ’517 Accused Product practices identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application. For example, as shown below, Capture Client can use Capture ATP to assign risk levels to the names of applications executing on a device. Capture ATP provides those same risk level analytics to network security appliances.



Application Risk

/ ANALYTICS / APPLICATION RISK

RISK LEVEL	NAME	DEVICE	INSTALLED DATE	VERSION	PUBLISHER
Critical	VLC media player	Shravanis-MacBook-Pro-4.local	4/15/2015 1:39:09 AM	2.2.1	VideoLAN
Medium	VMware vSphere Client 6.0		2/3/2020 10:49:25 PM	6.0.0.7597	VMware, Inc.
✓ No known risk	Sentinel Agent	DESKTOP-5NBG354	5/19/2020 5:30:00 AM	3.6.6.104	SentinelOne
✓ No known risk	libwebkit2gtk-4.0-37	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
✓ No known risk	libjavascriptcoregtk-4.0-18	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
✓ No known risk	gir1.2-webkit2-4.0	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
✓ No known risk	gir1.2-javascriptcoregtk-4.0	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
✓ No known risk	libapt-pkg5.90	Ram	5/19/2020 5:30:00 AM	1.9.4ubuntu0.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
✓ No known risk	apt-utils	Ram	5/19/2020 6:38:09 PM	1.9.4ubuntu0.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
✓ No known risk	apt	Ram	5/19/2020 6:38:05 PM	1.9.4ubuntu0.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>

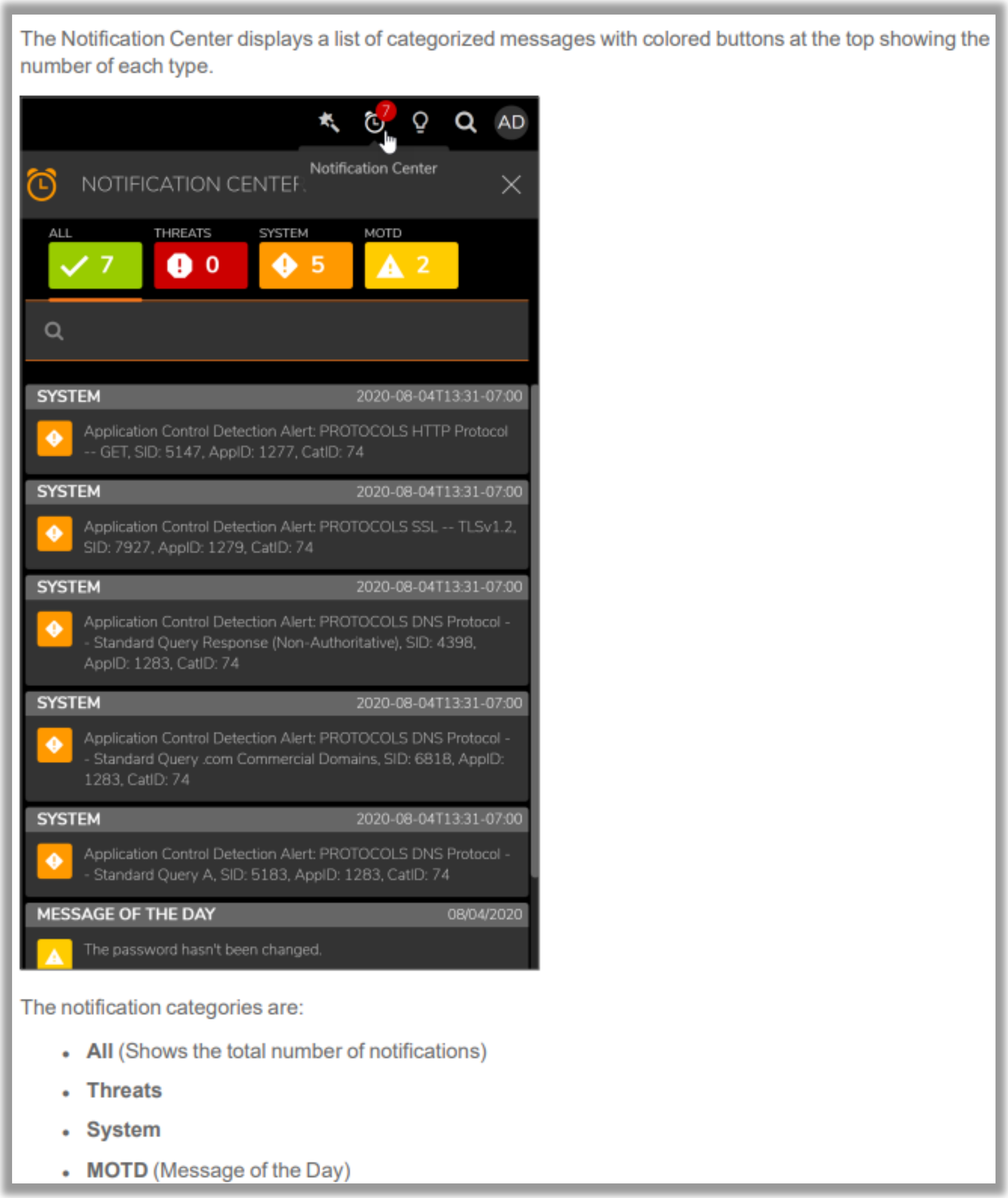
Showing 1-10 of 3017 records | 10 per page

Page 1 / 302

[80]

[79] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 51.

[80] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6193544296001



The Notification Center displays a list of categorized messages with colored buttons at the top showing the number of each type.

SYSTEM 2020-08-04T13:31-07:00
Application Control Detection Alert: PROTOCOLS HTTP Protocol -- GET, SID: 5147, AppID: 1277, CatID: 74

SYSTEM 2020-08-04T13:31-07:00
Application Control Detection Alert: PROTOCOLS SSL -- TLSv1.2, SID: 7927, AppID: 1279, CatID: 74

SYSTEM 2020-08-04T13:31-07:00
Application Control Detection Alert: PROTOCOLS DNS Protocol -- Standard Query Response (Non-Authoritative), SID: 4398, AppID: 1283, CatID: 74

SYSTEM 2020-08-04T13:31-07:00
Application Control Detection Alert: PROTOCOLS DNS Protocol -- Standard Query .com Commercial Domains, SID: 6818, AppID: 1283, CatID: 74

SYSTEM 2020-08-04T13:31-07:00
Application Control Detection Alert: PROTOCOLS DNS Protocol -- Standard Query A, SID: 5183, AppID: 1283, CatID: 74

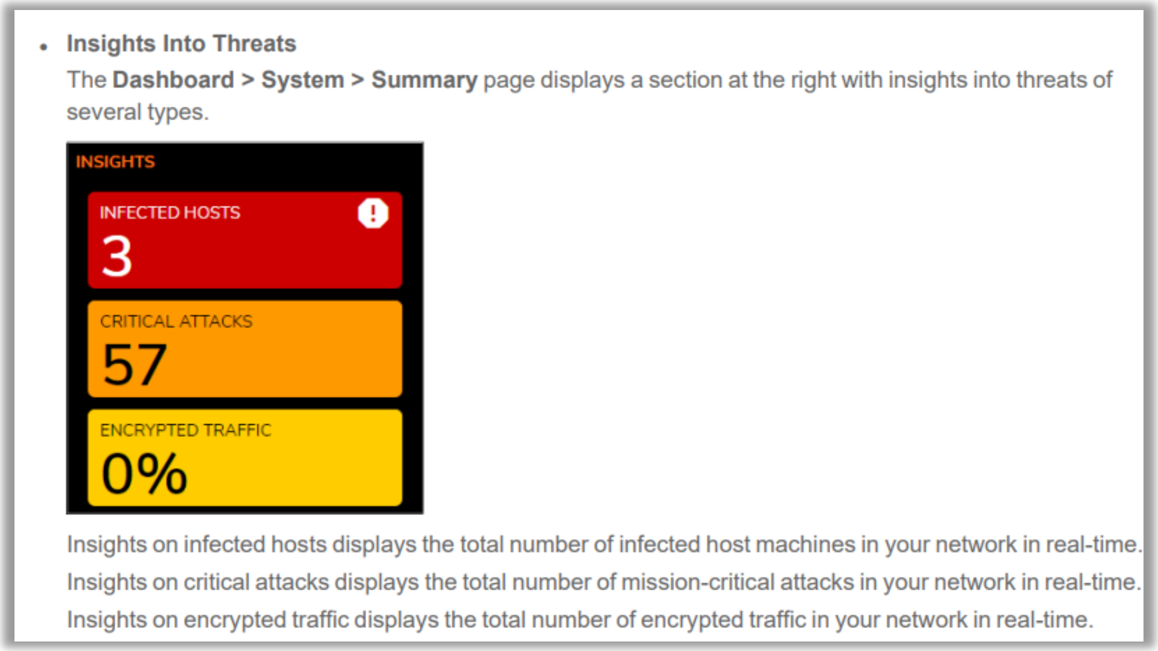
MESSAGE OF THE DAY 08/04/2020
The password hasn't been changed.

The notification categories are:

- **All** (Shows the total number of notifications)
- **Threats**
- **System**
- **MOTD** (Message of the Day)

[81]

[81] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 24.



- **Insights Into Threats**

  The **Dashboard > System > Summary** page displays a section at the right with insights into threats of several types.

INSIGHTS

INFECTED HOSTS
3

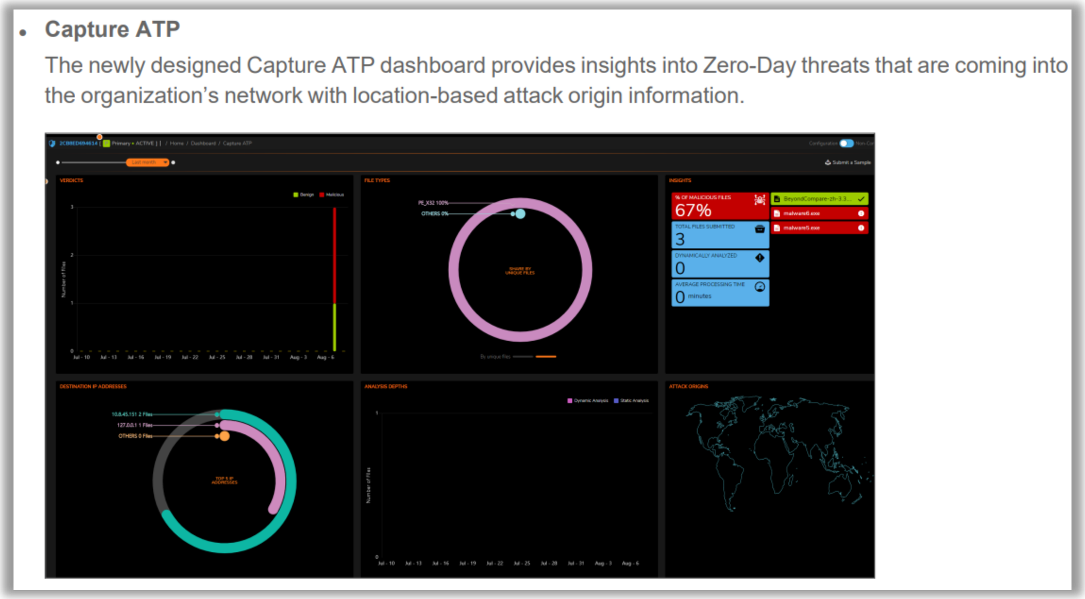
CRITICAL ATTACKS
57

ENCRYPTED TRAFFIC
0%

Insights on infected hosts displays the total number of infected host machines in your network in real-time.
Insights on critical attacks displays the total number of mission-critical attacks in your network in real-time.
Insights on encrypted traffic displays the total number of encrypted traffic in your network in real-time.

[82]

88. Every '517 Accused Product practices identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk. For example, Capture ATP identifies a behavior score (e.g., severity levels) for each runtime risk (e.g., vulnerability).

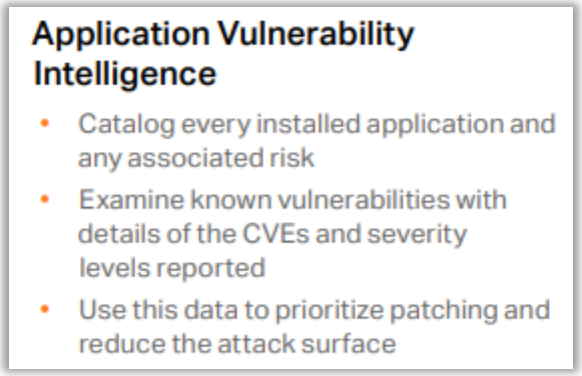


- **Capture ATP**

  The newly designed Capture ATP dashboard provides insights into Zero-Day threats that are coming into the organization's network with location-based attack origin information.

[83]

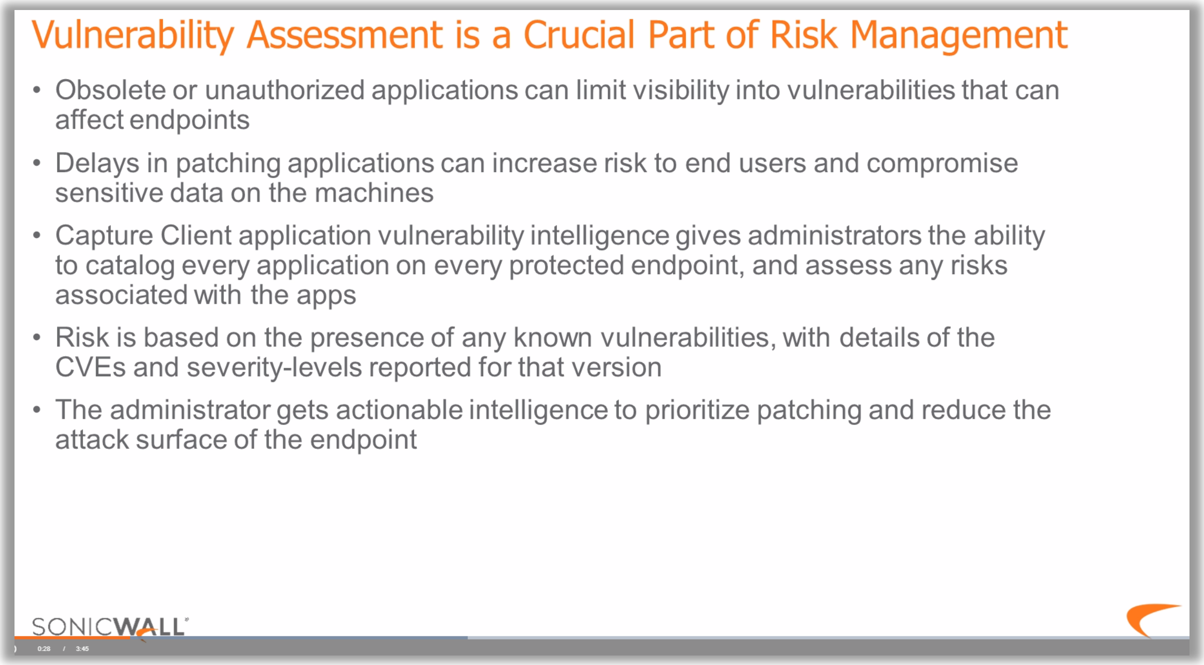
[82] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 39.
[83] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 41.



Application Vulnerability Intelligence

- Catalog every installed application and any associated risk
- Examine known vulnerabilities with details of the CVEs and severity levels reported
- Use this data to prioritize patching and reduce the attack surface

[84]



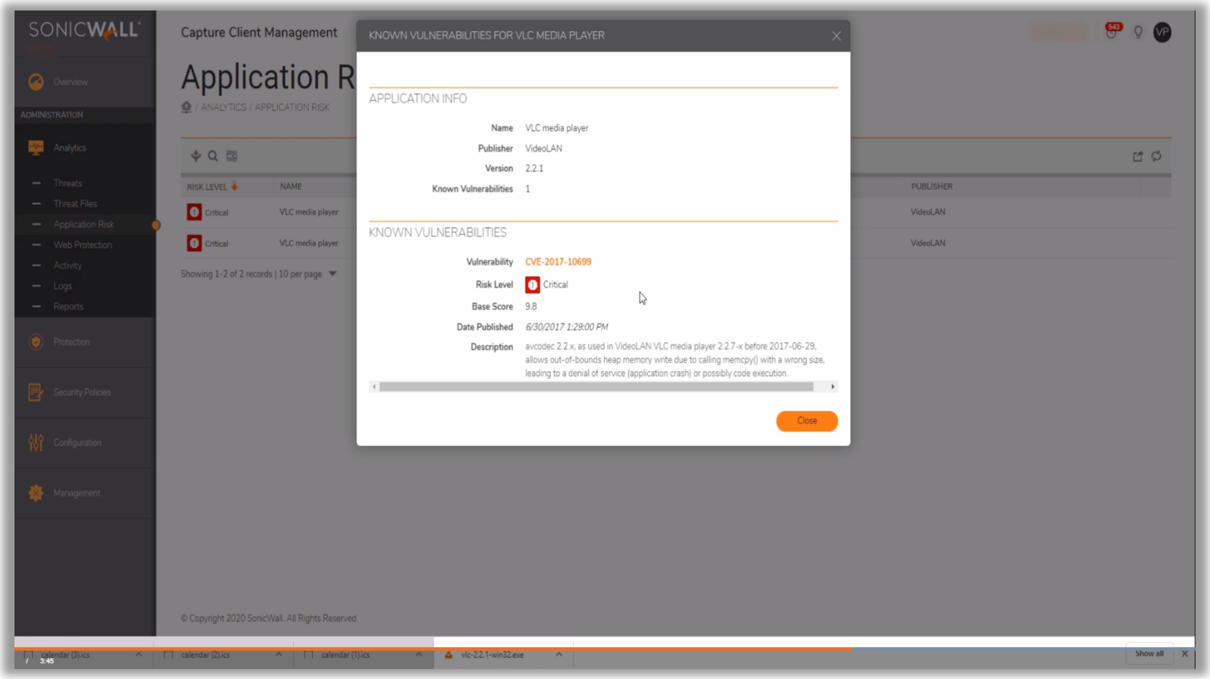
Vulnerability Assessment is a Crucial Part of Risk Management

- Obsolete or unauthorized applications can limit visibility into vulnerabilities that can affect endpoints
- Delays in patching applications can increase risk to end users and compromise sensitive data on the machines
- Capture Client application vulnerability intelligence gives administrators the ability to catalog every application on every protected endpoint, and assess any risks associated with the apps
- Risk is based on the presence of any known vulnerabilities, with details of the CVEs and severity-levels reported for that version
- The administrator gets actionable intelligence to prioritize patching and reduce the attack surface of the endpoint

[85]

[84] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.

[85] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6193544296001



KNOWN VULNERABILITIES FOR VLC MEDIA PLAYER

APPLICATION INFO

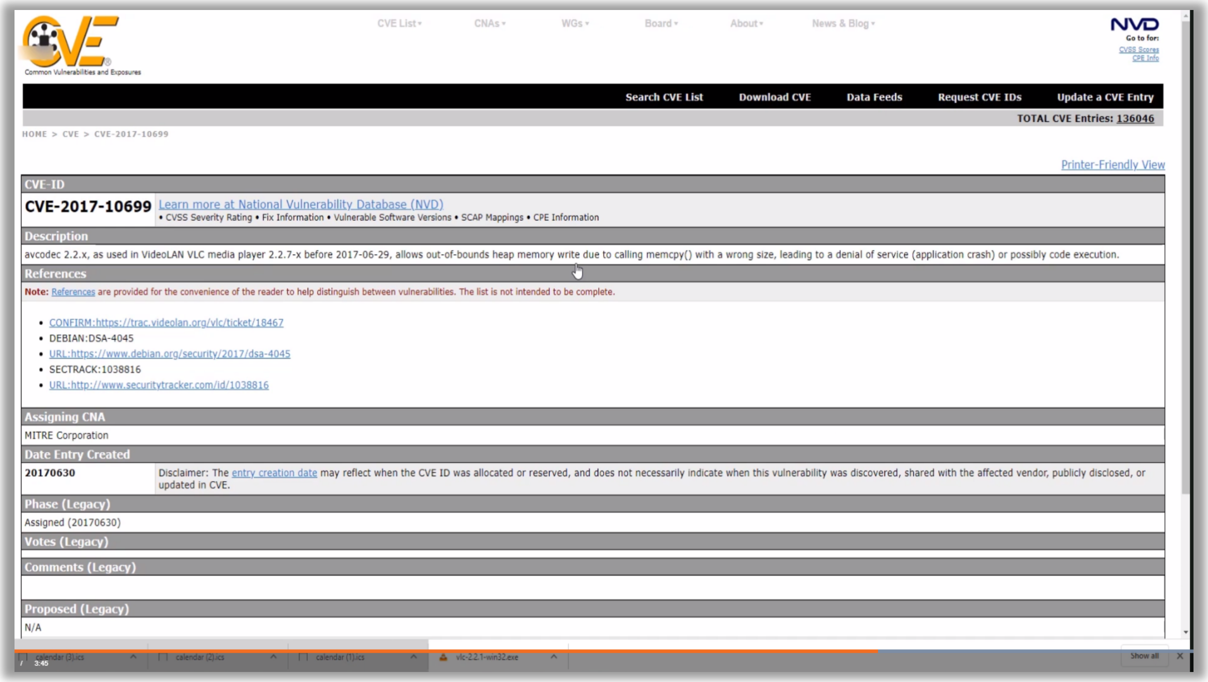
Name	VLC media player
Publisher	VideoLAN
Version	2.2.1
Known Vulnerabilities	1

KNOWN VULNERABILITIES

Vulnerability	CVE-2017-10699
Risk Level	Critical
Base Score	9.8
Date Published	*6/30/2017 1:29:00 PM*
Description	avcodec 2.2.x, as used in VideoLAN VLC media player 2.2.7-x before 2017-06-29, allows out-of-bounds heap memory write due to calling memcpy() with a wrong size, leading to a denial of service (application crash) or possibly code execution.

Close

86



TOTAL CVE Entries: 136046

HOME > CVE > CVE-2017-10699

Printer-Friendly View

CVE-ID

CVE-2017-10699 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

avcodec 2.2.x, as used in VideoLAN VLC media player 2.2.7-x before 2017-06-29, allows out-of-bounds heap memory write due to calling memcpy() with a wrong size, leading to a denial of service (application crash) or possibly code execution.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://trac.videolan.org/vlc/ticket/18467
- DEBIAN:DSA-4045
- URL:https://www.debian.org/security/2017/dsa-4045
- SECTRACK:1038816
- URL:http://www.securitytracker.com/id/1038816

Assigning CNA

MITRE Corporation

Date Entry Created

20170630 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20170630)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

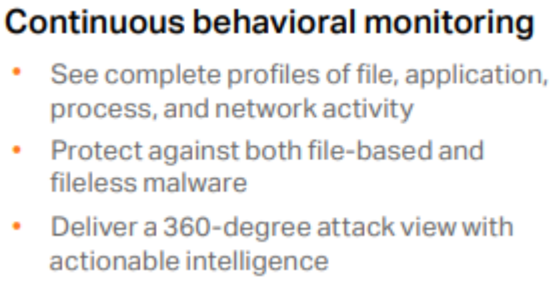
N/A

87

[86] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6193544296001

[87] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6193544296001

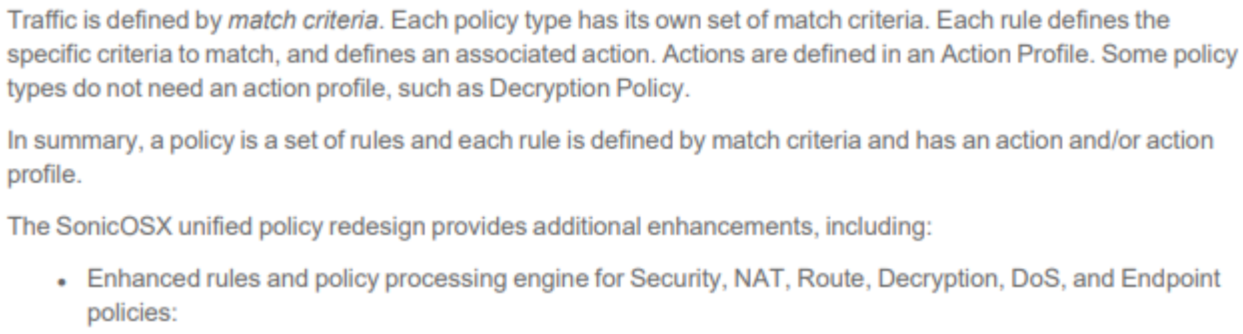
89. Every ’517 Accused Product practices identifying…wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action. For example, Capture ATP includes rules that meet certain match criteria, which can be any combination of a user action, an application action, and/or a system action.



Continuous behavioral monitoring

- See complete profiles of file, application, process, and network activity
- Protect against both file-based and fileless malware
- Deliver a 360-degree attack view with actionable intelligence

https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.



Traffic is defined by *match criteria*. Each policy type has its own set of match criteria. Each rule defines the specific criteria to match, and defines an associated action. Actions are defined in an Action Profile. Some policy types do not need an action profile, such as Decryption Policy.

In summary, a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.

The SonicOSX unified policy redesign provides additional enhancements, including:

- Enhanced rules and policy processing engine for Security, NAT, Route, Decryption, DoS, and Endpoint policies:

[88]

90. Defendant has and continues to directly infringe one or more claims of the ’517 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

91. Defendant has and continues to indirectly infringe one or more claims of the ’517 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using,

[88] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 51.

offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’517 Accused Products.

92. Defendant has and continues to indirectly infringe one or more claims of the ’517 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’517 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’517 Patent by providing these products to customers and end-users for use in an infringing manner.

93. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’517 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[89] Video Tutorials,[90] SonicWall University,[91] and Customer Service[92] websites.

94. Defendant has and continues to indirectly infringe one or more claims of the ’517 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this

[89] https://www.sonicwall.com/support/technical-documentation/?language=English

[90] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[91] https://www.sonicwall.com/partners/sonicwall-university/

[92] https://www.sonicwall.com/support/contact-support/customer-service/

Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’517 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls or Capture Client, that integrate with Sonicwall Capture ATP. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’517 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’517 Patent but remained willfully blind to the infringing nature of others’ actions.

95. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’517 Patent in an amount to be proved at trial.

96. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’517 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

97. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’517 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’517 Patent. Upon information and belief, Defendant had actual knowledge of the ’517 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the

’517 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT V
(Infringement of the ’948 Patent)

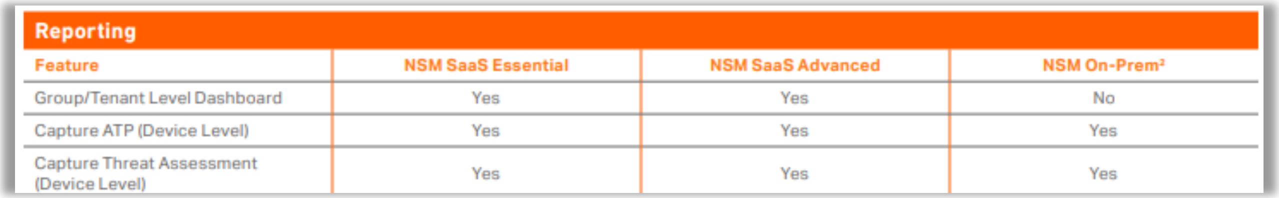
98. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

99. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’948 Patent.

100. Defendant has and continues to directly infringe the ’948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’948 Patent. Such products include at least SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) integrated with Network Security Manager (the “’948 Accused Products”) which practice a method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity

processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

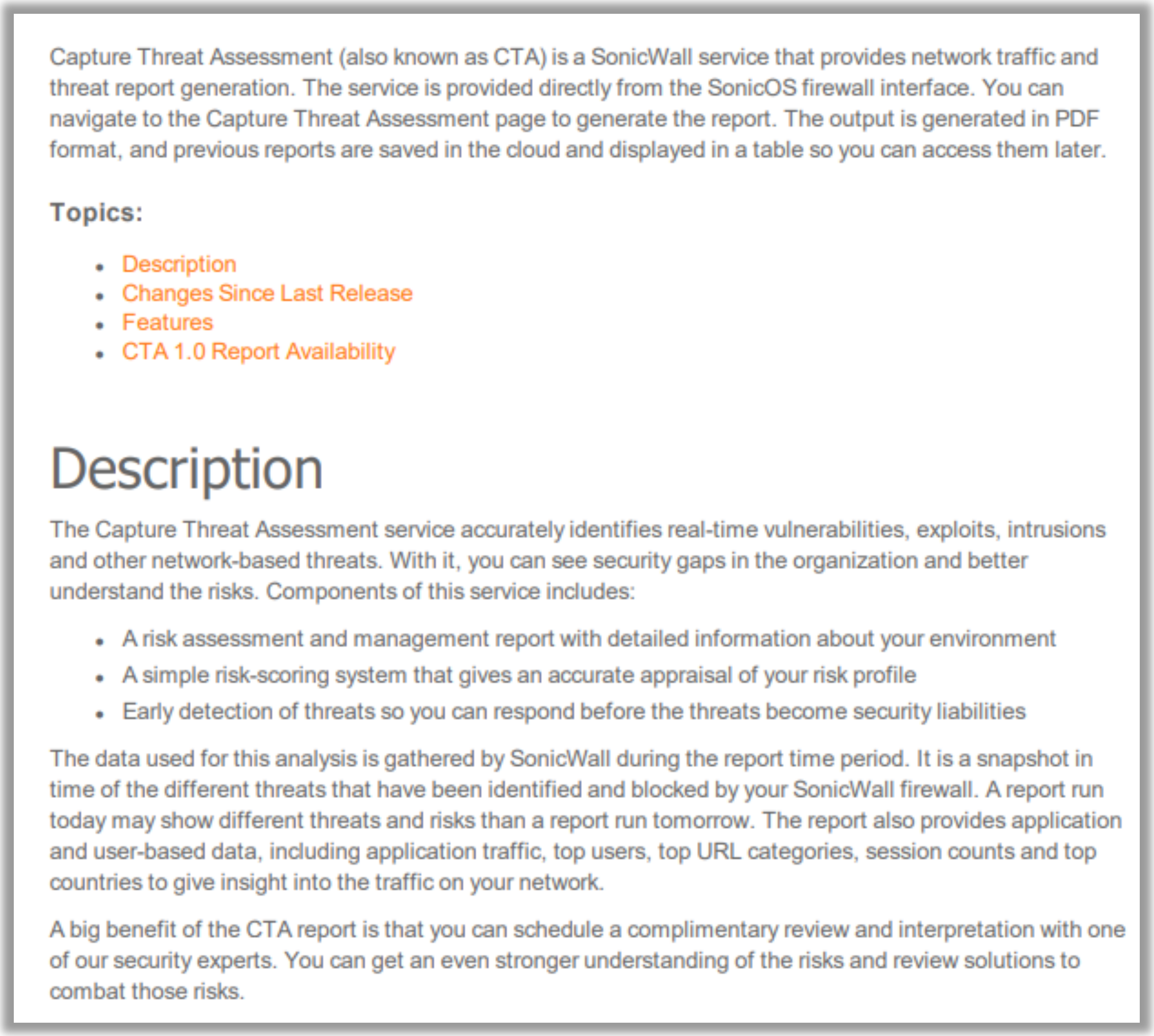
101. Every ’948 Accused Product practices monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application. For example, Capture Threat Assessment (also known as CTA) is a SonicWall service used by Network Security Manager and provided directly from the SonicOS firewall interface to determine at least system operations initiated by the application (e.g., “filesharing applications”), resource utilization by the application (e.g., “bandwidth hogging applications”), and integrity of the application (e.g., “vulnerable applications” and “risky applications” and “application by risk level”).



Reporting

Feature	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem[2]
Group/Tenant Level Dashboard	Yes	Yes	No
Capture ATP (Device Level)	Yes	Yes	Yes
Capture Threat Assessment (Device Level)	Yes	Yes	Yes

https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 6.



Capture Threat Assessment (also known as CTA) is a SonicWall service that provides network traffic and threat report generation. The service is provided directly from the SonicOS firewall interface. You can navigate to the Capture Threat Assessment page to generate the report. The output is generated in PDF format, and previous reports are saved in the cloud and displayed in a table so you can access them later.

Topics:

- Description
- Changes Since Last Release
- Features
- CTA 1.0 Report Availability

Description

The Capture Threat Assessment service accurately identifies real-time vulnerabilities, exploits, intrusions and other network-based threats. With it, you can see security gaps in the organization and better understand the risks. Components of this service includes:

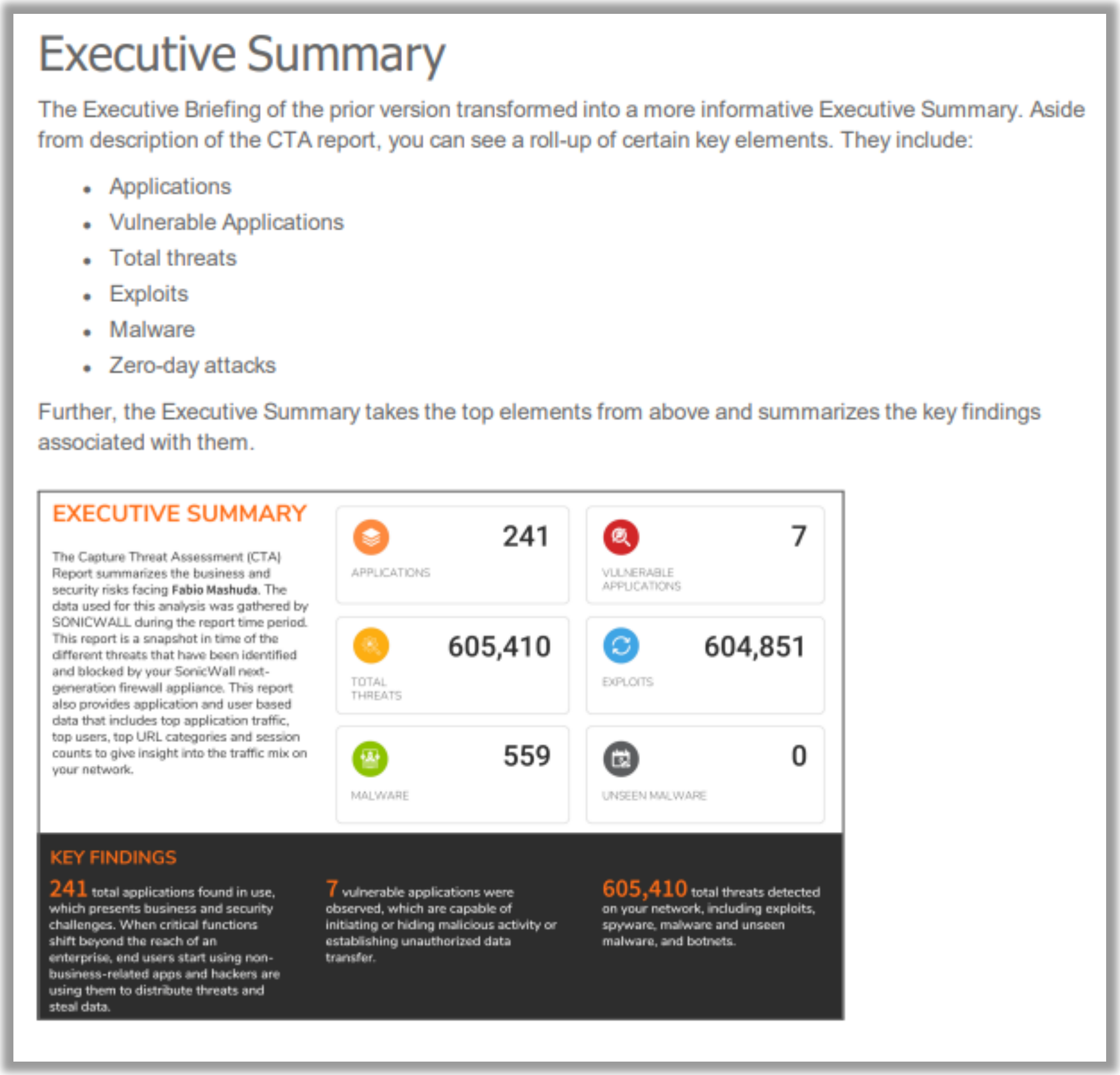
- A risk assessment and management report with detailed information about your environment
- A simple risk-scoring system that gives an accurate appraisal of your risk profile
- Early detection of threats so you can respond before the threats become security liabilities

The data used for this analysis is gathered by SonicWall during the report time period. It is a snapshot in time of the different threats that have been identified and blocked by your SonicWall firewall. A report run today may show different threats and risks than a report run tomorrow. The report also provides application and user-based data, including application traffic, top users, top URL categories, session counts and top countries to give insight into the traffic on your network.

A big benefit of the CTA report is that you can schedule a complimentary review and interpretation with one of our security experts. You can get an even stronger understanding of the risks and review solutions to combat those risks.

[93]

[93] https://www.sonicwall.com/techdocs/pdf/cta-user_guide.pdf, at 3.



Executive Summary

The Executive Briefing of the prior version transformed into a more informative Executive Summary. Aside from description of the CTA report, you can see a roll-up of certain key elements. They include:

- Applications
- Vulnerable Applications
- Total threats
- Exploits
- Malware
- Zero-day attacks

Further, the Executive Summary takes the top elements from above and summarizes the key findings associated with them.

EXECUTIVE SUMMARY

The Capture Threat Assessment (CTA) Report summarizes the business and security risks facing **Fabio Mashuda**. The data used for this analysis was gathered by SONICWALL during the report time period. This report is a snapshot in time of the different threats that have been identified and blocked by your SonicWall next-generation firewall appliance. This report also provides application and user based data that includes top application traffic, top users, top URL categories and session counts to give insight into the traffic mix on your network.

241 APPLICATIONS

7 VULNERABLE APPLICATIONS

605,410 TOTAL THREATS

604,851 EXPLOITS

559 MALWARE

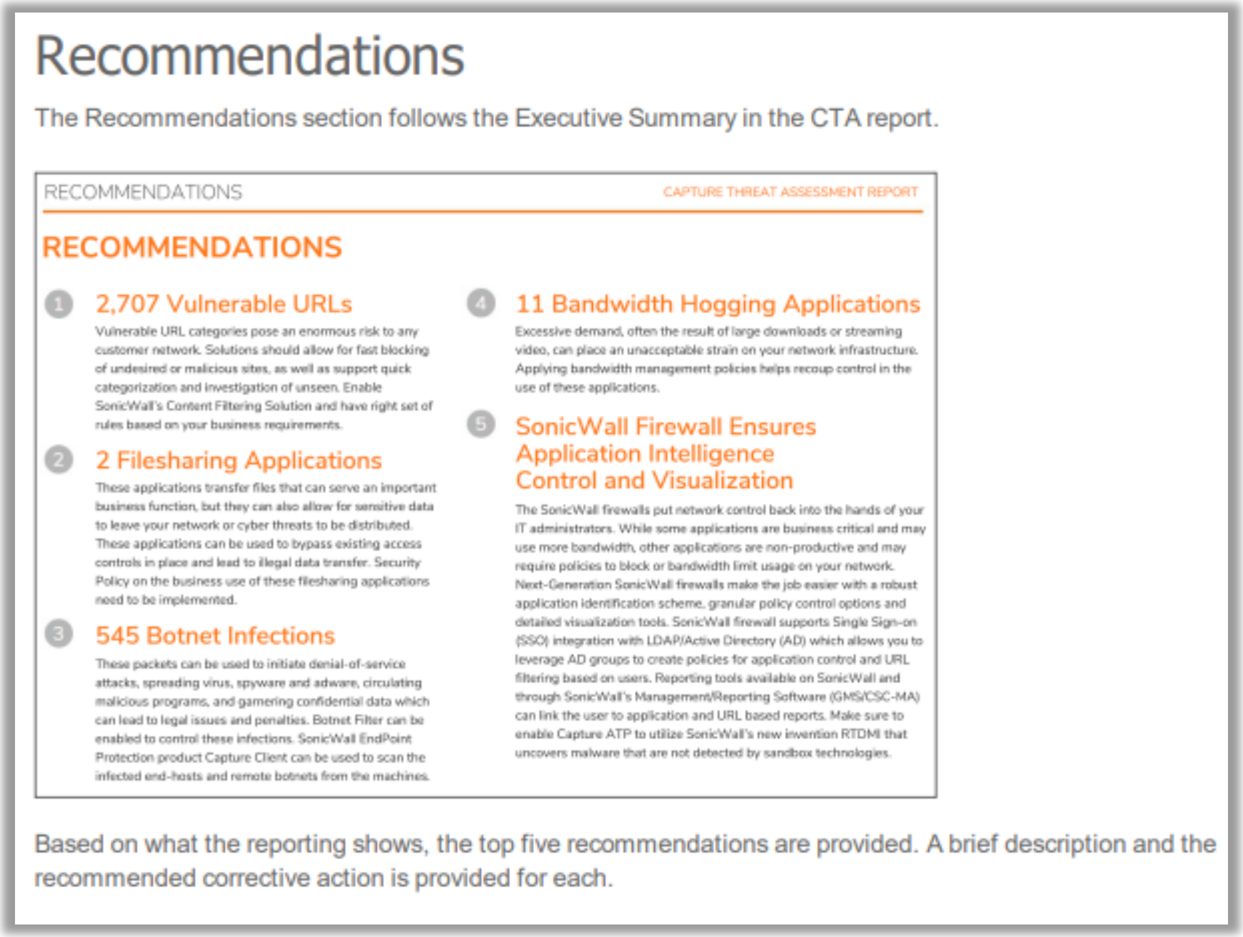
0 UNSEEN MALWARE

KEY FINDINGS

241 total applications found in use, which presents business and security challenges. When critical functions shift beyond the reach of an enterprise, end users start using non-business-related apps and hackers are using them to distribute threats and steal data.

7 vulnerable applications were observed, which are capable of initiating or hiding malicious activity or establishing unauthorized data transfer.

605,410 total threats detected on your network, including exploits, spyware, malware and unseen malware, and botnets.



Recommendations

The Recommendations section follows the Executive Summary in the CTA report.

RECOMMENDATIONS CAPTURE THREAT ASSESSMENT REPORT

RECOMMENDATIONS

1 **2,707 Vulnerable URLs**

Vulnerable URL categories pose an enormous risk to any customer network. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unseen. Enable SonicWall's Content Filtering Solution and have right set of rules based on your business requirements.

2 **2 Filesharing Applications**

These applications transfer files that can serve an important business function, but they can also allow for sensitive data to leave your network or cyber threats to be distributed. These applications can be used to bypass existing access controls in place and lead to illegal data transfer. Security Policy on the business use of these filesharing applications need to be implemented.

3 **545 Botnet Infections**

These packets can be used to initiate denial-of-service attacks, spreading virus, spyware and adware, circulating malicious programs, and gamering confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections. SonicWall EndPoint Protection product Capture Client can be used to scan the infected end-hosts and remote botnets from the machines.

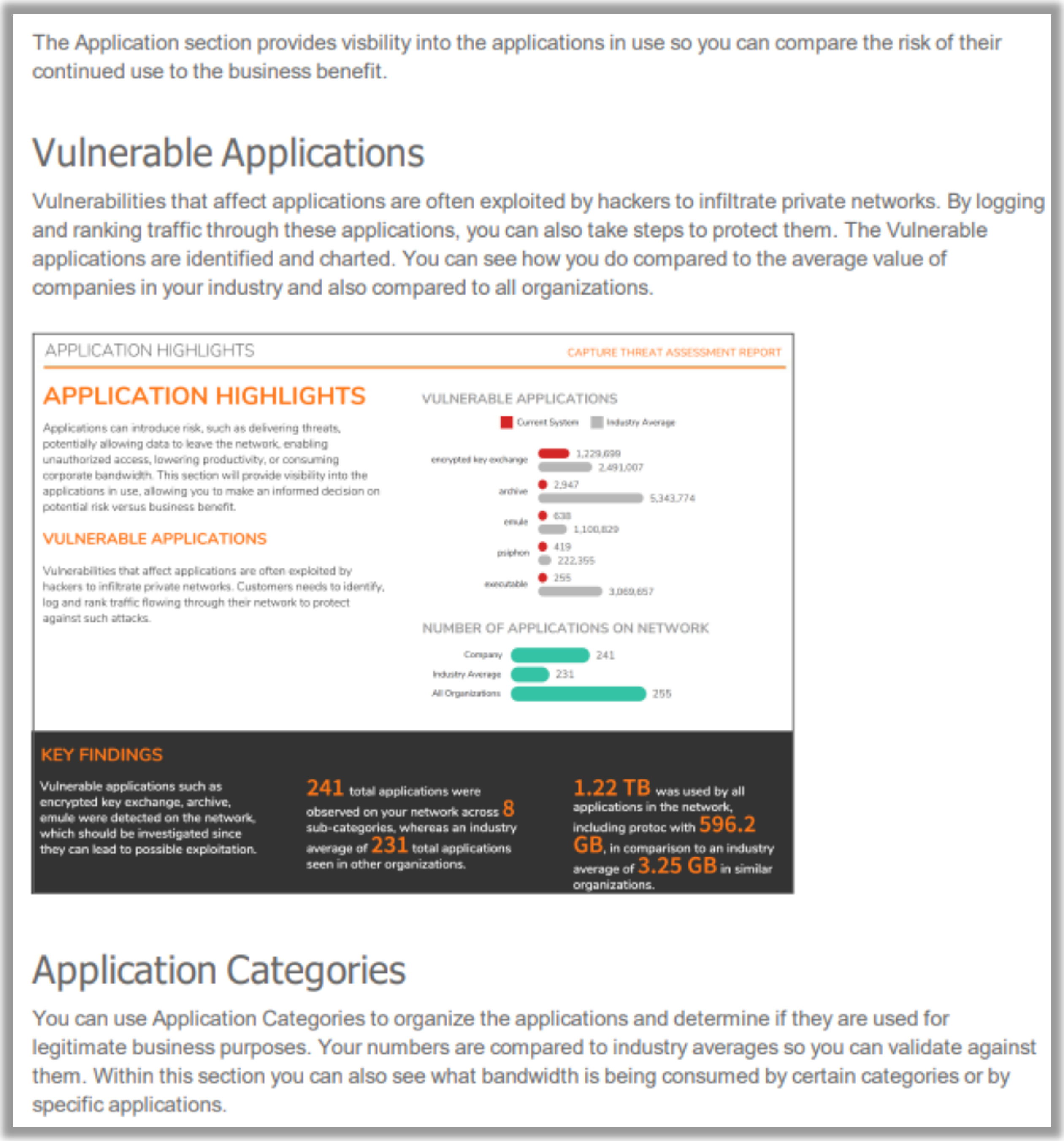
4 **11 Bandwidth Hogging Applications**

Excessive demand, often the result of large downloads or streaming video, can place an unacceptable strain on your network infrastructure. Applying bandwidth management policies helps recoup control in the use of these applications.

5 **SonicWall Firewall Ensures Application Intelligence Control and Visualization**

The SonicWall firewalls put network control back into the hands of your IT administrators. While some applications are business critical and may use more bandwidth, other applications are non-productive and may require policies to block or bandwidth limit usage on your network. Next-Generation SonicWall firewalls make the job easier with a robust application identification scheme, granular policy control options and detailed visualization tools. SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on SonicWall and through SonicWall's Management/Reporting Software (GMS/CSC-MA) can link the user to application and URL based reports. Make sure to enable Capture ATP to utilize SonicWall's new invention RTDMI that uncovers malware that are not detected by sandbox technologies.

Based on what the reporting shows, the top five recommendations are provided. A brief description and the recommended corrective action is provided for each.



The Application section provides visbility into the applications in use so you can compare the risk of their continued use to the business benefit.

Vulnerable Applications

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. By logging and ranking traffic through these applications, you can also take steps to protect them. The Vulnerable applications are identified and charted. You can see how you do compared to the average value of companies in your industry and also compared to all organizations.

APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION HIGHLIGHTS

Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision on potential risk versus business benefit.

VULNERABLE APPLICATIONS

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. Customers needs to identify, log and rank traffic flowing through their network to protect against such attacks.

KEY FINDINGS

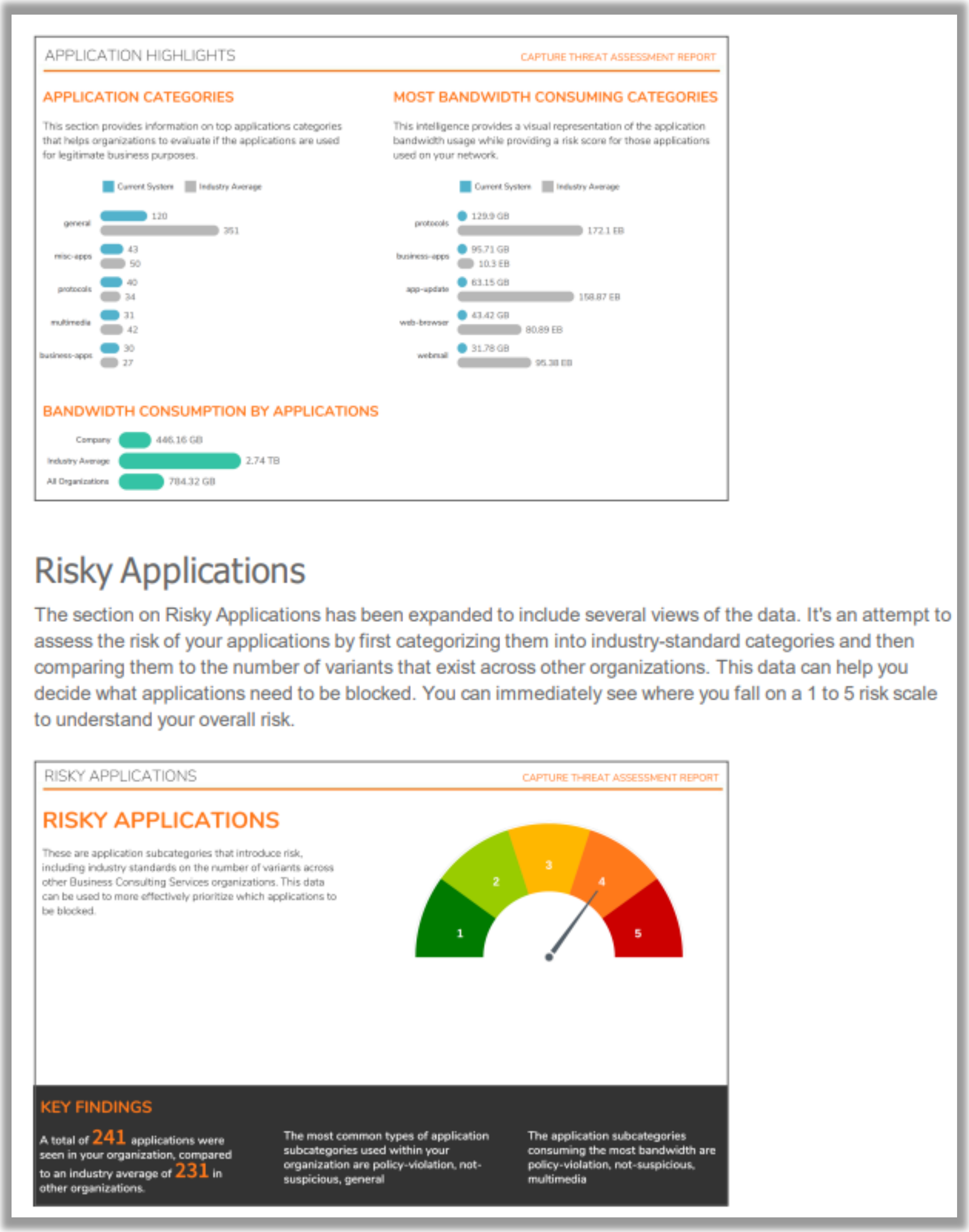
Vulnerable applications such as encrypted key exchange, archive, emule were detected on the network, which should be investigated since they can lead to possible exploitation.

241 total applications were observed on your network across 8 sub-categories, whereas an industry average of 231 total applications seen in other organizations.

1.22 TB was used by all applications in the network, including protoc with 596.2 GB, in comparison to an industry average of 3.25 GB in similar organizations.

Application Categories

You can use Application Categories to organize the applications and determine if they are used for legitimate business purposes. Your numbers are compared to industry averages so you can validate against them. Within this section you can also see what bandwidth is being consumed by certain categories or by specific applications.



APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION CATEGORIES

This section provides information on top applications categories that helps organizations to evaluate if the applications are used for legitimate business purposes.

MOST BANDWIDTH CONSUMING CATEGORIES

This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

BANDWIDTH CONSUMPTION BY APPLICATIONS

Risky Applications

The section on Risky Applications has been expanded to include several views of the data. It's an attempt to assess the risk of your applications by first categorizing them into industry-standard categories and then comparing them to the number of variants that exist across other organizations. This data can help you decide what applications need to be blocked. You can immediately see where you fall on a 1 to 5 risk scale to understand your overall risk.

RISKY APPLICATIONS

CAPTURE THREAT ASSESSMENT REPORT

RISKY APPLICATIONS

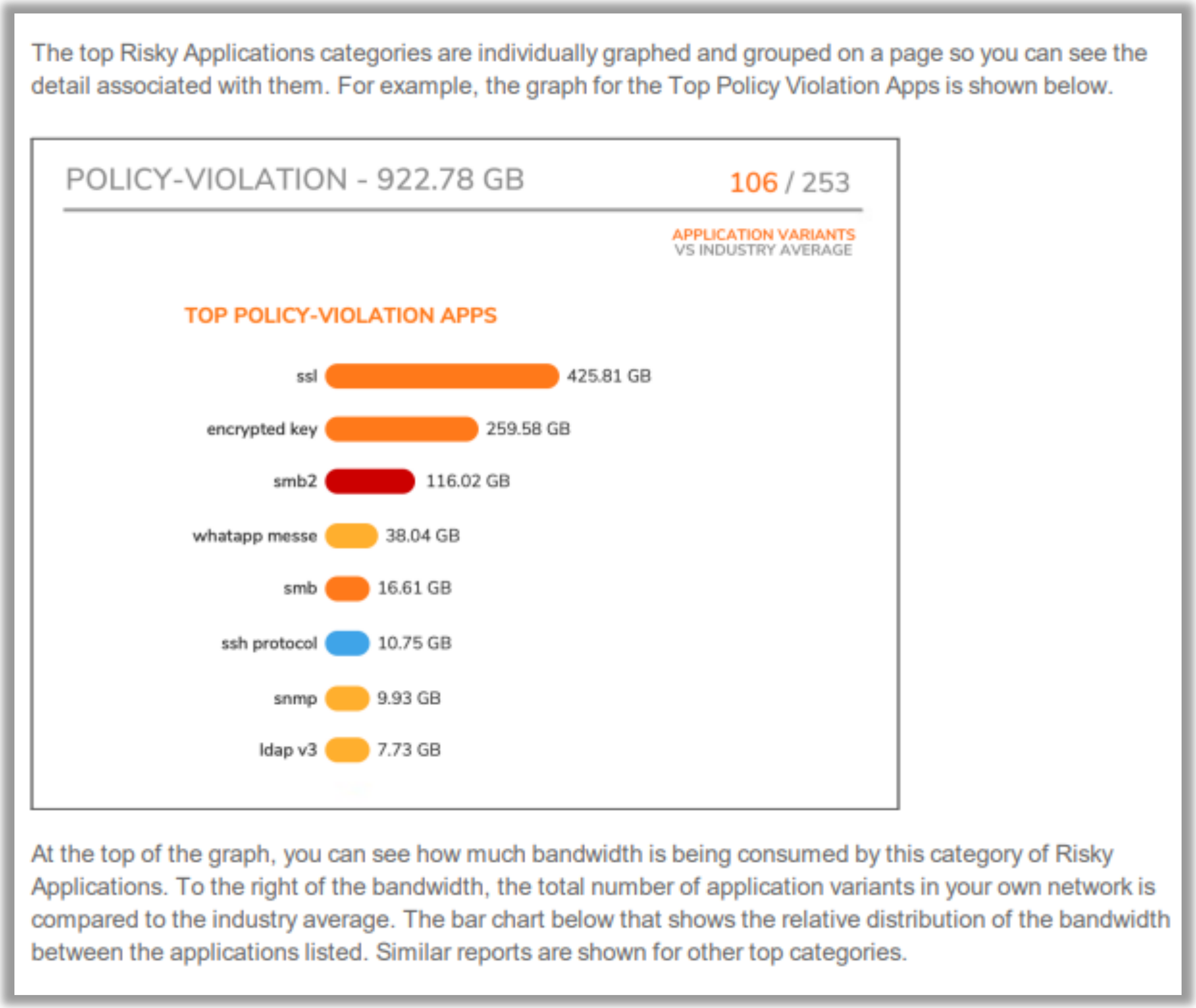
These are application subcategories that introduce risk, including industry standards on the number of variants across other Business Consulting Services organizations. This data can be used to more effectively prioritize which applications to be blocked.

KEY FINDINGS

A total of 241 applications were seen in your organization, compared to an industry average of 231 in other organizations.

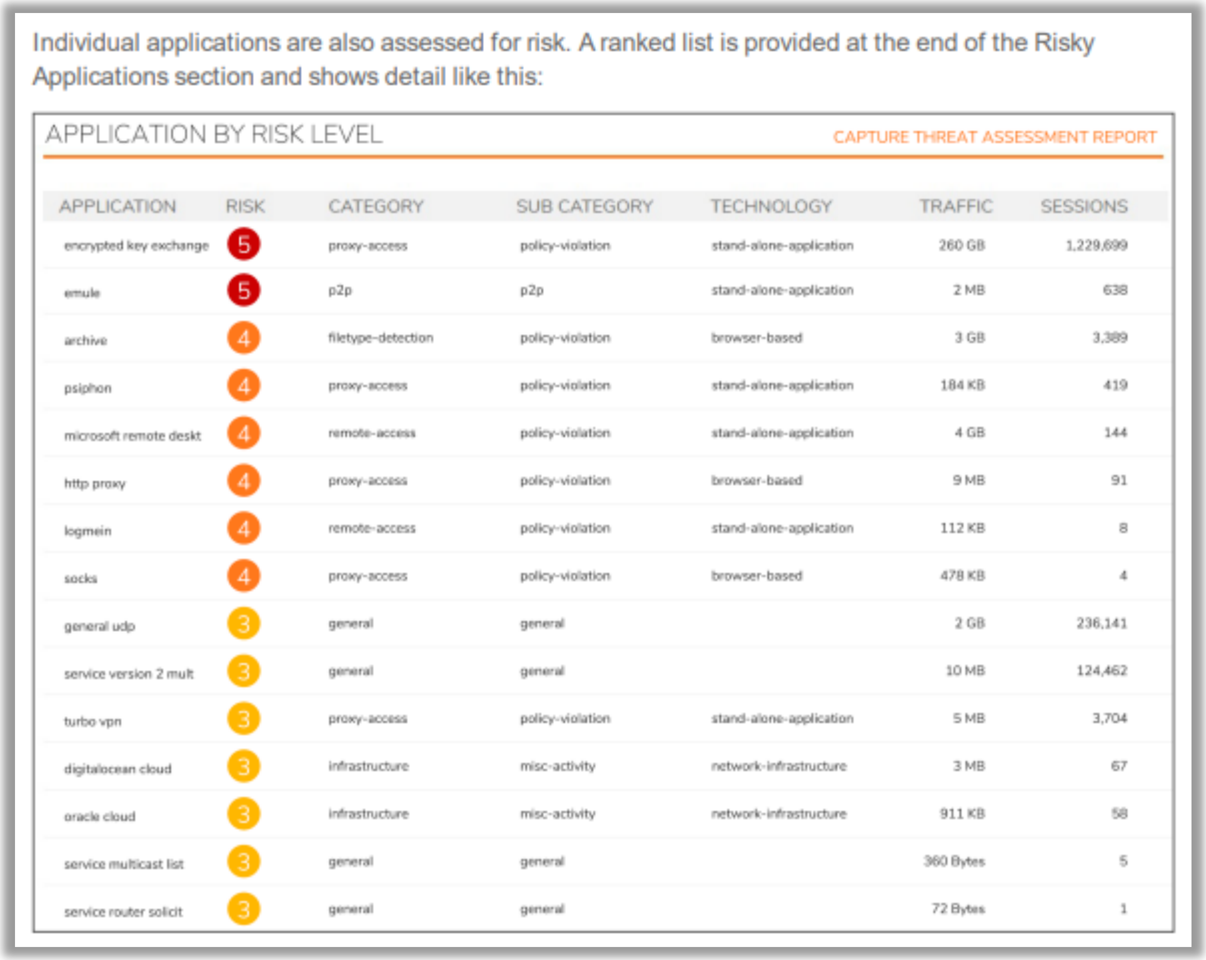
The most common types of application subcategories used within your organization are policy-violation, not-suspicious, general

The application subcategories consuming the most bandwidth are policy-violation, not-suspicious, multimedia



The top Risky Applications categories are individually graphed and grouped on a page so you can see the detail associated with them. For example, the graph for the Top Policy Violation Apps is shown below.

At the top of the graph, you can see how much bandwidth is being consumed by this category of Risky Applications. To the right of the bandwidth, the total number of application variants in your own network is compared to the industry average. The bar chart below that shows the relative distribution of the bandwidth between the applications listed. Similar reports are shown for other top categories.

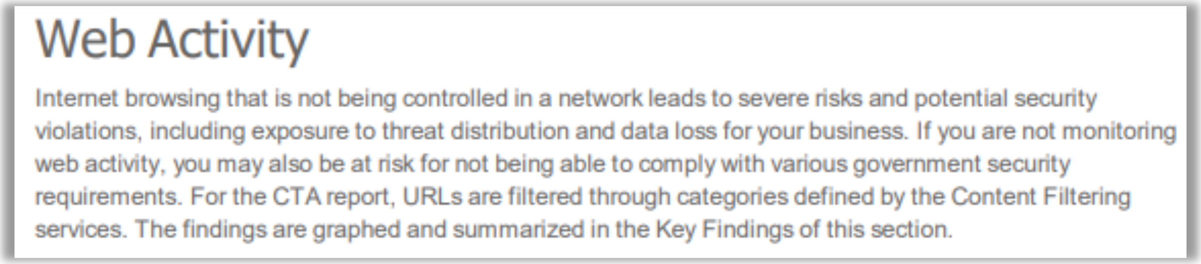


Individual applications are also assessed for risk. A ranked list is provided at the end of the Risky Applications section and shows detail like this:

APPLICATION BY RISK LEVEL

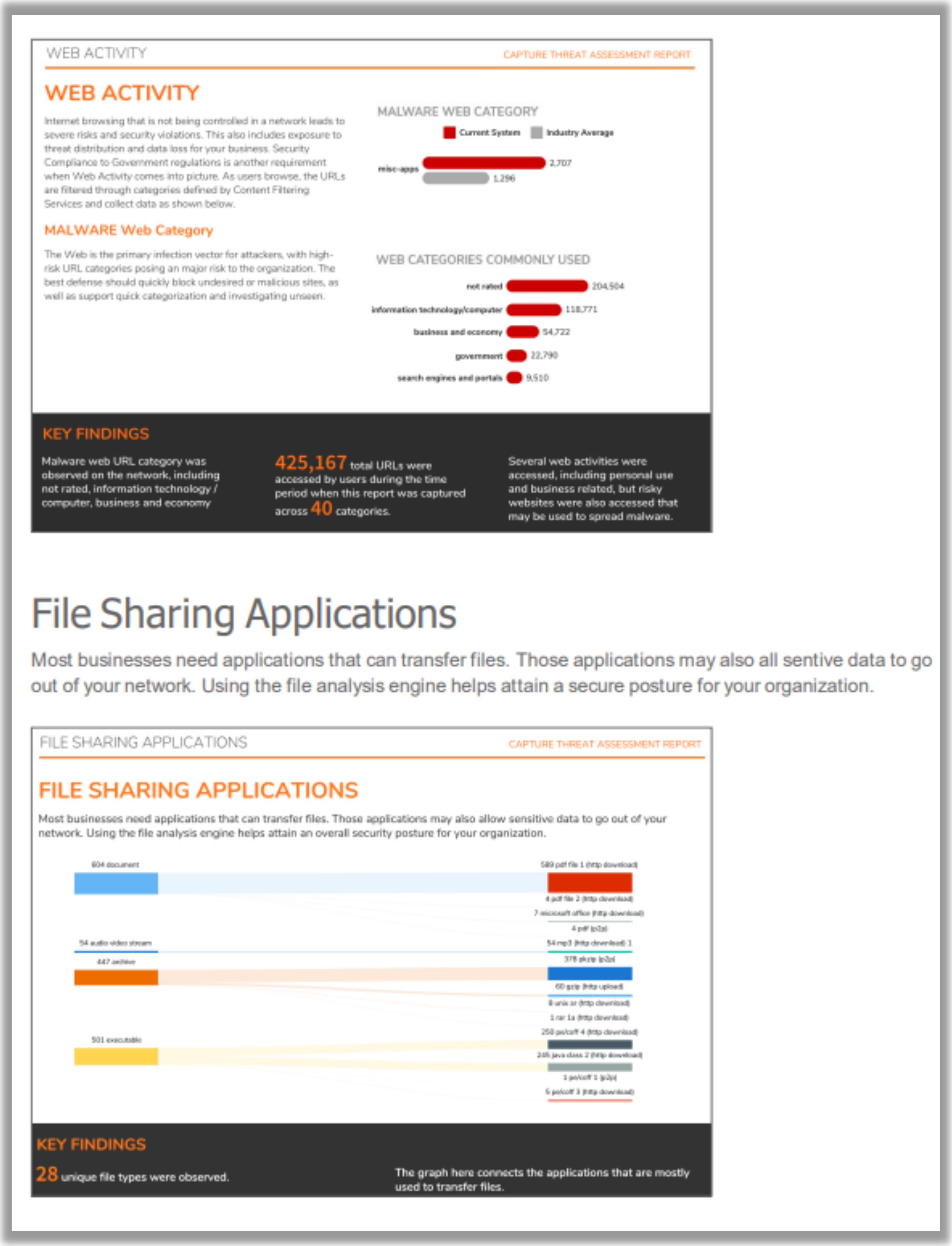
CAPTURE THREAT ASSESSMENT REPORT

APPLICATION	RISK	CATEGORY	SUB CATEGORY	TECHNOLOGY	TRAFFIC	SESSIONS
encrypted key exchange	5	proxy-access	policy-violation	stand-alone-application	260 GB	1,229,699
emule	5	p2p	p2p	stand-alone-application	2 MB	638
archive	4	filetype-detection	policy-violation	browser-based	3 GB	3,389
psiphon	4	proxy-access	policy-violation	stand-alone-application	184 KB	419
microsoft remote deskt	4	remote-access	policy-violation	stand-alone-application	4 GB	144
http proxy	4	proxy-access	policy-violation	browser-based	9 MB	91
logmein	4	remote-access	policy-violation	stand-alone-application	112 KB	8
socks	4	proxy-access	policy-violation	browser-based	478 KB	4
general udp	3	general	general		2 GB	236,141
service version 2 mult	3	general	general		10 MB	124,462
turbo vpn	3	proxy-access	policy-violation	stand-alone-application	5 MB	3,704
digitalocean cloud	3	infrastructure	misc-activity	network-infrastructure	3 MB	67
oracle cloud	3	infrastructure	misc-activity	network-infrastructure	911 KB	58
service multicast list	3	general	general		360 Bytes	5
service router solicit	3	general	general		72 Bytes	1



Web Activity

Internet browsing that is not being controlled in a network leads to severe risks and potential security violations, including exposure to threat distribution and data loss for your business. If you are not monitoring web activity, you may also be at risk for not being able to comply with various government security requirements. For the CTA report, URLs are filtered through categories defined by the Content Filtering services. The findings are graphed and summarized in the Key Findings of this section.



WEB ACTIVITY

CAPTURE THREAT ASSESSMENT REPORT

WEB ACTIVITY

Internet browsing that is not being controlled in a network leads to severe risks and security violations. This also includes exposure to threat distribution and data loss for your business. Security Compliance to Government regulations is another requirement when Web Activity comes into picture. As users browse, the URLs are filtered through categories defined by Content Filtering Services and collect data as shown below.

MALWARE Web Category

The Web is the primary infection vector for attackers, with high-risk URL categories posing an major risk to the organization. The best defense should quickly block undesired or malicious sites, as well as support quick categorization and investigating unseen.

KEY FINDINGS

Malware web URL category was observed on the network, including not rated, information technology / computer, business and economy

425,167 total URLs were accessed by users during the time period when this report was captured across 40 categories.

Several web activities were accessed, including personal use and business related, but risky websites were also accessed that may be used to spread malware.

File Sharing Applications

Most businesses need applications that can transfer files. Those applications may also all sentive data to go out of your network. Using the file analysis engine helps attain a secure posture for your organization.

FILE SHARING APPLICATIONS

CAPTURE THREAT ASSESSMENT REPORT

FILE SHARING APPLICATIONS

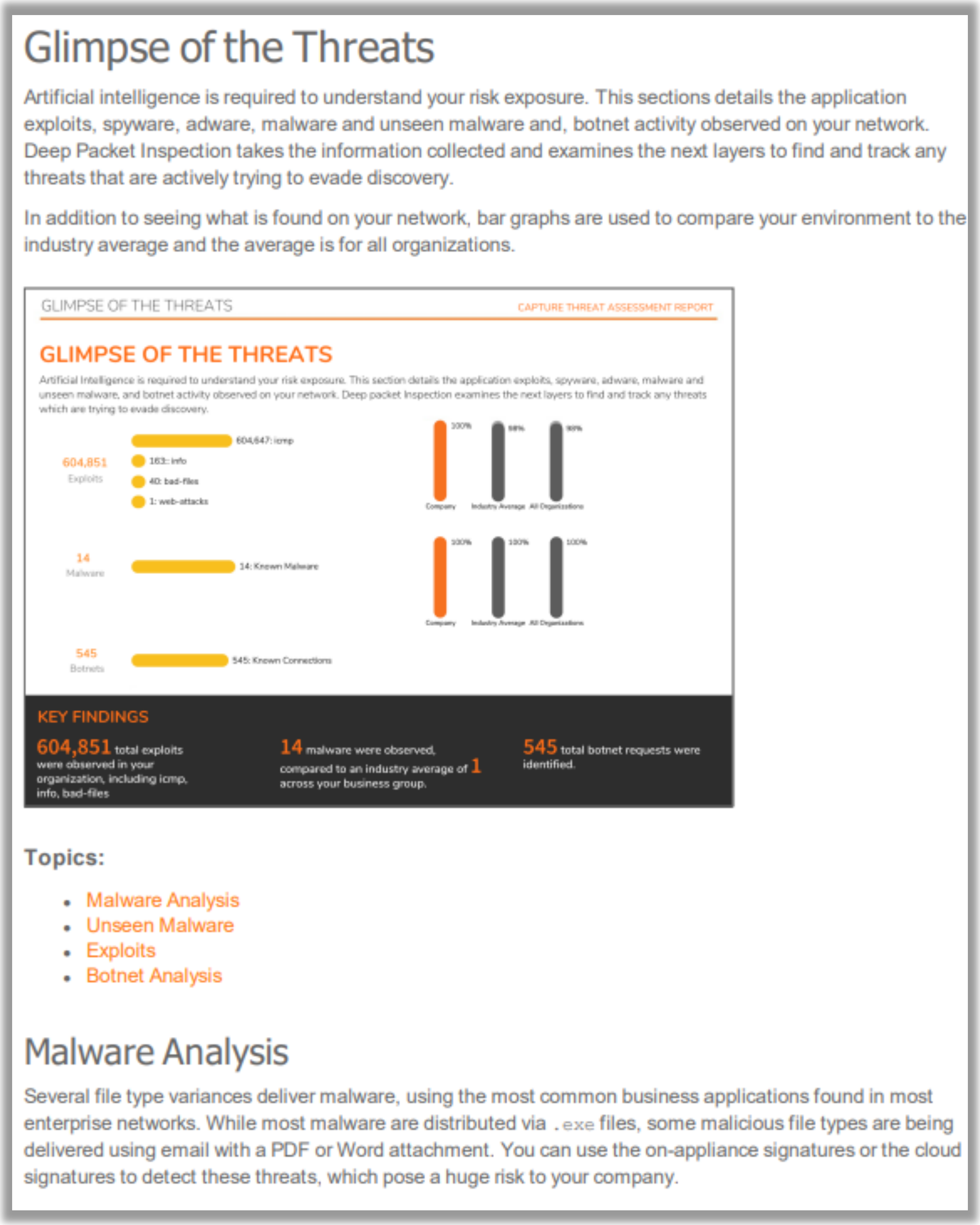
Most businesses need applications that can transfer files. Those applications may also allow sensitive data to go out of your network. Using the file analysis engine helps attain an overall security posture for your organization.

604 document
54 audio video stream
447 archive
501 executable
589 pdf file 1 (http download)
4 pdf file 2 (http download)
7 microsoft office (http download)
4 pdf (p2p)
54 mp3 (http download) 1
378 pkzip (p2p)
60 gzip (http upload)
8 unix ar (http download)
1 rar 1a (http download)
258 pe/coff 4 (http download)
245 java class 2 (http download)
1 pe/coff 1 (p2p)
5 pe/coff 3 (http download)

KEY FINDINGS

28 unique file types were observed.

The graph here connects the applications that are mostly used to transfer files.



Glimpse of the Threats

Artificial intelligence is required to understand your risk exposure. This sections details the application exploits, spyware, adware, malware and unseen malware and, botnet activity observed on your network. Deep Packet Inspection takes the information collected and examines the next layers to find and track any threats that are actively trying to evade discovery.

In addition to seeing what is found on your network, bar graphs are used to compare your environment to the industry average and the average is for all organizations.

GLIMPSE OF THE THREATS

CAPTURE THREAT ASSESSMENT REPORT

GLIMPSE OF THE THREATS

Artificial Intelligence is required to understand your risk exposure. This section details the application exploits, spyware, adware, malware and unseen malware, and botnet activity observed on your network. Deep packet Inspection examines the next layers to find and track any threats which are trying to evade discovery.

KEY FINDINGS

604,851 total exploits were observed in your organization, including icmp, info, bad-files

14 malware were observed, compared to an industry average of 1 across your business group.

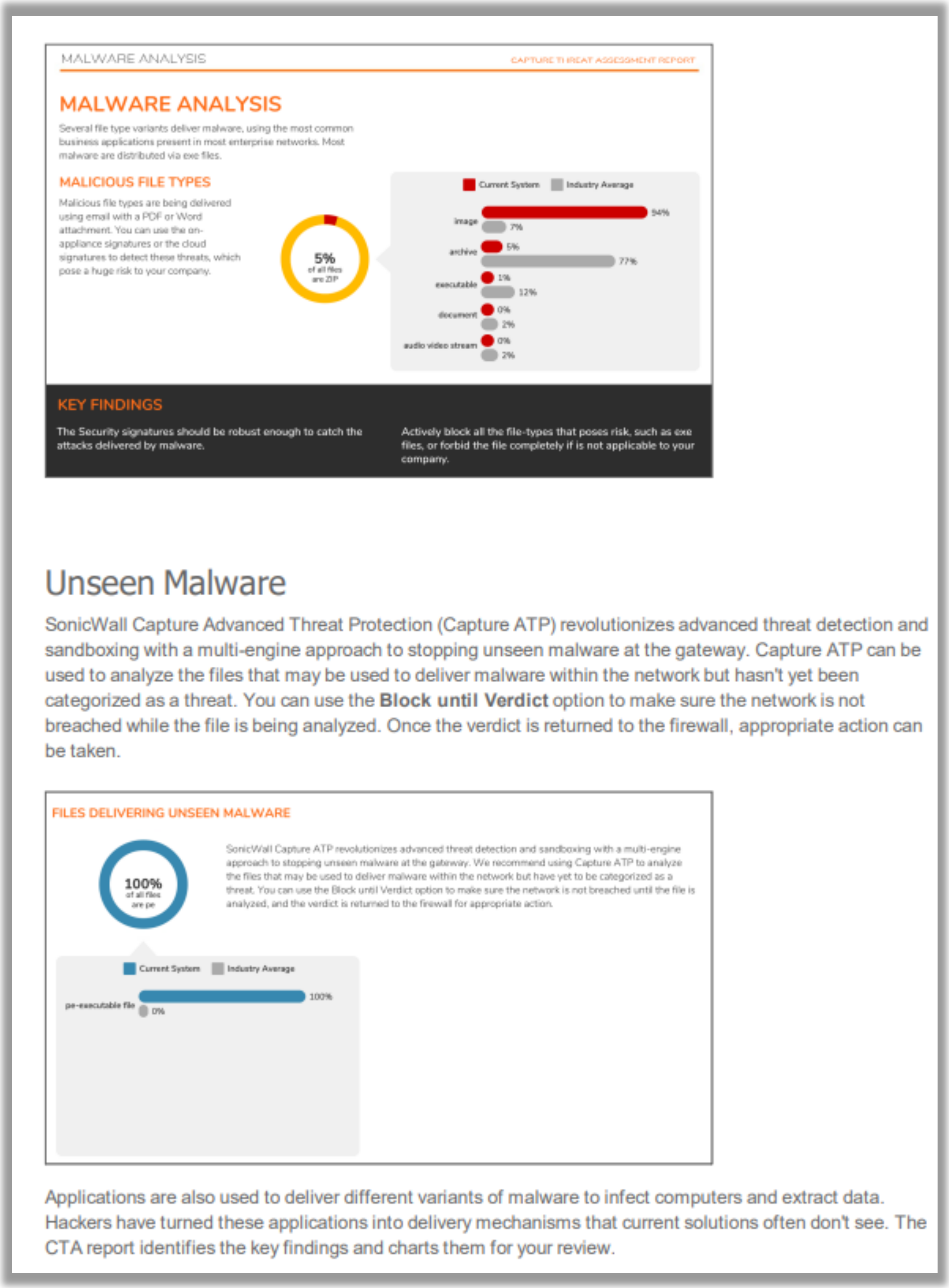
545 total botnet requests were identified.

Topics:

- Malware Analysis
- Unseen Malware
- Exploits
- Botnet Analysis

Malware Analysis

Several file type variances deliver malware, using the most common business applications found in most enterprise networks. While most malware are distributed via `.exe` files, some malicious file types are being delivered using email with a PDF or Word attachment. You can use the on-appliance signatures or the cloud signatures to detect these threats, which pose a huge risk to your company.



MALWARE ANALYSIS — CAPTURE THREAT ASSESSMENT REPORT

MALWARE ANALYSIS

Several file type variants deliver malware, using the most common business applications present in most enterprise networks. Most malware are distributed via exe files.

MALICIOUS FILE TYPES

Malicious file types are being delivered using email with a PDF or Word attachment. You can use the on-appliance signatures or the cloud signatures to detect these threats, which pose a huge risk to your company.

KEY FINDINGS

The Security signatures should be robust enough to catch the attacks delivered by malware.

Actively block all the file-types that poses risk, such as exe files, or forbid the file completely if is not applicable to your company.

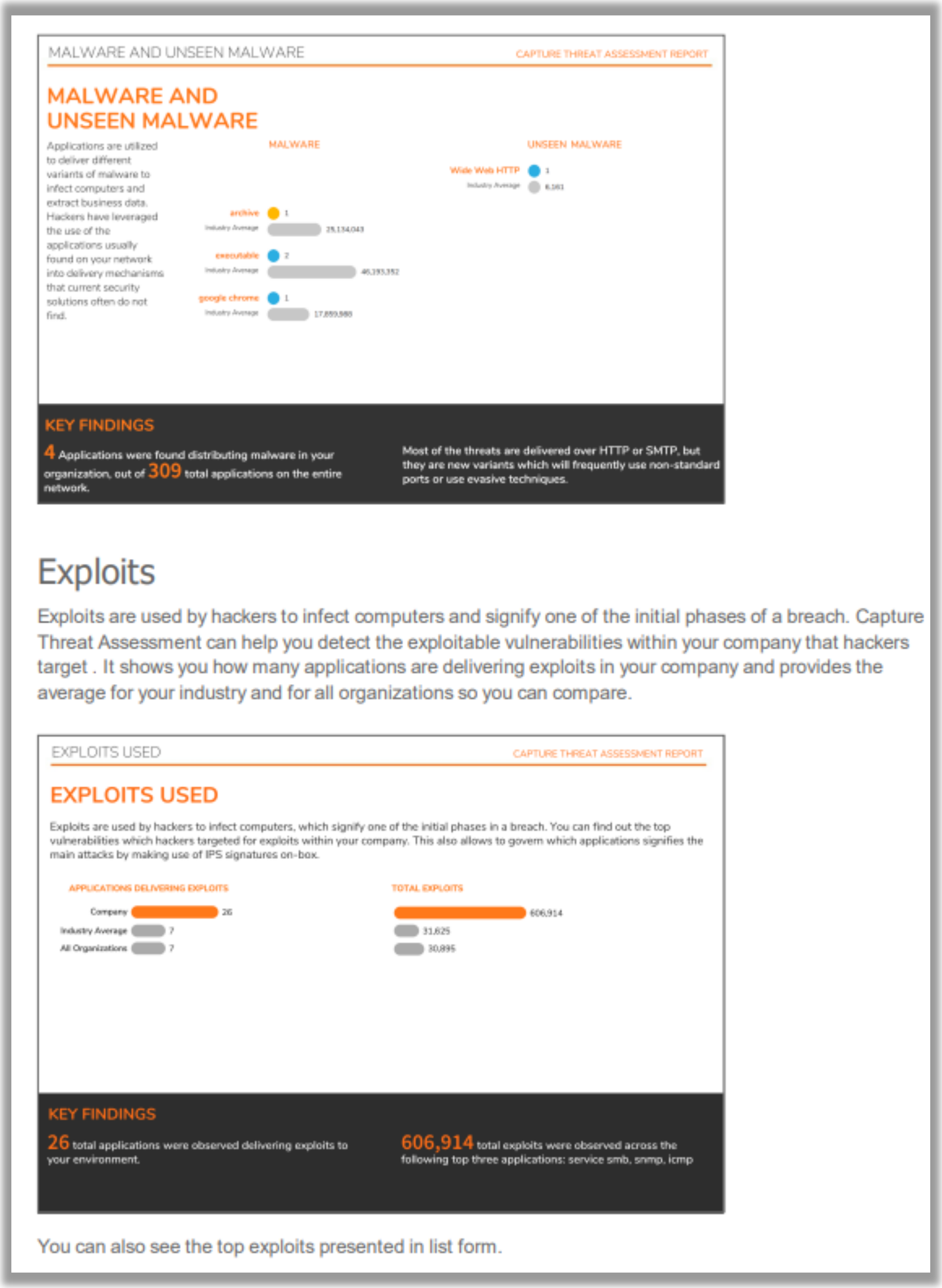
Unseen Malware

SonicWall Capture Advanced Threat Protection (Capture ATP) revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. Capture ATP can be used to analyze the files that may be used to deliver malware within the network but hasn't yet been categorized as a threat. You can use the **Block until Verdict** option to make sure the network is not breached while the file is being analyzed. Once the verdict is returned to the firewall, appropriate action can be taken.

FILES DELIVERING UNSEEN MALWARE

SonicWall Capture ATP revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. We recommend using Capture ATP to analyze the files that may be used to deliver malware within the network but have yet to be categorized as a threat. You can use the Block until Verdict option to make sure the network is not breached until the file is analyzed, and the verdict is returned to the firewall for appropriate action.

Applications are also used to deliver different variants of malware to infect computers and extract data. Hackers have turned these applications into delivery mechanisms that current solutions often don't see. The CTA report identifies the key findings and charts them for your review.



MALWARE AND UNSEEN MALWARE

CAPTURE THREAT ASSESSMENT REPORT

MALWARE AND UNSEEN MALWARE

Applications are utilized to deliver different variants of malware to infect computers and extract business data. Hackers have leveraged the use of the applications usually found on your network into delivery mechanisms that current security solutions often do not find.

MALWARE

archive ● 1
Industry Average 25,134,043
executable ● 2
Industry Average 46,193,352
google chrome ● 1
Industry Average 17,859,988

UNSEEN MALWARE

Wide Web HTTP ● 1
Industry Average ● 6,161

KEY FINDINGS

4 Applications were found distributing malware in your organization, out of 309 total applications on the entire network.

Most of the threats are delivered over HTTP or SMTP, but they are new variants which will frequently use non-standard ports or use evasive techniques.

Exploits

Exploits are used by hackers to infect computers and signify one of the initial phases of a breach. Capture Threat Assessment can help you detect the exploitable vulnerabilities within your company that hackers target . It shows you how many applications are delivering exploits in your company and provides the average for your industry and for all organizations so you can compare.

EXPLOITS USED

CAPTURE THREAT ASSESSMENT REPORT

EXPLOITS USED

Exploits are used by hackers to infect computers, which signify one of the initial phases in a breach. You can find out the top vulnerabilities which hackers targeted for exploits within your company. This also allows to govern which applications signifies the main attacks by making use of IPS signatures on-box.

APPLICATIONS DELIVERING EXPLOITS

Company 26
Industry Average 7
All Organizations 7

TOTAL EXPLOITS

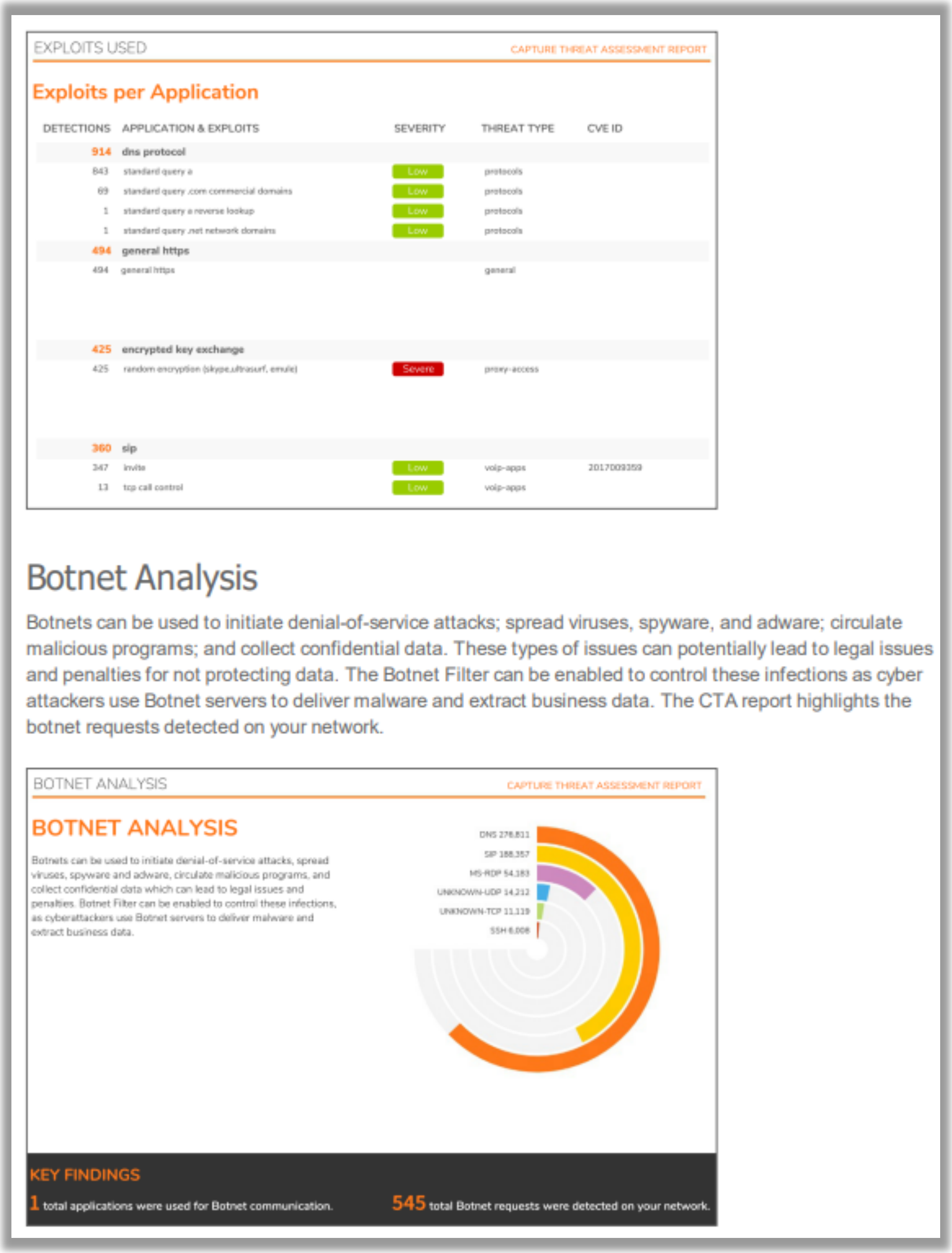
606,914
31,625
30,895

KEY FINDINGS

26 total applications were observed delivering exploits to your environment.

606,914 total exploits were observed across the following top three applications: service smb, snmp, icmp

You can also see the top exploits presented in list form.



EXPLOITS USED

CAPTURE THREAT ASSESSMENT REPORT

Exploits per Application

DETECTIONS	APPLICATION & EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
914	**dns protocol**			
843	standard query a	Low	protocols	
69	standard query .com commercial domains	Low	protocols	
1	standard query a reverse lookup	Low	protocols	
1	standard query .net network domains	Low	protocols	
494	**general https**			
494	general https		general	
425	**encrypted key exchange**			
425	random encryption (skype,ultrasurf, emule)	Severe	proxy-access	
360	**sip**			
347	invite	Low	voip-apps	2017009359
13	tcp call control	Low	voip-apps	

Botnet Analysis

Botnets can be used to initiate denial-of-service attacks; spread viruses, spyware, and adware; circulate malicious programs; and collect confidential data. These types of issues can potentially lead to legal issues and penalties for not protecting data. The Botnet Filter can be enabled to control these infections as cyber attackers use Botnet servers to deliver malware and extract business data. The CTA report highlights the botnet requests detected on your network.

BOTNET ANALYSIS

CAPTURE THREAT ASSESSMENT REPORT

BOTNET ANALYSIS

Botnets can be used to initiate denial-of-service attacks, spread viruses, spyware and adware, circulate malicious programs, and collect confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections, as cyberattackers use Botnet servers to deliver malware and extract business data.

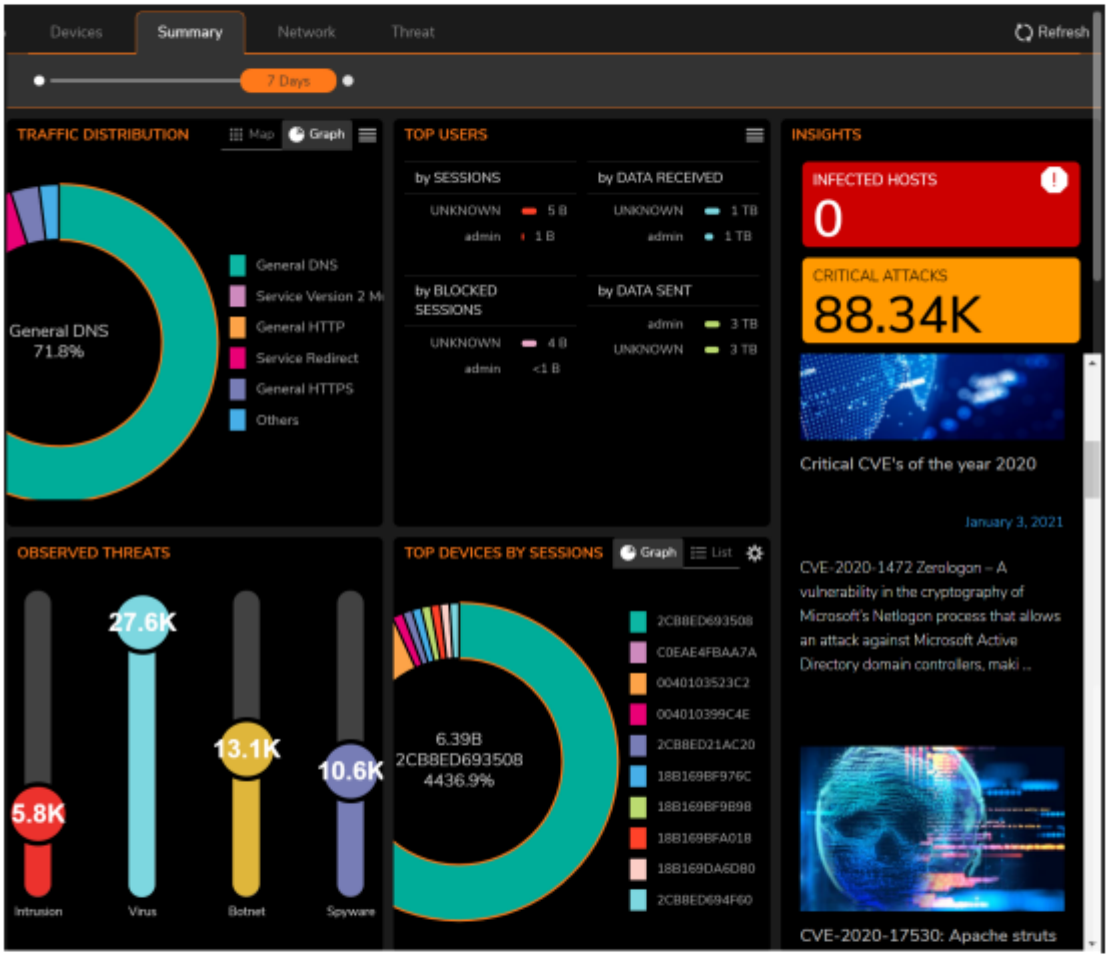
KEY FINDINGS

1 total applications were used for Botnet communication.

545 total Botnet requests were detected on your network.

[94]

[94] https://www.sonicwall.com/techdocs/pdf/cta-user_guide.pdf, at 5-16.



by SESSIONS		by DATA RECEIVED	
UNKNOWN	5 B	UNKNOWN	1 TB
admin	1 B	admin	1 TB

by BLOCKED SESSIONS		by DATA SENT	
UNKNOWN	4 B	admin	3 TB
admin	<1 B	UNKNOWN	3 TB

Critical CVE's of the year 2020

January 3, 2021

CVE-2020-1472 Zerologon – A vulnerability in the cryptography of Microsoft's Netlogon process that allows an attack against Microsoft Active Directory domain controllers, maki ...

CVE-2020-17530: Apache struts

- **TRAFFIC DISTRIBUTION**: Shows the graphical representation of the percent distribution of the number of network sessions based on protocol.
- **TOP USERS**: Shows the top users by the number of sessions, amount of data received, amount of data sent, and the number of blocked connections.
- **OBSERVED THREATS**: Shows the different types of threats and the number of threats of each threat type across managed devices.
- **TOP DEVICES BY SESSIONS**: Shows the list of devices that are sorted in descending order of the category you select. Click the **Gear** icon to select your desired category; the default selection is **Sessions**.

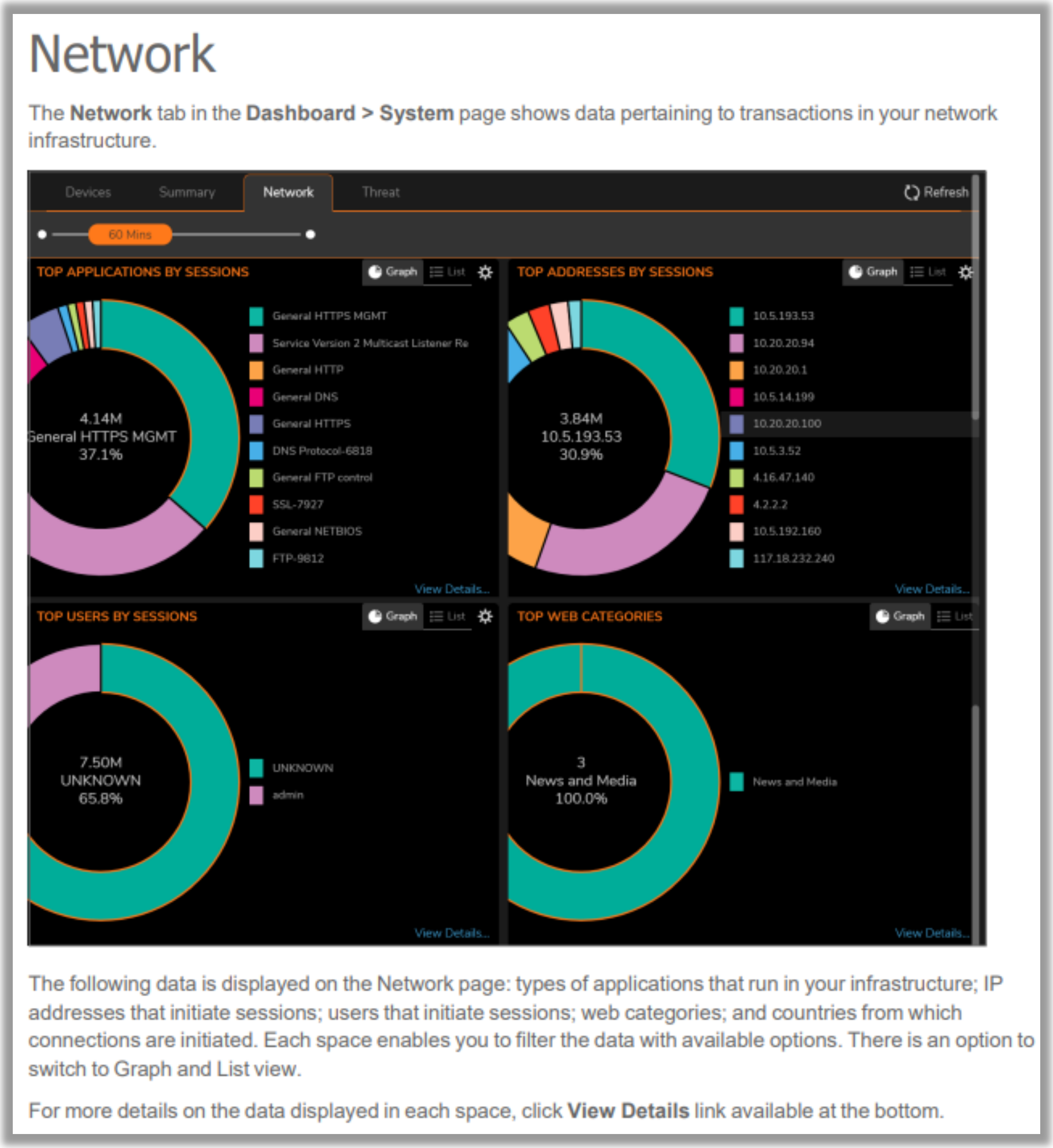
The **Insights** section (scroll to the right if it's not visible) gives information about number of infected hosts and the number of critical attacks.

[95]

102. Every '948 Accused Product practices generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event

[95] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 14.

correlation matrix, a risk correlation matrix, and a trust supervisor. For example, Network Security Manager includes a network analyzer which "shows data pertaining to transactions in your network infrastructure," as shown below.



Network

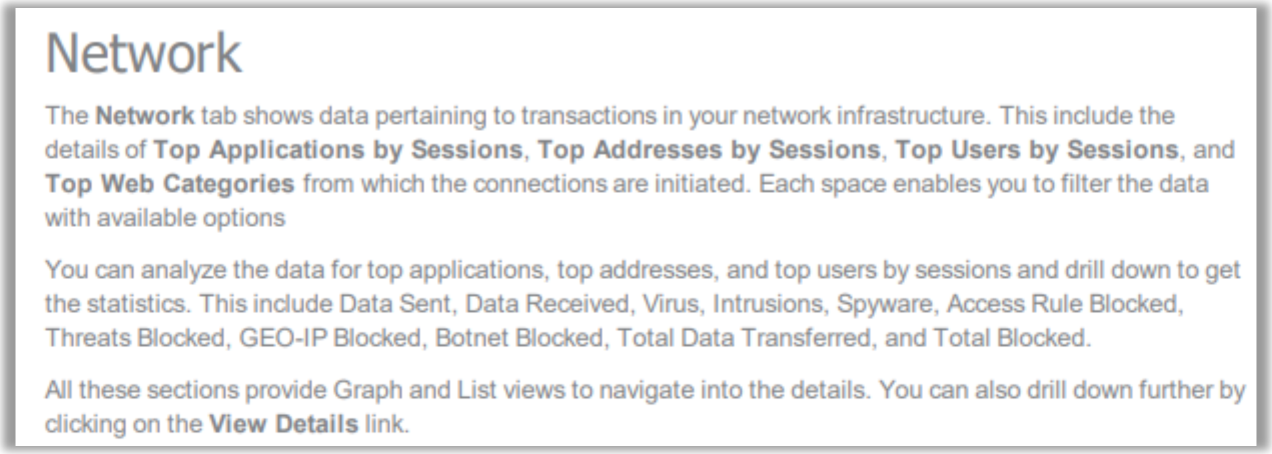
The **Network** tab in the **Dashboard > System** page shows data pertaining to transactions in your network infrastructure.

The following data is displayed on the Network page: types of applications that run in your infrastructure; IP addresses that initiate sessions; users that initiate sessions; web categories; and countries from which connections are initiated. Each space enables you to filter the data with available options. There is an option to switch to Graph and List view.

For more details on the data displayed in each space, click **View Details** link available at the bottom.

[96]

[96] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 15.



Network

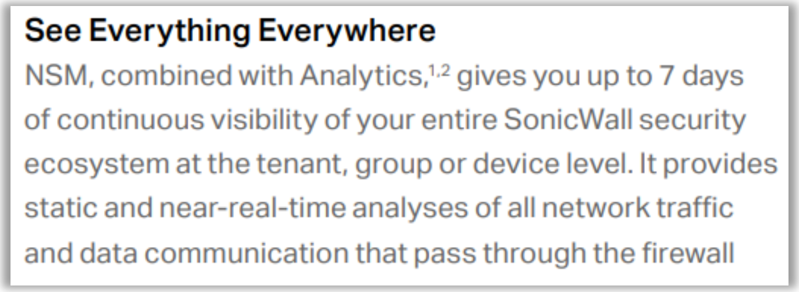
The **Network** tab shows data pertaining to transactions in your network infrastructure. This include the details of **Top Applications by Sessions**, **Top Addresses by Sessions**, **Top Users by Sessions**, and **Top Web Categories** from which the connections are initiated. Each space enables you to filter the data with available options

You can analyze the data for top applications, top addresses, and top users by sessions and drill down to get the statistics. This include Data Sent, Data Received, Virus, Intrusions, Spyware, Access Rule Blocked, Threats Blocked, GEO-IP Blocked, Botnet Blocked, Total Data Transferred, and Total Blocked.

All these sections provide Graph and List views to navigate into the details. You can also drill down further by clicking on the **View Details** link.

[97]

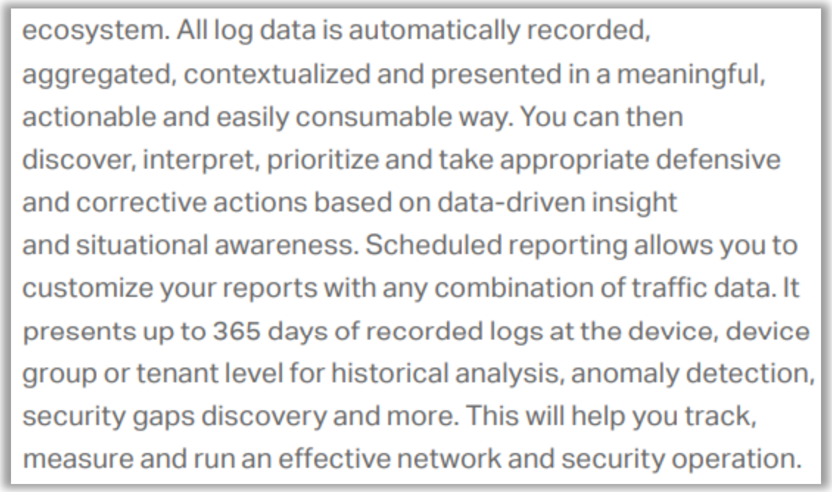
103. For example, Network Security Manager includes an event correlation matrix which "provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way," as shown below. Network Security Manager also includes an integrity processor that allows for "scheduled reporting" including "historical analysis, anomaly detection, security gaps discovery and more."



See Everything Everywhere

NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall

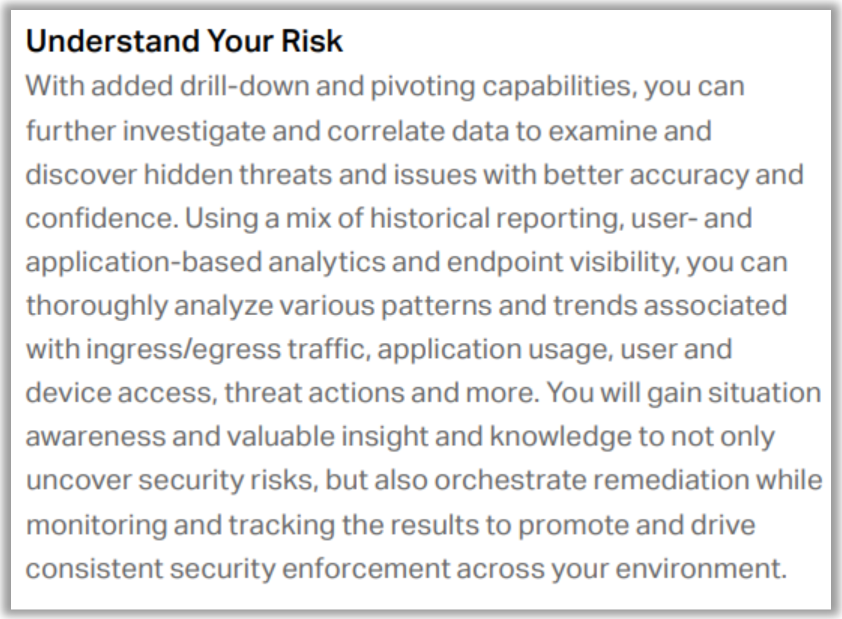
[97] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 18.



ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way. You can then discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more. This will help you track, measure and run an effective network and security operation.[98]

104. For example, Network Security Manager includes a risk correlation matrix which "correlate[s] data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions and more," as shown below. Network Security Manager also includes a trust supervisor that "orchestrate[s] remediation while monitoring and tracking the results...[for] consistent security enforcement."

[98] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

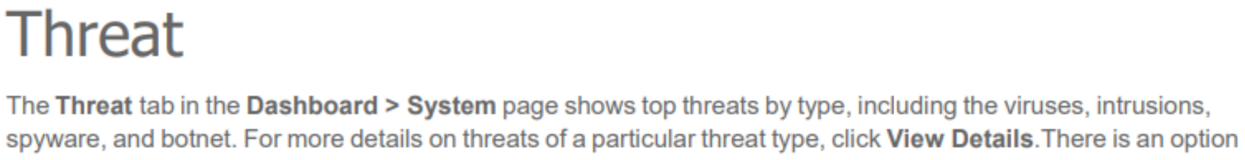


Understand Your Risk

With added drill-down and pivoting capabilities, you can further investigate and correlate data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions and more. You will gain situation awareness and valuable insight and knowledge to not only uncover security risks, but also orchestrate remediation while monitoring and tracking the results to promote and drive consistent security enforcement across your environment.

[99]

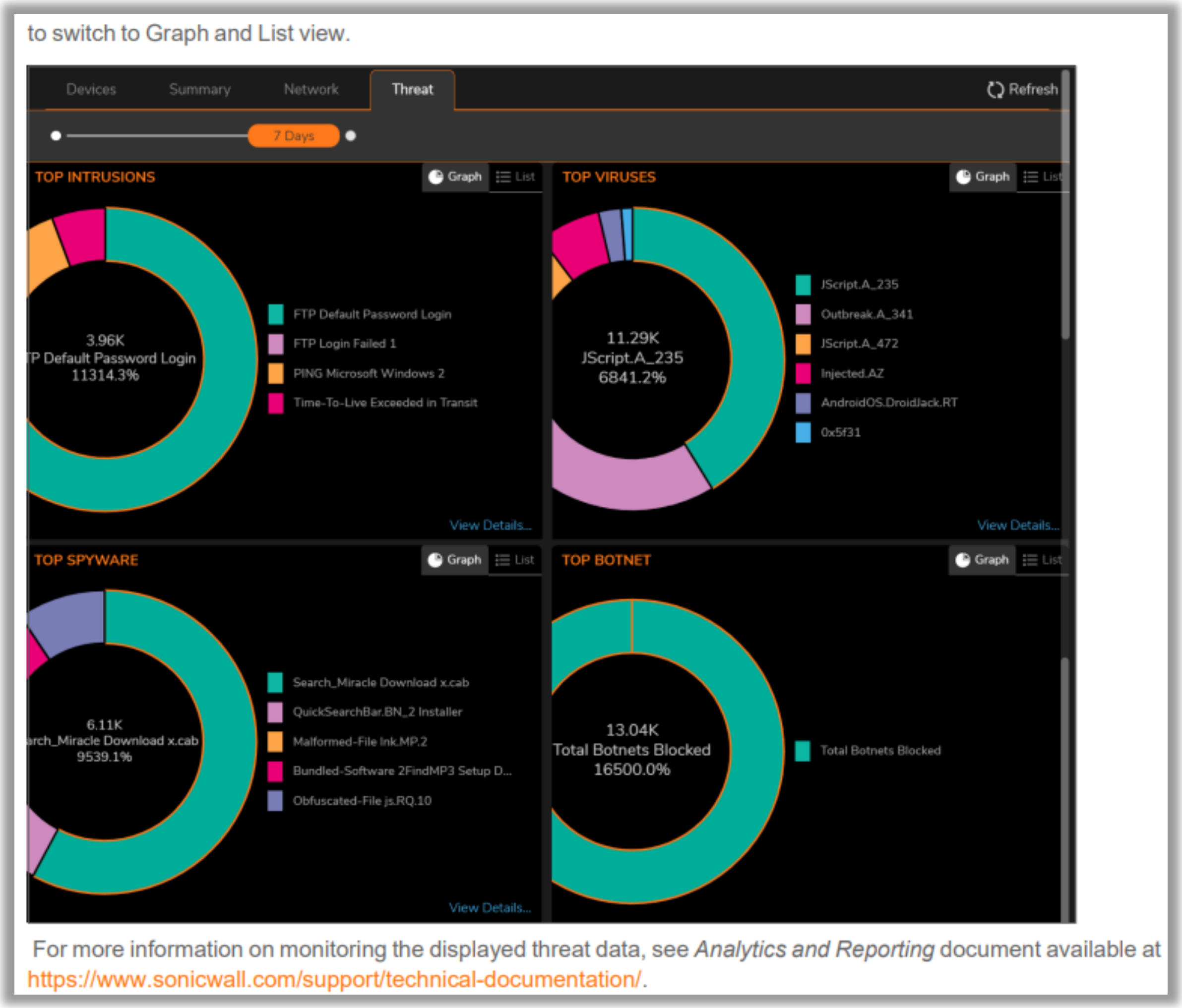
105. Every ’948 Accused Product practices correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events. For example, Network Security Manager correlate threat classifications based on the type, including the viruses, intrusions, spyware, and botnet, and view the details for each threat classification.



Threat

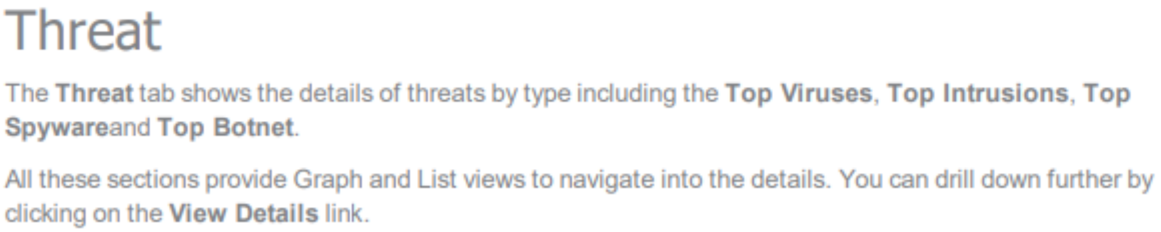
The **Threat** tab in the **Dashboard > System** page shows top threats by type, including the viruses, intrusions, spyware, and botnet. For more details on threats of a particular threat type, click **View Details**.There is an option

[99] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf


to switch to Graph and List view.

For more information on monitoring the displayed threat data, see *Analytics and Reporting* document available at https://www.sonicwall.com/support/technical-documentation/.

[100]


Threat

The **Threat** tab shows the details of threats by type including the **Top Viruses**, **Top Intrusions**, **Top Spyware**and **Top Botnet**.

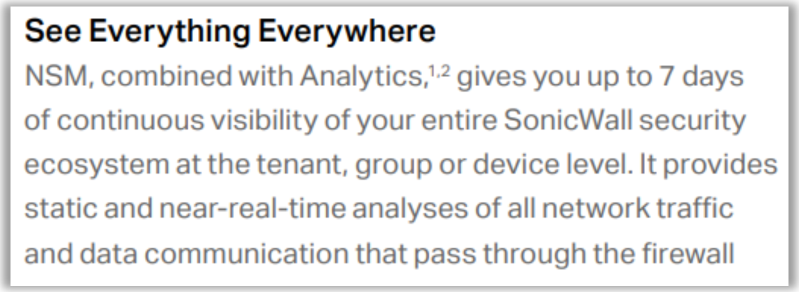
All these sections provide Graph and List views to navigate into the details. You can drill down further by clicking on the **View Details** link.

[101]

106. Every ’948 Accused Product practices displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application. For example, Network Security Manager displays real-

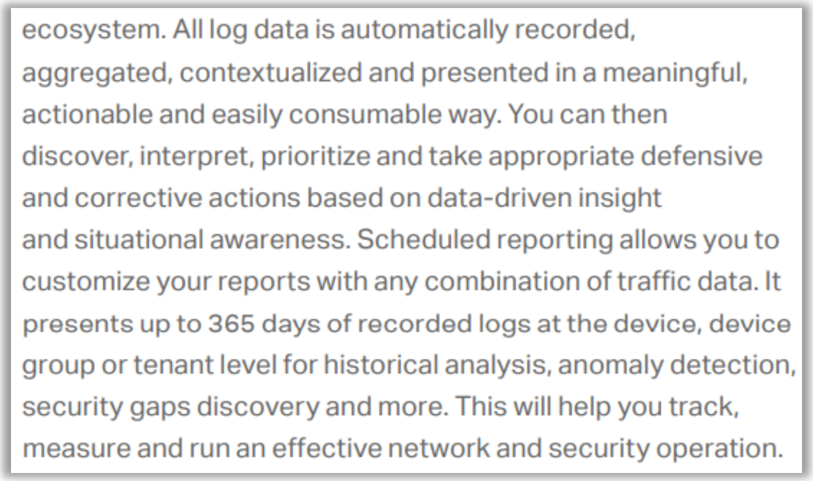
[100] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 15-16.
[101] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 18.

time status indications for the operational integrity of the application in many runtime dashboards, including at least RealTime Reports, Dashboard Reports, and Details Reports.

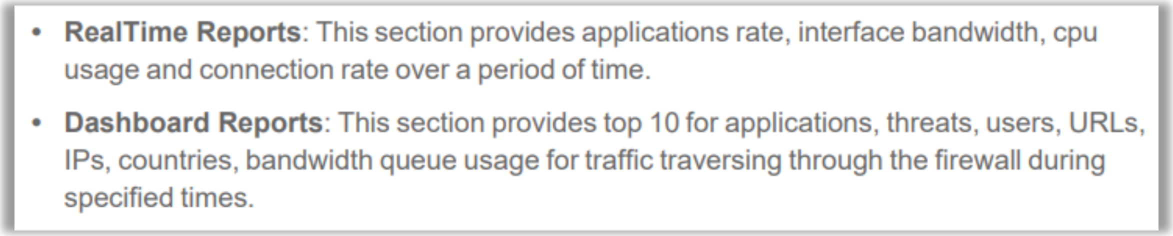


See Everything Everywhere

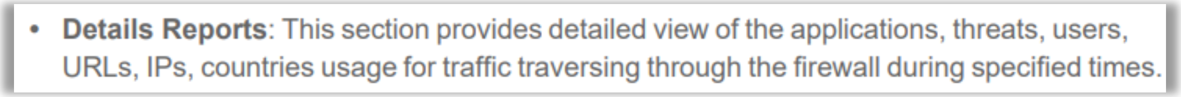
NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall



ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way. You can then discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more. This will help you track, measure and run an effective network and security operation. [102]



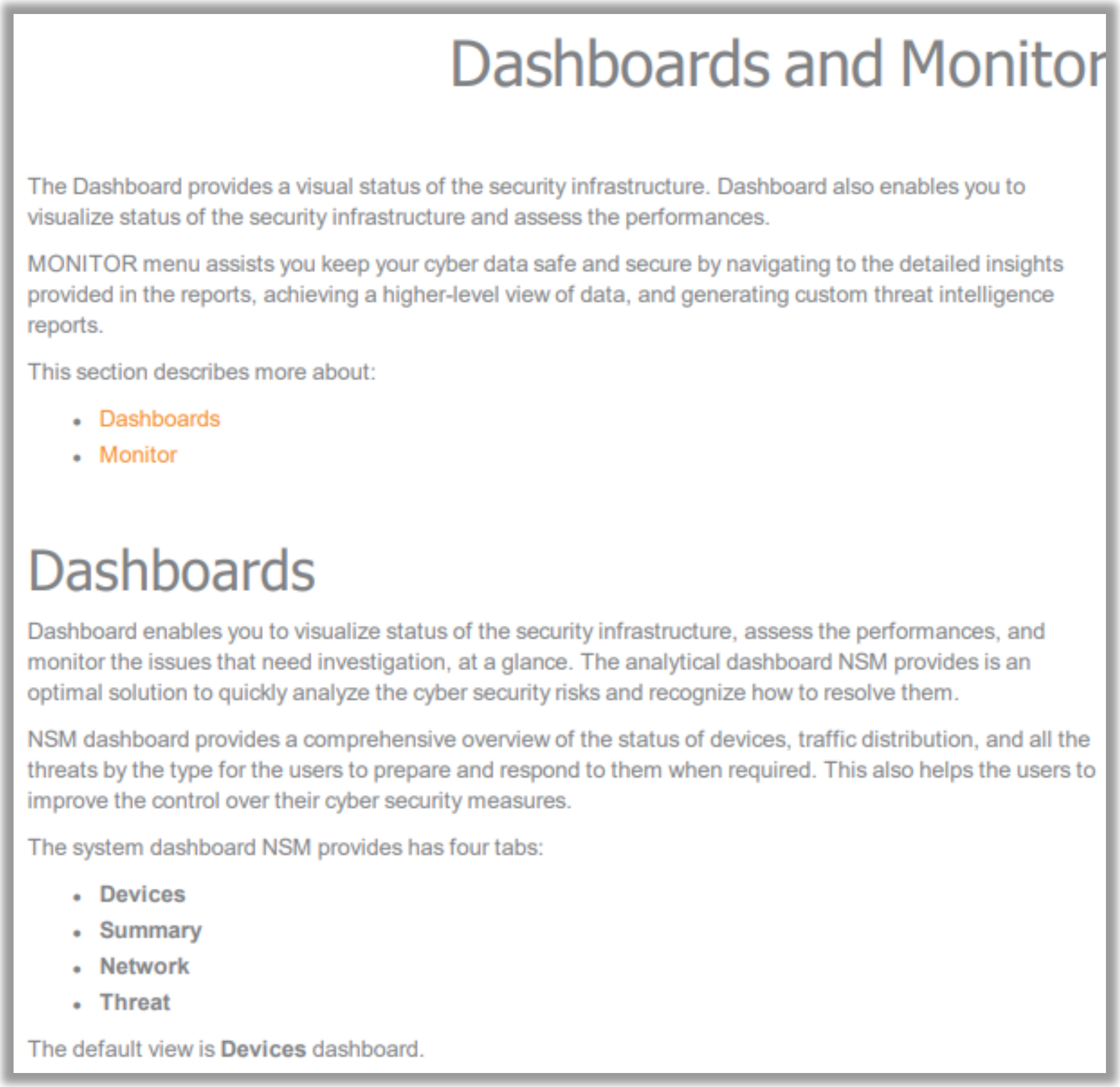
- **RealTime Reports**: This section provides applications rate, interface bandwidth, cpu usage and connection rate over a period of time.
- **Dashboard Reports**: This section provides top 10 for applications, threats, users, URLs, IPs, countries, bandwidth queue usage for traffic traversing through the firewall during specified times.



- **Details Reports**: This section provides detailed view of the applications, threats, users, URLs, IPs, countries usage for traffic traversing through the firewall during specified times. [103]

[102] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

[103] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 125-126.



Dashboards and Monitor

The Dashboard provides a visual status of the security infrastructure. Dashboard also enables you to visualize status of the security infrastructure and assess the performances.

MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports.

This section describes more about:

- Dashboards
- Monitor

Dashboards

Dashboard enables you to visualize status of the security infrastructure, assess the performances, and monitor the issues that need investigation, at a glance. The analytical dashboard NSM provides is an optimal solution to quickly analyze the cyber security risks and recognize how to resolve them.

NSM dashboard provides a comprehensive overview of the status of devices, traffic distribution, and all the threats by the type for the users to prepare and respond to them when required. This also helps the users to improve the control over their cyber security measures.

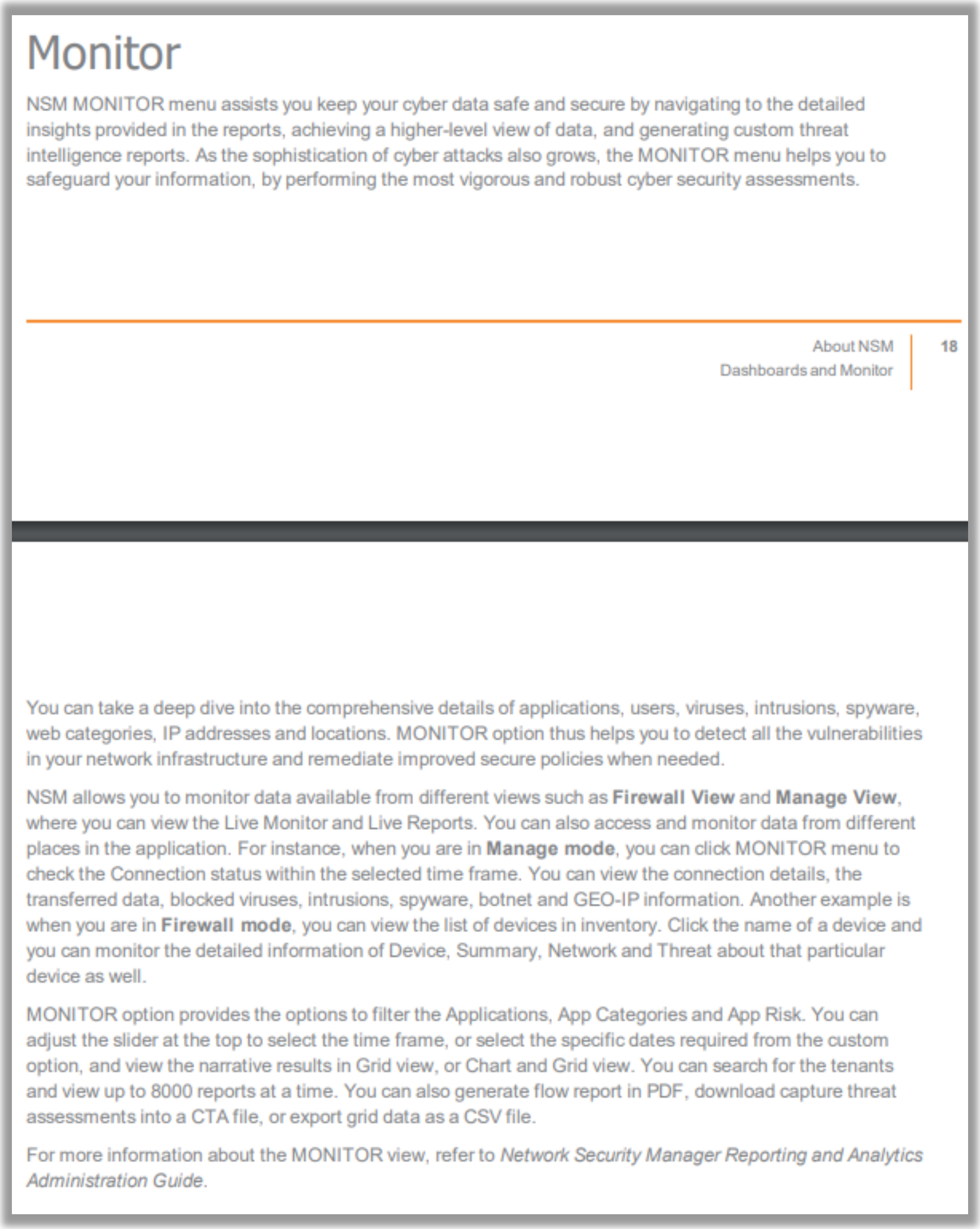
The system dashboard NSM provides has four tabs:

- **Devices**
- **Summary**
- **Network**
- **Threat**

The default view is **Devices** dashboard.

[104]

[104] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 16.



Monitor

NSM MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports. As the sophistication of cyber attacks also grows, the MONITOR menu helps you to safeguard your information, by performing the most vigorous and robust cyber security assessments.

About NSM
Dashboards and Monitor | 18

You can take a deep dive into the comprehensive details of applications, users, viruses, intrusions, spyware, web categories, IP addresses and locations. MONITOR option thus helps you to detect all the vulnerabilities in your network infrastructure and remediate improved secure policies when needed.

NSM allows you to monitor data available from different views such as **Firewall View** and **Manage View**, where you can view the Live Monitor and Live Reports. You can also access and monitor data from different places in the application. For instance, when you are in **Manage mode**, you can click MONITOR menu to check the Connection status within the selected time frame. You can view the connection details, the transferred data, blocked viruses, intrusions, spyware, botnet and GEO-IP information. Another example is when you are in **Firewall mode**, you can view the list of devices in inventory. Click the name of a device and you can monitor the detailed information of Device, Summary, Network and Threat about that particular device as well.

MONITOR option provides the options to filter the Applications, App Categories and App Risk. You can adjust the slider at the top to select the time frame, or select the specific dates required from the custom option, and view the narrative results in Grid view, or Chart and Grid view. You can search for the tenants and view up to 8000 reports at a time. You can also generate flow report in PDF, download capture threat assessments into a CTA file, or export grid data as a CSV file.

For more information about the MONITOR view, refer to *Network Security Manager Reporting and Analytics Administration Guide*.

[105]

107. Defendant has and continues to directly infringe one or more claims of the ’948 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using,

[105] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 18-19.

offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

108. Defendant has and continues to indirectly infringe one or more claims of the ’948 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’948 Accused Products.

109. Defendant has and continues to indirectly infringe one or more claims of the ’948 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’948 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’948 Patent by providing these products to customers and end-users for use in an infringing manner.

110. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’948 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing

manner, including at least though its SonicWall Technical Documentation,[106] Video Tutorials,[107] SonicWall University,[108] and Customer Service[109] websites.

111. Defendant has and continues to indirectly infringe one or more claims of the ’948 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’948 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’948 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’948 Patent but remained willfully blind to the infringing nature of others’ actions.

112. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’948 Patent in an amount to be proved at trial.

113. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’948 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

114. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe

[106] https://www.sonicwall.com/support/technical-documentation/?language=English
[107] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12
[108] https://www.sonicwall.com/partners/sonicwall-university/
[109] https://www.sonicwall.com/support/contact-support/customer-service/

the ’948 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’948 Patent. Upon information and belief, Defendant had actual knowledge of the ’948 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’948 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT VI
(Infringement of the ’616 Patent)

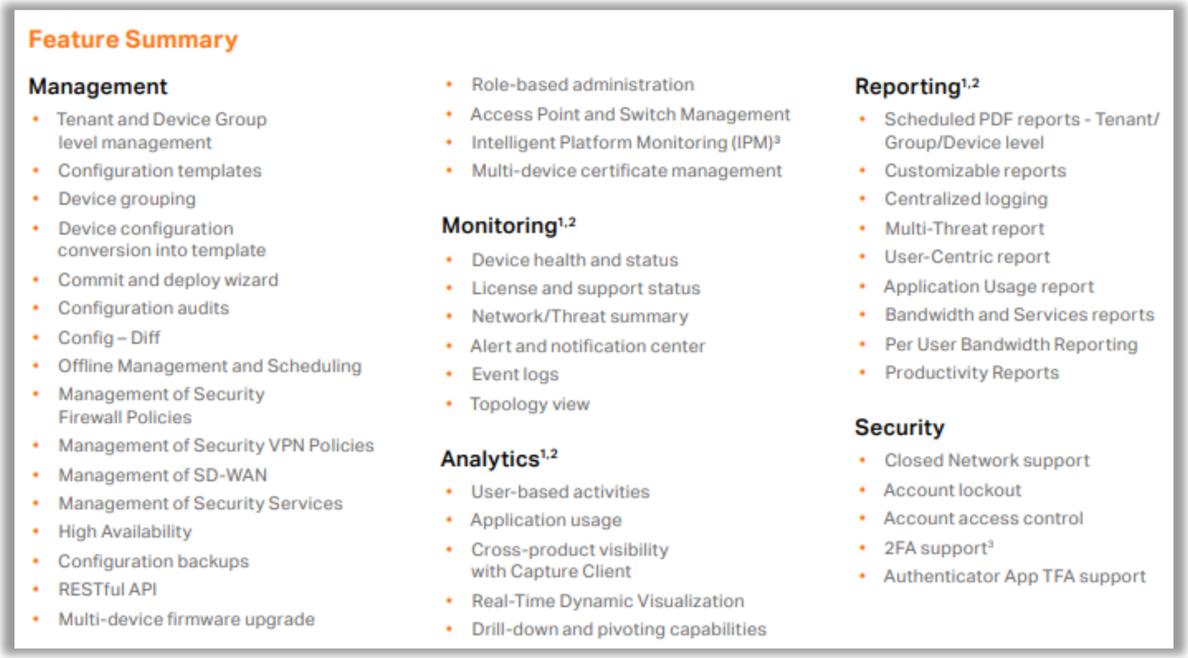
115. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

116. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’616 Patent.

117. Defendant has and continues to directly infringe the ’616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’616 Patent. Such products include at least SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp

12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) integrated with Network Security Manager or SonicWall Capture Client (the "'616 Accused Products") which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

118. Every '616 Accused Product practices a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. For example, SonicWall firewalls are network trust agents because they perform "network telemetry sharing" in order to "share[] network threat alerts." For further example, Capture Clients on endpoints are endpoint trust agents that "share[] user info, device info, and client version."



Feature Summary

Management

- Tenant and Device Group level management
- Configuration templates
- Device grouping
- Device configuration conversion into template
- Commit and deploy wizard
- Configuration audits
- Config – Diff
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of SD-WAN
- Management of Security Services
- High Availability
- Configuration backups
- RESTful API
- Multi-device firmware upgrade
- Role-based administration
- Access Point and Switch Management
- Intelligent Platform Monitoring (IPM)[3]
- Multi-device certificate management

Monitoring[1,2]

- Device health and status
- License and support status
- Network/Threat summary
- Alert and notification center
- Event logs
- Topology view

Analytics[1,2]

- User-based activities
- Application usage
- Cross-product visibility with Capture Client
- Real-Time Dynamic Visualization
- Drill-down and pivoting capabilities

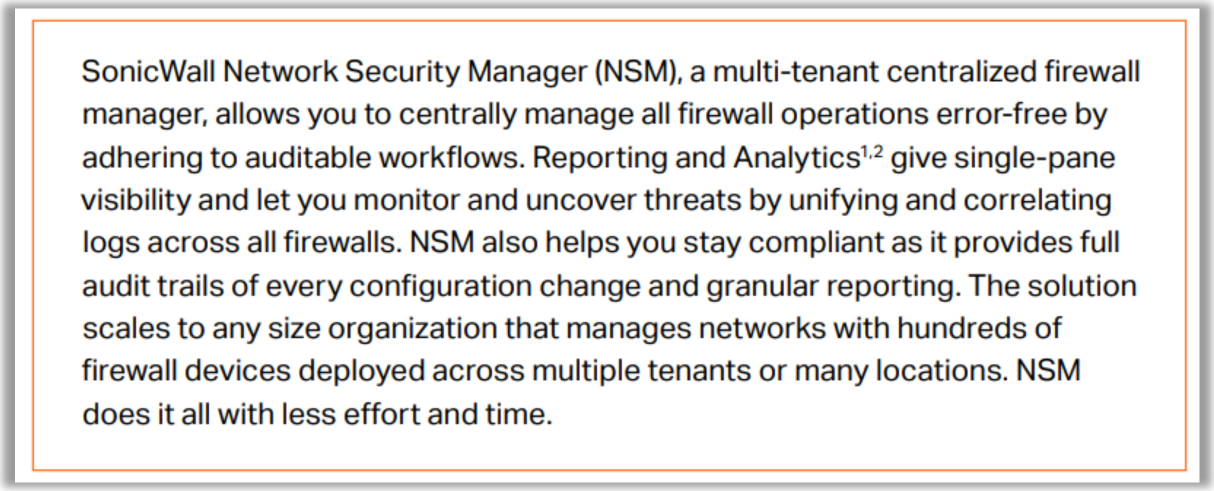
Reporting[1,2]

- Scheduled PDF reports - Tenant/Group/Device level
- Customizable reports
- Centralized logging
- Multi-Threat report
- User-Centric report
- Application Usage report
- Bandwidth and Services reports
- Per User Bandwidth Reporting
- Productivity Reports

Security

- Closed Network support
- Account lockout
- Account access control
- 2FA support[3]
- Authenticator App TFA support

[110]

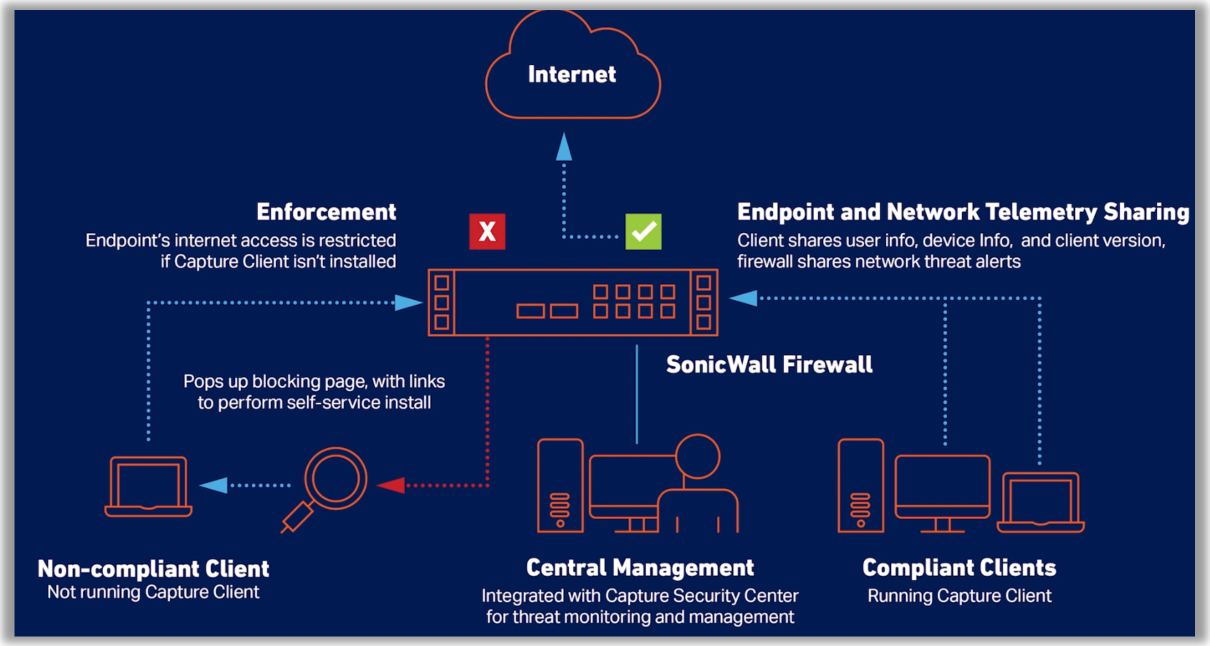


SonicWall Network Security Manager (NSM), a multi-tenant centralized firewall manager, allows you to centrally manage all firewall operations error-free by adhering to auditable workflows. Reporting and Analytics[1,2] give single-pane visibility and let you monitor and uncover threats by unifying and correlating logs across all firewalls. NSM also helps you stay compliant as it provides full audit trails of every configuration change and granular reporting. The solution scales to any size organization that manages networks with hundreds of firewall devices deployed across multiple tenants or many locations. NSM does it all with less effort and time.

[111]

[110] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

[111] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 2.



Internet

Enforcement
Endpoint's internet access is restricted
if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version,
firewall shares network threat alerts

SonicWall Firewall

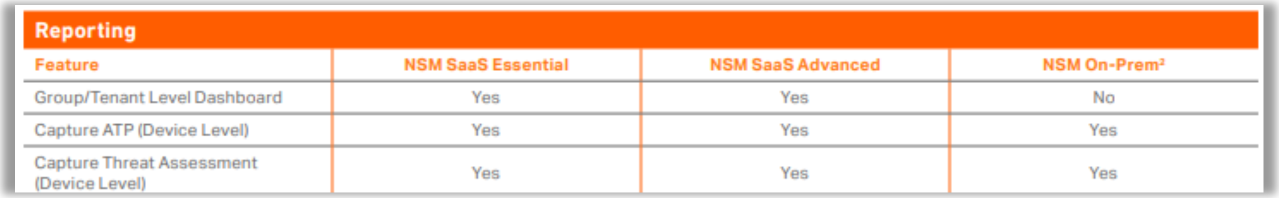
Pops up blocking page, with links
to perform self-service install

Non-compliant Client
Not running Capture Client

Central Management
Integrated with Capture Security Center
for threat monitoring and management

Compliant Clients
Running Capture Client

[112]



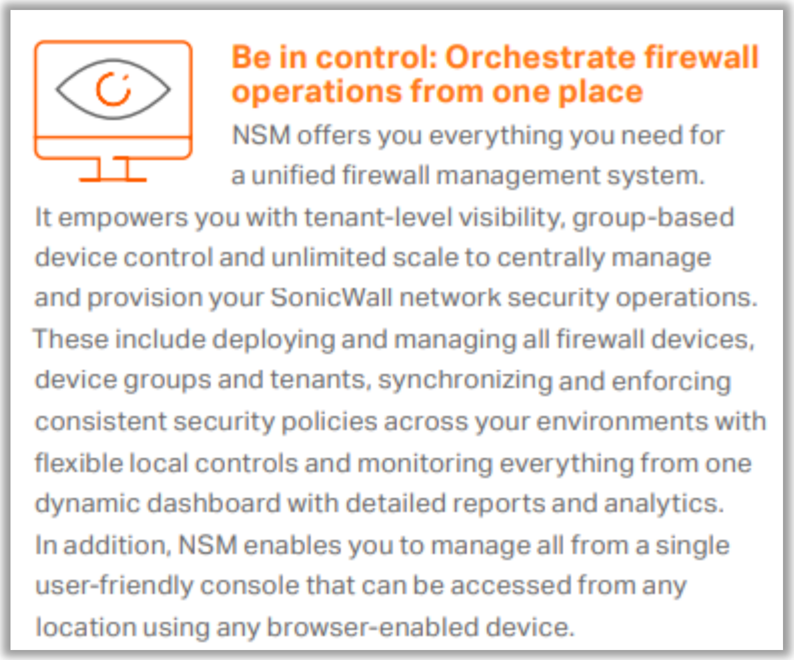
Reporting

Feature	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem²
Group/Tenant Level Dashboard	Yes	Yes	No
Capture ATP (Device Level)	Yes	Yes	Yes
Capture Threat Assessment (Device Level)	Yes	Yes	Yes

https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 6.

119. For further example, Network Security Manager includes a trust orchestrator server to "orchestrate firewall operations from one place" – "a single user-friendly console that can be accessed from any location using any browser-enabled device.

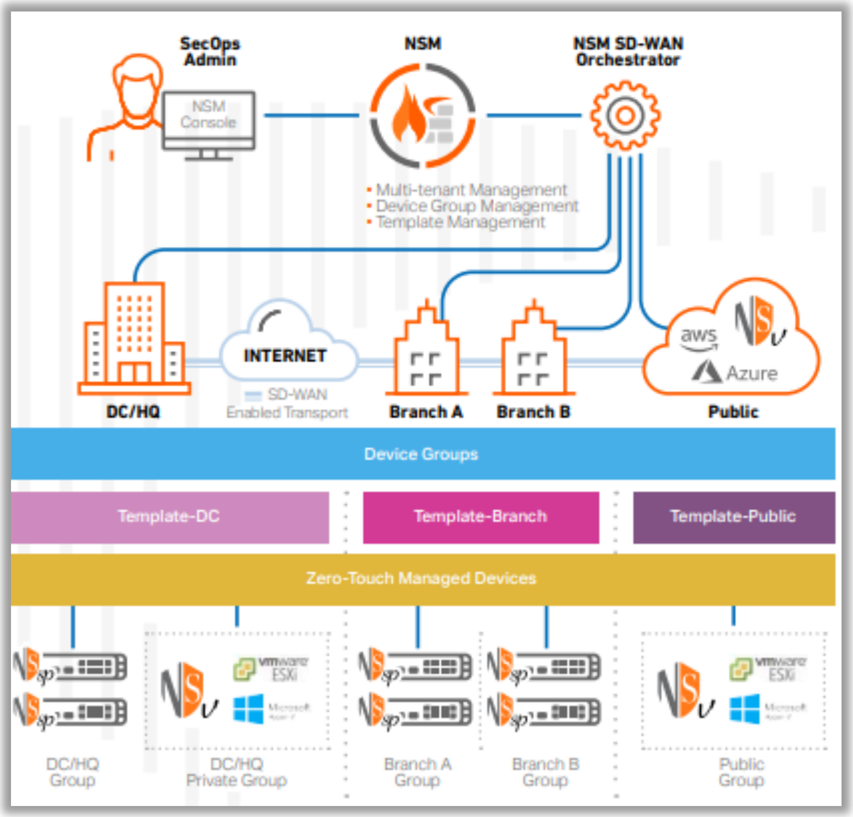
[112] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112



Be in control: Orchestrate firewall operations from one place

NSM offers you everything you need for a unified firewall management system. It empowers you with tenant-level visibility, group-based device control and unlimited scale to centrally manage and provision your SonicWall network security operations. These include deploying and managing all firewall devices, device groups and tenants, synchronizing and enforcing consistent security policies across your environments with flexible local controls and monitoring everything from one dynamic dashboard with detailed reports and analytics. In addition, NSM enables you to manage all from a single user-friendly console that can be accessed from any location using any browser-enabled device.

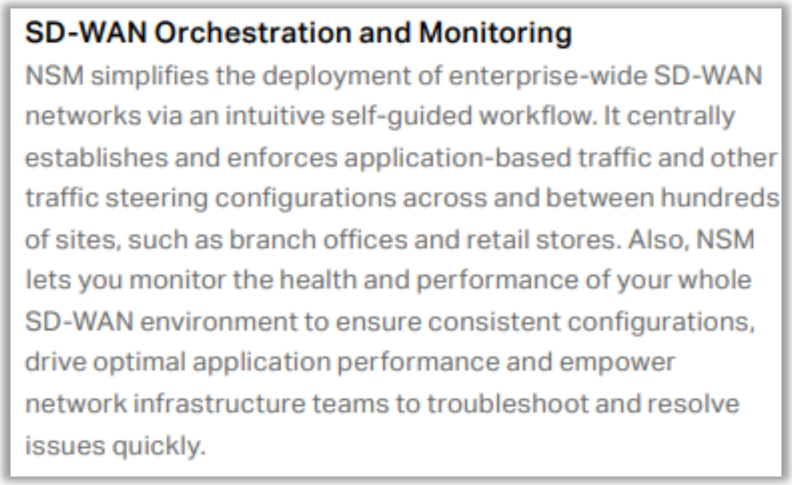
[113]



[114]

[113] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 2.

[114] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 1.

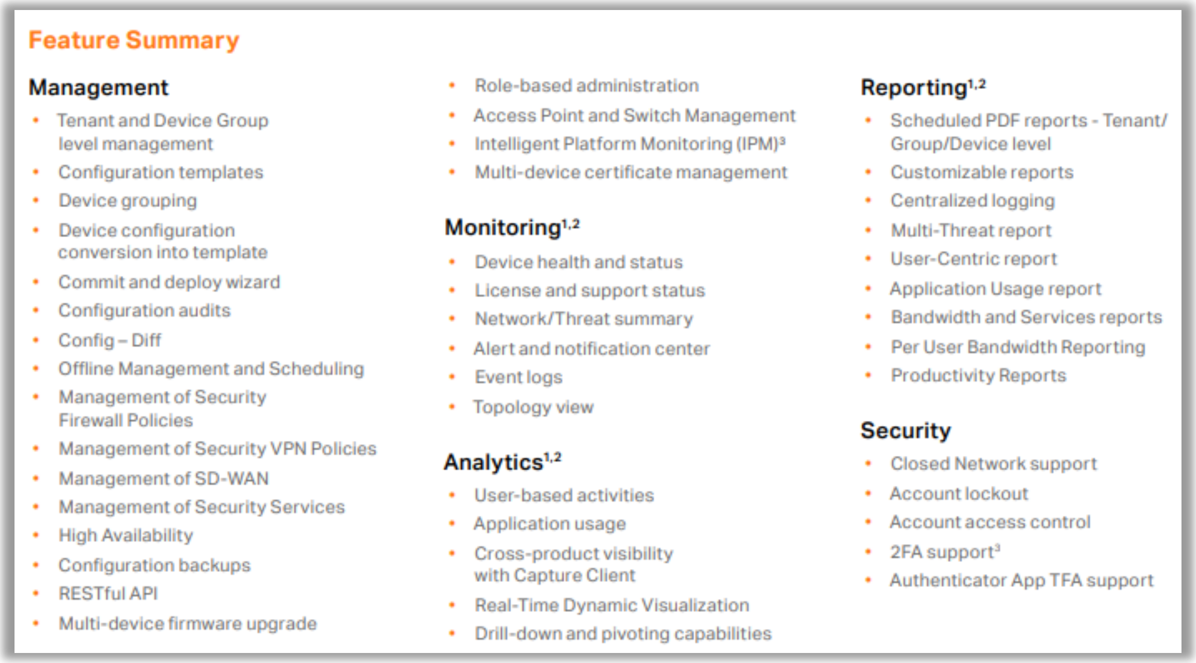


SD-WAN Orchestration and Monitoring

NSM simplifies the deployment of enterprise-wide SD-WAN networks via an intuitive self-guided workflow. It centrally establishes and enforces application-based traffic and other traffic steering configurations across and between hundreds of sites, such as branch offices and retail stores. Also, NSM lets you monitor the health and performance of your whole SD-WAN environment to ensure consistent configurations, drive optimal application performance and empower network infrastructure teams to troubleshoot and resolve issues quickly.

[115]

120. Every ’616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime. For example, Network Security Manager uses cross-product visibility with Capture Client, as an endpoint trust agent to provide endpoint telemetry sharing, including “user info, device info, and client version.”



Feature Summary

Management

- Tenant and Device Group level management
- Configuration templates
- Device grouping
- Device configuration conversion into template
- Commit and deploy wizard
- Configuration audits
- Config – Diff
- Offline Management and Scheduling
- Management of Security Firewall Policies
- Management of Security VPN Policies
- Management of SD-WAN
- Management of Security Services
- High Availability
- Configuration backups
- RESTful API
- Multi-device firmware upgrade
- Role-based administration
- Access Point and Switch Management
- Intelligent Platform Monitoring (IPM)[3]
- Multi-device certificate management

Monitoring[1,2]

- Device health and status
- License and support status
- Network/Threat summary
- Alert and notification center
- Event logs
- Topology view

Analytics[1,2]

- User-based activities
- Application usage
- Cross-product visibility with Capture Client
- Real-Time Dynamic Visualization
- Drill-down and pivoting capabilities

Reporting[1,2]

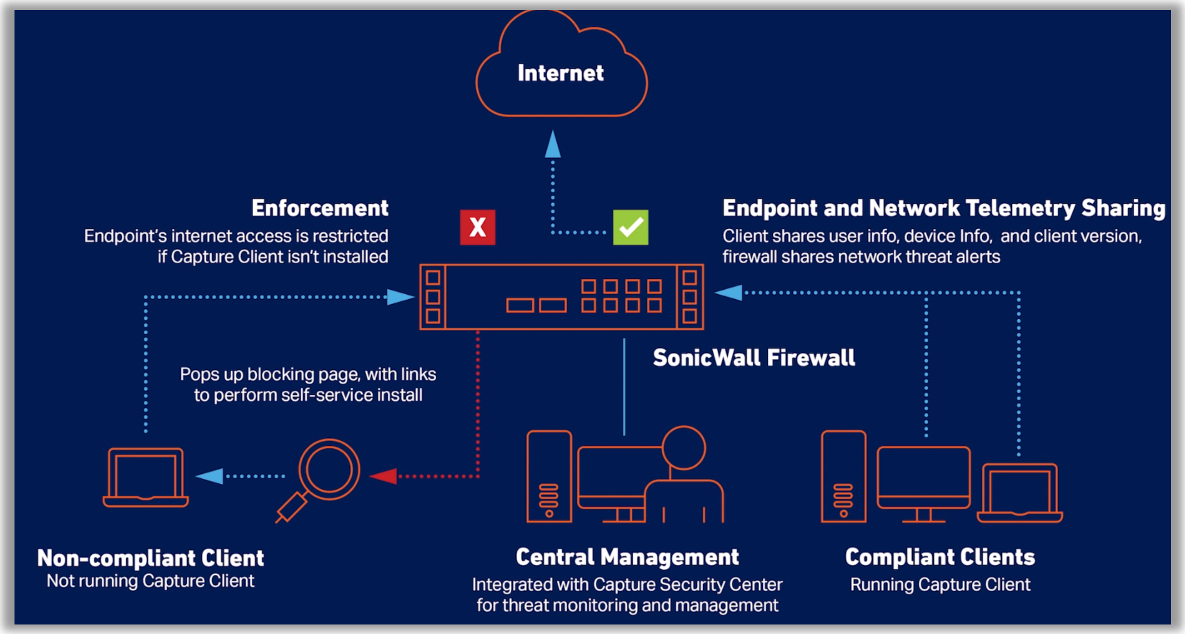
- Scheduled PDF reports - Tenant/ Group/Device level
- Customizable reports
- Centralized logging
- Multi-Threat report
- User-Centric report
- Application Usage report
- Bandwidth and Services reports
- Per User Bandwidth Reporting
- Productivity Reports

Security

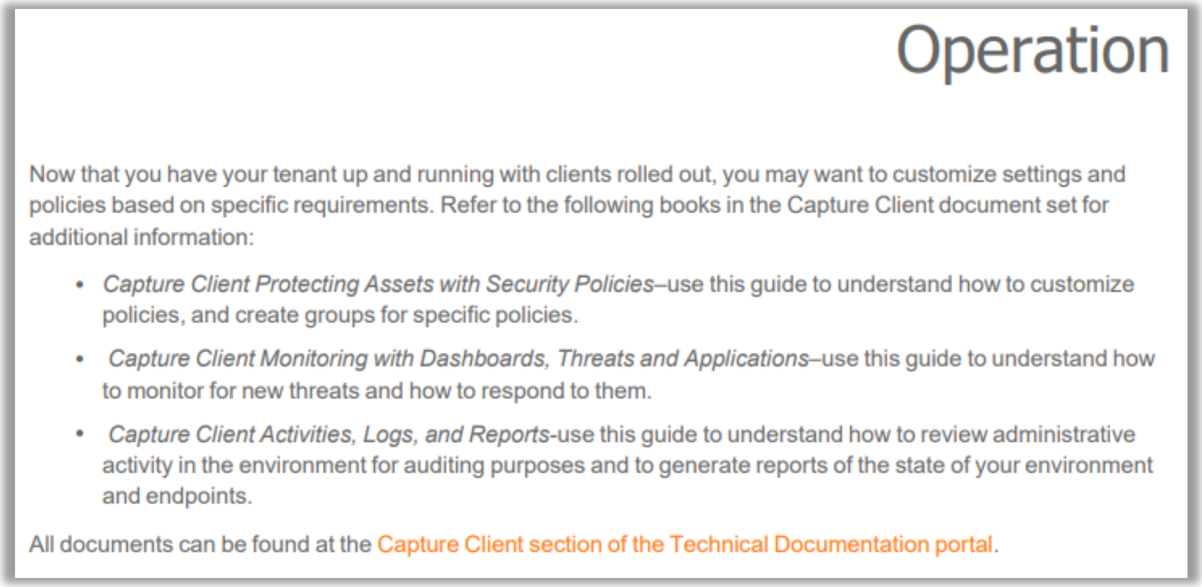
- Closed Network support
- Account lockout
- Account access control
- 2FA support[3]
- Authenticator App TFA support

[116]

[115] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 3.
[116] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf


Internet
Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center for threat monitoring and management
Compliant Clients
Running Capture Client

[117]



Operation

Now that you have your tenant up and running with clients rolled out, you may want to customize settings and policies based on specific requirements. Refer to the following books in the Capture Client document set for additional information:

- *Capture Client Protecting Assets with Security Policies*–use this guide to understand how to customize policies, and create groups for specific policies.
- *Capture Client Monitoring with Dashboards, Threats and Applications*–use this guide to understand how to monitor for new threats and how to respond to them.
- *Capture Client Activities, Logs, and Reports*-use this guide to understand how to review administrative activity in the environment for auditing purposes and to generate reports of the state of your environment and endpoints.

All documents can be found at the Capture Client section of the Technical Documentation portal.

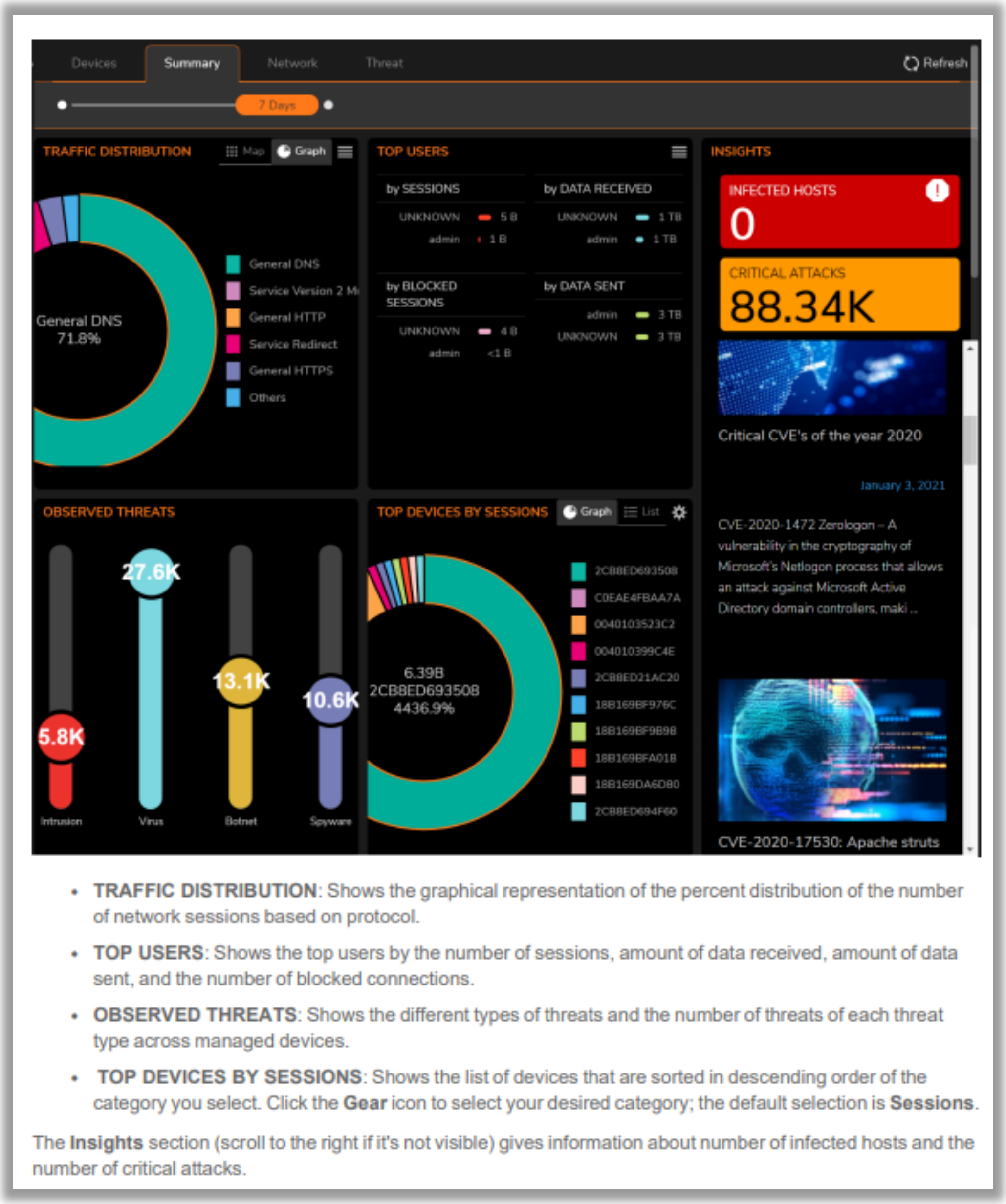
[118]

121. Every '616 Accused Product practices receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime. For example, the NSM Console receives endpoint

[117] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[118] https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 27.

events and applications executing on the endpoint, including "traffic distribution," "top users," and "observed threats". For further example, Capture Client provides application risk noting the applications executing on the endpoint at runtime.

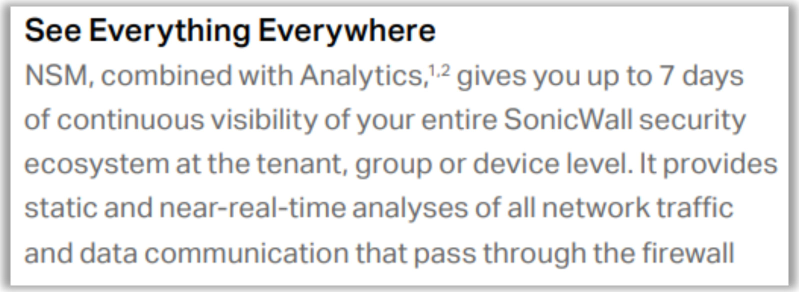


- **TRAFFIC DISTRIBUTION**: Shows the graphical representation of the percent distribution of the number of network sessions based on protocol.
- **TOP USERS**: Shows the top users by the number of sessions, amount of data received, amount of data sent, and the number of blocked connections.
- **OBSERVED THREATS**: Shows the different types of threats and the number of threats of each threat type across managed devices.
- **TOP DEVICES BY SESSIONS**: Shows the list of devices that are sorted in descending order of the category you select. Click the **Gear** icon to select your desired category; the default selection is **Sessions**.

The **Insights** section (scroll to the right if it's not visible) gives information about number of infected hosts and the number of critical attacks.

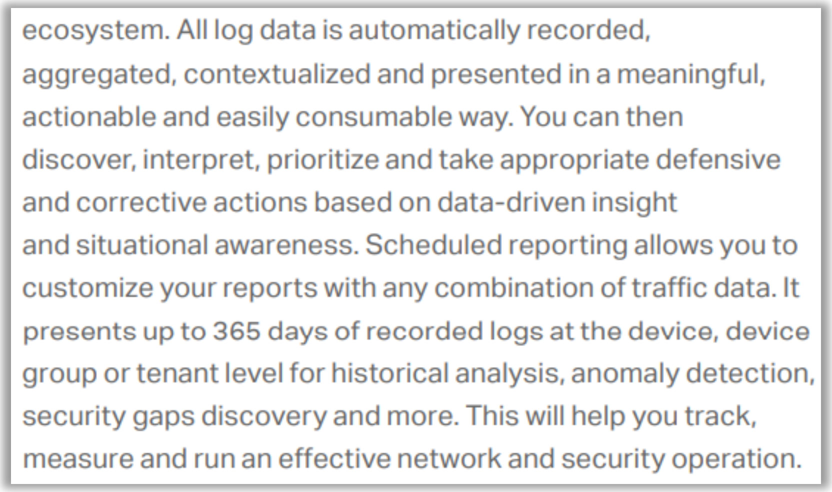
[119]

[119] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 14.



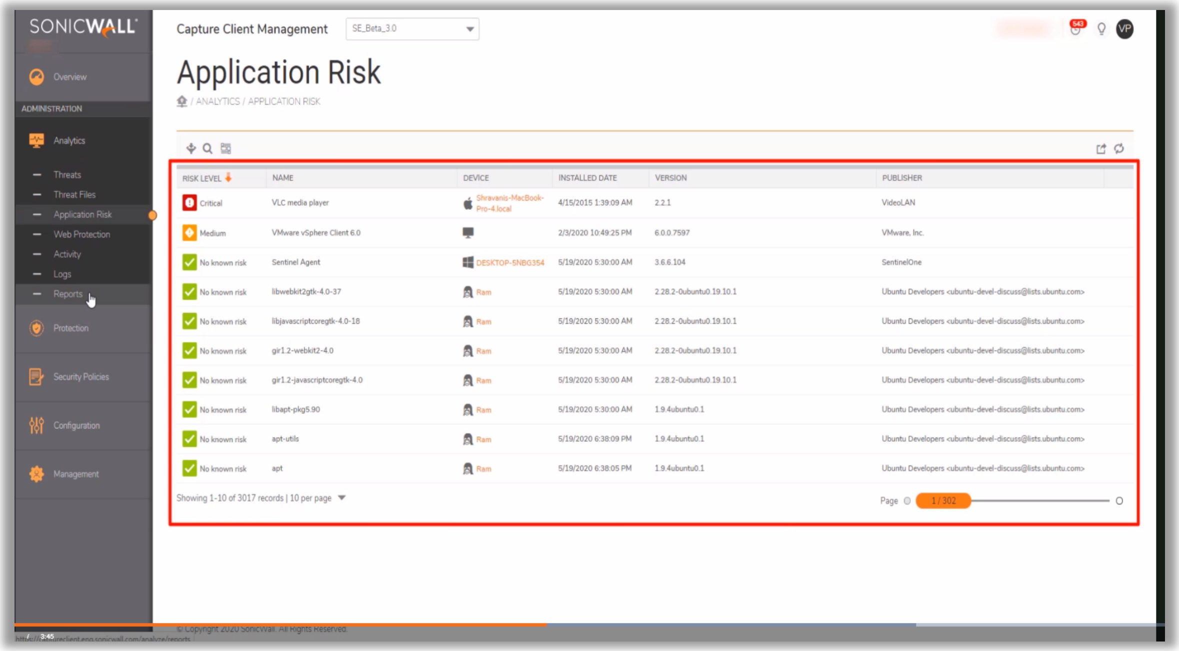
See Everything Everywhere

NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall



ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way. You can then discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more. This will help you track, measure and run an effective network and security operation. [120]

[120] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 3-4.



Application Risk

/ ANALYTICS / APPLICATION RISK

RISK LEVEL	NAME	DEVICE	INSTALLED DATE	VERSION	PUBLISHER
Critical	VLC media player	Shravanis-MacBook-Pro-4.local	4/15/2015 1:39:09 AM	2.2.1	VideoLAN
Medium	VMware vSphere Client 6.0		2/3/2020 10:49:25 PM	6.0.0.7597	VMware, Inc.
No known risk	Sentinel Agent	DESKTOP-5NBG354	5/19/2020 5:30:00 AM	3.6.6.104	SentinelOne
No known risk	libwebkit2gtk-4.0-37	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
No known risk	libjavascriptcoregtk-4.0-18	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
No known risk	gir1.2-webkit2-4.0	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
No known risk	gir1.2-javascriptcoregtk-4.0	Ram	5/19/2020 5:30:00 AM	2.28.2-0ubuntu0.19.10.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
No known risk	libapt-pkg5.90	Ram	5/19/2020 5:30:00 AM	1.9.4ubuntu0.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
No known risk	apt-utils	Ram	5/19/2020 6:38:09 PM	1.9.4ubuntu0.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
No known risk	apt	Ram	5/19/2020 6:38:05 PM	1.9.4ubuntu0.1	Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>

Showing 1-10 of 3017 records | 10 per page

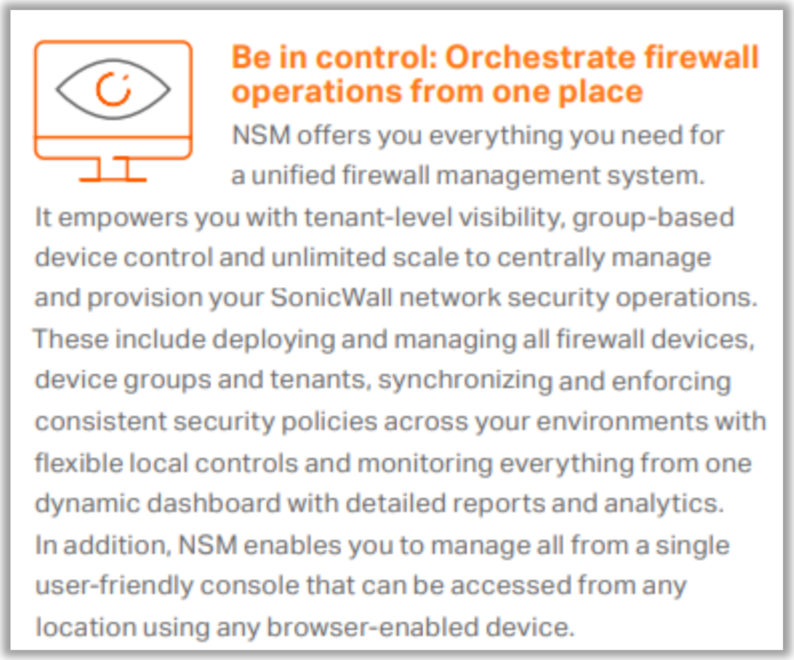
Page 1 / 302

© Copyright 2020 SonicWall. All Rights Reserved.

[121]

122. Every ’616 Accused Product practices analyzing, by the trust orchestration server, the received endpoint events. For example, NSM analyzes received endpoint events to provide “detailed reports and analytics” “from a single user-friendly console.”

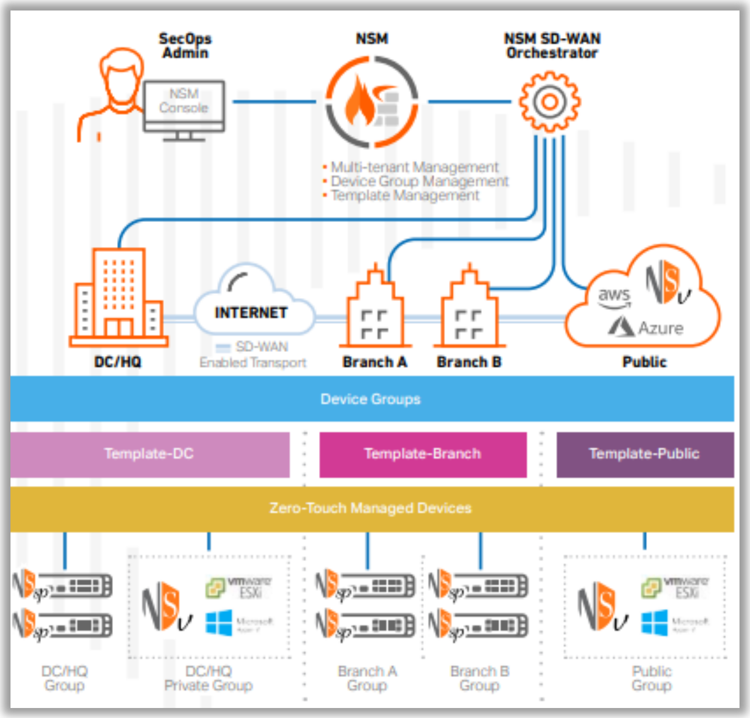
[121] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6193544296001



Be in control: Orchestrate firewall operations from one place

NSM offers you everything you need for a unified firewall management system. It empowers you with tenant-level visibility, group-based device control and unlimited scale to centrally manage and provision your SonicWall network security operations. These include deploying and managing all firewall devices, device groups and tenants, synchronizing and enforcing consistent security policies across your environments with flexible local controls and monitoring everything from one dynamic dashboard with detailed reports and analytics. In addition, NSM enables you to manage all from a single user-friendly console that can be accessed from any location using any browser-enabled device.

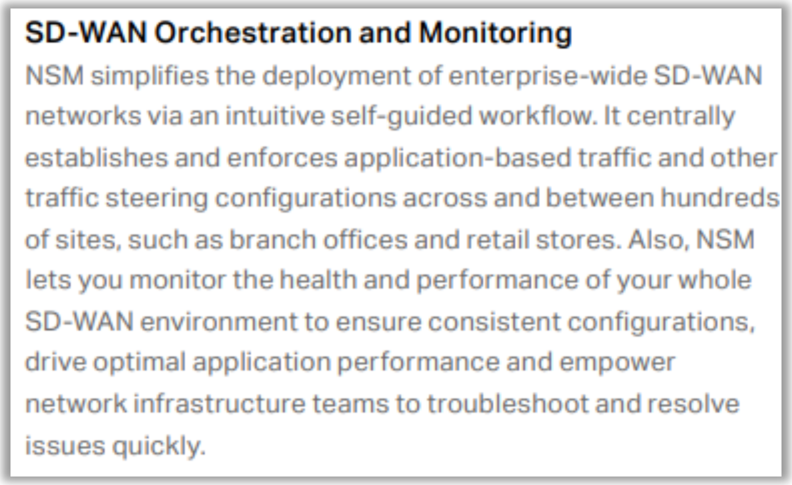
[122]



[123]

[122] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 2.

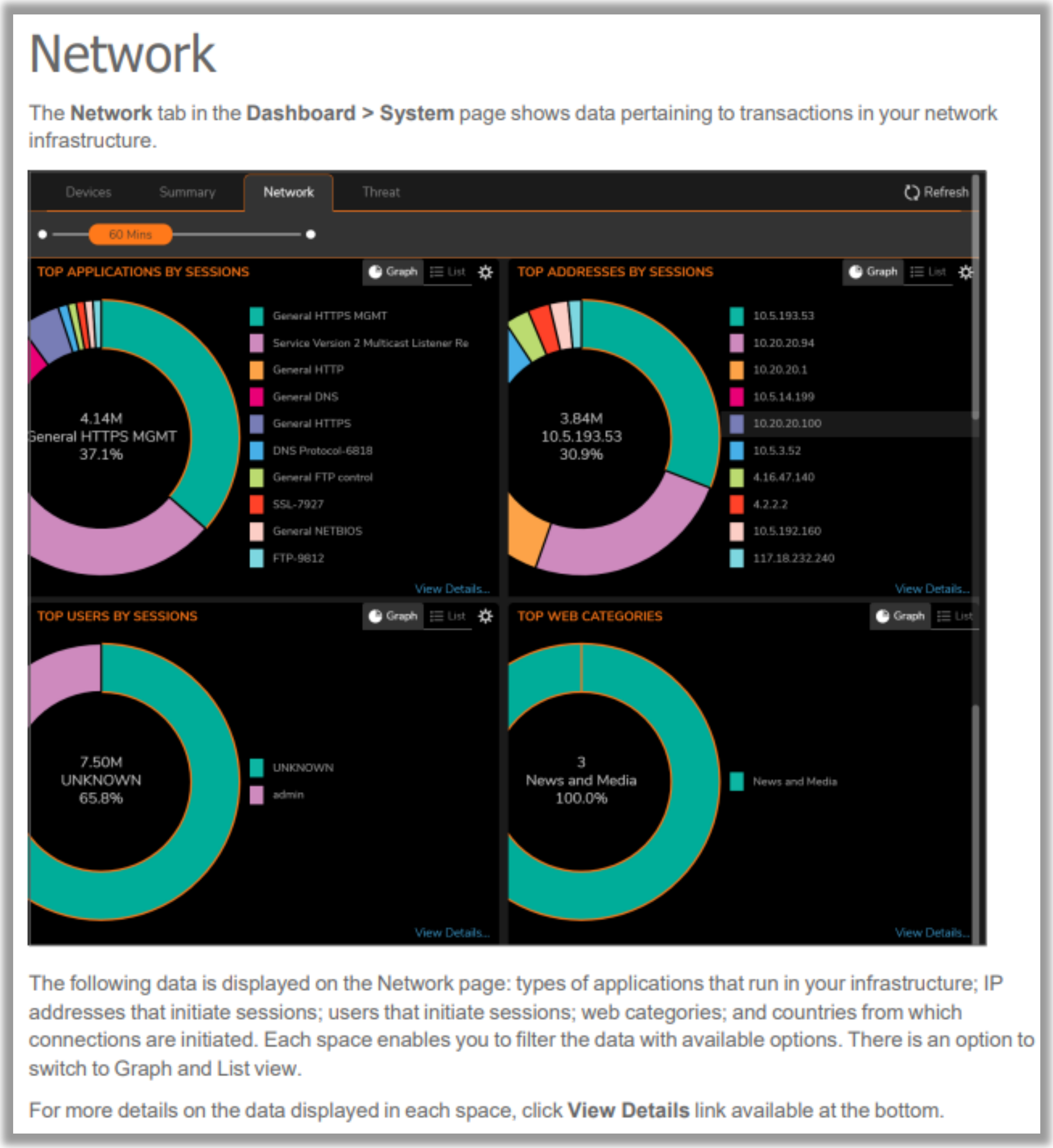
[123] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 1.



SD-WAN Orchestration and Monitoring

NSM simplifies the deployment of enterprise-wide SD-WAN networks via an intuitive self-guided workflow. It centrally establishes and enforces application-based traffic and other traffic steering configurations across and between hundreds of sites, such as branch offices and retail stores. Also, NSM lets you monitor the health and performance of your whole SD-WAN environment to ensure consistent configurations, drive optimal application performance and empower network infrastructure teams to troubleshoot and resolve issues quickly.[124]

[124] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 3.



Network

The **Network** tab in the **Dashboard > System** page shows data pertaining to transactions in your network infrastructure.

The following data is displayed on the Network page: types of applications that run in your infrastructure; IP addresses that initiate sessions; users that initiate sessions; web categories; and countries from which connections are initiated. Each space enables you to filter the data with available options. There is an option to switch to Graph and List view.

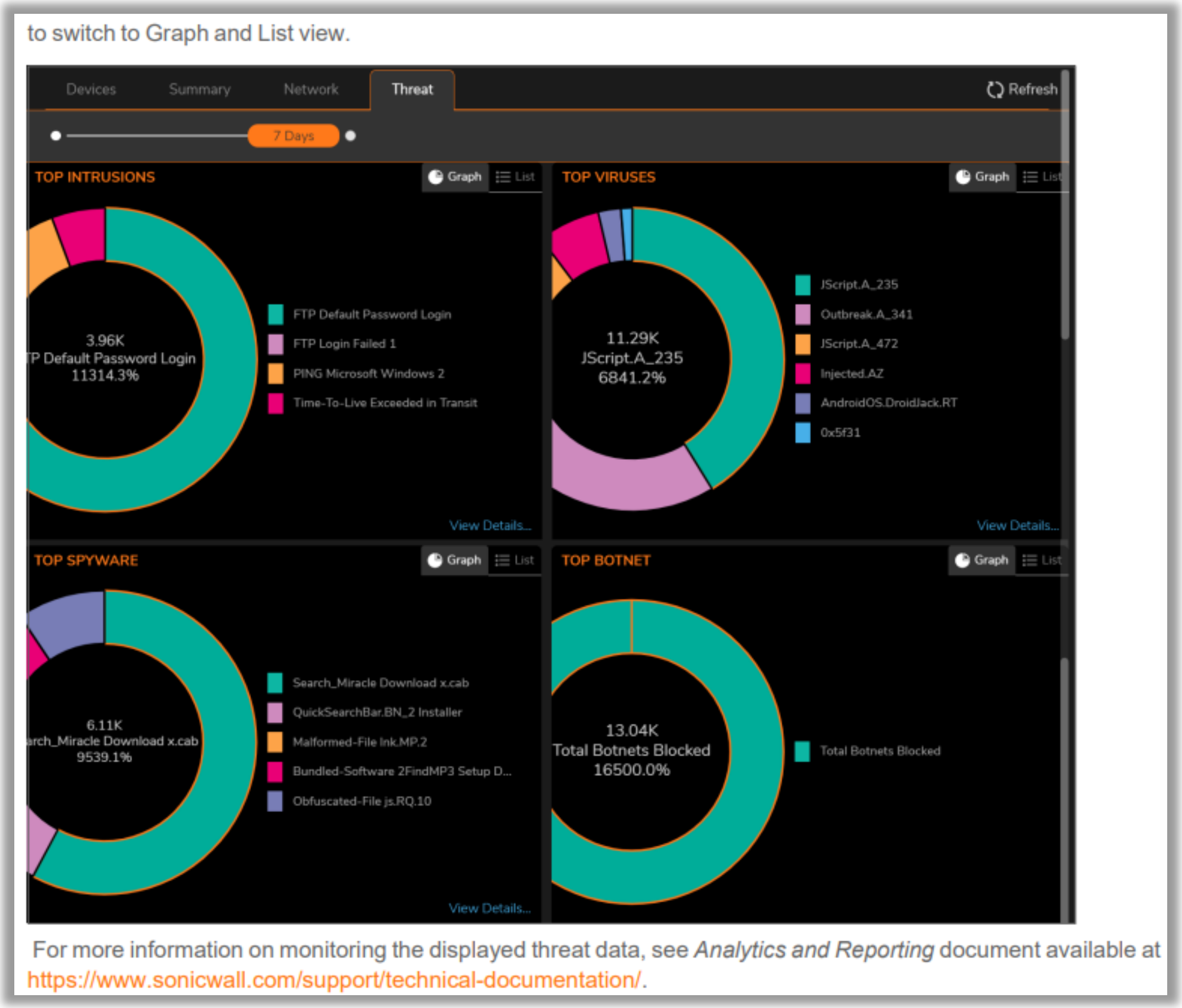
For more details on the data displayed in each space, click **View Details** link available at the bottom.

[125]

Threat

The **Threat** tab in the **Dashboard > System** page shows top threats by type, including the viruses, intrusions, spyware, and botnet. For more details on threats of a particular threat type, click **View Details**.There is an option

[125] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 15.

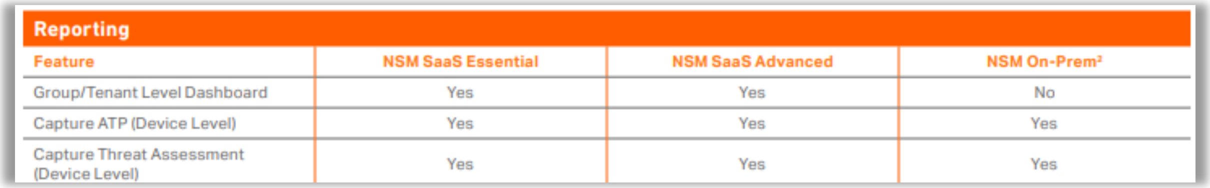


to switch to Graph and List view.

For more information on monitoring the displayed threat data, see *Analytics and Reporting* document available at https://www.sonicwall.com/support/technical-documentation/.

[126]

123. Every '616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, NSM receives third-party network endpoint assessments (e.g., Capture Threat Assessment).



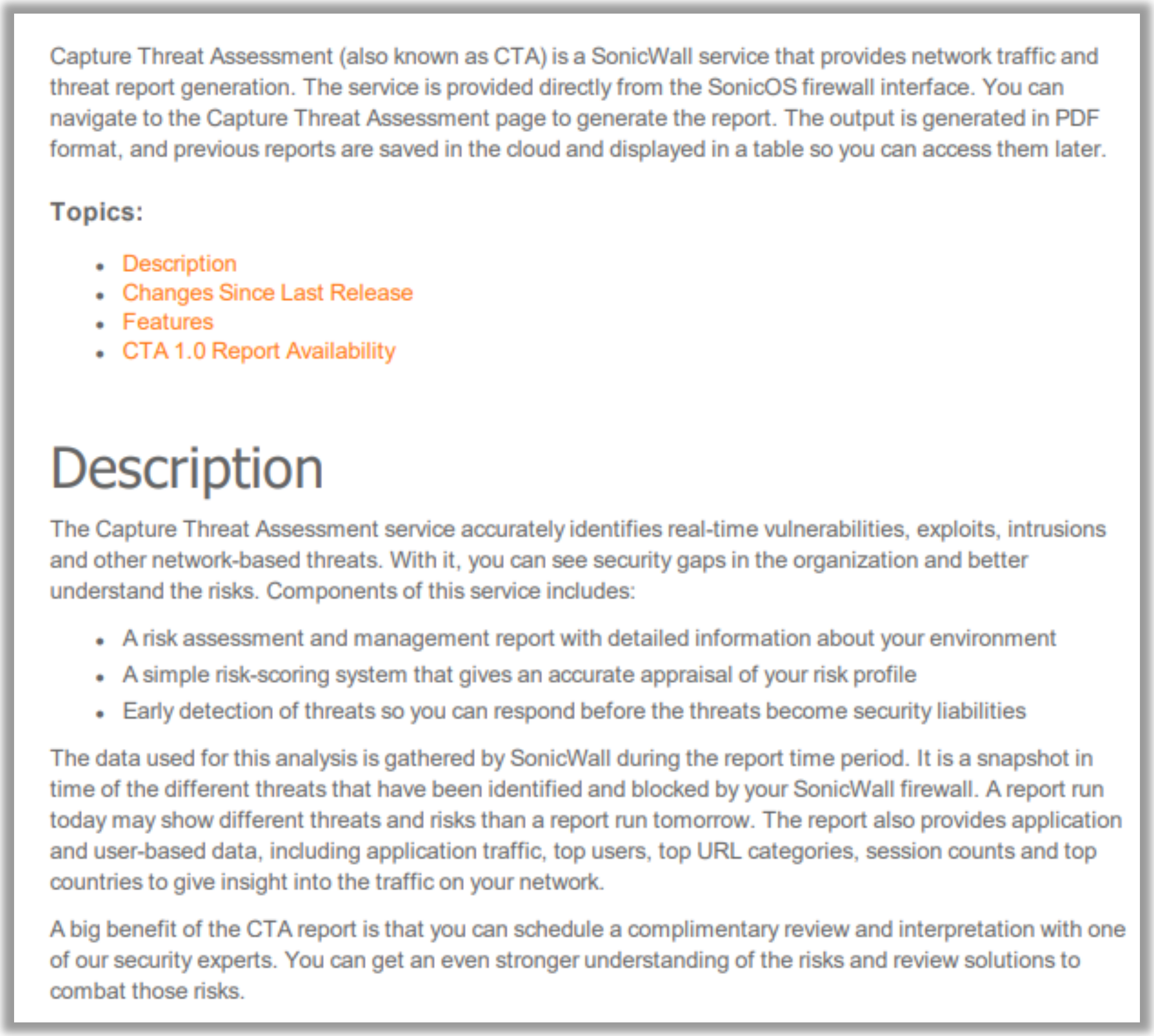
Reporting

Feature	NSM SaaS Essential	NSM SaaS Advanced	NSM On-Prem²
Group/Tenant Level Dashboard	Yes	Yes	No
Capture ATP (Device Level)	Yes	Yes	Yes
Capture Threat Assessment (Device Level)	Yes	Yes	Yes

[127]

[126] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 15-16.

[127] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf, at 6.



Capture Threat Assessment (also known as CTA) is a SonicWall service that provides network traffic and threat report generation. The service is provided directly from the SonicOS firewall interface. You can navigate to the Capture Threat Assessment page to generate the report. The output is generated in PDF format, and previous reports are saved in the cloud and displayed in a table so you can access them later.

Topics:

- Description
- Changes Since Last Release
- Features
- CTA 1.0 Report Availability

Description

The Capture Threat Assessment service accurately identifies real-time vulnerabilities, exploits, intrusions and other network-based threats. With it, you can see security gaps in the organization and better understand the risks. Components of this service includes:

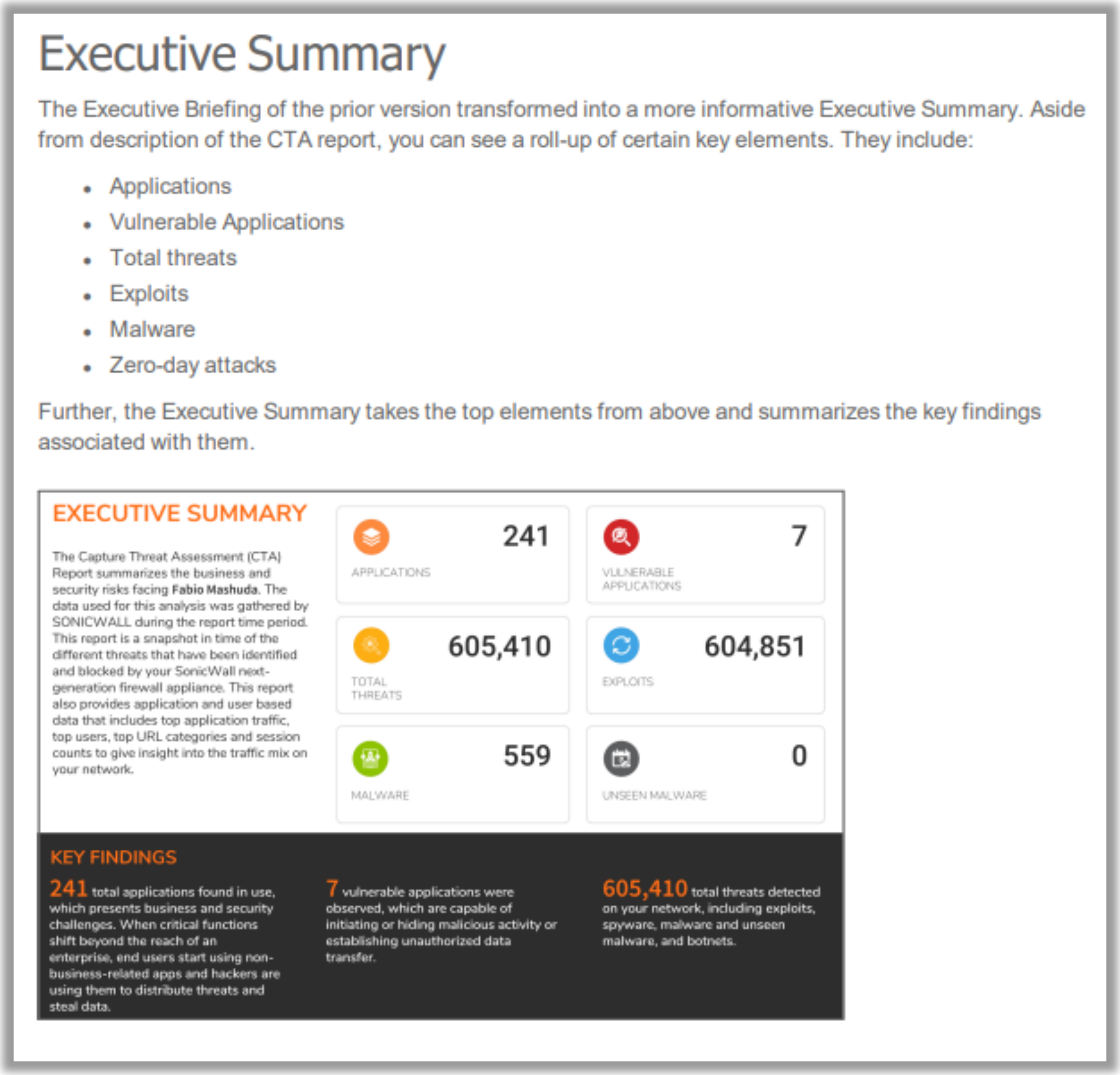
- A risk assessment and management report with detailed information about your environment
- A simple risk-scoring system that gives an accurate appraisal of your risk profile
- Early detection of threats so you can respond before the threats become security liabilities

The data used for this analysis is gathered by SonicWall during the report time period. It is a snapshot in time of the different threats that have been identified and blocked by your SonicWall firewall. A report run today may show different threats and risks than a report run tomorrow. The report also provides application and user-based data, including application traffic, top users, top URL categories, session counts and top countries to give insight into the traffic on your network.

A big benefit of the CTA report is that you can schedule a complimentary review and interpretation with one of our security experts. You can get an even stronger understanding of the risks and review solutions to combat those risks.[128]

[128] https://www.sonicwall.com/techdocs/pdf/cta-user_guide.pdf, at 3.

RUSS AUGUST & KABAT



Executive Summary

The Executive Briefing of the prior version transformed into a more informative Executive Summary. Aside from description of the CTA report, you can see a roll-up of certain key elements. They include:

- Applications
- Vulnerable Applications
- Total threats
- Exploits
- Malware
- Zero-day attacks

Further, the Executive Summary takes the top elements from above and summarizes the key findings associated with them.

EXECUTIVE SUMMARY

The Capture Threat Assessment (CTA) Report summarizes the business and security risks facing **Fabio Mashuda**. The data used for this analysis was gathered by SONICWALL during the report time period. This report is a snapshot in time of the different threats that have been identified and blocked by your SonicWall next-generation firewall appliance. This report also provides application and user based data that includes top application traffic, top users, top URL categories and session counts to give insight into the traffic mix on your network.

241 APPLICATIONS

7 VULNERABLE APPLICATIONS

605,410 TOTAL THREATS

604,851 EXPLOITS

559 MALWARE

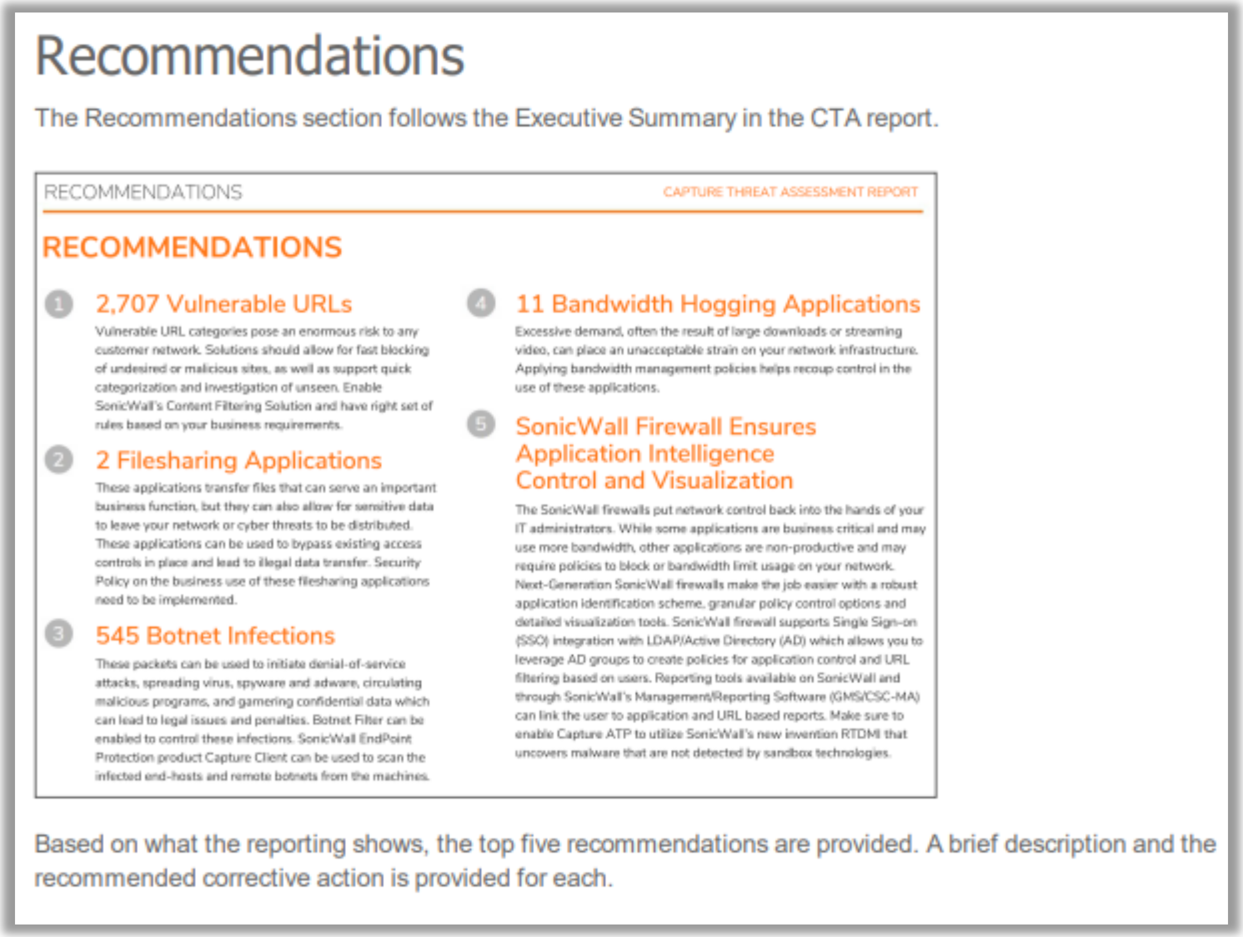
0 UNSEEN MALWARE

KEY FINDINGS

241 total applications found in use, which presents business and security challenges. When critical functions shift beyond the reach of an enterprise, end users start using non-business-related apps and hackers are using them to distribute threats and steal data.

7 vulnerable applications were observed, which are capable of initiating or hiding malicious activity or establishing unauthorized data transfer.

605,410 total threats detected on your network, including exploits, spyware, malware and unseen malware, and botnets.



Recommendations

The Recommendations section follows the Executive Summary in the CTA report.

RECOMMENDATIONS CAPTURE THREAT ASSESSMENT REPORT

RECOMMENDATIONS

1 **2,707 Vulnerable URLs**

Vulnerable URL categories pose an enormous risk to any customer network. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unseen. Enable SonicWall's Content Filtering Solution and have right set of rules based on your business requirements.

2 **2 Filesharing Applications**

These applications transfer files that can serve an important business function, but they can also allow for sensitive data to leave your network or cyber threats to be distributed. These applications can be used to bypass existing access controls in place and lead to illegal data transfer. Security Policy on the business use of these filesharing applications need to be implemented.

3 **545 Botnet Infections**

These packets can be used to initiate denial-of-service attacks, spreading virus, spyware and adware, circulating malicious programs, and gamering confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections. SonicWall EndPoint Protection product Capture Client can be used to scan the infected end-hosts and remote botnets from the machines.

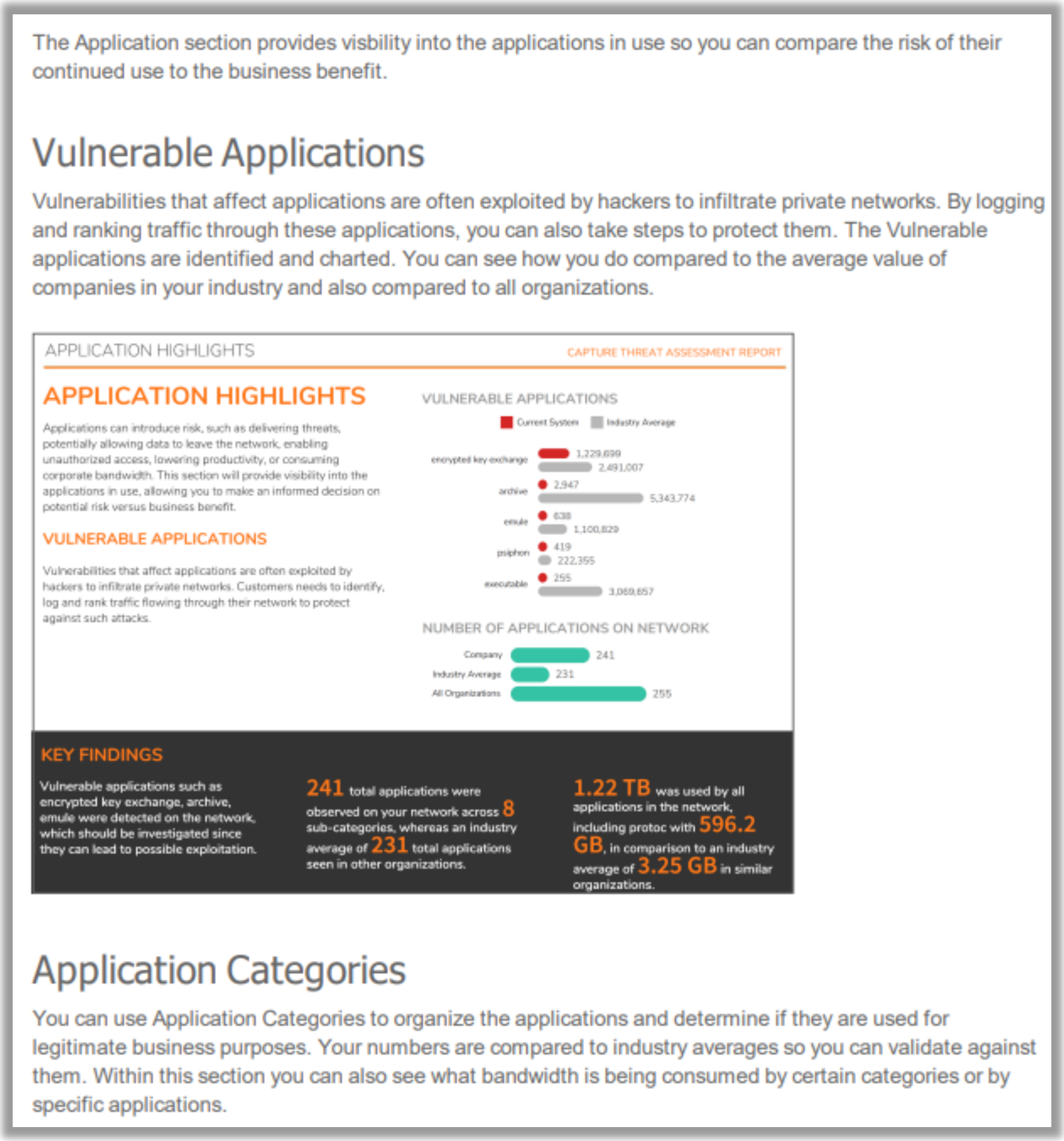
4 **11 Bandwidth Hogging Applications**

Excessive demand, often the result of large downloads or streaming video, can place an unacceptable strain on your network infrastructure. Applying bandwidth management policies helps recoup control in the use of these applications.

5 **SonicWall Firewall Ensures Application Intelligence Control and Visualization**

The SonicWall firewalls put network control back into the hands of your IT administrators. While some applications are business critical and may use more bandwidth, other applications are non-productive and may require policies to block or bandwidth limit usage on your network. Next-Generation SonicWall firewalls make the job easier with a robust application identification scheme, granular policy control options and detailed visualization tools. SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on SonicWall and through SonicWall's Management/Reporting Software (GMS/CSC-MA) can link the user to application and URL based reports. Make sure to enable Capture ATP to utilize SonicWall's new invention RTDMI that uncovers malware that are not detected by sandbox technologies.

Based on what the reporting shows, the top five recommendations are provided. A brief description and the recommended corrective action is provided for each.



The Application section provides visbility into the applications in use so you can compare the risk of their continued use to the business benefit.

Vulnerable Applications

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. By logging and ranking traffic through these applications, you can also take steps to protect them. The Vulnerable applications are identified and charted. You can see how you do compared to the average value of companies in your industry and also compared to all organizations.

APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION HIGHLIGHTS

Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision on potential risk versus business benefit.

VULNERABLE APPLICATIONS

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. Customers needs to identify, log and rank traffic flowing through their network to protect against such attacks.

KEY FINDINGS

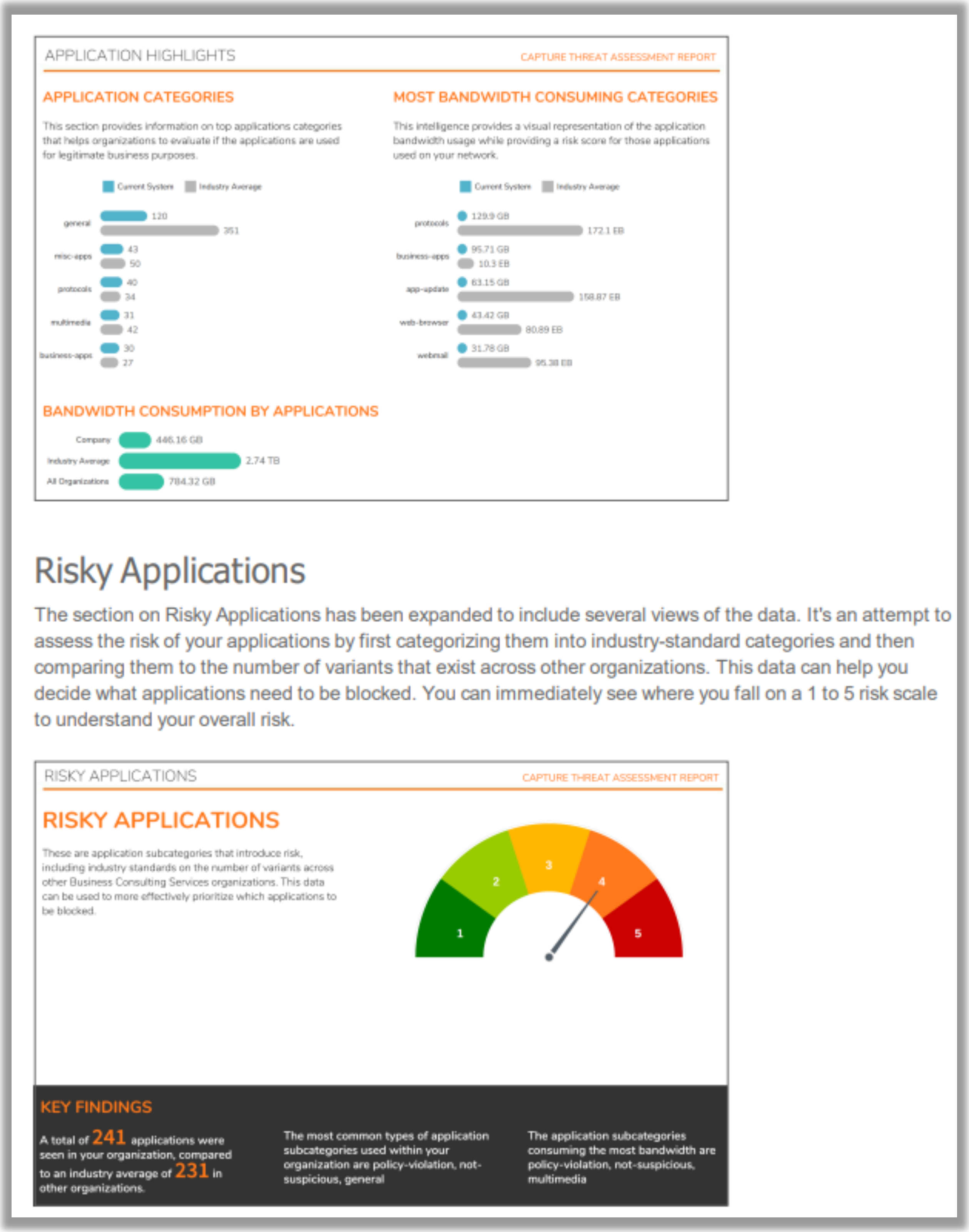
Vulnerable applications such as encrypted key exchange, archive, emule were detected on the network, which should be investigated since they can lead to possible exploitation.

241 total applications were observed on your network across 8 sub-categories, whereas an industry average of 231 total applications seen in other organizations.

1.22 TB was used by all applications in the network, including protoc with 596.2 GB, in comparison to an industry average of 3.25 GB in similar organizations.

Application Categories

You can use Application Categories to organize the applications and determine if they are used for legitimate business purposes. Your numbers are compared to industry averages so you can validate against them. Within this section you can also see what bandwidth is being consumed by certain categories or by specific applications.



APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION CATEGORIES

This section provides information on top applications categories that helps organizations to evaluate if the applications are used for legitimate business purposes.

MOST BANDWIDTH CONSUMING CATEGORIES

This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

BANDWIDTH CONSUMPTION BY APPLICATIONS

Risky Applications

The section on Risky Applications has been expanded to include several views of the data. It's an attempt to assess the risk of your applications by first categorizing them into industry-standard categories and then comparing them to the number of variants that exist across other organizations. This data can help you decide what applications need to be blocked. You can immediately see where you fall on a 1 to 5 risk scale to understand your overall risk.

RISKY APPLICATIONS

CAPTURE THREAT ASSESSMENT REPORT

RISKY APPLICATIONS

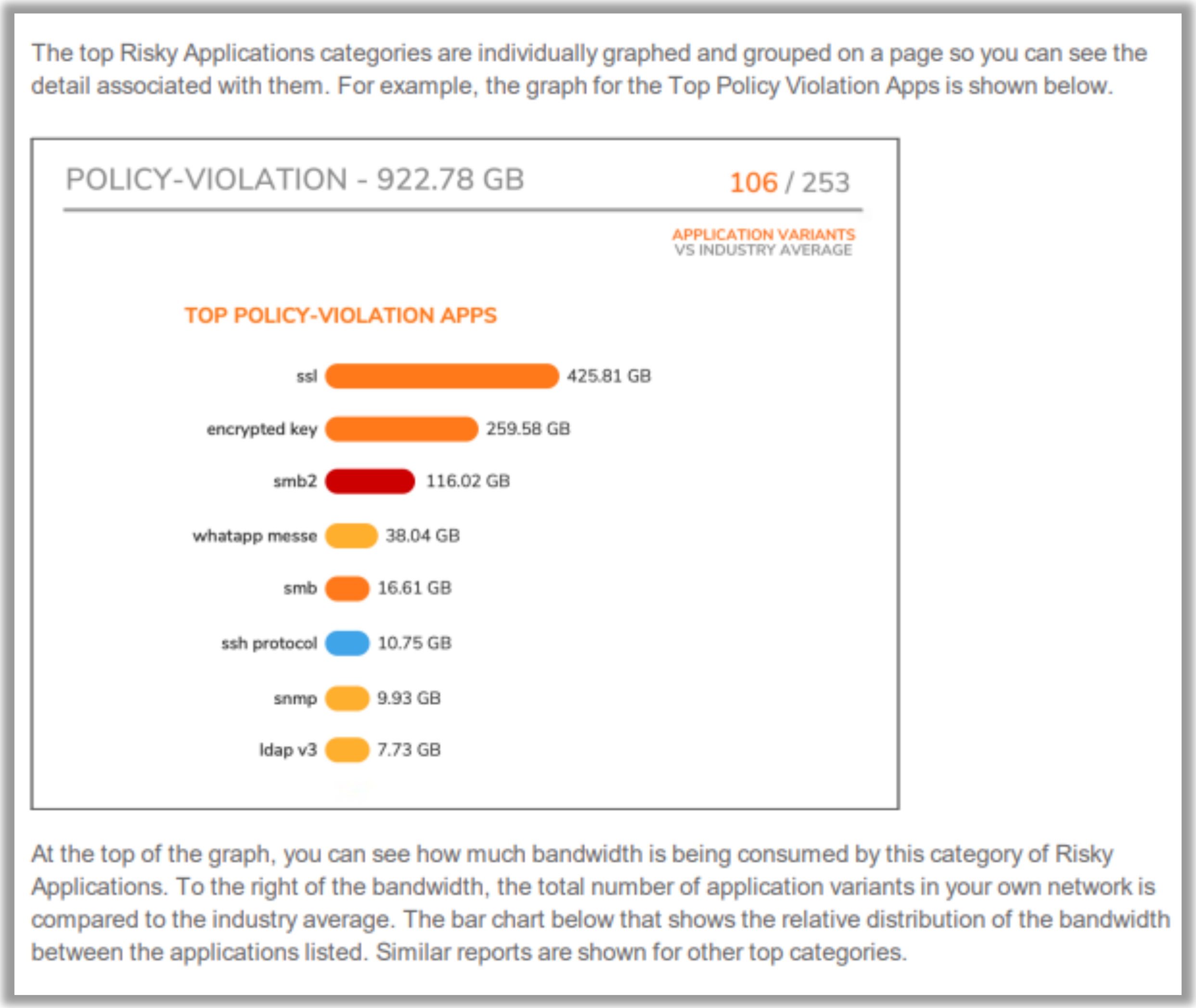
These are application subcategories that introduce risk, including industry standards on the number of variants across other Business Consulting Services organizations. This data can be used to more effectively prioritize which applications to be blocked.

KEY FINDINGS

A total of 241 applications were seen in your organization, compared to an industry average of 231 in other organizations.

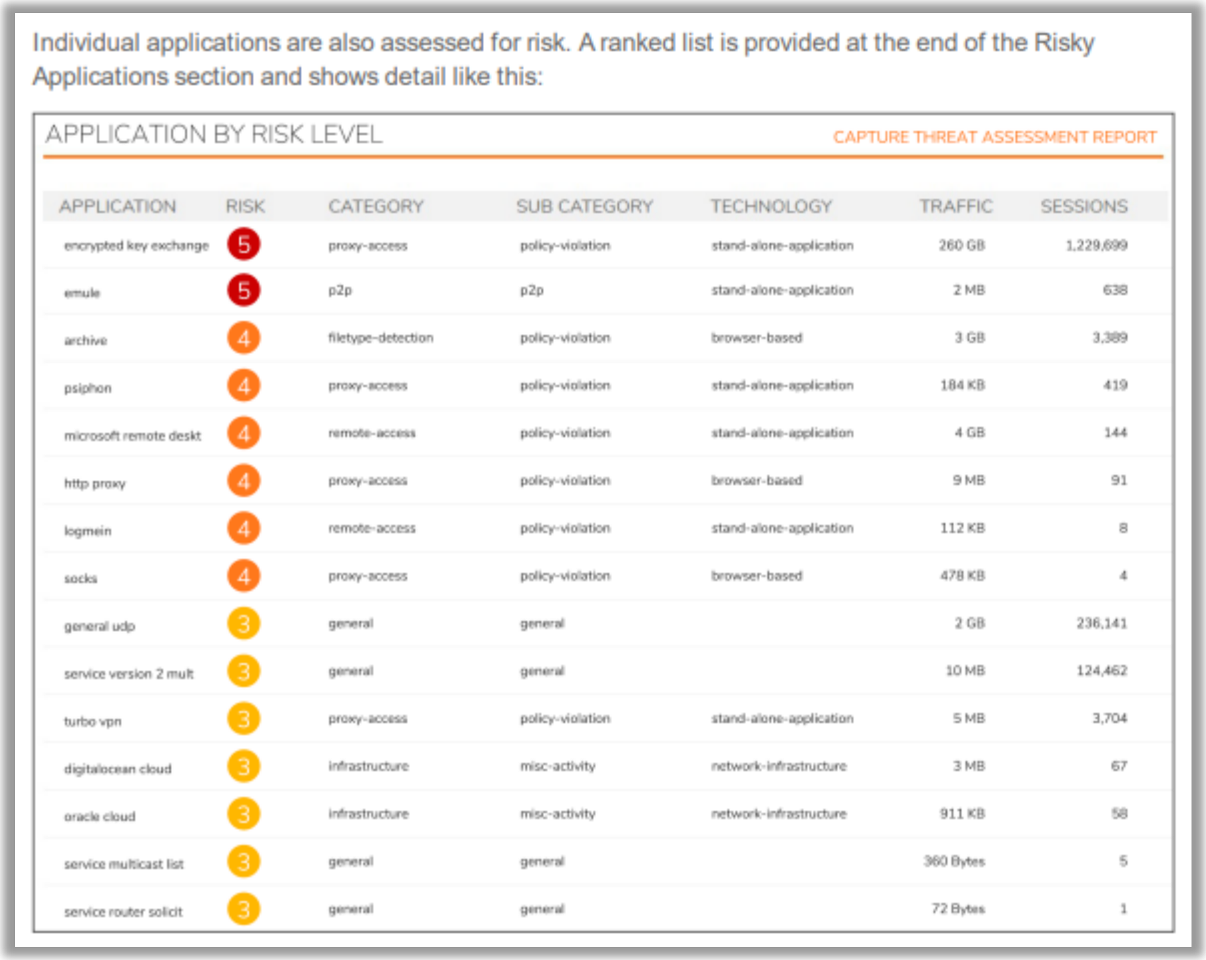
The most common types of application subcategories used within your organization are policy-violation, not-suspicious, general

The application subcategories consuming the most bandwidth are policy-violation, not-suspicious, multimedia



The top Risky Applications categories are individually graphed and grouped on a page so you can see the detail associated with them. For example, the graph for the Top Policy Violation Apps is shown below.

At the top of the graph, you can see how much bandwidth is being consumed by this category of Risky Applications. To the right of the bandwidth, the total number of application variants in your own network is compared to the industry average. The bar chart below that shows the relative distribution of the bandwidth between the applications listed. Similar reports are shown for other top categories.

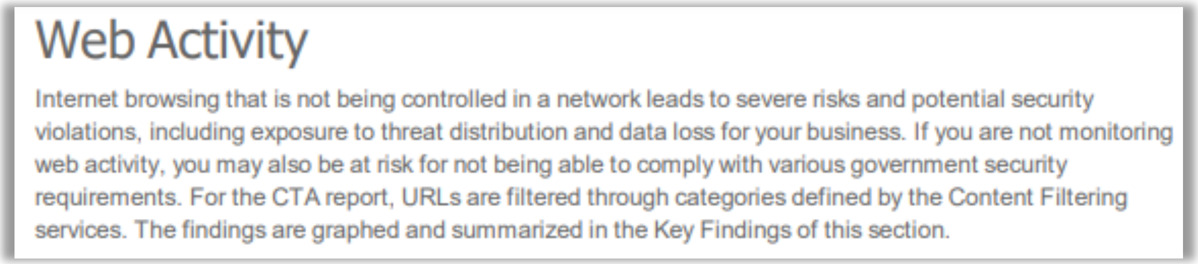


Individual applications are also assessed for risk. A ranked list is provided at the end of the Risky Applications section and shows detail like this:

APPLICATION BY RISK LEVEL

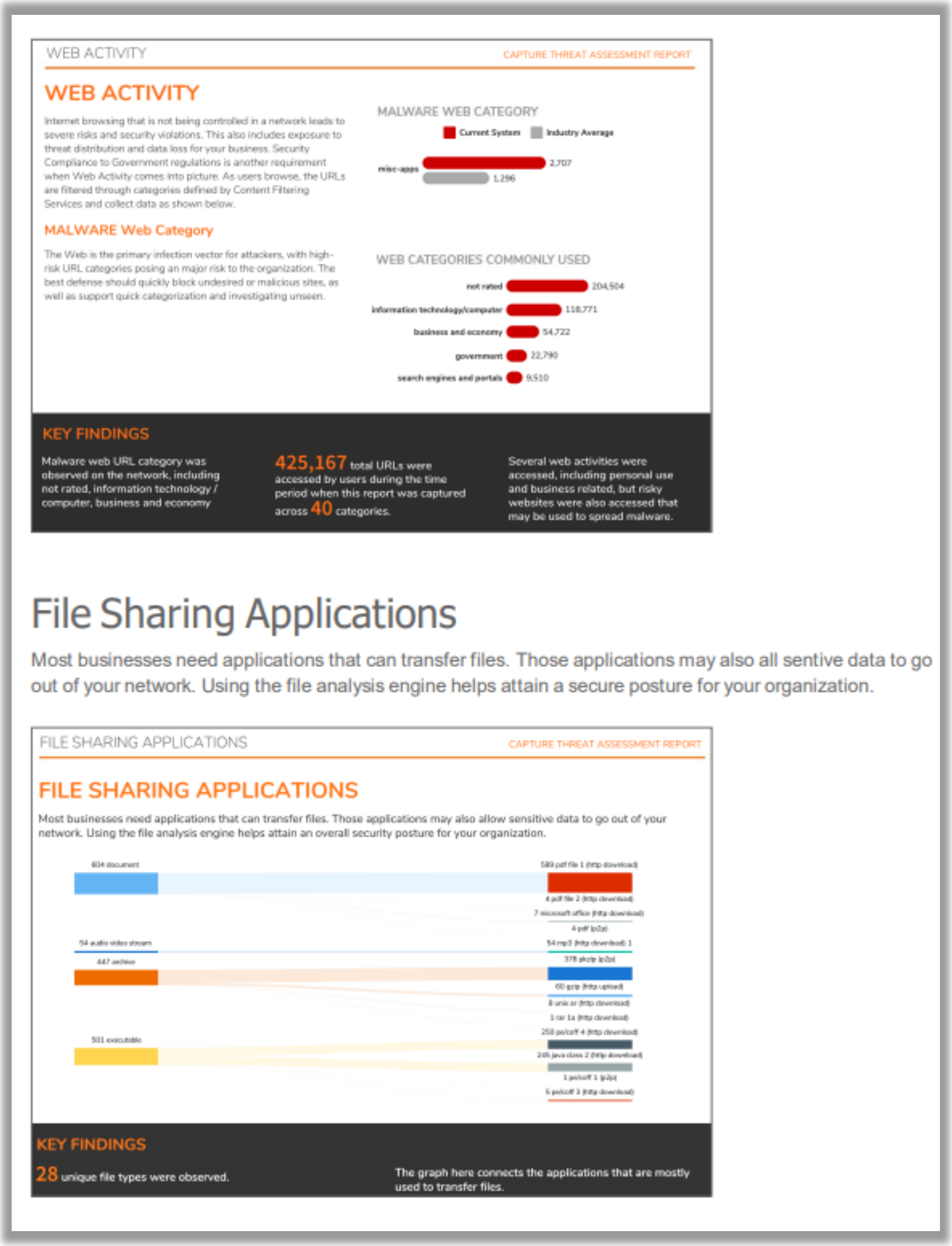
CAPTURE THREAT ASSESSMENT REPORT

APPLICATION	RISK	CATEGORY	SUB CATEGORY	TECHNOLOGY	TRAFFIC	SESSIONS
encrypted key exchange	5	proxy-access	policy-violation	stand-alone-application	260 GB	1,229,699
emule	5	p2p	p2p	stand-alone-application	2 MB	638
archive	4	filetype-detection	policy-violation	browser-based	3 GB	3,389
psiphon	4	proxy-access	policy-violation	stand-alone-application	184 KB	419
microsoft remote deskt	4	remote-access	policy-violation	stand-alone-application	4 GB	144
http proxy	4	proxy-access	policy-violation	browser-based	9 MB	91
logmein	4	remote-access	policy-violation	stand-alone-application	112 KB	8
socks	4	proxy-access	policy-violation	browser-based	478 KB	4
general udp	3	general	general		2 GB	236,141
service version 2 mult	3	general	general		10 MB	124,462
turbo vpn	3	proxy-access	policy-violation	stand-alone-application	5 MB	3,704
digitalocean cloud	3	infrastructure	misc-activity	network-infrastructure	3 MB	67
oracle cloud	3	infrastructure	misc-activity	network-infrastructure	911 KB	58
service multicast list	3	general	general		360 Bytes	5
service router solicit	3	general	general		72 Bytes	1



Web Activity

Internet browsing that is not being controlled in a network leads to severe risks and potential security violations, including exposure to threat distribution and data loss for your business. If you are not monitoring web activity, you may also be at risk for not being able to comply with various government security requirements. For the CTA report, URLs are filtered through categories defined by the Content Filtering services. The findings are graphed and summarized in the Key Findings of this section.



WEB ACTIVITY

CAPTURE THREAT ASSESSMENT REPORT

WEB ACTIVITY

Internet browsing that is not being controlled in a network leads to severe risks and security violations. This also includes exposure to threat distribution and data loss for your business. Security Compliance to Government regulations is another requirement when Web Activity comes into picture. As users browse, the URLs are filtered through categories defined by Content Filtering Services and collect data as shown below.

MALWARE Web Category

The Web is the primary infection vector for attackers, with high-risk URL categories posing an major risk to the organization. The best defense should quickly block undesired or malicious sites, as well as support quick categorization and investigating unseen.

MALWARE WEB CATEGORY

WEB CATEGORIES COMMONLY USED

KEY FINDINGS

Malware web URL category was observed on the network, including not rated, information technology / computer, business and economy

425,167 total URLs were accessed by users during the time period when this report was captured across 40 categories.

Several web activities were accessed, including personal use and business related, but risky websites were also accessed that may be used to spread malware.

File Sharing Applications

Most businesses need applications that can transfer files. Those applications may also all sentive data to go out of your network. Using the file analysis engine helps attain a secure posture for your organization.

FILE SHARING APPLICATIONS

CAPTURE THREAT ASSESSMENT REPORT

FILE SHARING APPLICATIONS

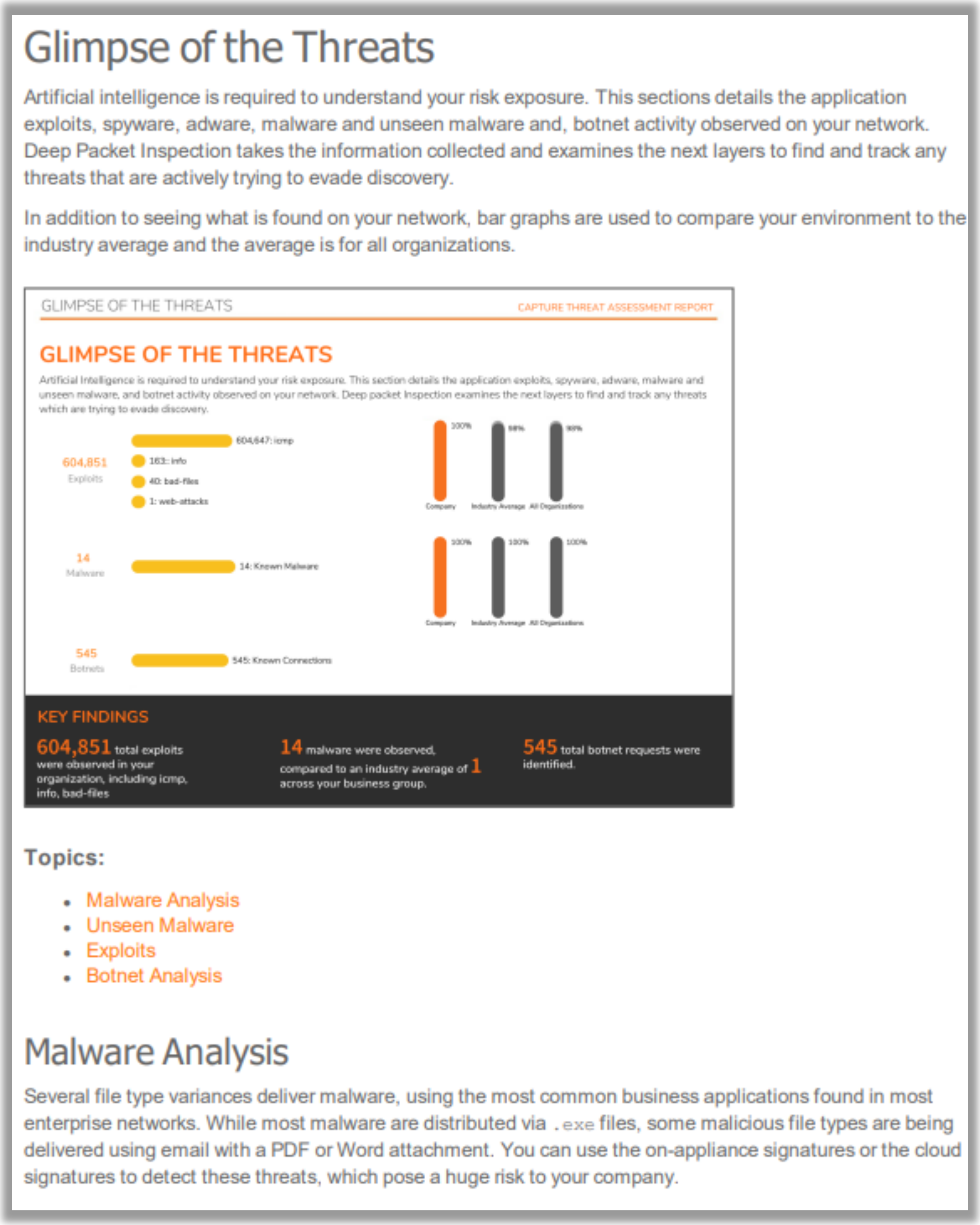
Most businesses need applications that can transfer files. Those applications may also allow sensitive data to go out of your network. Using the file analysis engine helps attain an overall security posture for your organization.

604 document
589 pdf file 1 (http download)
4 pdf file 2 (http download)
7 microsoft office (http download)
4 pdf (p2p)
54 audio video stream
54 mp3 (http download) 1
447 archive
378 pkzip (p2p)
60 gzip (http upload)
8 unix ar (http download)
1 rar 1a (http download)
501 executable
258 pe/coff 4 (http download)
245 java class 2 (http download)
1 pe/coff 1 (p2p)
5 pe/coff 3 (http download)

KEY FINDINGS

28 unique file types were observed.

The graph here connects the applications that are mostly used to transfer files.



Glimpse of the Threats

Artificial intelligence is required to understand your risk exposure. This sections details the application exploits, spyware, adware, malware and unseen malware and, botnet activity observed on your network. Deep Packet Inspection takes the information collected and examines the next layers to find and track any threats that are actively trying to evade discovery.

In addition to seeing what is found on your network, bar graphs are used to compare your environment to the industry average and the average is for all organizations.

GLIMPSE OF THE THREATS CAPTURE THREAT ASSESSMENT REPORT

GLIMPSE OF THE THREATS

Artificial Intelligence is required to understand your risk exposure. This section details the application exploits, spyware, adware, malware and unseen malware, and botnet activity observed on your network. Deep packet Inspection examines the next layers to find and track any threats which are trying to evade discovery.

KEY FINDINGS

604,851 total exploits were observed in your organization, including icmp, info, bad-files

14 malware were observed, compared to an industry average of 1 across your business group.

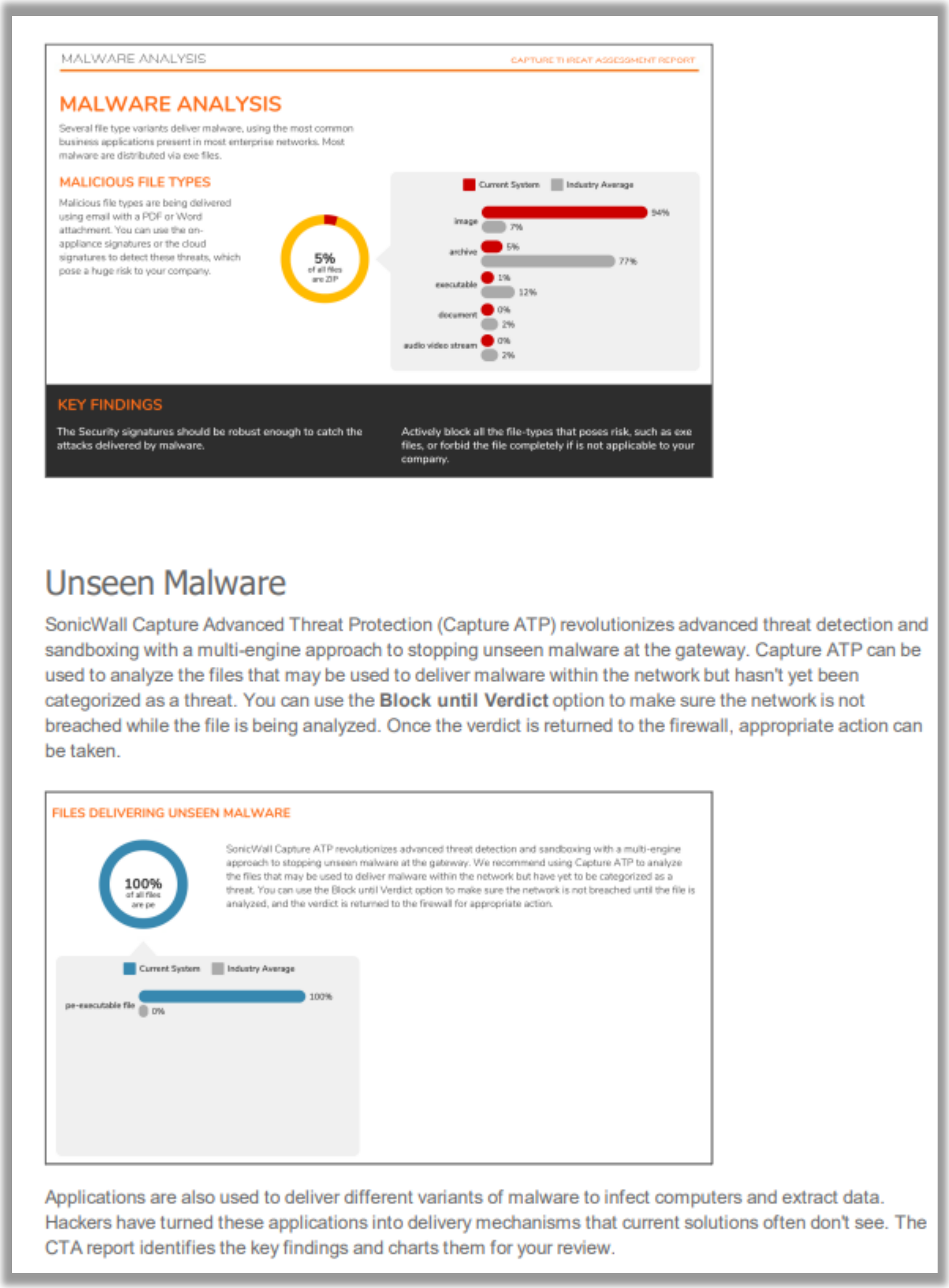
545 total botnet requests were identified.

Topics:

- Malware Analysis
- Unseen Malware
- Exploits
- Botnet Analysis

Malware Analysis

Several file type variances deliver malware, using the most common business applications found in most enterprise networks. While most malware are distributed via `.exe` files, some malicious file types are being delivered using email with a PDF or Word attachment. You can use the on-appliance signatures or the cloud signatures to detect these threats, which pose a huge risk to your company.



MALWARE ANALYSIS CAPTURE THREAT ASSESSMENT REPORT

MALWARE ANALYSIS

Several file type variants deliver malware, using the most common business applications present in most enterprise networks. Most malware are distributed via exe files.

MALICIOUS FILE TYPES

Malicious file types are being delivered using email with a PDF or Word attachment. You can use the on-appliance signatures or the cloud signatures to detect these threats, which pose a huge risk to your company.

KEY FINDINGS

The Security signatures should be robust enough to catch the attacks delivered by malware.

Actively block all the file-types that poses risk, such as exe files, or forbid the file completely if is not applicable to your company.

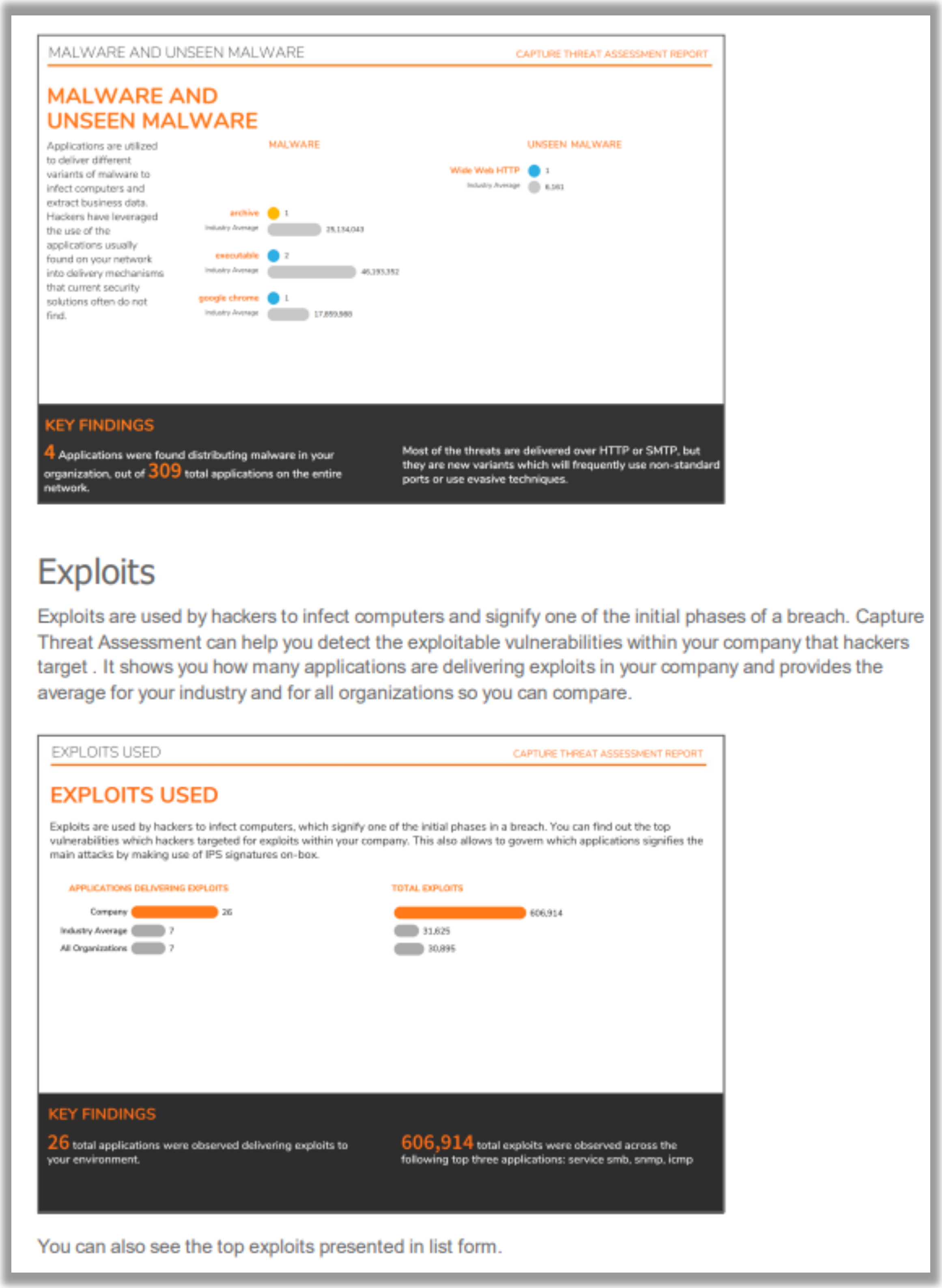
Unseen Malware

SonicWall Capture Advanced Threat Protection (Capture ATP) revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. Capture ATP can be used to analyze the files that may be used to deliver malware within the network but hasn't yet been categorized as a threat. You can use the **Block until Verdict** option to make sure the network is not breached while the file is being analyzed. Once the verdict is returned to the firewall, appropriate action can be taken.

FILES DELIVERING UNSEEN MALWARE

SonicWall Capture ATP revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. We recommend using Capture ATP to analyze the files that may be used to deliver malware within the network but have yet to be categorized as a threat. You can use the Block until Verdict option to make sure the network is not breached until the file is analyzed, and the verdict is returned to the firewall for appropriate action.

Applications are also used to deliver different variants of malware to infect computers and extract data. Hackers have turned these applications into delivery mechanisms that current solutions often don't see. The CTA report identifies the key findings and charts them for your review.



MALWARE AND UNSEEN MALWARE CAPTURE THREAT ASSESSMENT REPORT

MALWARE AND UNSEEN MALWARE

Applications are utilized to deliver different variants of malware to infect computers and extract business data. Hackers have leveraged the use of the applications usually found on your network into delivery mechanisms that current security solutions often do not find.

KEY FINDINGS

4 Applications were found distributing malware in your organization, out of 309 total applications on the entire network.

Most of the threats are delivered over HTTP or SMTP, but they are new variants which will frequently use non-standard ports or use evasive techniques.

Exploits

Exploits are used by hackers to infect computers and signify one of the initial phases of a breach. Capture Threat Assessment can help you detect the exploitable vulnerabilities within your company that hackers target . It shows you how many applications are delivering exploits in your company and provides the average for your industry and for all organizations so you can compare.

EXPLOITS USED CAPTURE THREAT ASSESSMENT REPORT

EXPLOITS USED

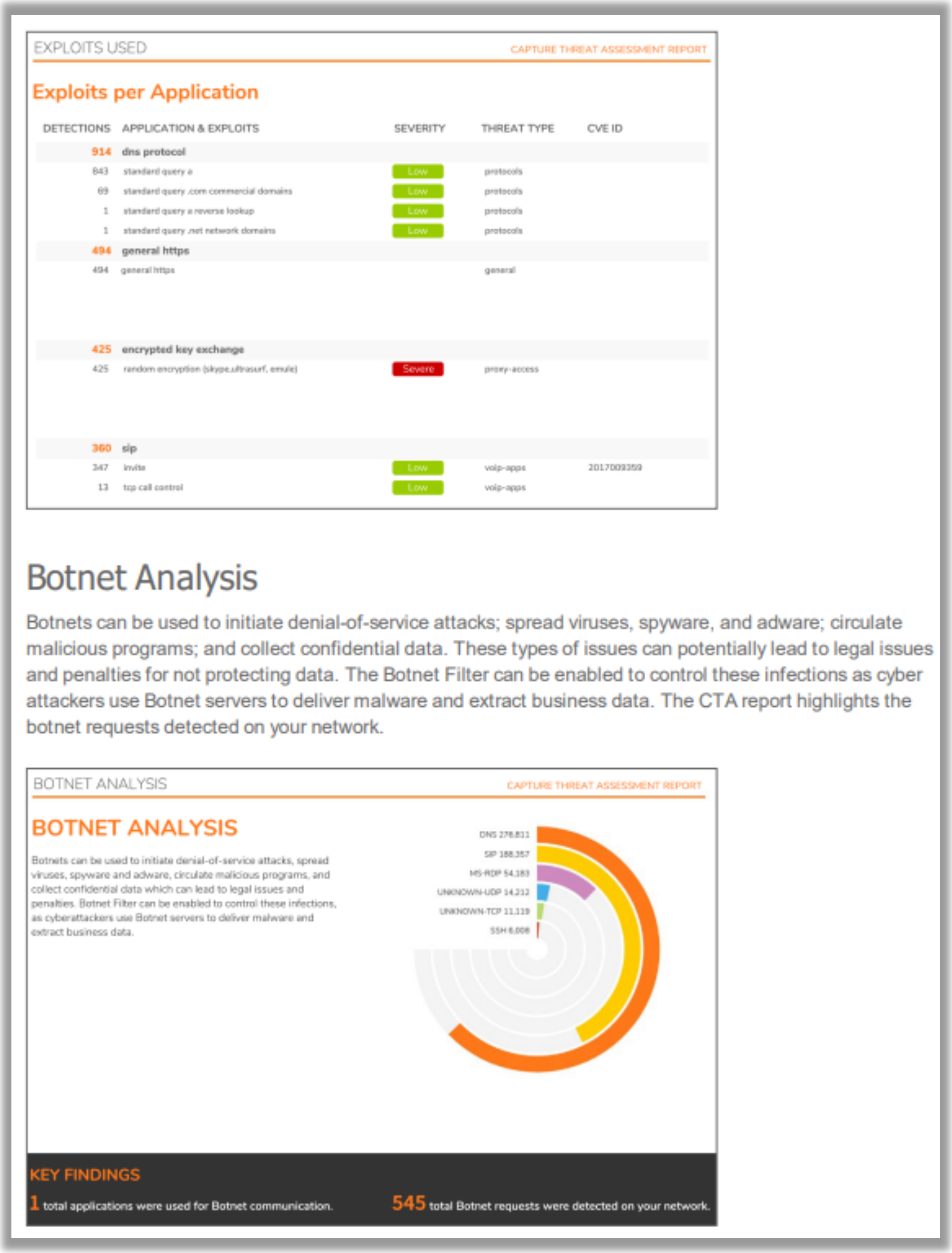
Exploits are used by hackers to infect computers, which signify one of the initial phases in a breach. You can find out the top vulnerabilities which hackers targeted for exploits within your company. This also allows to govern which applications signifies the main attacks by making use of IPS signatures on-box.

KEY FINDINGS

26 total applications were observed delivering exploits to your environment.

606,914 total exploits were observed across the following top three applications: service smb, snmp, icmp

You can also see the top exploits presented in list form.



EXPLOITS USED

CAPTURE THREAT ASSESSMENT REPORT

Exploits per Application

DETECTIONS	APPLICATION & EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
914	**dns protocol**			
843	standard query a	Low	protocols	
69	standard query .com commercial domains	Low	protocols	
1	standard query a reverse lookup	Low	protocols	
1	standard query .net network domains	Low	protocols	
494	**general https**			
494	general https		general	
425	**encrypted key exchange**			
425	random encryption (skype,ultrasurf, emule)	Severe	proxy-access	
360	**sip**			
347	invite	Low	voip-apps	2017009359
13	tcp call control	Low	voip-apps	

Botnet Analysis

Botnets can be used to initiate denial-of-service attacks; spread viruses, spyware, and adware; circulate malicious programs; and collect confidential data. These types of issues can potentially lead to legal issues and penalties for not protecting data. The Botnet Filter can be enabled to control these infections as cyber attackers use Botnet servers to deliver malware and extract business data. The CTA report highlights the botnet requests detected on your network.

BOTNET ANALYSIS

CAPTURE THREAT ASSESSMENT REPORT

BOTNET ANALYSIS

Botnets can be used to initiate denial-of-service attacks, spread viruses, spyware and adware, circulate malicious programs, and collect confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections, as cyberattackers use Botnet servers to deliver malware and extract business data.

KEY FINDINGS

1 total applications were used for Botnet communication.

545 total Botnet requests were detected on your network.

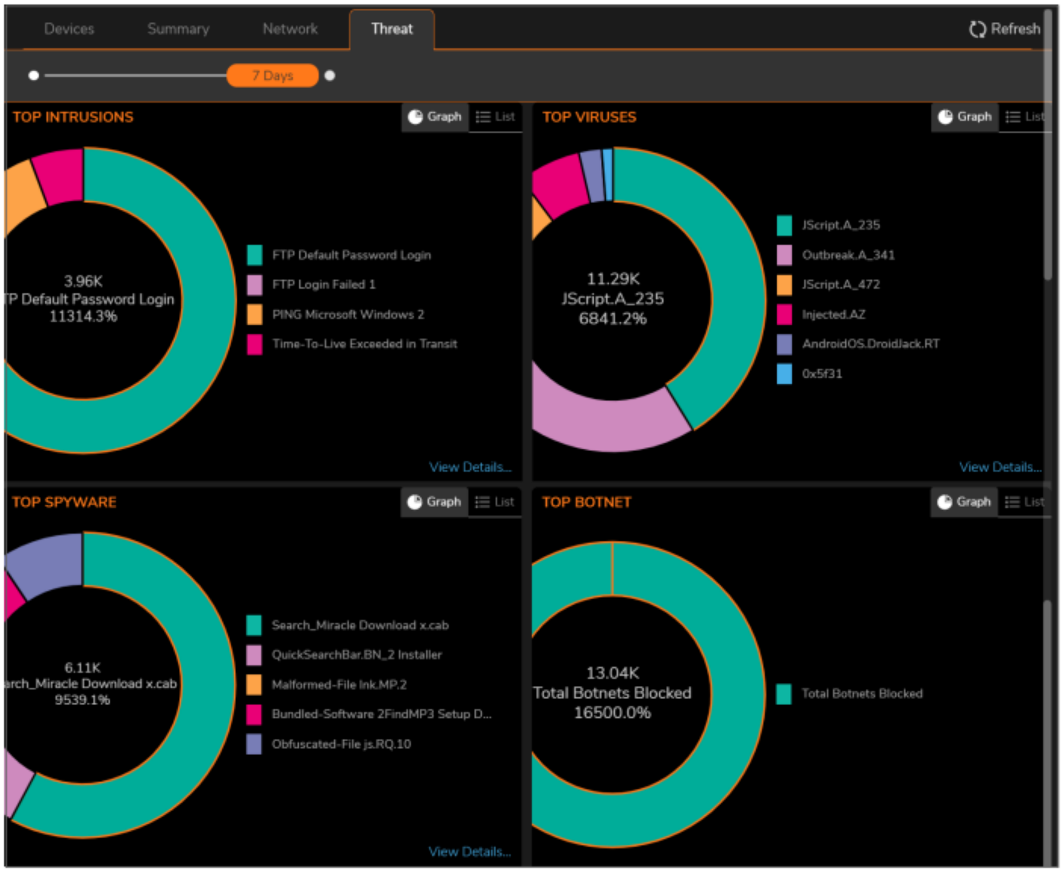
[129]

[129] https://www.sonicwall.com/techdocs/pdf/cta-user_guide.pdf, at 5-16.

124. Every ’616 Accused Product practices generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments. For example, NSM generates threat data at least in part on analyzing the third-party network endpoint assessments (*e.g.*, Capture Threat Assessment).

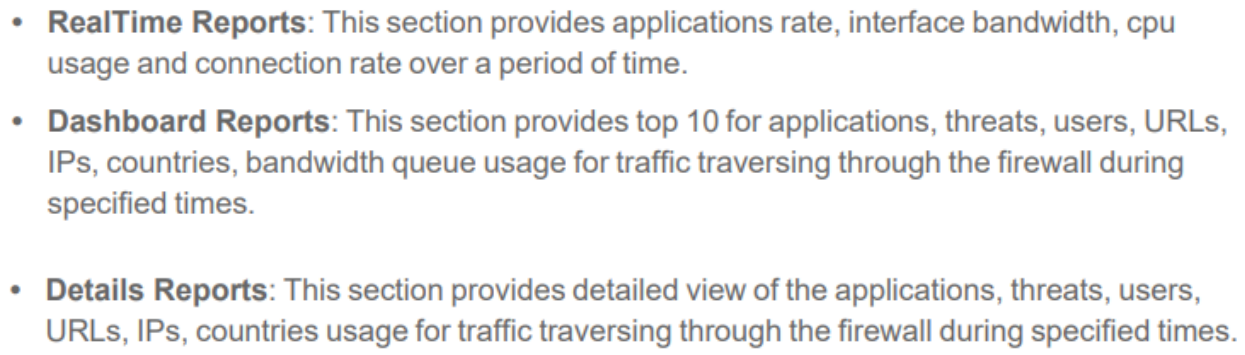
Threat

The **Threat** tab in the **Dashboard > System** page shows top threats by type, including the viruses, intrusions, spyware, and botnet. For more details on threats of a particular threat type, click **View Details**.There is an option to switch to Graph and List view.



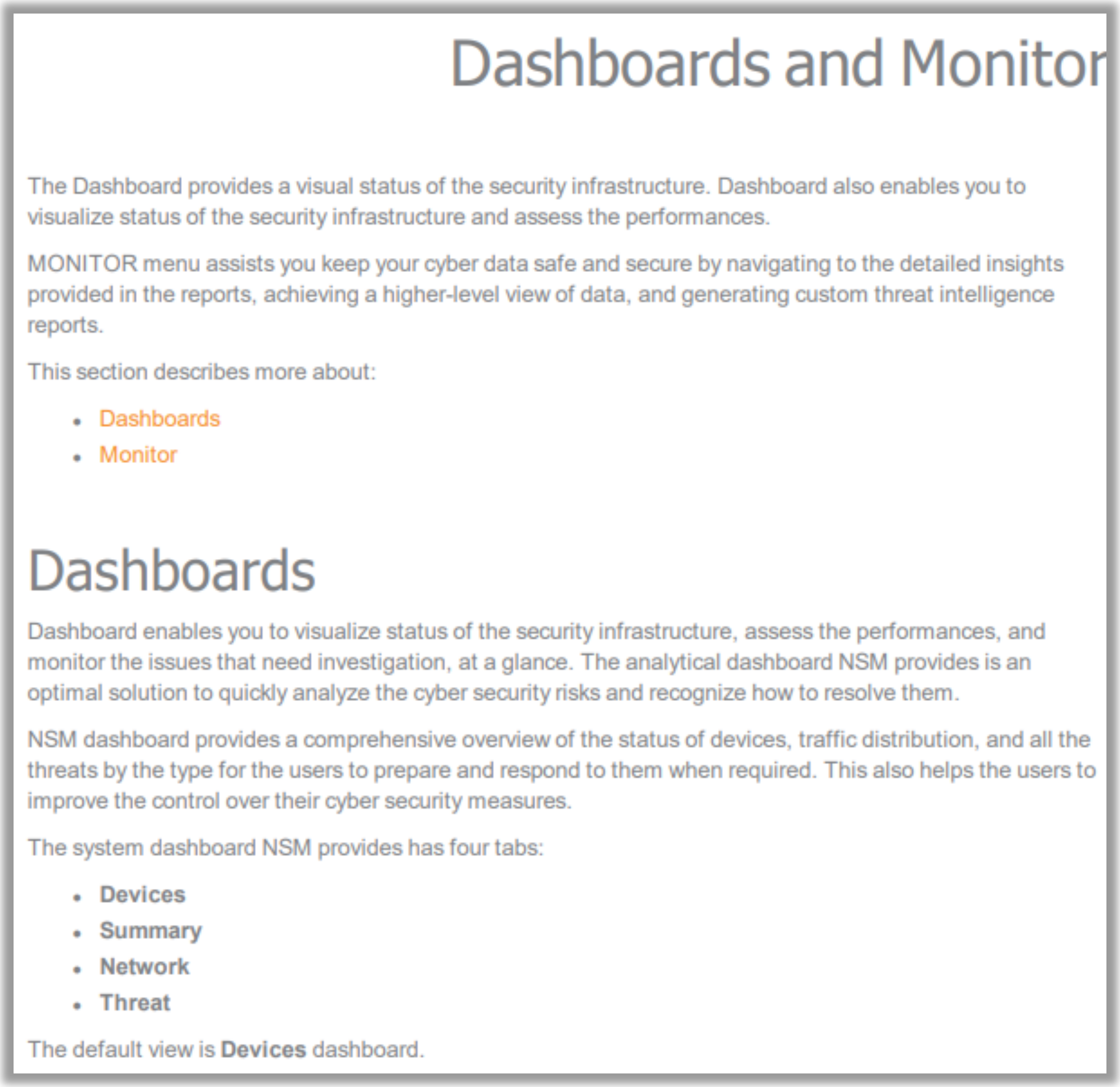
For more information on monitoring the displayed threat data, see *Analytics and Reporting* document available at https://www.sonicwall.com/support/technical-documentation/.[130]

[130] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 15-16.



- **RealTime Reports**: This section provides applications rate, interface bandwidth, cpu usage and connection rate over a period of time.
- **Dashboard Reports**: This section provides top 10 for applications, threats, users, URLs, IPs, countries, bandwidth queue usage for traffic traversing through the firewall during specified times.
- **Details Reports**: This section provides detailed view of the applications, threats, users, URLs, IPs, countries usage for traffic traversing through the firewall during specified times.

[131]



Dashboards and Monitor

The Dashboard provides a visual status of the security infrastructure. Dashboard also enables you to visualize status of the security infrastructure and assess the performances.

MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports.

This section describes more about:

- Dashboards
- Monitor

Dashboards

Dashboard enables you to visualize status of the security infrastructure, assess the performances, and monitor the issues that need investigation, at a glance. The analytical dashboard NSM provides is an optimal solution to quickly analyze the cyber security risks and recognize how to resolve them.

NSM dashboard provides a comprehensive overview of the status of devices, traffic distribution, and all the threats by the type for the users to prepare and respond to them when required. This also helps the users to improve the control over their cyber security measures.

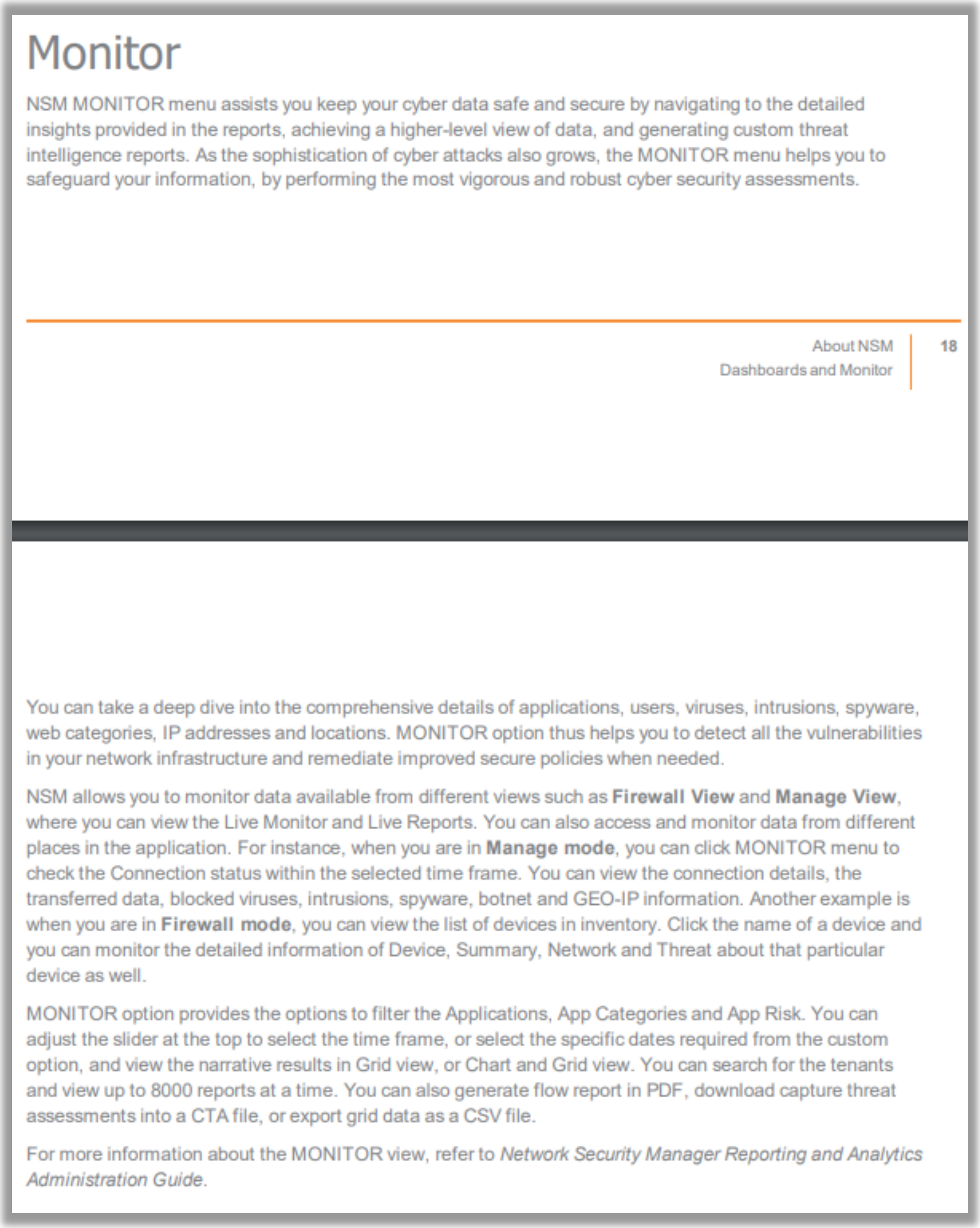
The system dashboard NSM provides has four tabs:

- **Devices**
- **Summary**
- **Network**
- **Threat**

The default view is **Devices** dashboard.

[132]

[131] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 125-126.
[132] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 16.



Monitor

NSM MONITOR menu assists you keep your cyber data safe and secure by navigating to the detailed insights provided in the reports, achieving a higher-level view of data, and generating custom threat intelligence reports. As the sophistication of cyber attacks also grows, the MONITOR menu helps you to safeguard your information, by performing the most vigorous and robust cyber security assessments.

About NSM
Dashboards and Monitor | 18

You can take a deep dive into the comprehensive details of applications, users, viruses, intrusions, spyware, web categories, IP addresses and locations. MONITOR option thus helps you to detect all the vulnerabilities in your network infrastructure and remediate improved secure policies when needed.

NSM allows you to monitor data available from different views such as **Firewall View** and **Manage View**, where you can view the Live Monitor and Live Reports. You can also access and monitor data from different places in the application. For instance, when you are in **Manage mode**, you can click MONITOR menu to check the Connection status within the selected time frame. You can view the connection details, the transferred data, blocked viruses, intrusions, spyware, botnet and GEO-IP information. Another example is when you are in **Firewall mode**, you can view the list of devices in inventory. Click the name of a device and you can monitor the detailed information of Device, Summary, Network and Threat about that particular device as well.

MONITOR option provides the options to filter the Applications, App Categories and App Risk. You can adjust the slider at the top to select the time frame, or select the specific dates required from the custom option, and view the narrative results in Grid view, or Chart and Grid view. You can search for the tenants and view up to 8000 reports at a time. You can also generate flow report in PDF, download capture threat assessments into a CTA file, or export grid data as a CSV file.

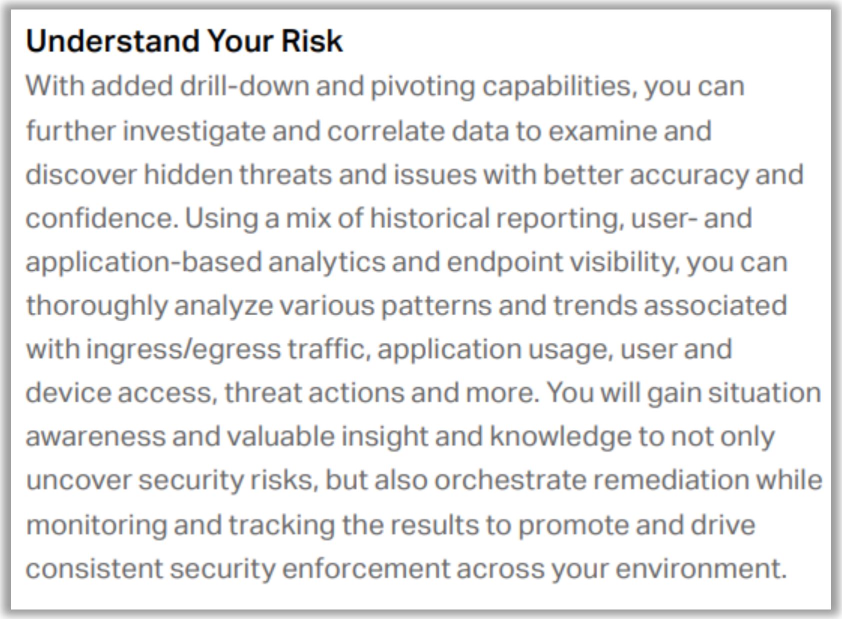
For more information about the MONITOR view, refer to *Network Security Manager Reporting and Analytics Administration Guide*.

[133]

125. Every '616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, Network Security

[133] https://www.sonicwall.com/techdocs/pdf/nsm-about_guide.pdf, at 18-19.

Manager correlates the received endpoint events and the generated temporal events (*e.g.*, correlate data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions and more.").

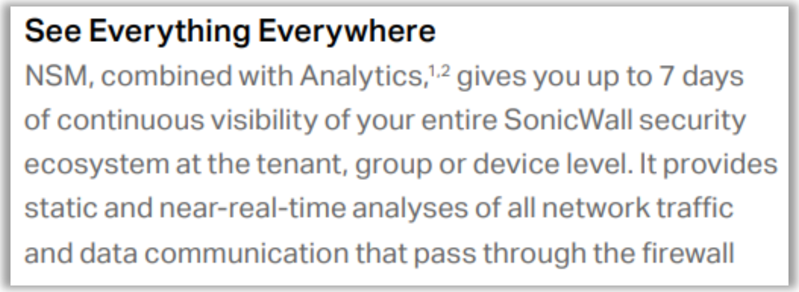


Understand Your Risk

With added drill-down and pivoting capabilities, you can further investigate and correlate data to examine and discover hidden threats and issues with better accuracy and confidence. Using a mix of historical reporting, user- and application-based analytics and endpoint visibility, you can thoroughly analyze various patterns and trends associated with ingress/egress traffic, application usage, user and device access, threat actions and more. You will gain situation awareness and valuable insight and knowledge to not only uncover security risks, but also orchestrate remediation while monitoring and tracking the results to promote and drive consistent security enforcement across your environment.

[134]

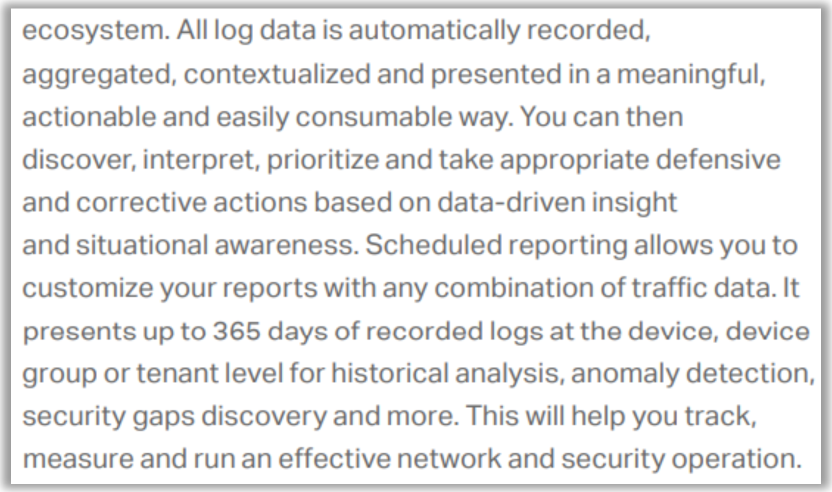
126. Every '616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, Network Security Manager generates an integrity profile for the system through scheduled reporting and "recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more."



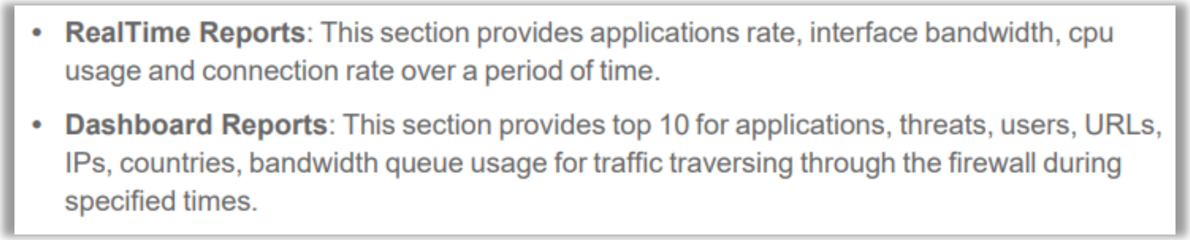
See Everything Everywhere

NSM, combined with Analytics,[1,2] gives you up to 7 days of continuous visibility of your entire SonicWall security ecosystem at the tenant, group or device level. It provides static and near-real-time analyses of all network traffic and data communication that pass through the firewall

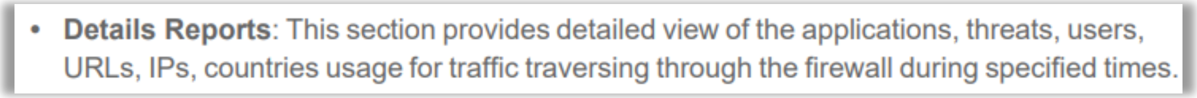
[134] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf



ecosystem. All log data is automatically recorded, aggregated, contextualized and presented in a meaningful, actionable and easily consumable way. You can then discover, interpret, prioritize and take appropriate defensive and corrective actions based on data-driven insight and situational awareness. Scheduled reporting allows you to customize your reports with any combination of traffic data. It presents up to 365 days of recorded logs at the device, device group or tenant level for historical analysis, anomaly detection, security gaps discovery and more. This will help you track, measure and run an effective network and security operation.[135]



- **RealTime Reports**: This section provides applications rate, interface bandwidth, cpu usage and connection rate over a period of time.
- **Dashboard Reports**: This section provides top 10 for applications, threats, users, URLs, IPs, countries, bandwidth queue usage for traffic traversing through the firewall during specified times.



- **Details Reports**: This section provides detailed view of the applications, threats, users, URLs, IPs, countries usage for traffic traversing through the firewall during specified times.[136]

127. Defendant has and continues to directly infringe one or more claims of the ’616 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

128. Defendant has and continues to indirectly infringe one or more claims of the ’616 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’616 Accused Products.

[135] https://www.sonicwall.com/medialibrary/en/datasheet/network-security-manager.pdf

[136] https://www.sonicwall.com/techdocs/pdf/nsm-administration.pdf, at 125-126.

129. Defendant has and continues to indirectly infringe one or more claims of the ’616 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’616 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’616 Patent by providing these products to customers and end-users for use in an infringing manner.

130. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’616 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[137] Video Tutorials,[138] SonicWall University,[139] and Customer Service[140] websites.

131. Defendant has and continues to indirectly infringe one or more claims of the ’616 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’616 Patent. Such components include, for example, SonicWall’s network

[137] https://www.sonicwall.com/support/technical-documentation/?language=English

[138] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[139] https://www.sonicwall.com/partners/sonicwall-university/

[140] https://www.sonicwall.com/support/contact-support/customer-service/

security appliances such as firewalls. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’616 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’616 Patent but remained willfully blind to the infringing nature of others’ actions.

132. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’616 Patent in an amount to be proved at trial.

133. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’616 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

134. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’616 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’616 Patent. Upon information and belief, Defendant had actual knowledge of the ’616 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’616 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT VII
(Infringement of the ’038 Patent)

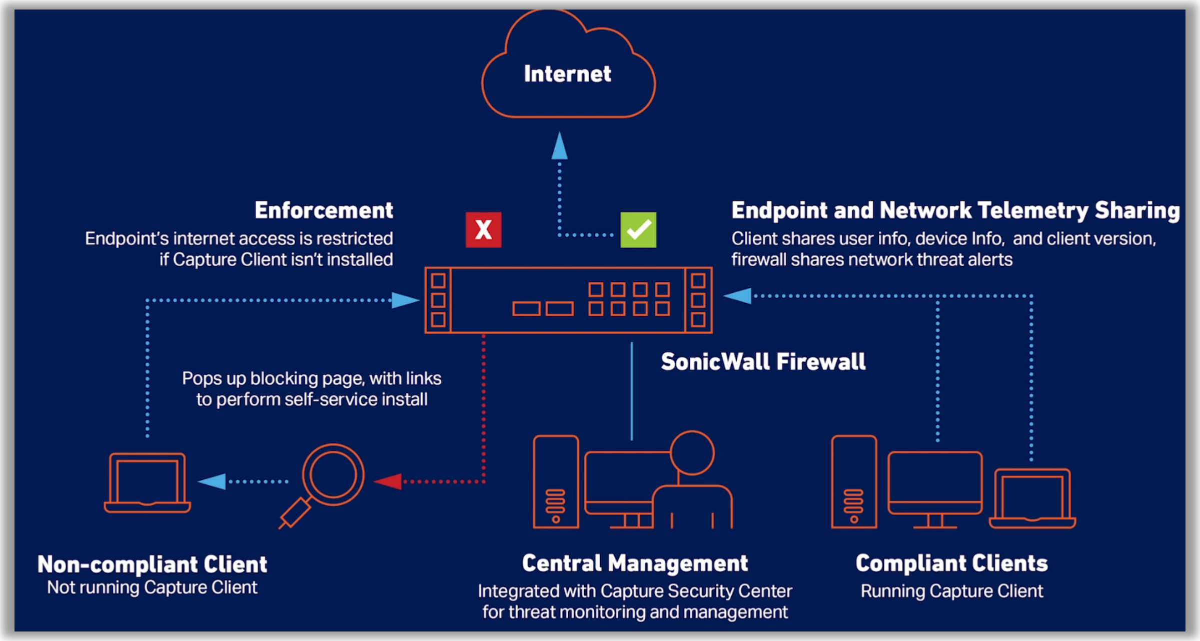
135. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

136. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’038 Patent.

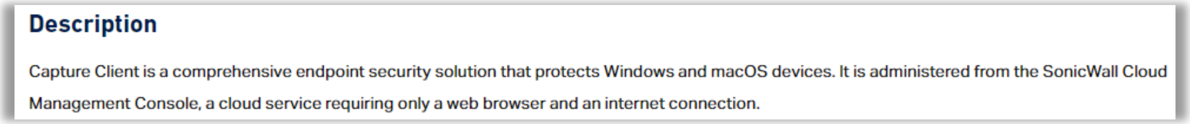
137. Defendant has and continues to directly infringe the ’038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’038 Patent. Such products include at least SonicWall Capture Client alone, or in combination with SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) (the “’038 Accused Products”) which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and initiating, by the computing system, based on the compliance state, an

action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

138. Every ’038 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies. For example, Capture Client “is administered from the SonicWall Cloud Management Console” (e.g., a computing system remote from the endpoint), “a cloud service requiring only a web browser and an internet connection.


Internet
Enforcement
Endpoint’s internet access is restricted if Capture Client isn’t installed
X
✓
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center for threat monitoring and management
Compliant Clients
Running Capture Client

[141]



Description

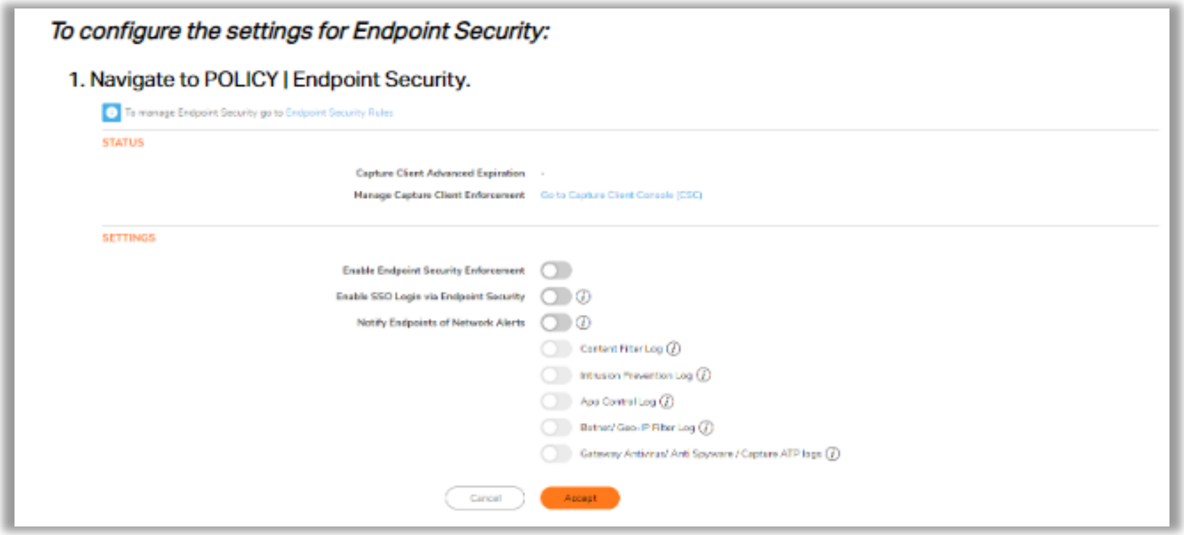
Capture Client is a comprehensive endpoint security solution that protects Windows and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection.

[142]

[141] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[142] https://www.sonicwall.com/support/knowledge-base/capture-client-system-requirements/210512075820480/

139. Every ’038 Accused Product practices maintaining the plurality of policies in a data store on the computing system. For example, Capture Client allows the storage of various endpoint security policies: “POLICY | Endpoint Security.” These policies can later be managed through the Capture Client Console, indicating that they are stored on the computing system.



To configure the settings for Endpoint Security:

1. Navigate to POLICY | Endpoint Security.

To manage Endpoint Security go to Endpoint Security Rules

STATUS

Capture Client Advanced Expiration -

Manage Capture Client Enforcement Go to Capture Client Console (CSC)

SETTINGS

Enable Endpoint Security Enforcement

Enable SSO Login via Endpoint Security

Notify Endpoints of Network Alerts

Content Filter Log

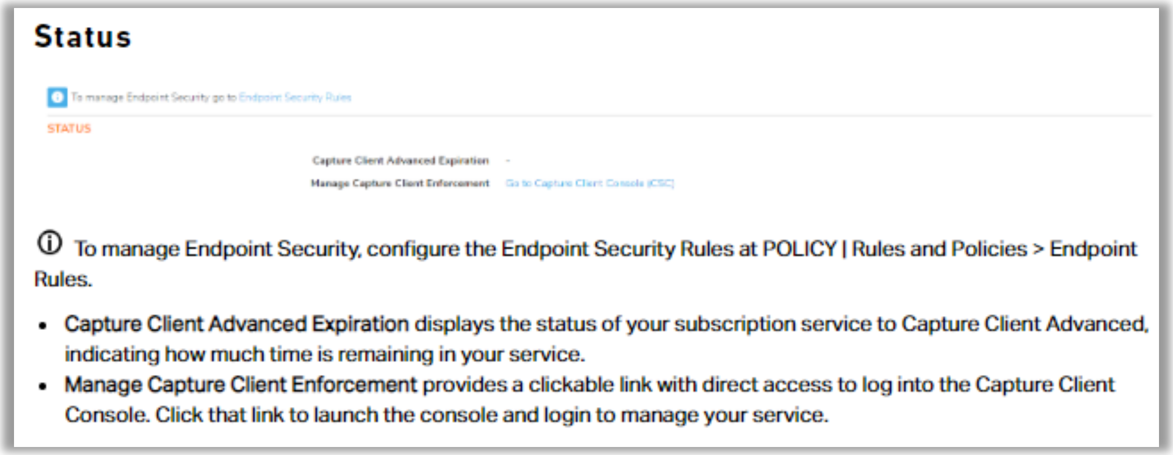
Intrusion Prevention Log

App Control Log

Botnet/ Geo-IP Filter Log

Gateway Antivirus/ Anti Spyware / Capture ATP logs

[143]



Status

To manage Endpoint Security go to Endpoint Security Rules

STATUS

Capture Client Advanced Expiration -

Manage Capture Client Enforcement Go to Capture Client Console (CSC)

ⓘ To manage Endpoint Security, configure the Endpoint Security Rules at POLICY | Rules and Policies > Endpoint Rules.

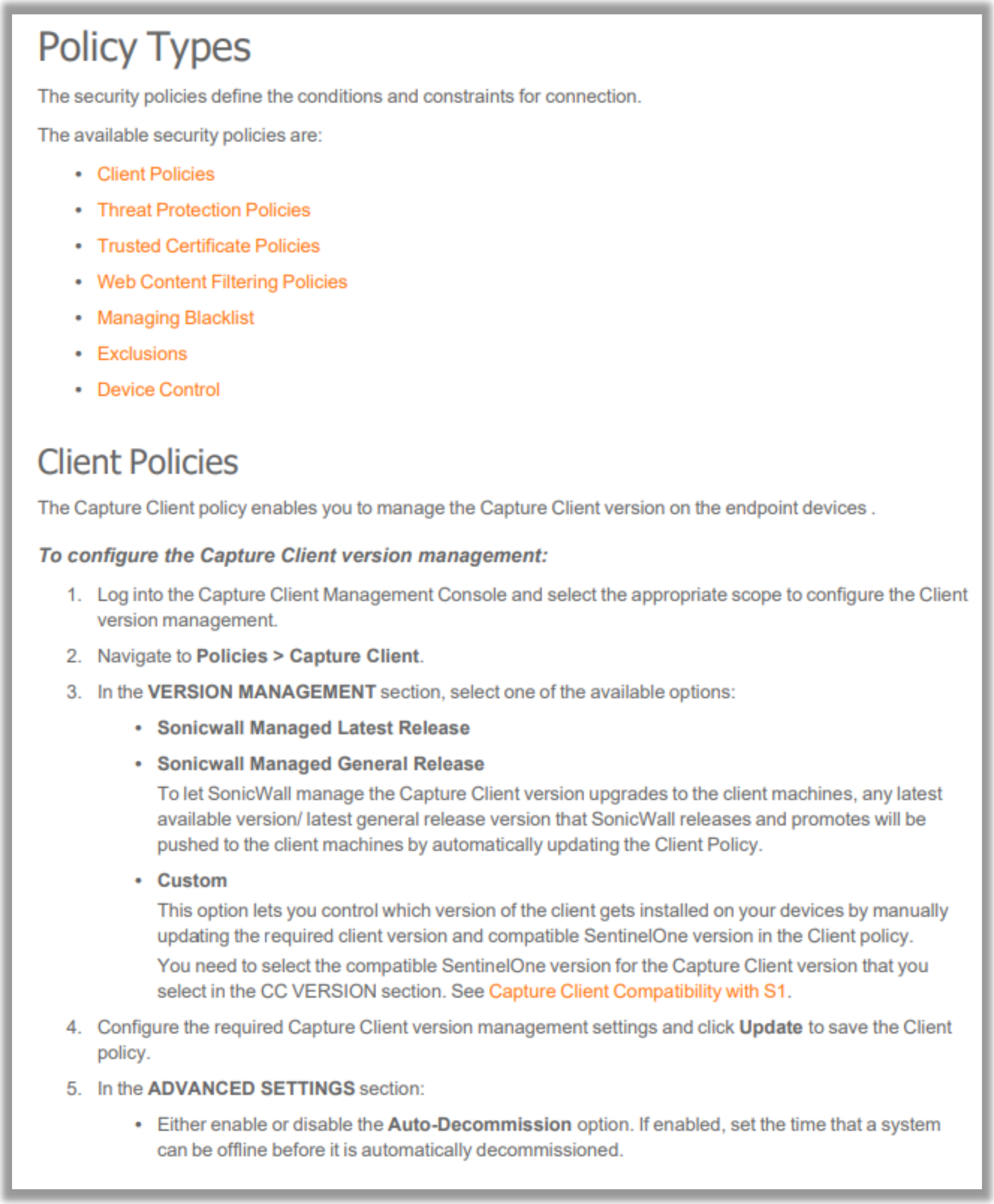
- **Capture Client Advanced Expiration** displays the status of your subscription service to Capture Client Advanced, indicating how much time is remaining in your service.
- **Manage Capture Client Enforcement** provides a clickable link with direct access to log into the Capture Client Console. Click that link to launch the console and login to manage your service.

[144]

[143] https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-endpoint_security/Content/endpoint-security.htm/

[144] https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-endpoint_security/Content/endpoint-security-status.htm/

140. Every ’038 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Capture Client identifies, from the plurality of policies, operating conditions (*e.g.*, threats and suspicious activities) on the endpoint to monitor in order to determine mitigation mode: Detect, Protect, or Capture ATP.



Policy Types

The security policies define the conditions and constraints for connection.

The available security policies are:

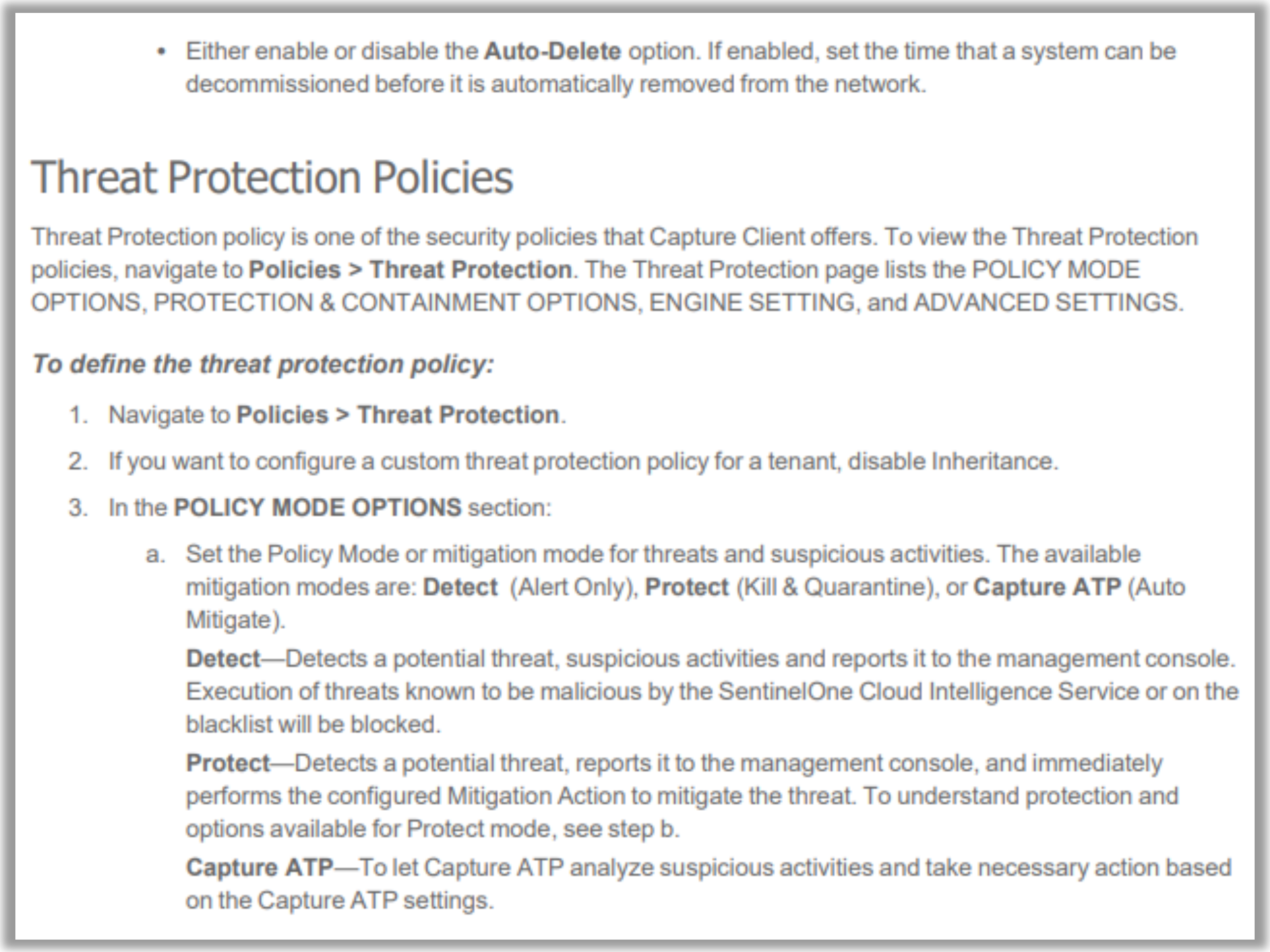
- Client Policies
- Threat Protection Policies
- Trusted Certificate Policies
- Web Content Filtering Policies
- Managing Blacklist
- Exclusions
- Device Control

Client Policies

The Capture Client policy enables you to manage the Capture Client version on the endpoint devices .

To configure the Capture Client version management:

1. Log into the Capture Client Management Console and select the appropriate scope to configure the Client version management.
2. Navigate to **Policies > Capture Client**.
3. In the **VERSION MANAGEMENT** section, select one of the available options:
    - **Sonicwall Managed Latest Release**
    - **Sonicwall Managed General Release**
      To let SonicWall manage the Capture Client version upgrades to the client machines, any latest available version/ latest general release version that SonicWall releases and promotes will be pushed to the client machines by automatically updating the Client Policy.
    - **Custom**
      This option lets you control which version of the client gets installed on your devices by manually updating the required client version and compatible SentinelOne version in the Client policy.
      You need to select the compatible SentinelOne version for the Capture Client version that you select in the CC VERSION section. See Capture Client Compatibility with S1.
4. Configure the required Capture Client version management settings and click **Update** to save the Client policy.
5. In the **ADVANCED SETTINGS** section:
    - Either enable or disable the **Auto-Decommission** option. If enabled, set the time that a system can be offline before it is automatically decommissioned.



- Either enable or disable the **Auto-Delete** option. If enabled, set the time that a system can be decommissioned before it is automatically removed from the network.

Threat Protection Policies

Threat Protection policy is one of the security policies that Capture Client offers. To view the Threat Protection policies, navigate to **Policies > Threat Protection**. The Threat Protection page lists the POLICY MODE OPTIONS, PROTECTION & CONTAINMENT OPTIONS, ENGINE SETTING, and ADVANCED SETTINGS.

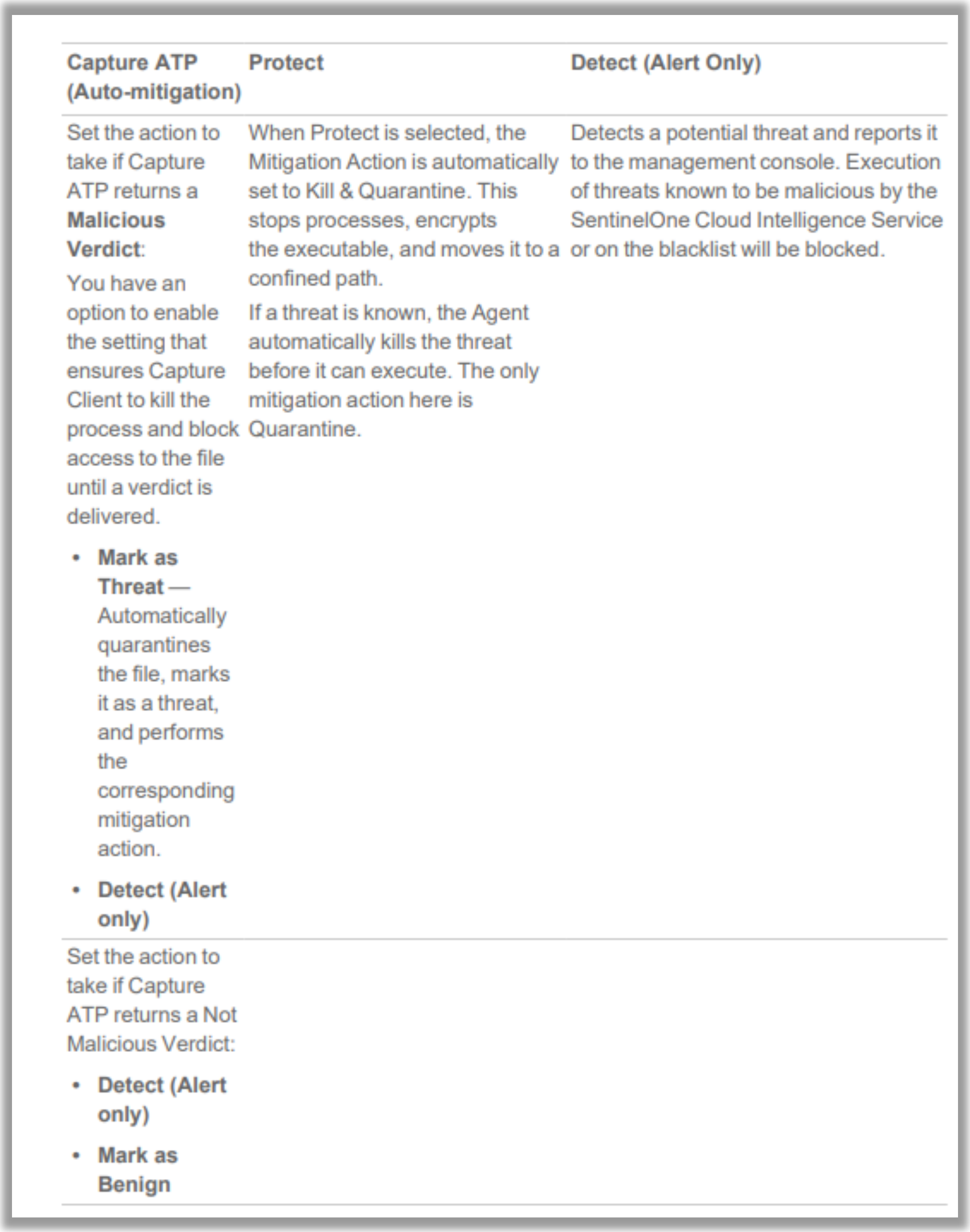
To define the threat protection policy:

1. Navigate to **Policies > Threat Protection**.
2. If you want to configure a custom threat protection policy for a tenant, disable Inheritance.
3. In the **POLICY MODE OPTIONS** section:
   a. Set the Policy Mode or mitigation mode for threats and suspicious activities. The available mitigation modes are: **Detect** (Alert Only), **Protect** (Kill & Quarantine), or **Capture ATP** (Auto Mitigate).

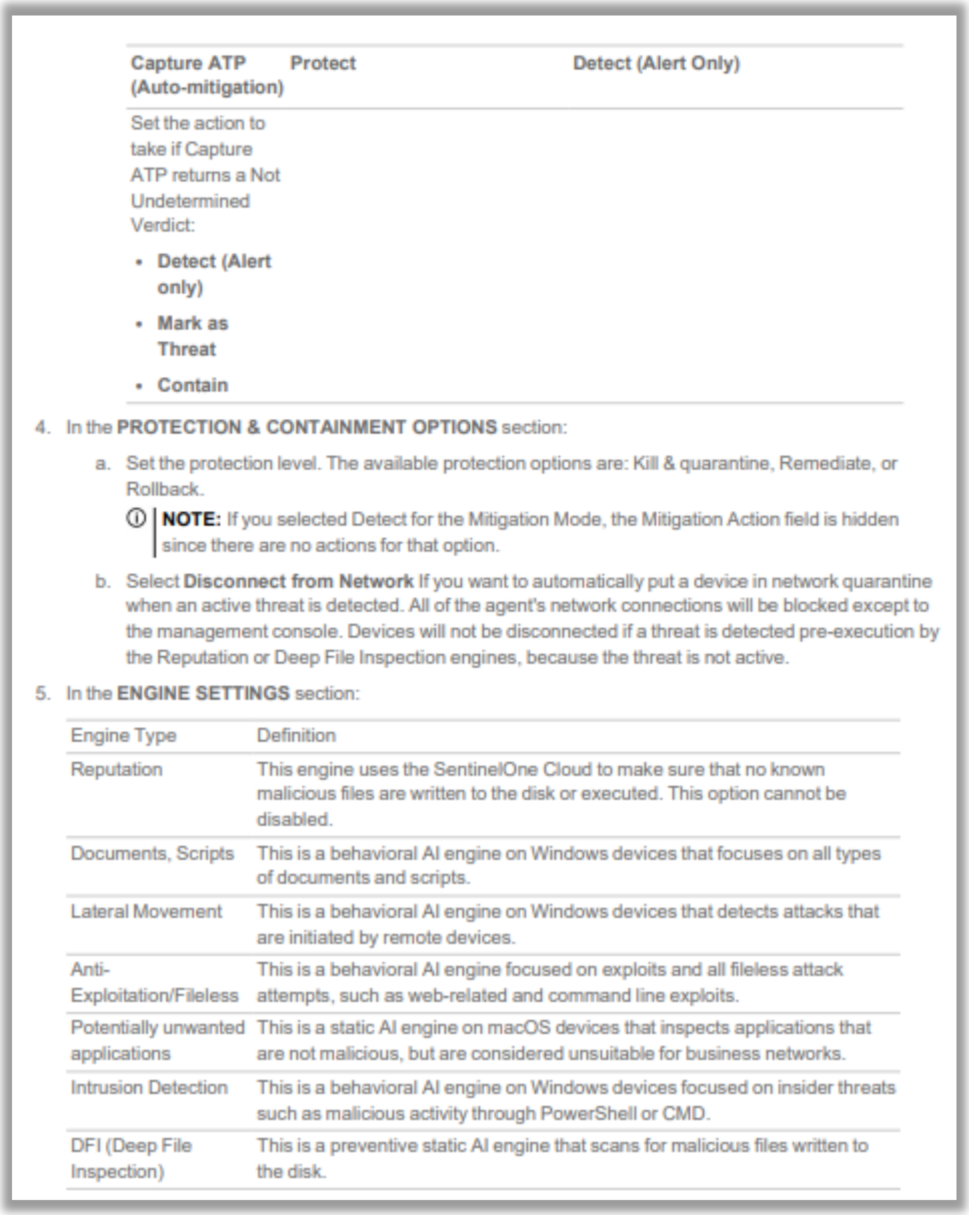
      Detect—Detects a potential threat, suspicious activities and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.

      Protect—Detects a potential threat, reports it to the management console, and immediately performs the configured Mitigation Action to mitigate the threat. To understand protection and options available for Protect mode, see step b.

      Capture ATP—To let Capture ATP analyze suspicious activities and take necessary action based on the Capture ATP settings.



Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a **Malicious Verdict**: You have an option to enable the setting that ensures Capture Client to kill the process and block access to the file until a verdict is delivered. • **Mark as Threat** — Automatically quarantines the file, marks it as a threat, and performs the corresponding mitigation action. • **Detect (Alert only)**	When Protect is selected, the Mitigation Action is automatically set to Kill & Quarantine. This stops processes, encrypts the executable, and moves it to a confined path. If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action here is Quarantine.	Detects a potential threat and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.
Set the action to take if Capture ATP returns a Not Malicious Verdict: • **Detect (Alert only)** • **Mark as Benign**		



Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a Not Undetermined Verdict: • **Detect (Alert only)** • **Mark as Threat** • **Contain**		

4. In the **PROTECTION & CONTAINMENT OPTIONS** section:

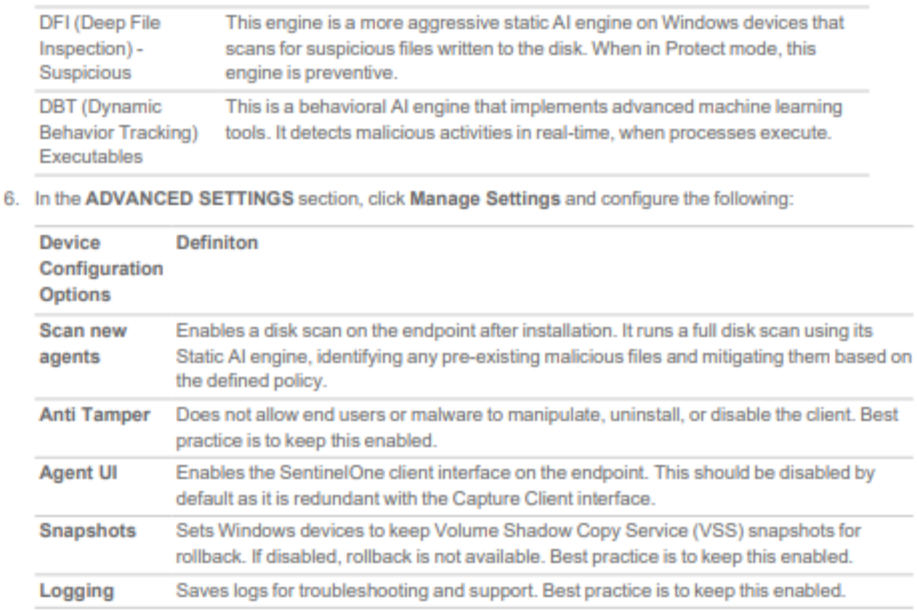
   a. Set the protection level. The available protection options are: Kill & quarantine, Remediate, or Rollback.

   ⓘ **NOTE:** If you selected Detect for the Mitigation Mode, the Mitigation Action field is hidden since there are no actions for that option.

   b. Select **Disconnect from Network** If you want to automatically put a device in network quarantine when an active threat is detected. All of the agent's network connections will be blocked except to the management console. Devices will not be disconnected if a threat is detected pre-execution by the Reputation or Deep File Inspection engines, because the threat is not active.

5. In the **ENGINE SETTINGS** section:

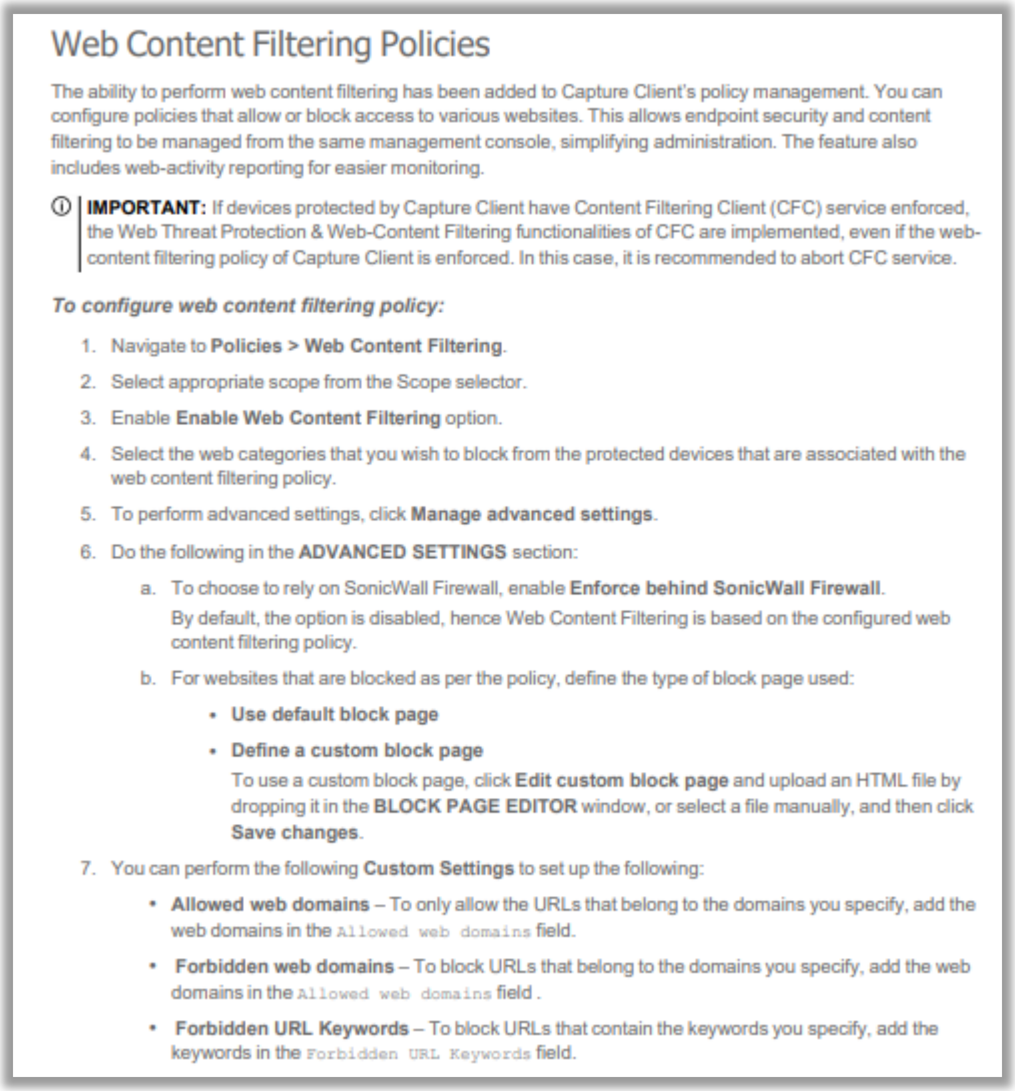
Engine Type	Definition
Reputation	This engine uses the SentinelOne Cloud to make sure that no known malicious files are written to the disk or executed. This option cannot be disabled.
Documents, Scripts	This is a behavioral AI engine on Windows devices that focuses on all types of documents and scripts.
Lateral Movement	This is a behavioral AI engine on Windows devices that detects attacks that are initiated by remote devices.
Anti-Exploitation/Fileless	This is a behavioral AI engine focused on exploits and all fileless attack attempts, such as web-related and command line exploits.
Potentially unwanted applications	This is a static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.
Intrusion Detection	This is a behavioral AI engine on Windows devices focused on insider threats such as malicious activity through PowerShell or CMD.
DFI (Deep File Inspection)	This is a preventive static AI engine that scans for malicious files written to the disk.



DFI (Deep File Inspection) - Suspicious	This engine is a more aggressive static AI engine on Windows devices that scans for suspicious files written to the disk. When in Protect mode, this engine is preventive.
DBT (Dynamic Behavior Tracking) Executables	This is a behavioral AI engine that implements advanced machine learning tools. It detects malicious activities in real-time, when processes execute.

6. In the **ADVANCED SETTINGS** section, click **Manage Settings** and configure the following:

Device Configuration Options	**Definiton**
Scan new agents	Enables a disk scan on the endpoint after installation. It runs a full disk scan using its Static AI engine, identifying any pre-existing malicious files and mitigating them based on the defined policy.
Anti Tamper	Does not allow end users or malware to manipulate, uninstall, or disable the client. Best practice is to keep this enabled.
Agent UI	Enables the SentinelOne client interface on the endpoint. This should be disabled by default as it is redundant with the Capture Client interface.
Snapshots	Sets Windows devices to keep Volume Shadow Copy Service (VSS) snapshots for rollback. If disabled, rollback is not available. Best practice is to keep this enabled.
Logging	Saves logs for troubleshooting and support. Best practice is to keep this enabled.



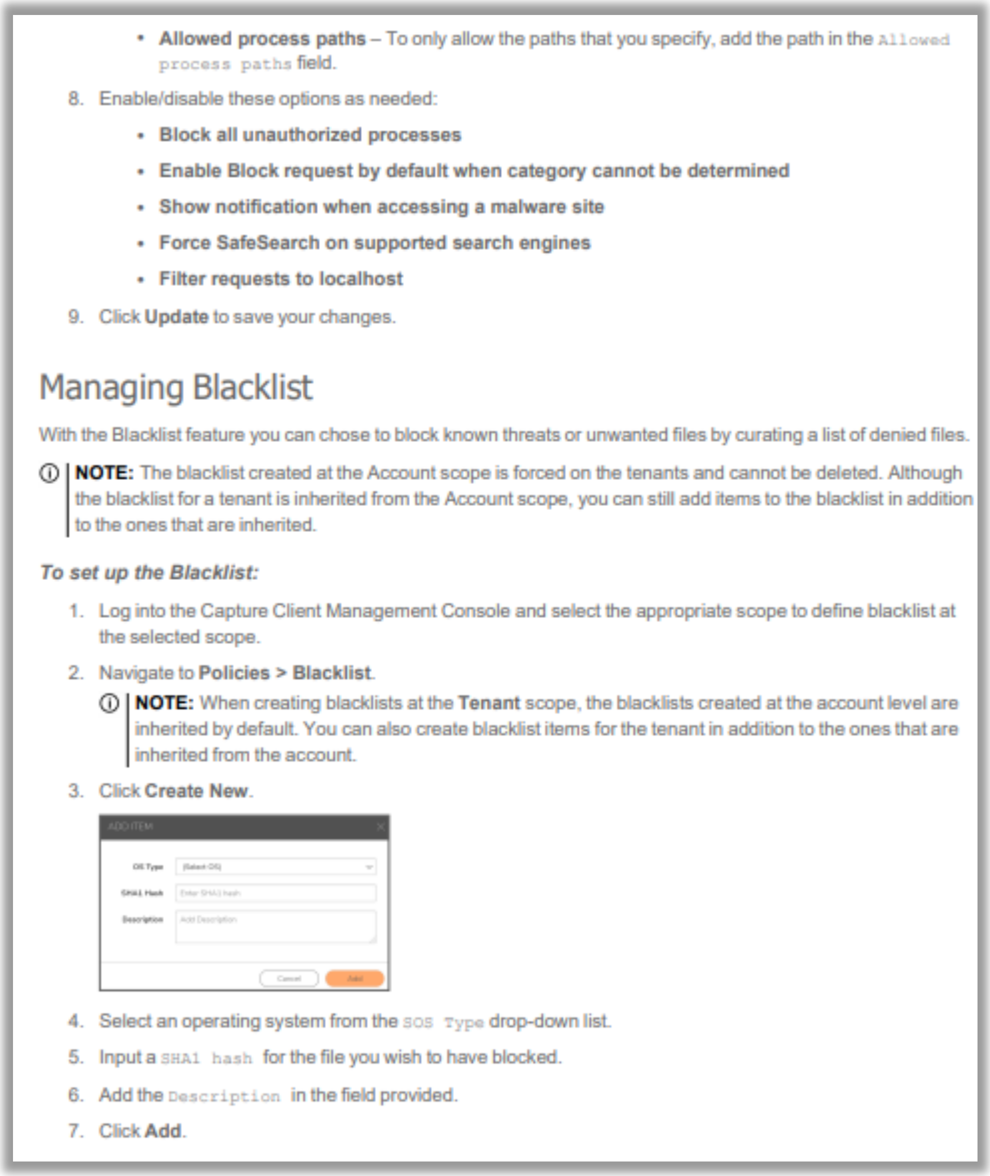
Web Content Filtering Policies

The ability to perform web content filtering has been added to Capture Client's policy management. You can configure policies that allow or block access to various websites. This allows endpoint security and content filtering to be managed from the same management console, simplifying administration. The feature also includes web-activity reporting for easier monitoring.

ⓘ **IMPORTANT:** If devices protected by Capture Client have Content Filtering Client (CFC) service enforced, the Web Threat Protection & Web-Content Filtering functionalities of CFC are implemented, even if the web-content filtering policy of Capture Client is enforced. In this case, it is recommended to abort CFC service.

To configure web content filtering policy:

1. Navigate to **Policies > Web Content Filtering**.
2. Select appropriate scope from the Scope selector.
3. Enable **Enable Web Content Filtering** option.
4. Select the web categories that you wish to block from the protected devices that are associated with the web content filtering policy.
5. To perform advanced settings, click **Manage advanced settings**.
6. Do the following in the **ADVANCED SETTINGS** section:
   a. To choose to rely on SonicWall Firewall, enable **Enforce behind SonicWall Firewall**.
      By default, the option is disabled, hence Web Content Filtering is based on the configured web content filtering policy.
   b. For websites that are blocked as per the policy, define the type of block page used:
      - **Use default block page**
      - **Define a custom block page**
        To use a custom block page, click **Edit custom block page** and upload an HTML file by dropping it in the **BLOCK PAGE EDITOR** window, or select a file manually, and then click **Save changes**.
7. You can perform the following **Custom Settings** to set up the following:
   - **Allowed web domains** – To only allow the URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field.
   - **Forbidden web domains** – To block URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field .
   - **Forbidden URL Keywords** – To block URLs that contain the keywords you specify, add the keywords in the `Forbidden URL Keywords` field.



- **Allowed process paths** – To only allow the paths that you specify, add the path in the `Allowed process paths` field.

8. Enable/disable these options as needed:
   - **Block all unauthorized processes**
   - **Enable Block request by default when category cannot be determined**
   - **Show notification when accessing a malware site**
   - **Force SafeSearch on supported search engines**
   - **Filter requests to localhost**
9. Click **Update** to save your changes.

Managing Blacklist

With the Blacklist feature you can chose to block known threats or unwanted files by curating a list of denied files.

ⓘ **NOTE:** The blacklist created at the Account scope is forced on the tenants and cannot be deleted. Although the blacklist for a tenant is inherited from the Account scope, you can still add items to the blacklist in addition to the ones that are inherited.

To set up the Blacklist:

1. Log into the Capture Client Management Console and select the appropriate scope to define blacklist at the selected scope.
2. Navigate to **Policies > Blacklist**.

   ⓘ **NOTE:** When creating blacklists at the **Tenant** scope, the blacklists created at the account level are inherited by default. You can also create blacklist items for the tenant in addition to the ones that are inherited from the account.
3. Click **Create New**.

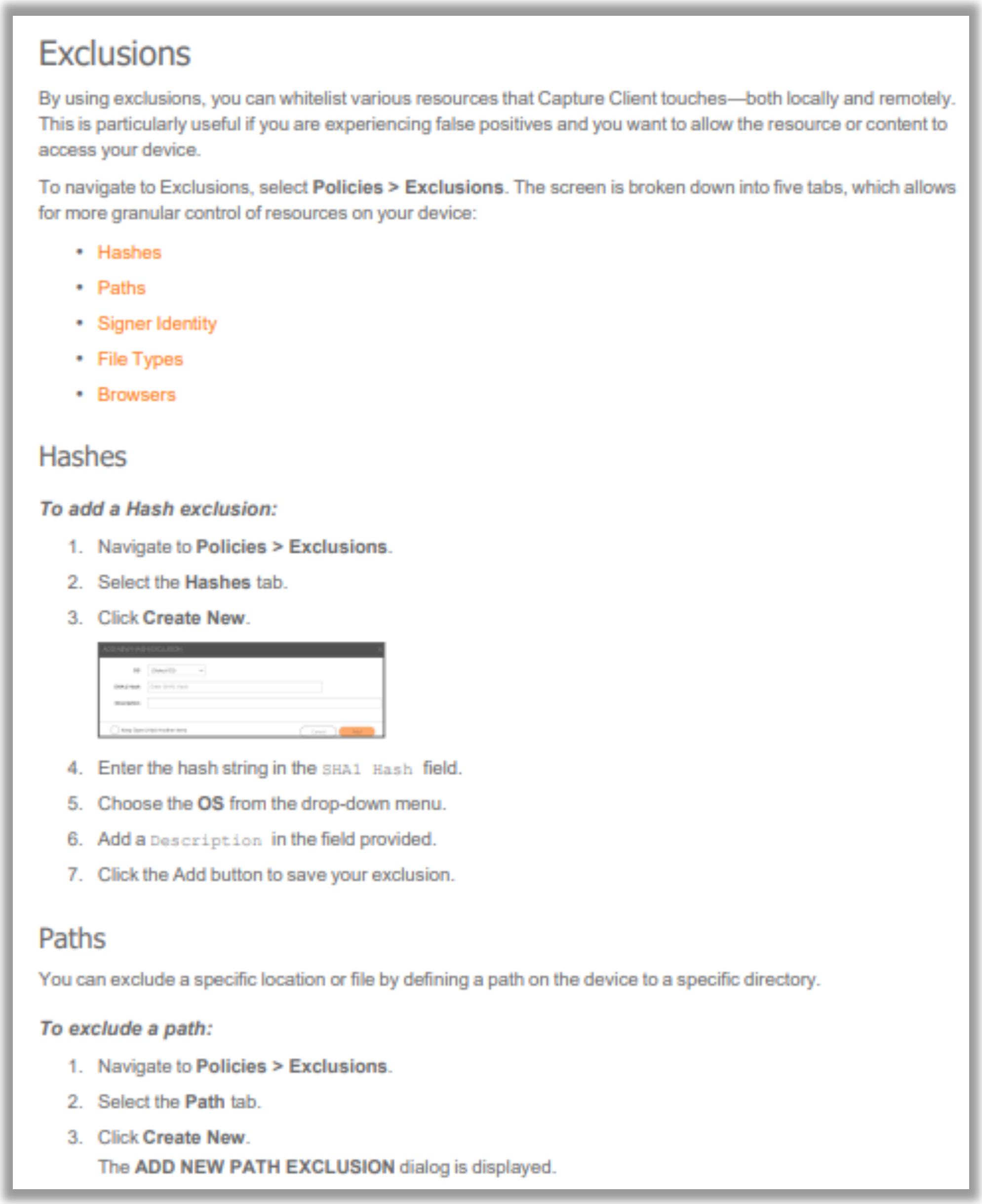
   ADD ITEM

   OS Type [Select OS]

   SHA1 Hash Enter SHA1 hash

   Description Add Description

   Cancel Add
4. Select an operating system from the `SOS Type` drop-down list.
5. Input a `SHA1 hash` for the file you wish to have blocked.
6. Add the `Description` in the field provided.
7. Click **Add**.



Exclusions

By using exclusions, you can whitelist various resources that Capture Client touches—both locally and remotely. This is particularly useful if you are experiencing false positives and you want to allow the resource or content to access your device.

To navigate to Exclusions, select **Policies > Exclusions**. The screen is broken down into five tabs, which allows for more granular control of resources on your device:

- Hashes
- Paths
- Signer Identity
- File Types
- Browsers

Hashes

To add a Hash exclusion:

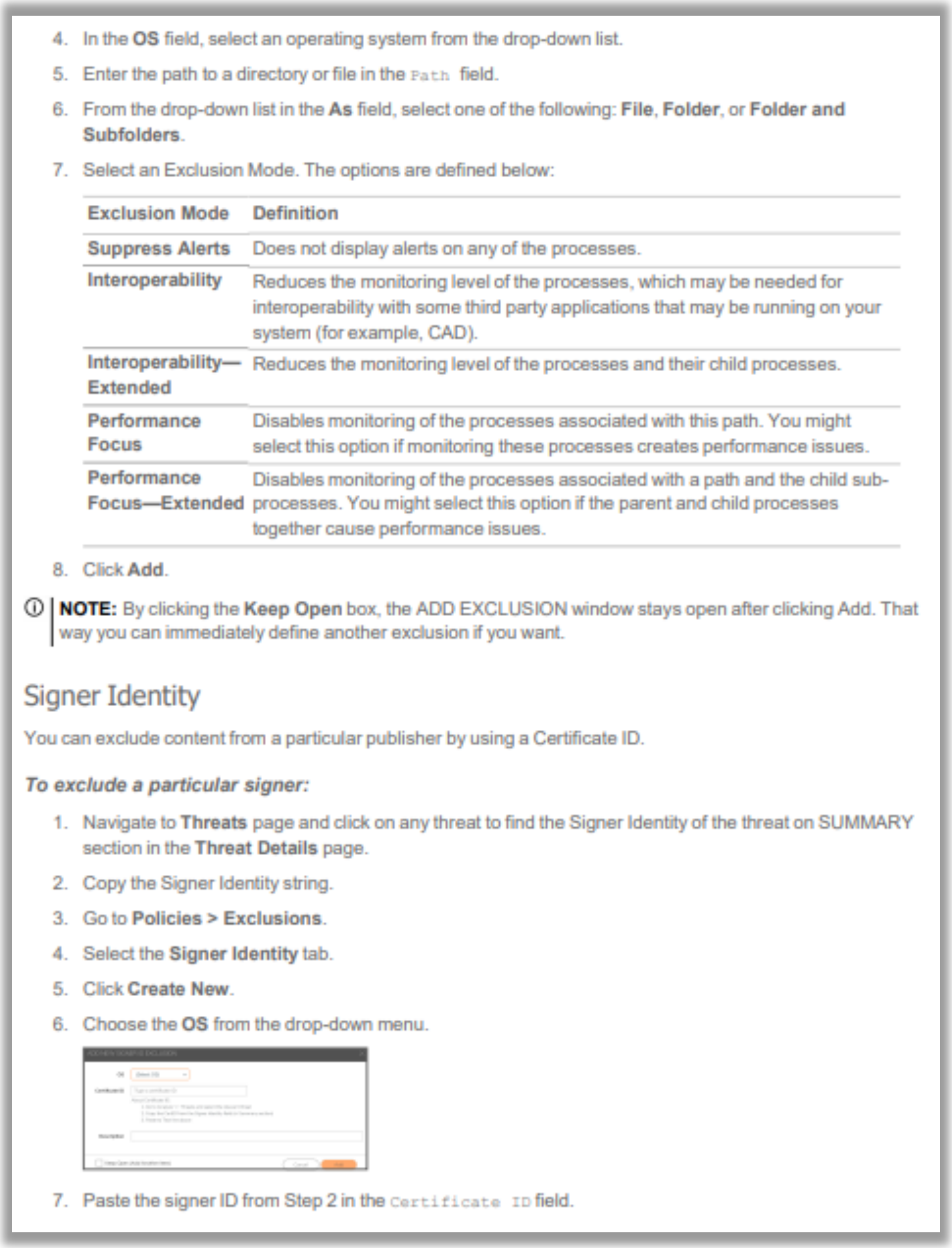
1. Navigate to **Policies > Exclusions**.
2. Select the **Hashes** tab.
3. Click **Create New**.
4. Enter the hash string in the `SHA1 Hash` field.
5. Choose the **OS** from the drop-down menu.
6. Add a `Description` in the field provided.
7. Click the Add button to save your exclusion.

Paths

You can exclude a specific location or file by defining a path on the device to a specific directory.

To exclude a path:

1. Navigate to **Policies > Exclusions**.
2. Select the **Path** tab.
3. Click **Create New**.
   The **ADD NEW PATH EXCLUSION** dialog is displayed.



4. In the **OS** field, select an operating system from the drop-down list.
5. Enter the path to a directory or file in the `Path` field.
6. From the drop-down list in the **As** field, select one of the following: **File**, **Folder**, or **Folder and Subfolders**.
7. Select an Exclusion Mode. The options are defined below:

Exclusion Mode	Definition
Suppress Alerts	Does not display alerts on any of the processes.
Interoperability	Reduces the monitoring level of the processes, which may be needed for interoperability with some third party applications that may be running on your system (for example, CAD).
Interoperability—Extended	Reduces the monitoring level of the processes and their child processes.
Performance Focus	Disables monitoring of the processes associated with this path. You might select this option if monitoring these processes creates performance issues.
Performance Focus—Extended	Disables monitoring of the processes associated with a path and the child sub-processes. You might select this option if the parent and child processes together cause performance issues.

8. Click **Add**.

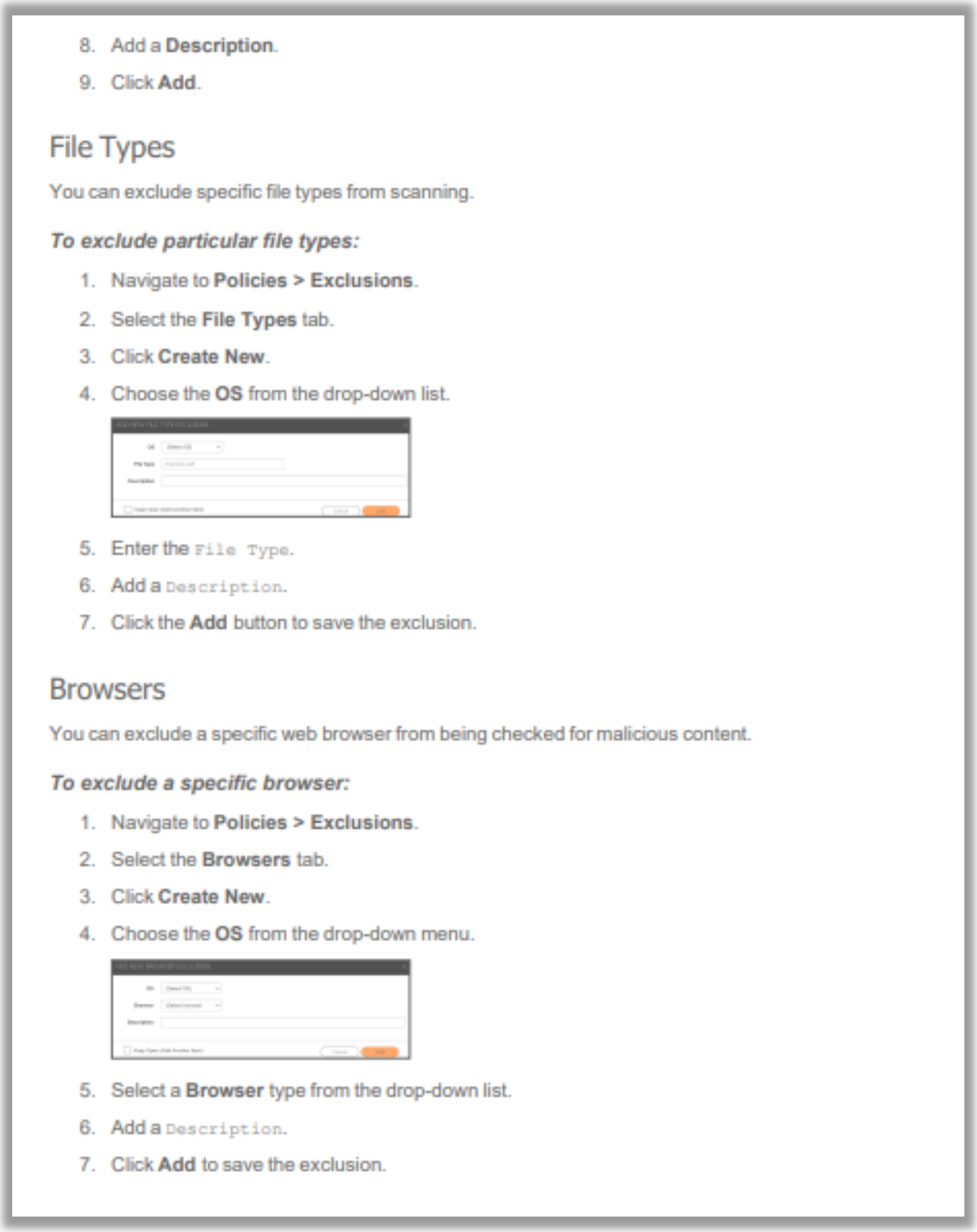
ⓘ **NOTE:** By clicking the **Keep Open** box, the ADD EXCLUSION window stays open after clicking Add. That way you can immediately define another exclusion if you want.

Signer Identity

You can exclude content from a particular publisher by using a Certificate ID.

To exclude a particular signer:

1. Navigate to **Threats** page and click on any threat to find the Signer Identity of the threat on SUMMARY section in the **Threat Details** page.
2. Copy the Signer Identity string.
3. Go to **Policies > Exclusions**.
4. Select the **Signer Identity** tab.
5. Click **Create New**.
6. Choose the **OS** from the drop-down menu.
7. Paste the signer ID from Step 2 in the `Certificate ID` field.



8. Add a **Description**.
9. Click **Add**.

File Types

You can exclude specific file types from scanning.

To exclude particular file types:

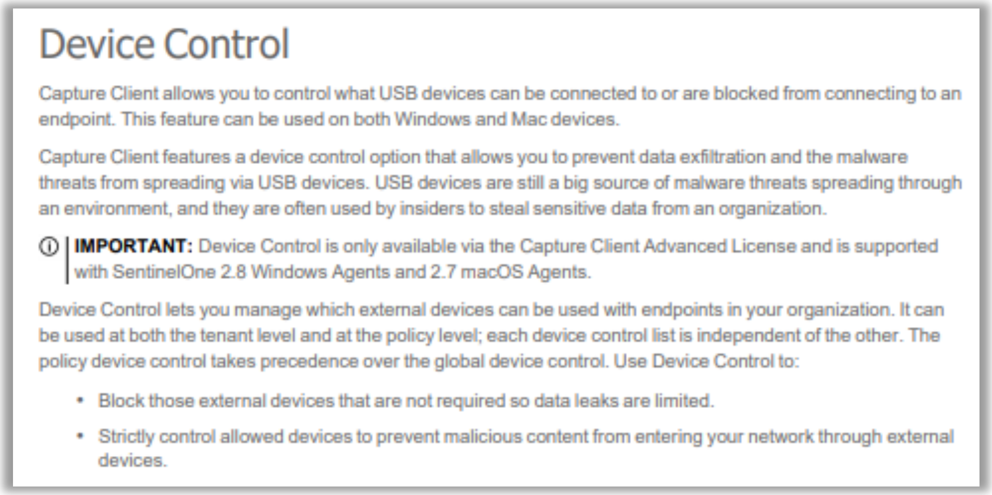
1. Navigate to **Policies > Exclusions**.
2. Select the **File Types** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down list.
5. Enter the `File Type`.
6. Add a `Description`.
7. Click the **Add** button to save the exclusion.

Browsers

You can exclude a specific web browser from being checked for malicious content.

To exclude a specific browser:

1. Navigate to **Policies > Exclusions**.
2. Select the **Browsers** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down menu.
5. Select a **Browser** type from the drop-down list.
6. Add a `Description`.
7. Click **Add** to save the exclusion.



Device Control

Capture Client allows you to control what USB devices can be connected to or are blocked from connecting to an endpoint. This feature can be used on both Windows and Mac devices.

Capture Client features a device control option that allows you to prevent data exfiltration and the malware threats from spreading via USB devices. USB devices are still a big source of malware threats spreading through an environment, and they are often used by insiders to steal sensitive data from an organization.

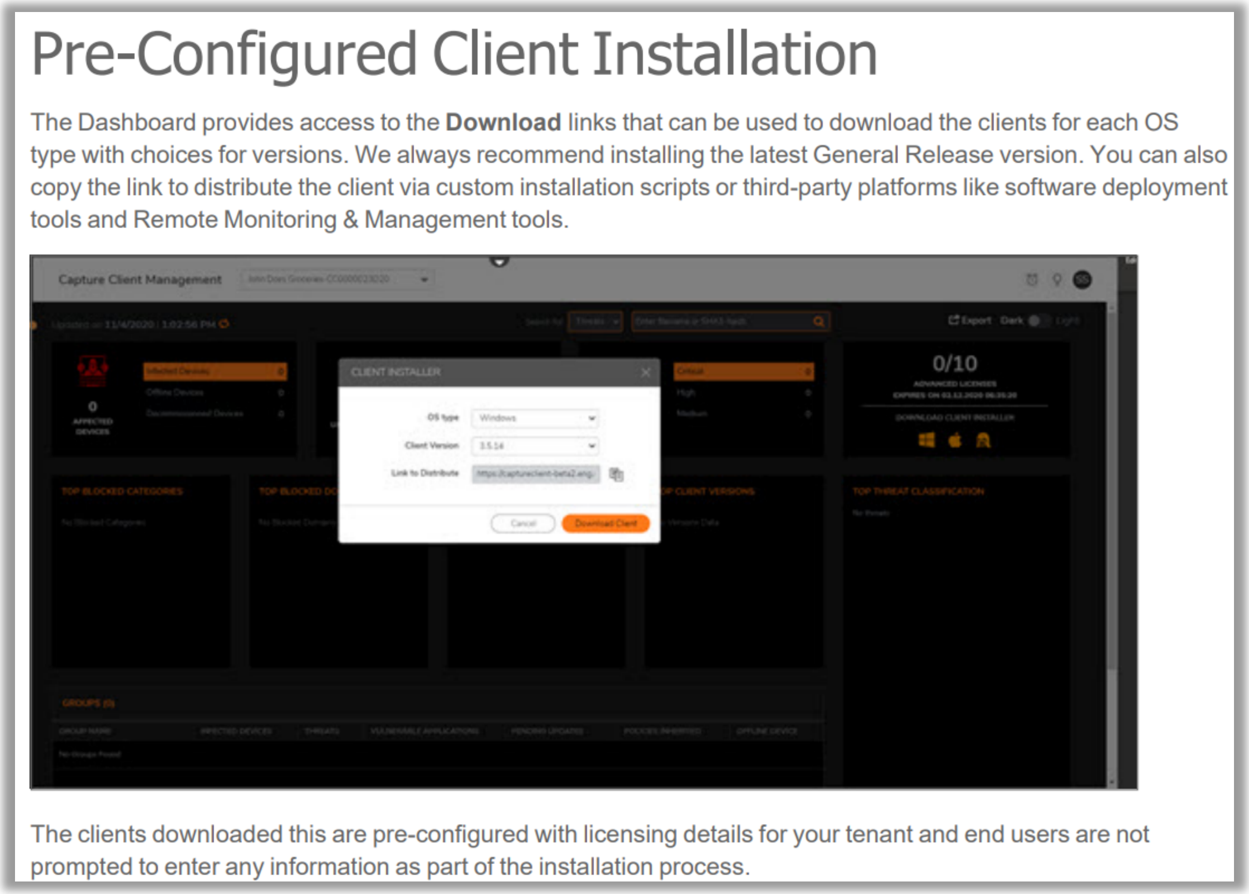
ⓘ **IMPORTANT:** Device Control is only available via the Capture Client Advanced License and is supported with SentinelOne 2.8 Windows Agents and 2.7 macOS Agents.

Device Control lets you manage which external devices can be used with endpoints in your organization. It can be used at both the tenant level and at the policy level; each device control list is independent of the other. The policy device control takes precedence over the global device control. Use Device Control to:

- Block those external devices that are not required so data leaks are limited.
- Strictly control allowed devices to prevent malicious content from entering your network through external devices.

[145]

141. Every '038 Accused Product practices configuring one or more software agents on the endpoint to monitor the plurality of operating conditions. For example, Capture Client is a software agent downloaded on the endpoint for monitoring the endpoint.



Pre-Configured Client Installation

The Dashboard provides access to the **Download** links that can be used to download the clients for each OS type with choices for versions. We always recommend installing the latest General Release version. You can also copy the link to distribute the client via custom installation scripts or third-party platforms like software deployment tools and Remote Monitoring & Management tools.

CLIENT INSTALLER

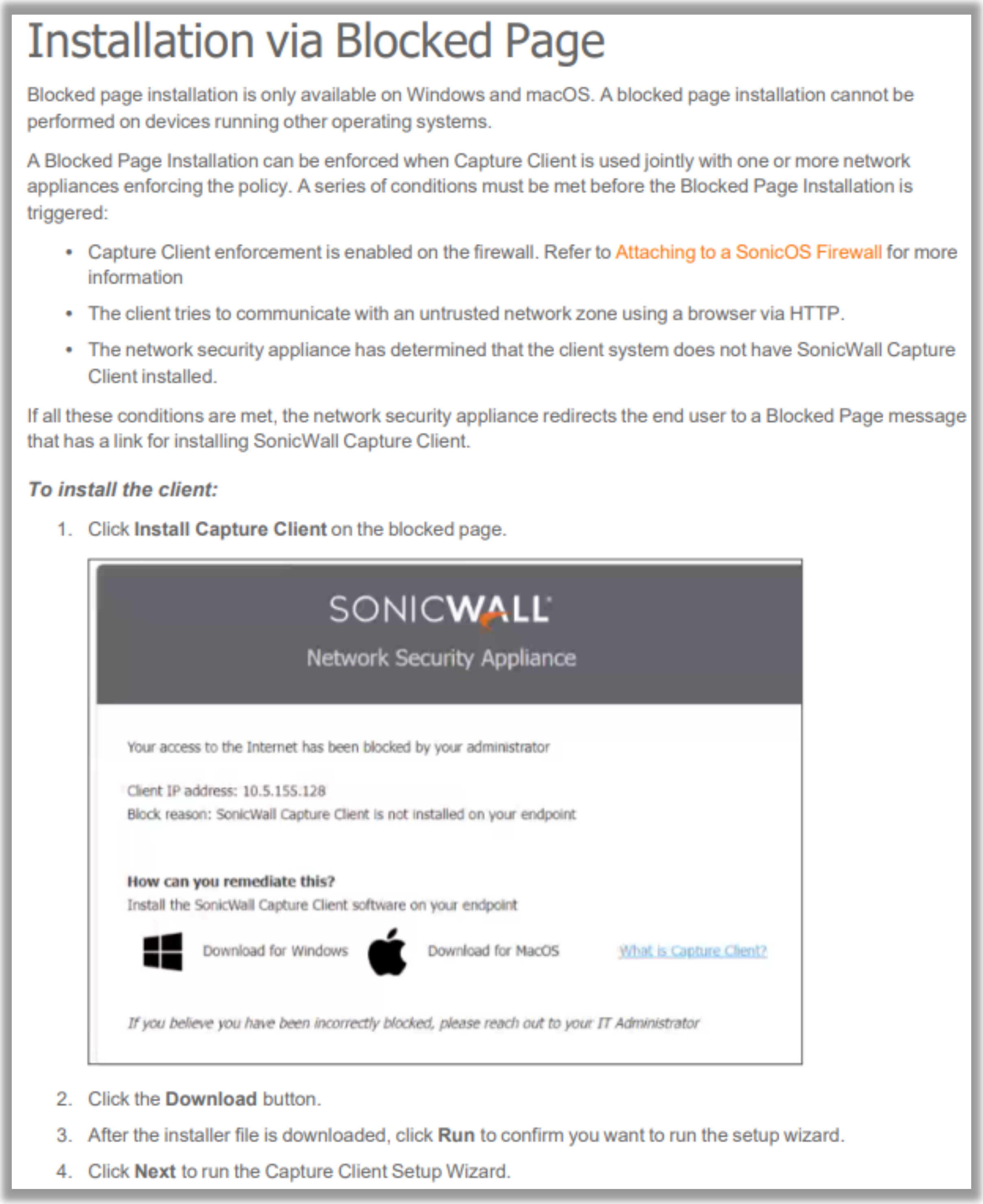
OS type: Windows

Client Version: 3.5.14

Link to Distribute: https://captureclient-beta2.eng

The clients downloaded this are pre-configured with licensing details for your tenant and end users are not prompted to enter any information as part of the installation process.

[145] https://www.sonicwall.com/techdocs/pdf/capture_client-protecting_assets.pdf, at 10-22.



Installation via Blocked Page

Blocked page installation is only available on Windows and macOS. A blocked page installation cannot be performed on devices running other operating systems.

A Blocked Page Installation can be enforced when Capture Client is used jointly with one or more network appliances enforcing the policy. A series of conditions must be met before the Blocked Page Installation is triggered:

- Capture Client enforcement is enabled on the firewall. Refer to Attaching to a SonicOS Firewall for more information
- The client tries to communicate with an untrusted network zone using a browser via HTTP.
- The network security appliance has determined that the client system does not have SonicWall Capture Client installed.

If all these conditions are met, the network security appliance redirects the end user to a Blocked Page message that has a link for installing SonicWall Capture Client.

To install the client:

1. Click **Install Capture Client** on the blocked page.

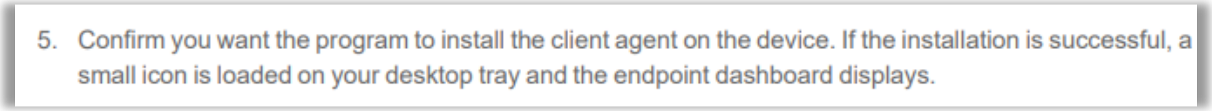
Your access to the Internet has been blocked by your administrator

Client IP address: 10.5.155.128
Block reason: SonicWall Capture Client is not installed on your endpoint

How can you remediate this?
Install the SonicWall Capture Client software on your endpoint

If you believe you have been incorrectly blocked, please reach out to your IT Administrator

2. Click the **Download** button.
3. After the installer file is downloaded, click **Run** to confirm you want to run the setup wizard.
4. Click **Next** to run the Capture Client Setup Wizard.

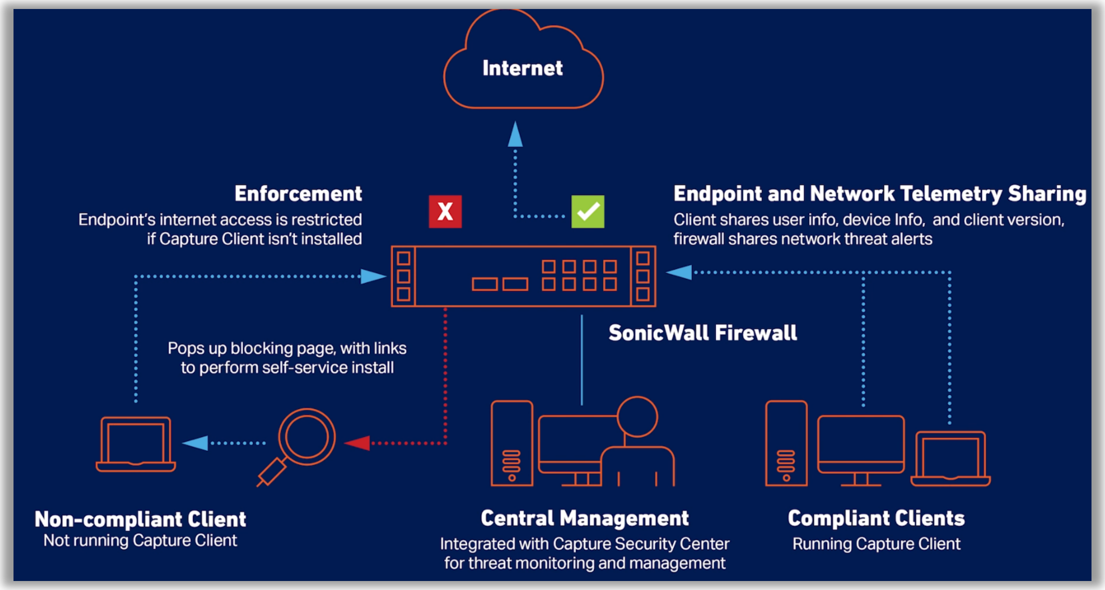


5. Confirm you want the program to install the client agent on the device. If the installation is successful, a small icon is loaded on your desktop tray and the endpoint dashboard displays.

[146]

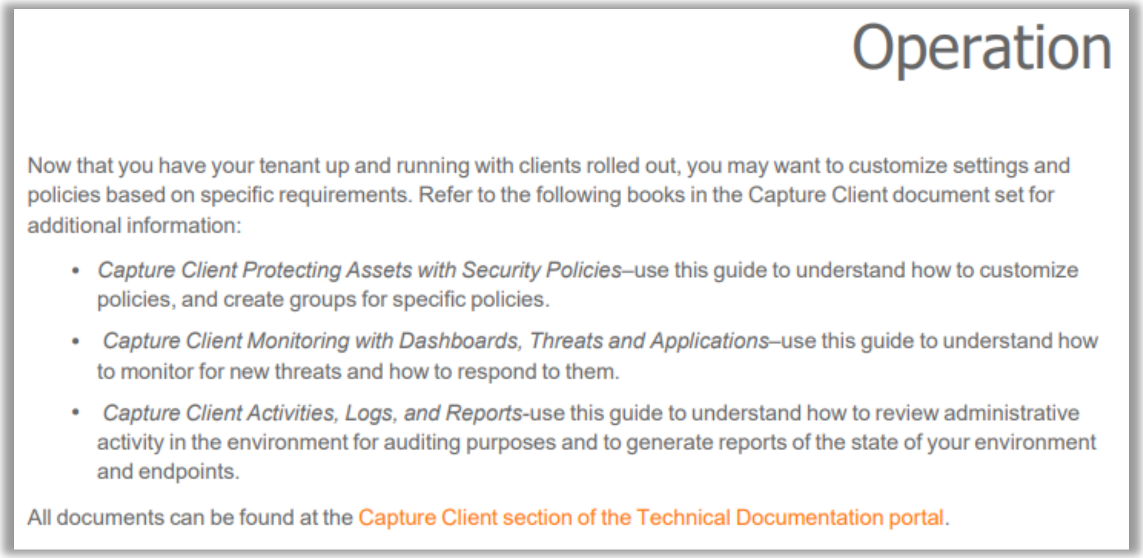
[146] https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 22-24.

142. Every ’038 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents. For example, Capture Client provides endpoint telemetry sharing, including user info, device info, and client version and monitors the endpoint for new threats in order to “generate reports of the state of your environment and endpoints.”


Internet
Enforcement
Endpoint's internet access is restricted
if Capture Client isn't installed
X
✓
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version,
firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links
to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center
for threat monitoring and management
Compliant Clients
Running Capture Client

[147]

[147] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112



Operation

Now that you have your tenant up and running with clients rolled out, you may want to customize settings and policies based on specific requirements. Refer to the following books in the Capture Client document set for additional information:

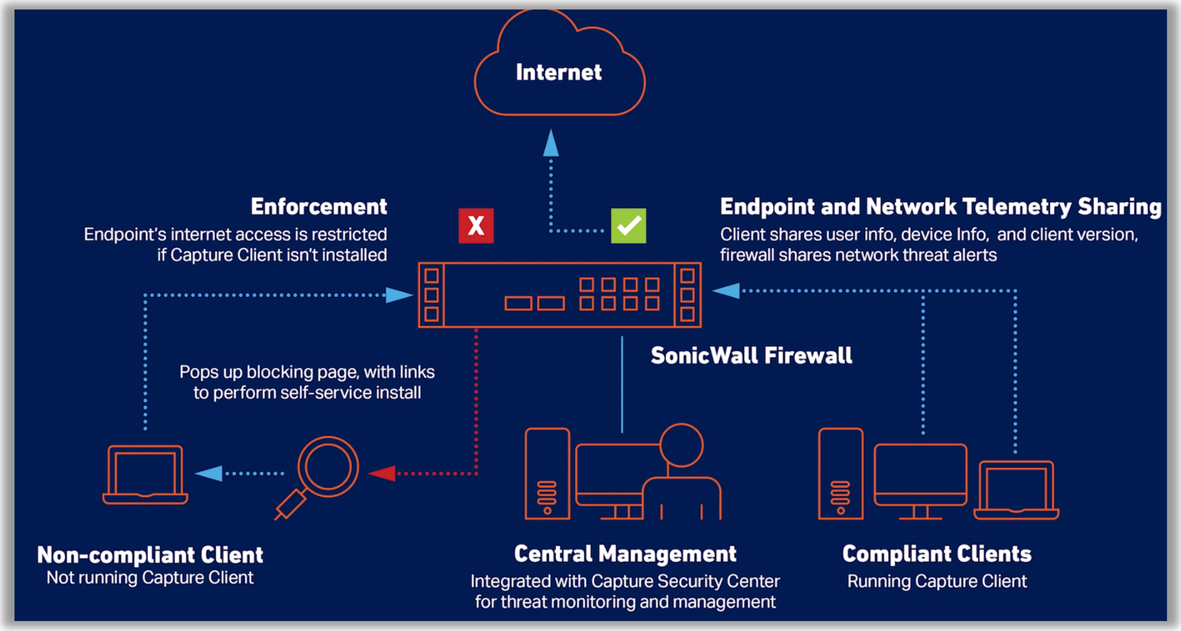
- *Capture Client Protecting Assets with Security Policies*–use this guide to understand how to customize policies, and create groups for specific policies.
- *Capture Client Monitoring with Dashboards, Threats and Applications*–use this guide to understand how to monitor for new threats and how to respond to them.
- *Capture Client Activities, Logs, and Reports*-use this guide to understand how to review administrative activity in the environment for auditing purposes and to generate reports of the state of your environment and endpoints.

All documents can be found at the Capture Client section of the Technical Documentation portal.

[148]

143. Every '038 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, Capture Client determines a compliance state of the endpoint based on whether the monitored status information meets the compliances policies that are managed at the cloud-based management console. For further example, a basic policy is whether Capture Client is running on the endpoint. If so, the endpoint is compliant; if not, the endpoint is not compliant.

[148] https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 27.



Internet

Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts

SonicWall Firewall

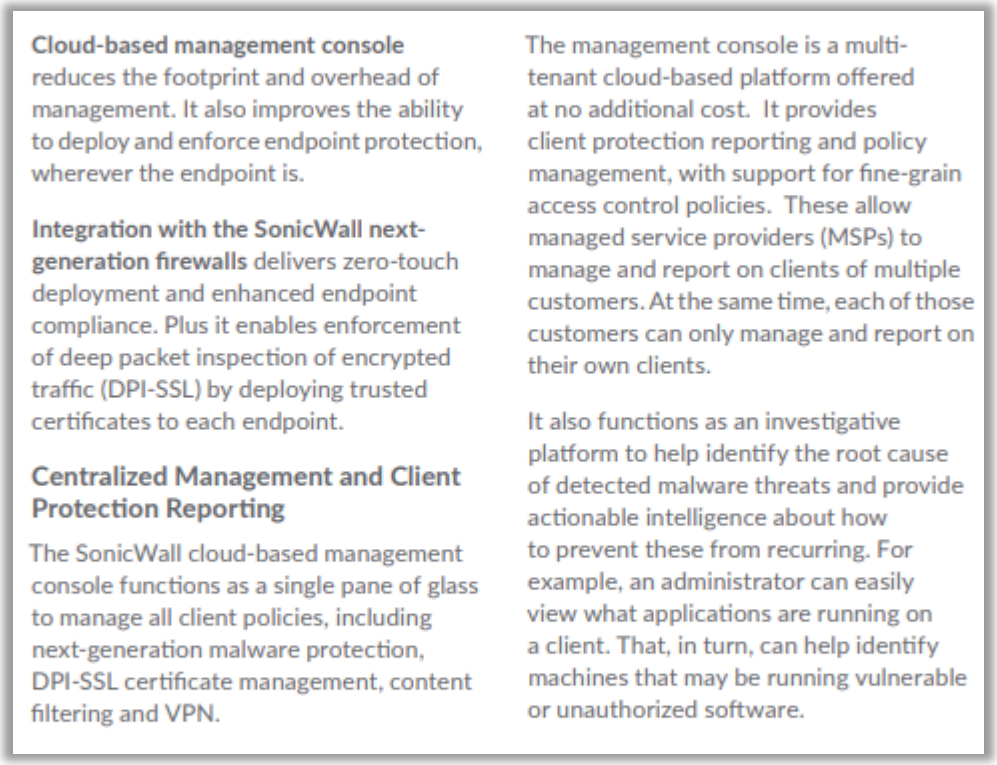
Pops up blocking page, with links to perform self-service install

Non-compliant Client
Not running Capture Client

Central Management
Integrated with Capture Security Center for threat monitoring and management

Compliant Clients
Running Capture Client

[149]



Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

Centralized Management and Client Protection Reporting

The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

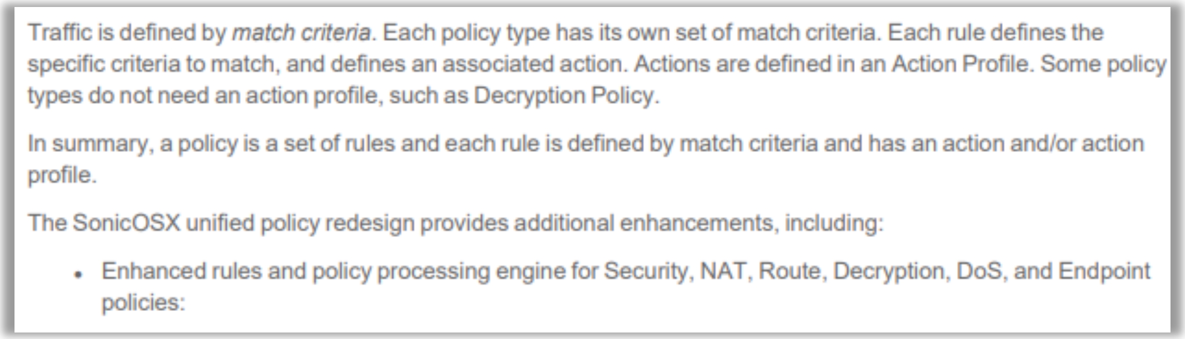
It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.

[150]

[149] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[150] https://www.sonicwall.com/medialibrary/pt/datasheet/sonicwall-capture-client.pdf

144. Every ’038 Accused Product practices initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint. For example, Capture Client can initiate actions since “each rule is defined by match criteria and has an action and/or action profile.” In one example, if an endpoint is not compliant by having downloaded the Capture Client, an identified action is that Internet access may be blocked.



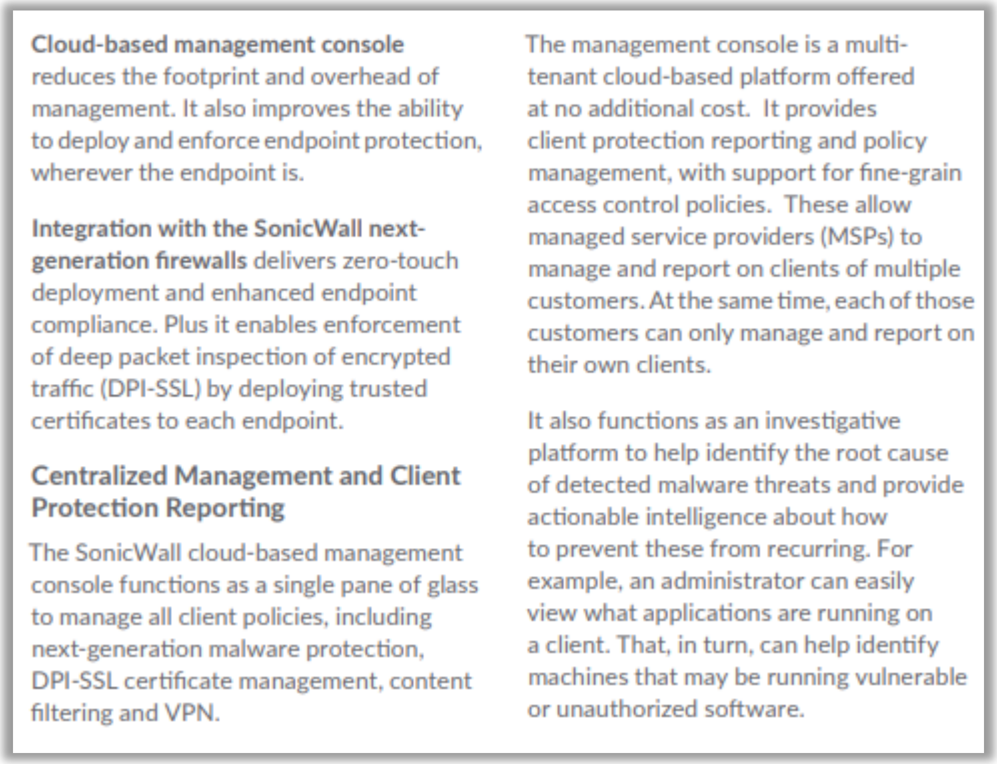
Traffic is defined by *match criteria*. Each policy type has its own set of match criteria. Each rule defines the specific criteria to match, and defines an associated action. Actions are defined in an Action Profile. Some policy types do not need an action profile, such as Decryption Policy.

In summary, a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.

The SonicOSX unified policy redesign provides additional enhancements, including:

- Enhanced rules and policy processing engine for Security, NAT, Route, Decryption, DoS, and Endpoint policies:

[151]



Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

Centralized Management and Client Protection Reporting

The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

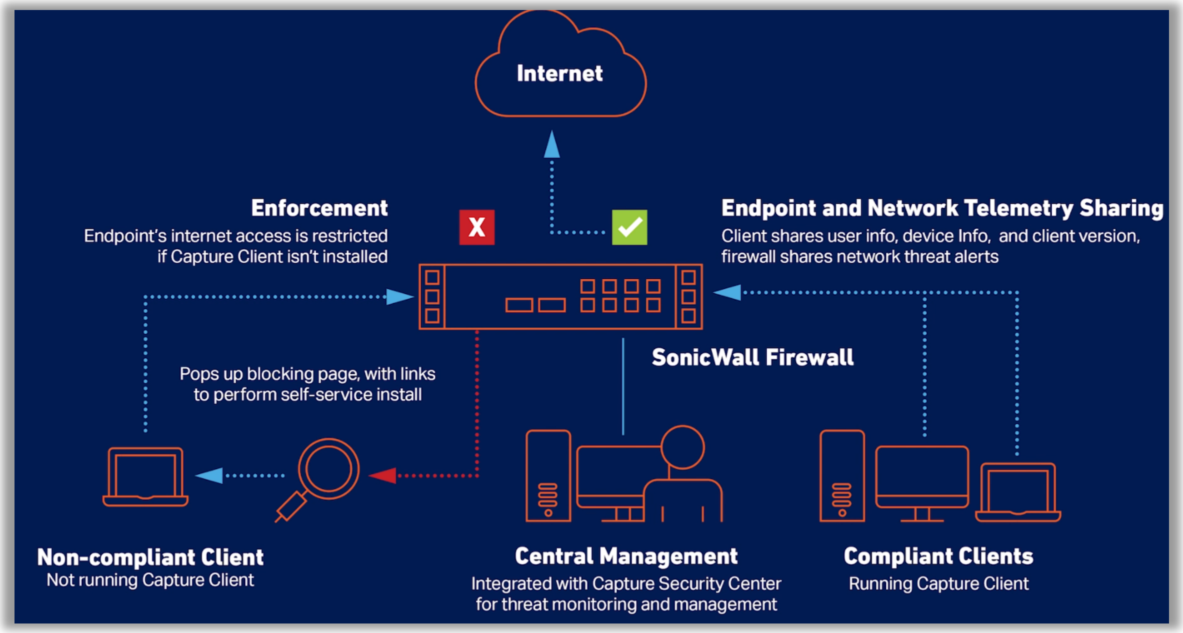
The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.

[152]

[151] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 51.

[152] https://www.sonicwall.com/medialibrary/pt/datasheet/sonicwall-capture-client.pdf


Internet
Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center for threat monitoring and management
Compliant Clients
Running Capture Client

[153]

145. Defendant has and continues to directly infringe one or more claims of the '038 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

146. Defendant has and continues to indirectly infringe one or more claims of the '038 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '038 Accused Products.

147. Defendant has and continues to indirectly infringe one or more claims of the '038 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge

[153] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

that these products, or the use thereof, infringe the ’038 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’038 Patent by providing these products to customers and end-users for use in an infringing manner.

148. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’038 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[154] Video Tutorials,[155] SonicWall University,[156] and Customer Service[157] websites.

149. Defendant has and continues to indirectly infringe one or more claims of the ’038 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’038 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls or Capture Client. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’038 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-

[154] https://www.sonicwall.com/support/technical-documentation/?language=English

[155] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[156] https://www.sonicwall.com/partners/sonicwall-university/

[157] https://www.sonicwall.com/support/contact-support/customer-service/

infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’038 Patent but remained willfully blind to the infringing nature of others’ actions.

150. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’038 Patent in an amount to be proved at trial.

151. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’038 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

152. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’038 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’038 Patent. Upon information and belief, Defendant had actual knowledge of the ’038 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’038 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT VIII
(Infringement of the ’918 Patent)

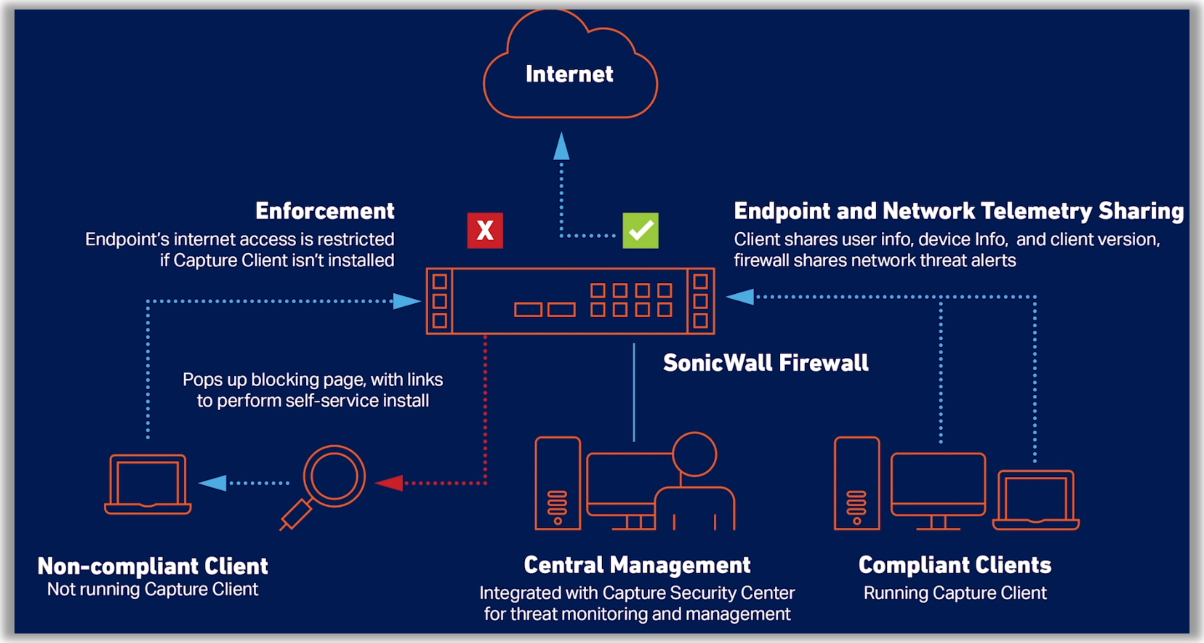
153. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

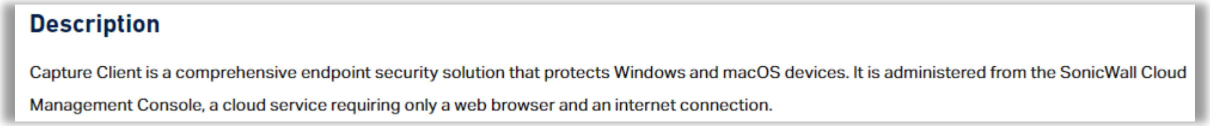
154. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’918 Patent.

155. Defendant has and continues to directly infringe the ’918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’918 Patent. Such products include at least SonicWall Capture Client alone, or in combination with SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) (the “’918 Accused Products”) which comprise a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint; determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store; authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state; and continuing to monitor the compliance

state by the endpoint and restricting access to the computing resource if the compliance state changes.

156. Every ’918 Accused Product comprises a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies. For example, Capture Client “is administered from the SonicWall Cloud Management Console” (e.g., a computing system remote from the endpoint), “a cloud service requiring only a web browser and an internet connection.


Internet
Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed
X
✓
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center for threat monitoring and management
Compliant Clients
Running Capture Client
[158]


Description

Capture Client is a comprehensive endpoint security solution that protects Windows and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection.

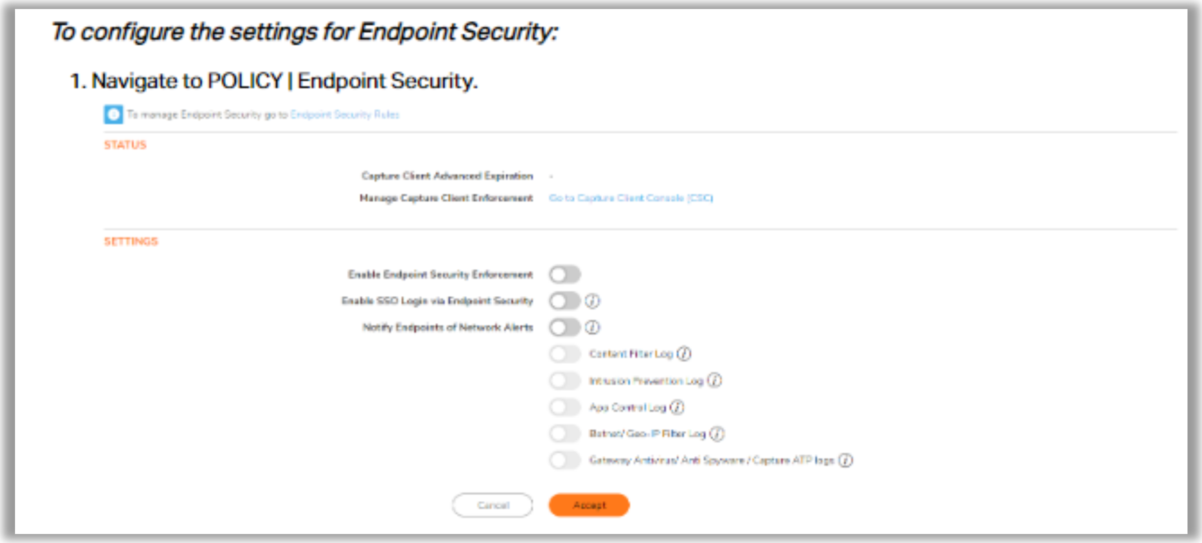
[159]

157. Every ’918 Accused Product practices maintaining the plurality of policies in a data store on the computing system. For example, Capture Client allows the storage of various endpoint

[158] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[159] https://www.sonicwall.com/support/knowledge-base/capture-client-system-requirements/210512075820480/

security policies: "POLICY | Endpoint Security." These policies can later be managed through the Capture Client Console, indicating that they are stored on the computing system.



To configure the settings for Endpoint Security:

1. Navigate to POLICY | Endpoint Security.

To manage Endpoint Security go to Endpoint Security Rules

STATUS

Capture Client Advanced Expiration -

Manage Capture Client Enforcement Go to Capture Client Console (CSC)

SETTINGS

Enable Endpoint Security Enforcement

Enable SSO Login via Endpoint Security

Notify Endpoints of Network Alerts

Content Filter Log

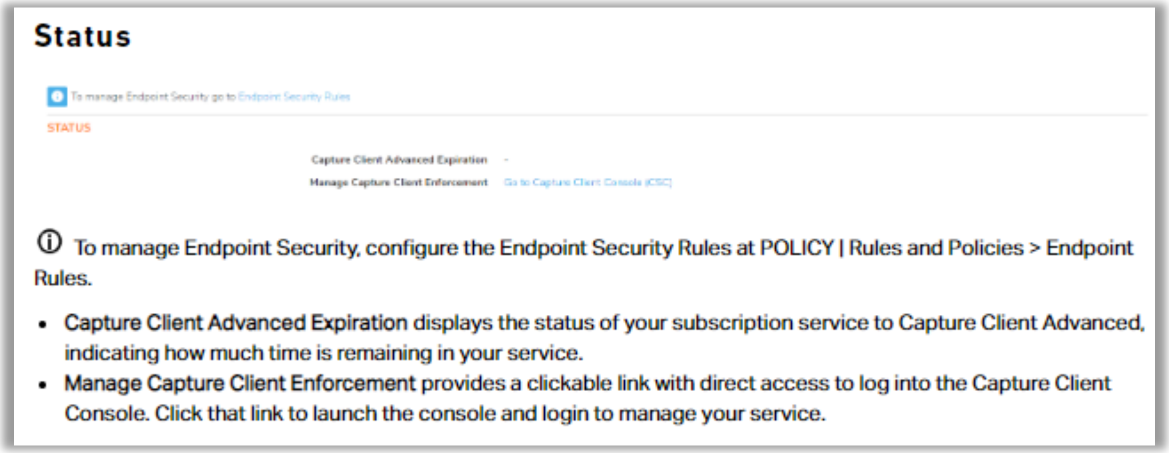
Intrusion Prevention Log

App Control Log

Botnet/ Geo-IP Filter Log

Gateway Antivirus/ Anti Spyware / Capture ATP logs

[160]



Status

To manage Endpoint Security go to Endpoint Security Rules

STATUS

Capture Client Advanced Expiration -

Manage Capture Client Enforcement Go to Capture Client Console (CSC)

ⓘ To manage Endpoint Security, configure the Endpoint Security Rules at POLICY | Rules and Policies > Endpoint Rules.

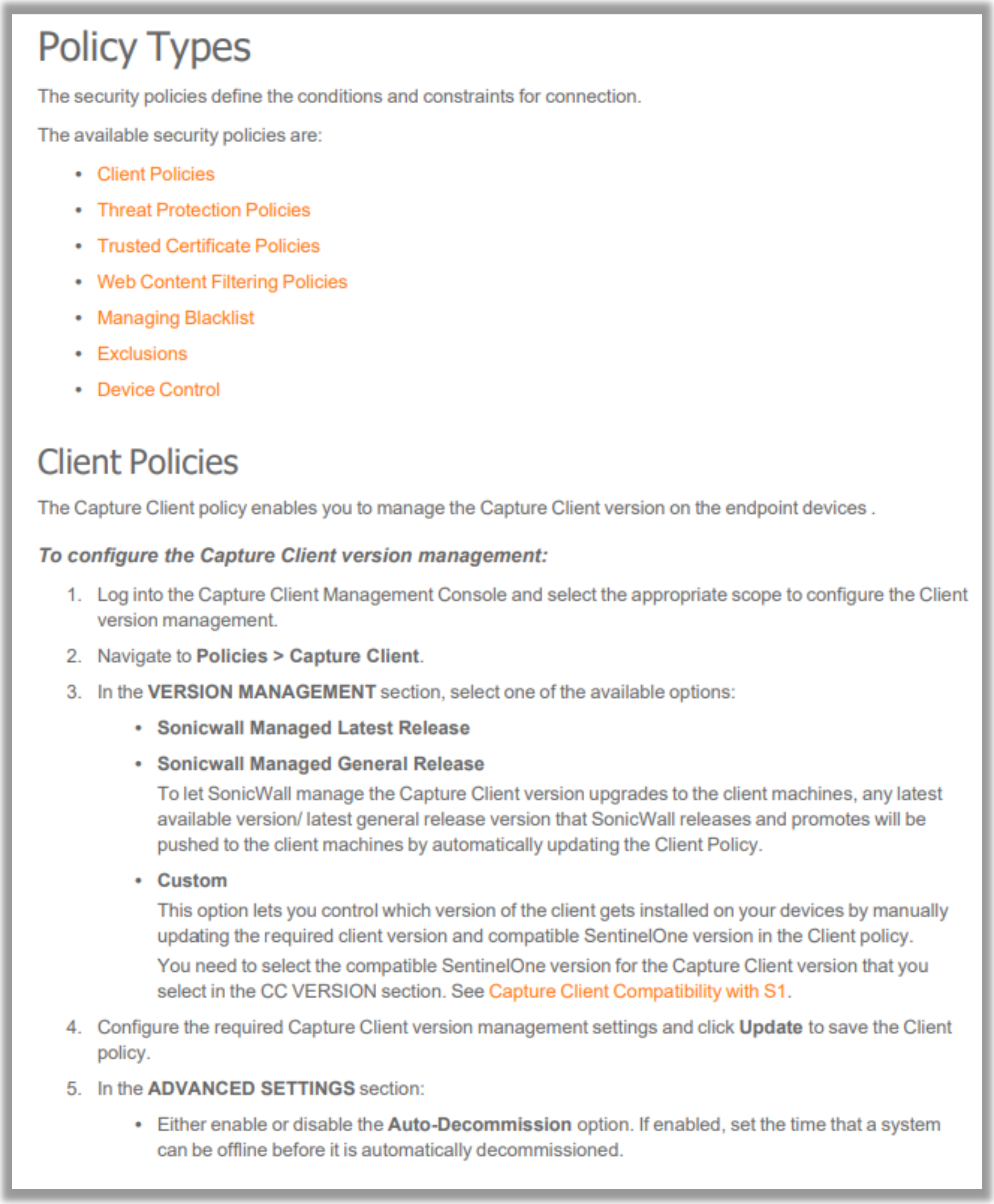
- **Capture Client Advanced Expiration** displays the status of your subscription service to Capture Client Advanced, indicating how much time is remaining in your service.
- **Manage Capture Client Enforcement** provides a clickable link with direct access to log into the Capture Client Console. Click that link to launch the console and login to manage your service.

[161]

158. Every '918 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Capture Client identifies, from the plurality of policies, operating conditions (*e.g.*, threats and suspicious activities) on the endpoint to monitor in order to determine mitigation mode: Detect, Protect, or Capture ATP.

[160] https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-endpoint_security/Content/endpoint-security.htm/

[161] https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-endpoint_security/Content/endpoint-security-status.htm/



Policy Types

The security policies define the conditions and constraints for connection.

The available security policies are:

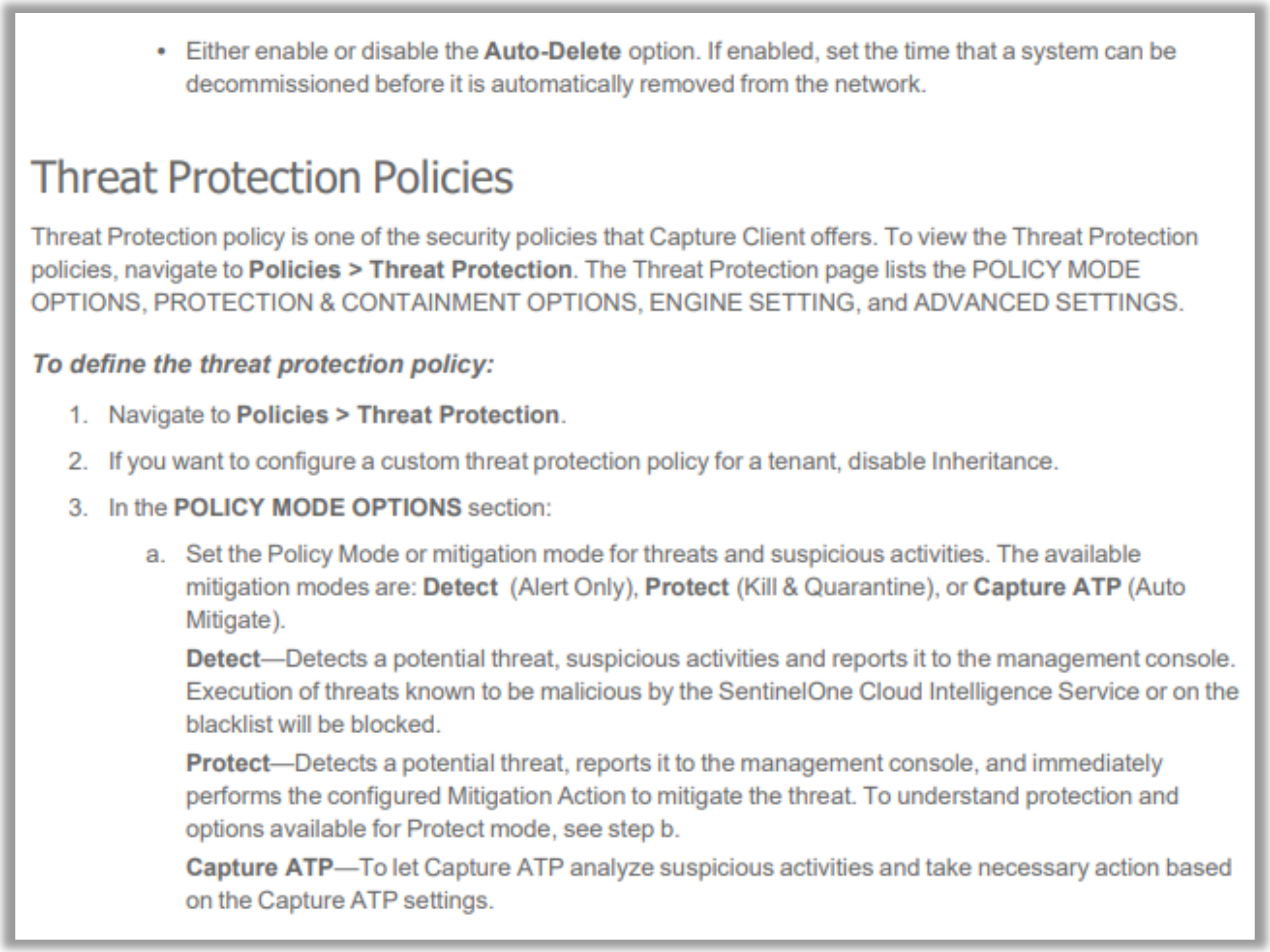
- Client Policies
- Threat Protection Policies
- Trusted Certificate Policies
- Web Content Filtering Policies
- Managing Blacklist
- Exclusions
- Device Control

Client Policies

The Capture Client policy enables you to manage the Capture Client version on the endpoint devices .

To configure the Capture Client version management:

1. Log into the Capture Client Management Console and select the appropriate scope to configure the Client version management.
2. Navigate to **Policies > Capture Client**.
3. In the **VERSION MANAGEMENT** section, select one of the available options:
   - **Sonicwall Managed Latest Release**
   - **Sonicwall Managed General Release**
     To let SonicWall manage the Capture Client version upgrades to the client machines, any latest available version/ latest general release version that SonicWall releases and promotes will be pushed to the client machines by automatically updating the Client Policy.
   - **Custom**
     This option lets you control which version of the client gets installed on your devices by manually updating the required client version and compatible SentinelOne version in the Client policy.
     You need to select the compatible SentinelOne version for the Capture Client version that you select in the CC VERSION section. See Capture Client Compatibility with S1.
4. Configure the required Capture Client version management settings and click **Update** to save the Client policy.
5. In the **ADVANCED SETTINGS** section:
   - Either enable or disable the **Auto-Decommission** option. If enabled, set the time that a system can be offline before it is automatically decommissioned.



- Either enable or disable the **Auto-Delete** option. If enabled, set the time that a system can be decommissioned before it is automatically removed from the network.

Threat Protection Policies

Threat Protection policy is one of the security policies that Capture Client offers. To view the Threat Protection policies, navigate to **Policies > Threat Protection**. The Threat Protection page lists the POLICY MODE OPTIONS, PROTECTION & CONTAINMENT OPTIONS, ENGINE SETTING, and ADVANCED SETTINGS.

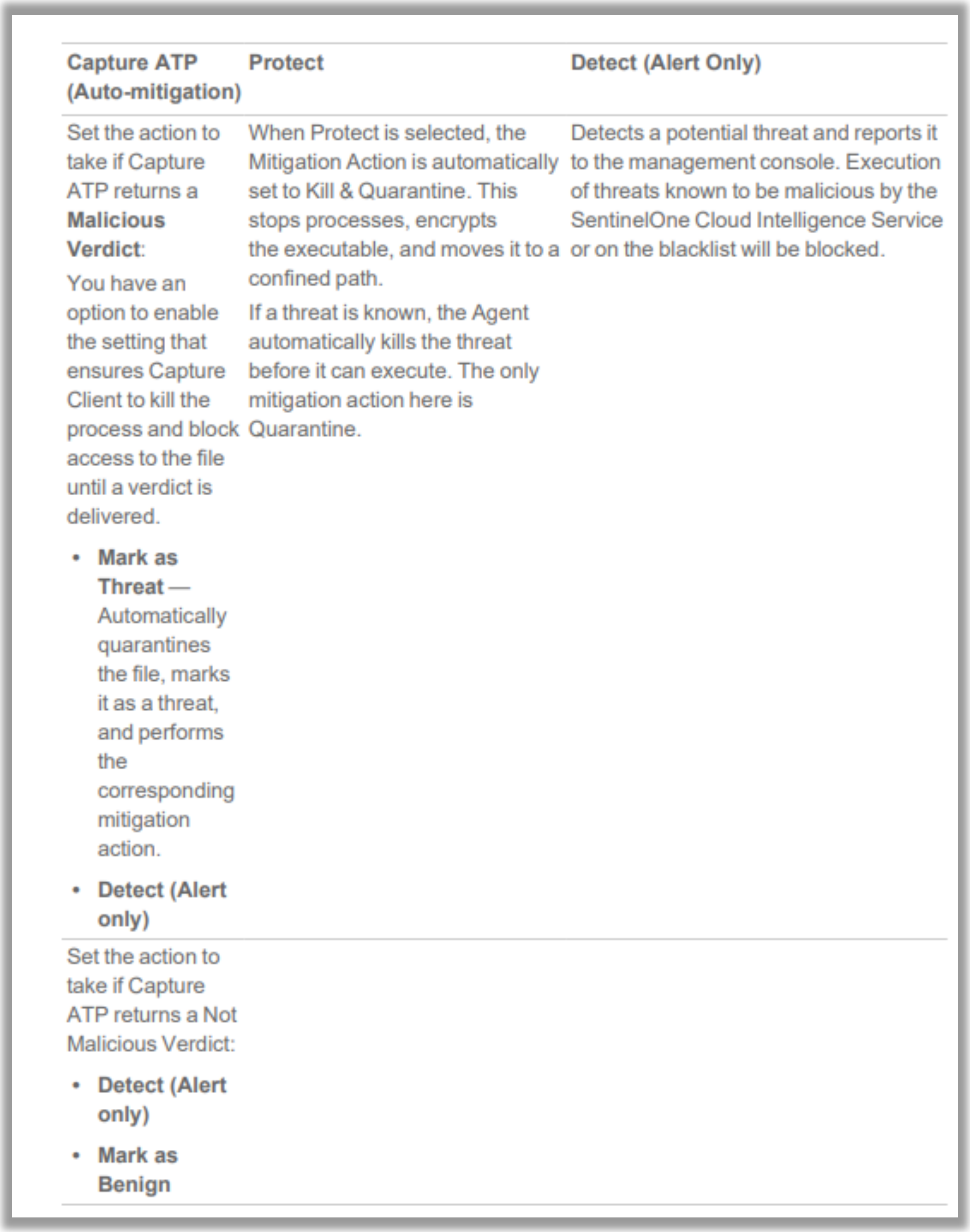
To define the threat protection policy:

1. Navigate to **Policies > Threat Protection**.
2. If you want to configure a custom threat protection policy for a tenant, disable Inheritance.
3. In the **POLICY MODE OPTIONS** section:
   a. Set the Policy Mode or mitigation mode for threats and suspicious activities. The available mitigation modes are: **Detect** (Alert Only), **Protect** (Kill & Quarantine), or **Capture ATP** (Auto Mitigate).

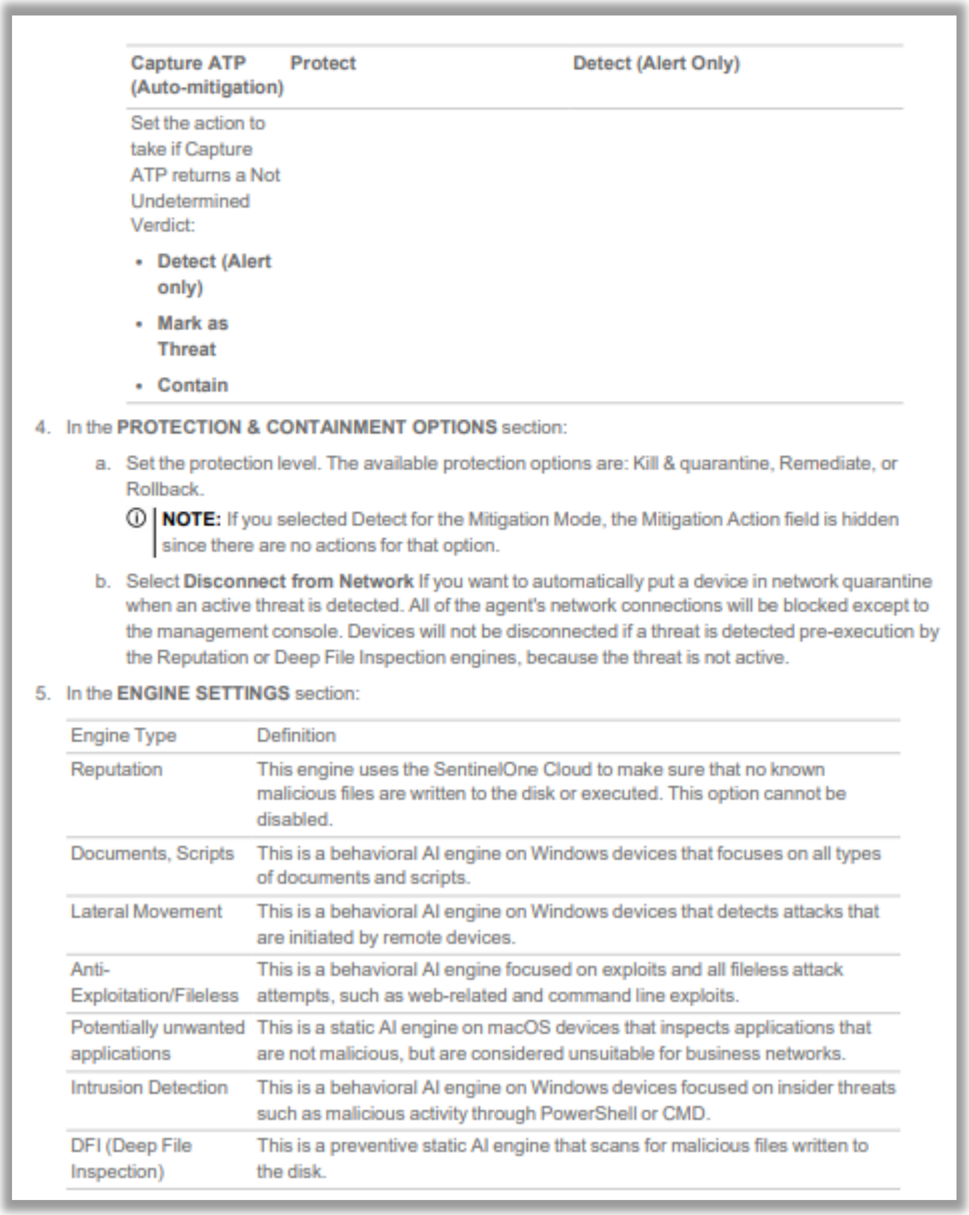
      Detect—Detects a potential threat, suspicious activities and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.

      Protect—Detects a potential threat, reports it to the management console, and immediately performs the configured Mitigation Action to mitigate the threat. To understand protection and options available for Protect mode, see step b.

      Capture ATP—To let Capture ATP analyze suspicious activities and take necessary action based on the Capture ATP settings.



Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a **Malicious Verdict**: You have an option to enable the setting that ensures Capture Client to kill the process and block access to the file until a verdict is delivered. • **Mark as Threat** — Automatically quarantines the file, marks it as a threat, and performs the corresponding mitigation action. • **Detect (Alert only)**	When Protect is selected, the Mitigation Action is automatically set to Kill & Quarantine. This stops processes, encrypts the executable, and moves it to a confined path. If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action here is Quarantine.	Detects a potential threat and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.
Set the action to take if Capture ATP returns a Not Malicious Verdict: • **Detect (Alert only)** • **Mark as Benign**		



Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a Not Undetermined Verdict: • **Detect (Alert only)** • **Mark as Threat** • **Contain**		

4. In the **PROTECTION & CONTAINMENT OPTIONS** section:

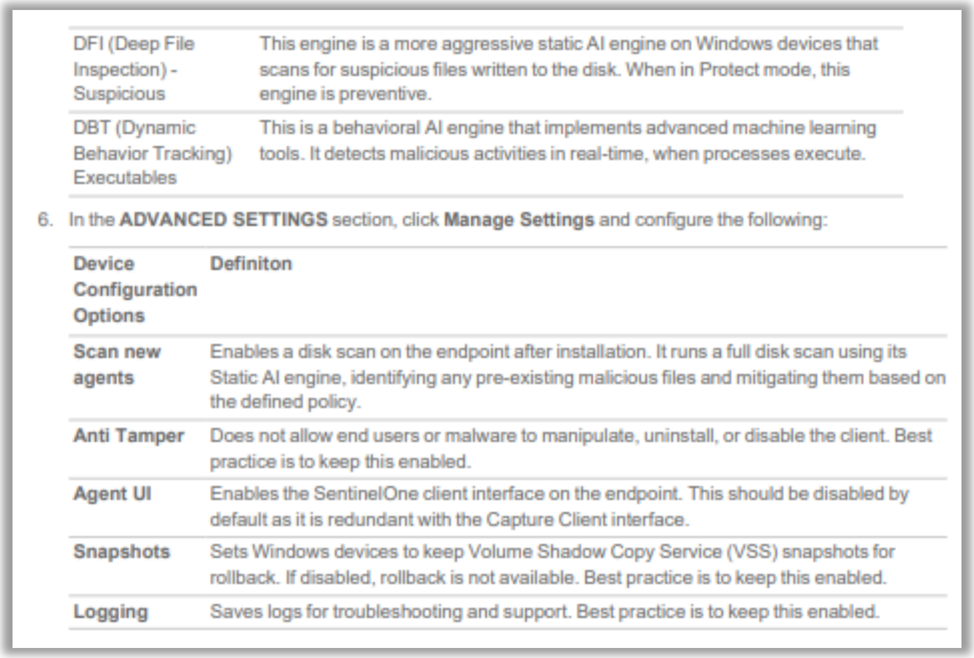
   a. Set the protection level. The available protection options are: Kill & quarantine, Remediate, or Rollback.

   ⓘ **NOTE:** If you selected Detect for the Mitigation Mode, the Mitigation Action field is hidden since there are no actions for that option.

   b. Select **Disconnect from Network** If you want to automatically put a device in network quarantine when an active threat is detected. All of the agent's network connections will be blocked except to the management console. Devices will not be disconnected if a threat is detected pre-execution by the Reputation or Deep File Inspection engines, because the threat is not active.

5. In the **ENGINE SETTINGS** section:

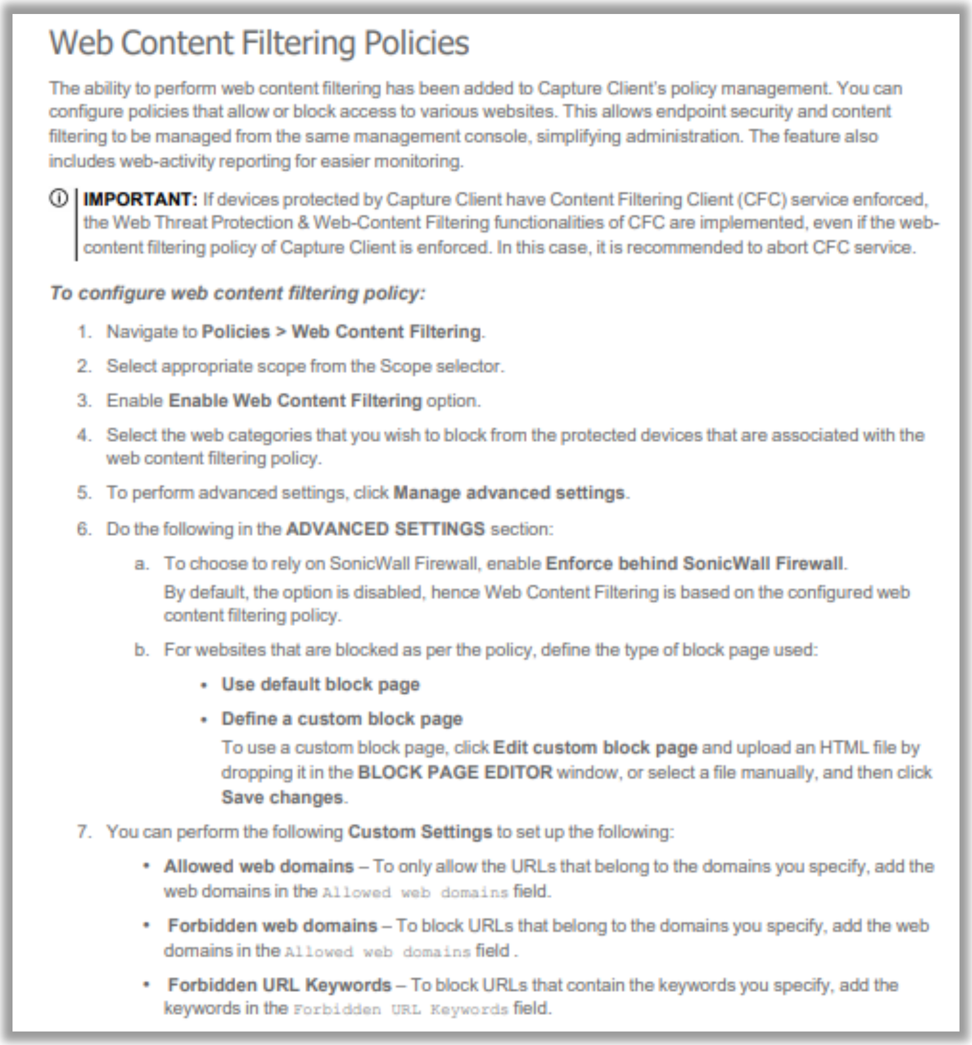
Engine Type	Definition
Reputation	This engine uses the SentinelOne Cloud to make sure that no known malicious files are written to the disk or executed. This option cannot be disabled.
Documents, Scripts	This is a behavioral AI engine on Windows devices that focuses on all types of documents and scripts.
Lateral Movement	This is a behavioral AI engine on Windows devices that detects attacks that are initiated by remote devices.
Anti-Exploitation/Fileless	This is a behavioral AI engine focused on exploits and all fileless attack attempts, such as web-related and command line exploits.
Potentially unwanted applications	This is a static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.
Intrusion Detection	This is a behavioral AI engine on Windows devices focused on insider threats such as malicious activity through PowerShell or CMD.
DFI (Deep File Inspection)	This is a preventive static AI engine that scans for malicious files written to the disk.



DFI (Deep File Inspection) - Suspicious	This engine is a more aggressive static AI engine on Windows devices that scans for suspicious files written to the disk. When in Protect mode, this engine is preventive.
DBT (Dynamic Behavior Tracking) Executables	This is a behavioral AI engine that implements advanced machine learning tools. It detects malicious activities in real-time, when processes execute.

6. In the **ADVANCED SETTINGS** section, click **Manage Settings** and configure the following:

Device Configuration Options	Definiton
Scan new agents	Enables a disk scan on the endpoint after installation. It runs a full disk scan using its Static AI engine, identifying any pre-existing malicious files and mitigating them based on the defined policy.
Anti Tamper	Does not allow end users or malware to manipulate, uninstall, or disable the client. Best practice is to keep this enabled.
Agent UI	Enables the SentinelOne client interface on the endpoint. This should be disabled by default as it is redundant with the Capture Client interface.
Snapshots	Sets Windows devices to keep Volume Shadow Copy Service (VSS) snapshots for rollback. If disabled, rollback is not available. Best practice is to keep this enabled.
Logging	Saves logs for troubleshooting and support. Best practice is to keep this enabled.



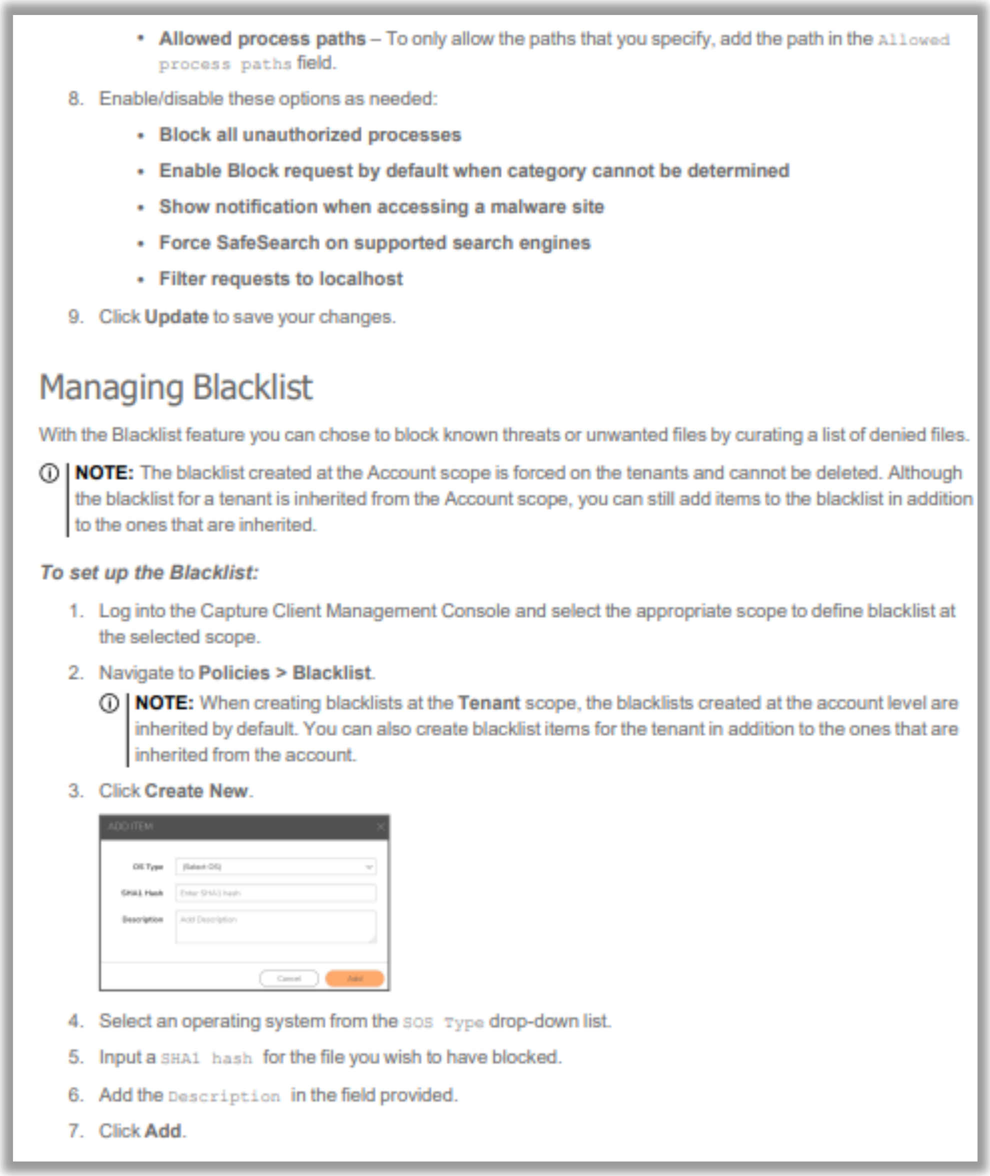
Web Content Filtering Policies

The ability to perform web content filtering has been added to Capture Client's policy management. You can configure policies that allow or block access to various websites. This allows endpoint security and content filtering to be managed from the same management console, simplifying administration. The feature also includes web-activity reporting for easier monitoring.

ⓘ **IMPORTANT:** If devices protected by Capture Client have Content Filtering Client (CFC) service enforced, the Web Threat Protection & Web-Content Filtering functionalities of CFC are implemented, even if the web-content filtering policy of Capture Client is enforced. In this case, it is recommended to abort CFC service.

To configure web content filtering policy:

1. Navigate to **Policies > Web Content Filtering**.
2. Select appropriate scope from the Scope selector.
3. Enable **Enable Web Content Filtering** option.
4. Select the web categories that you wish to block from the protected devices that are associated with the web content filtering policy.
5. To perform advanced settings, click **Manage advanced settings**.
6. Do the following in the **ADVANCED SETTINGS** section:
   a. To choose to rely on SonicWall Firewall, enable **Enforce behind SonicWall Firewall**.
      By default, the option is disabled, hence Web Content Filtering is based on the configured web content filtering policy.
   b. For websites that are blocked as per the policy, define the type of block page used:
      - **Use default block page**
      - **Define a custom block page**
        To use a custom block page, click **Edit custom block page** and upload an HTML file by dropping it in the **BLOCK PAGE EDITOR** window, or select a file manually, and then click **Save changes**.
7. You can perform the following **Custom Settings** to set up the following:
   - **Allowed web domains** – To only allow the URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field.
   - **Forbidden web domains** – To block URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field .
   - **Forbidden URL Keywords** – To block URLs that contain the keywords you specify, add the keywords in the `Forbidden URL Keywords` field.



- **Allowed process paths** – To only allow the paths that you specify, add the path in the `Allowed process paths` field.

8. Enable/disable these options as needed:
   - **Block all unauthorized processes**
   - **Enable Block request by default when category cannot be determined**
   - **Show notification when accessing a malware site**
   - **Force SafeSearch on supported search engines**
   - **Filter requests to localhost**
9. Click **Update** to save your changes.

Managing Blacklist

With the Blacklist feature you can chose to block known threats or unwanted files by curating a list of denied files.

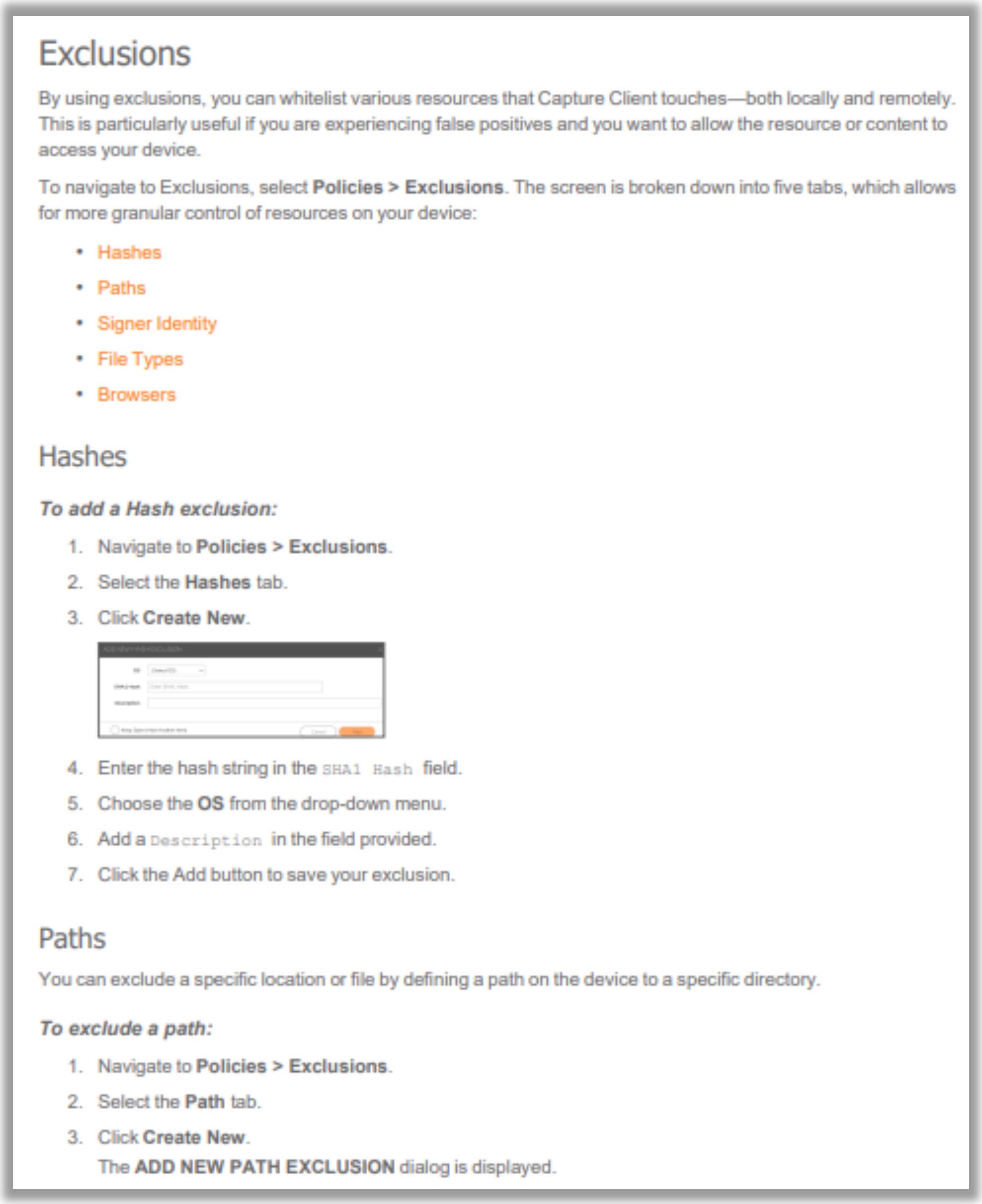
ⓘ **NOTE:** The blacklist created at the Account scope is forced on the tenants and cannot be deleted. Although the blacklist for a tenant is inherited from the Account scope, you can still add items to the blacklist in addition to the ones that are inherited.

To set up the Blacklist:

1. Log into the Capture Client Management Console and select the appropriate scope to define blacklist at the selected scope.
2. Navigate to **Policies > Blacklist**.

   ⓘ **NOTE:** When creating blacklists at the **Tenant** scope, the blacklists created at the account level are inherited by default. You can also create blacklist items for the tenant in addition to the ones that are inherited from the account.
3. Click **Create New**.

4. Select an operating system from the `SOS Type` drop-down list.
5. Input a `SHA1 hash` for the file you wish to have blocked.
6. Add the `Description` in the field provided.
7. Click **Add**.



Exclusions

By using exclusions, you can whitelist various resources that Capture Client touches—both locally and remotely. This is particularly useful if you are experiencing false positives and you want to allow the resource or content to access your device.

To navigate to Exclusions, select **Policies > Exclusions**. The screen is broken down into five tabs, which allows for more granular control of resources on your device:

- Hashes
- Paths
- Signer Identity
- File Types
- Browsers

Hashes

To add a Hash exclusion:

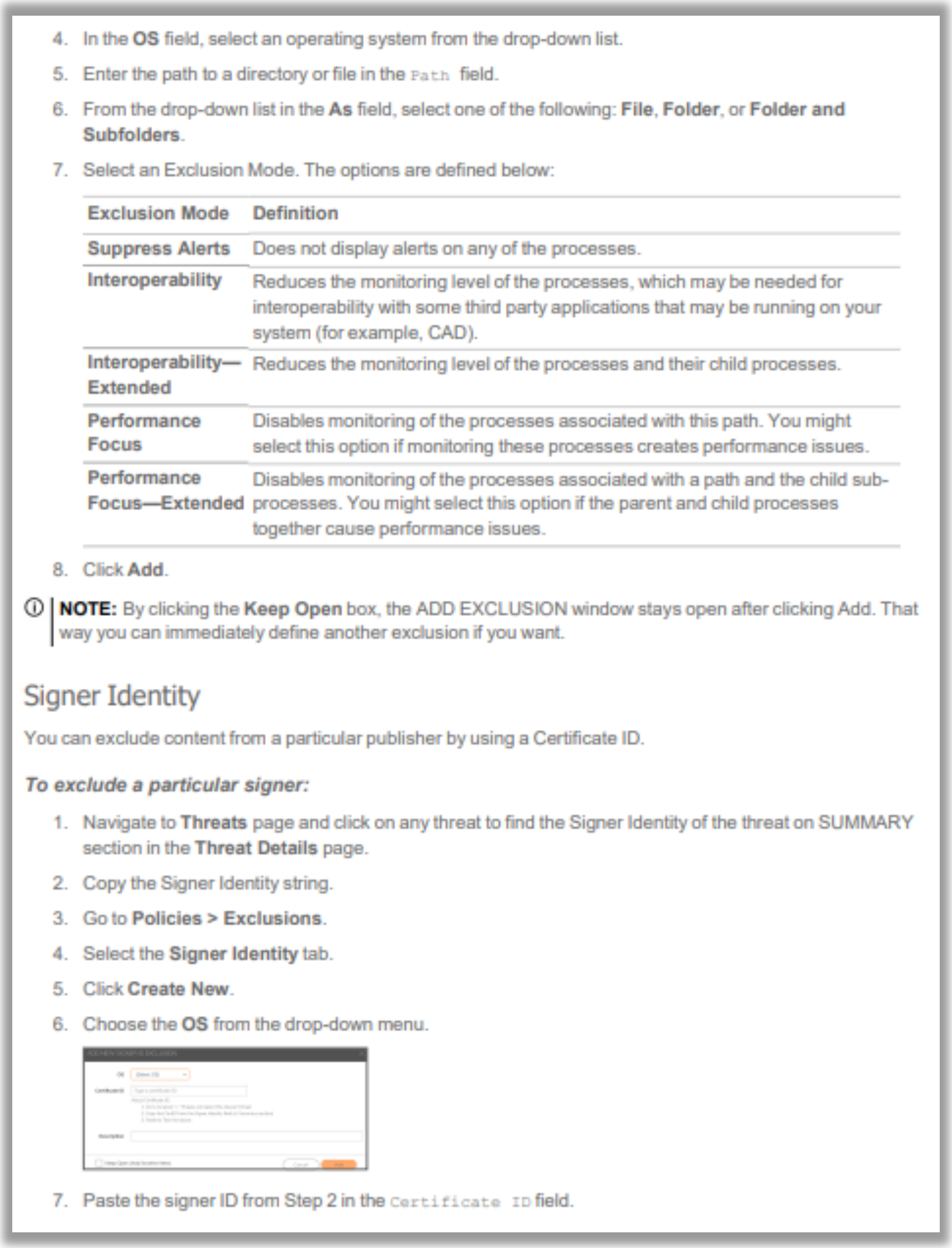
1. Navigate to **Policies > Exclusions**.
2. Select the **Hashes** tab.
3. Click **Create New**.
4. Enter the hash string in the `SHA1 Hash` field.
5. Choose the **OS** from the drop-down menu.
6. Add a `Description` in the field provided.
7. Click the Add button to save your exclusion.

Paths

You can exclude a specific location or file by defining a path on the device to a specific directory.

To exclude a path:

1. Navigate to **Policies > Exclusions**.
2. Select the **Path** tab.
3. Click **Create New**.
   The **ADD NEW PATH EXCLUSION** dialog is displayed.



4. In the **OS** field, select an operating system from the drop-down list.
5. Enter the path to a directory or file in the `Path` field.
6. From the drop-down list in the **As** field, select one of the following: **File**, **Folder**, or **Folder and Subfolders**.
7. Select an Exclusion Mode. The options are defined below:

Exclusion Mode	Definition
Suppress Alerts	Does not display alerts on any of the processes.
Interoperability	Reduces the monitoring level of the processes, which may be needed for interoperability with some third party applications that may be running on your system (for example, CAD).
Interoperability—Extended	Reduces the monitoring level of the processes and their child processes.
Performance Focus	Disables monitoring of the processes associated with this path. You might select this option if monitoring these processes creates performance issues.
Performance Focus—Extended	Disables monitoring of the processes associated with a path and the child sub-processes. You might select this option if the parent and child processes together cause performance issues.

8. Click **Add**.

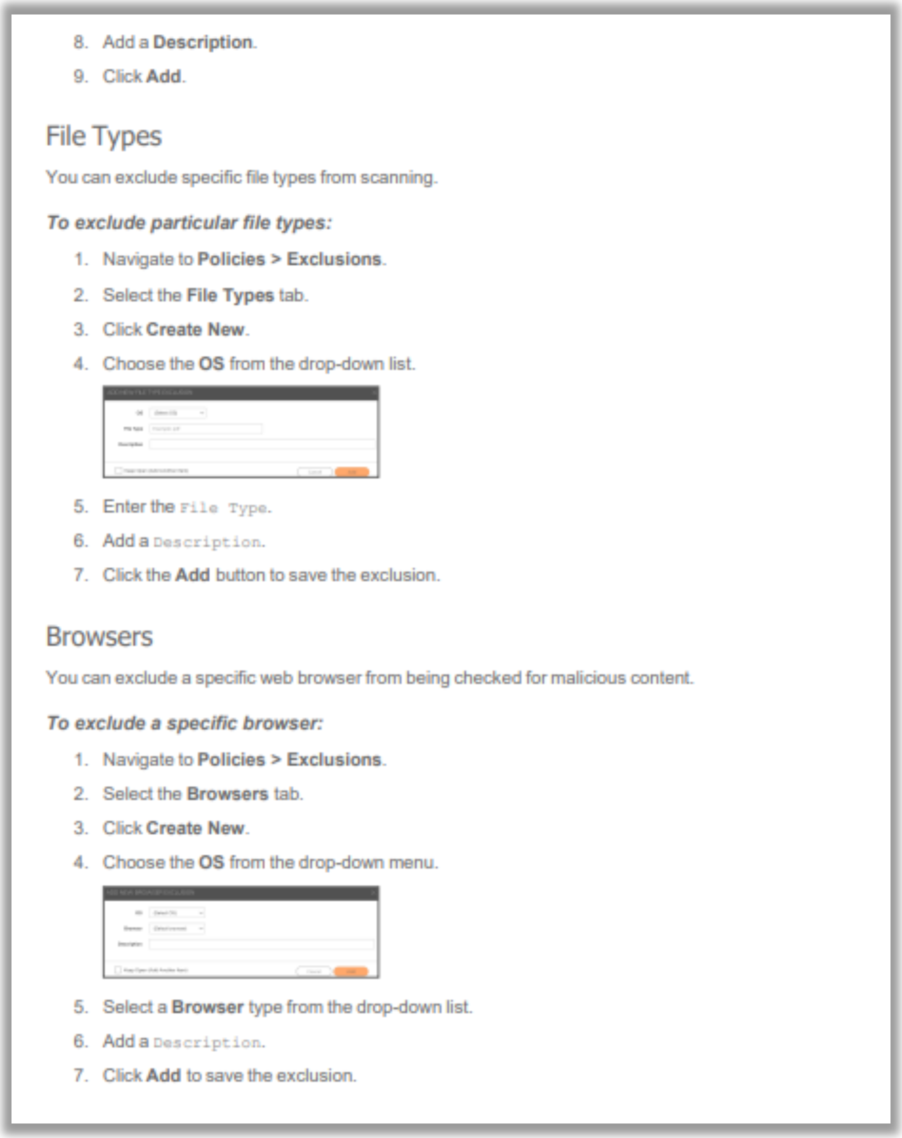
ⓘ **NOTE:** By clicking the **Keep Open** box, the ADD EXCLUSION window stays open after clicking Add. That way you can immediately define another exclusion if you want.

Signer Identity

You can exclude content from a particular publisher by using a Certificate ID.

To exclude a particular signer:

1. Navigate to **Threats** page and click on any threat to find the Signer Identity of the threat on SUMMARY section in the **Threat Details** page.
2. Copy the Signer Identity string.
3. Go to **Policies > Exclusions**.
4. Select the **Signer Identity** tab.
5. Click **Create New**.
6. Choose the **OS** from the drop-down menu.
7. Paste the signer ID from Step 2 in the `Certificate ID` field.



8. Add a **Description**.
9. Click **Add**.

File Types

You can exclude specific file types from scanning.

To exclude particular file types:

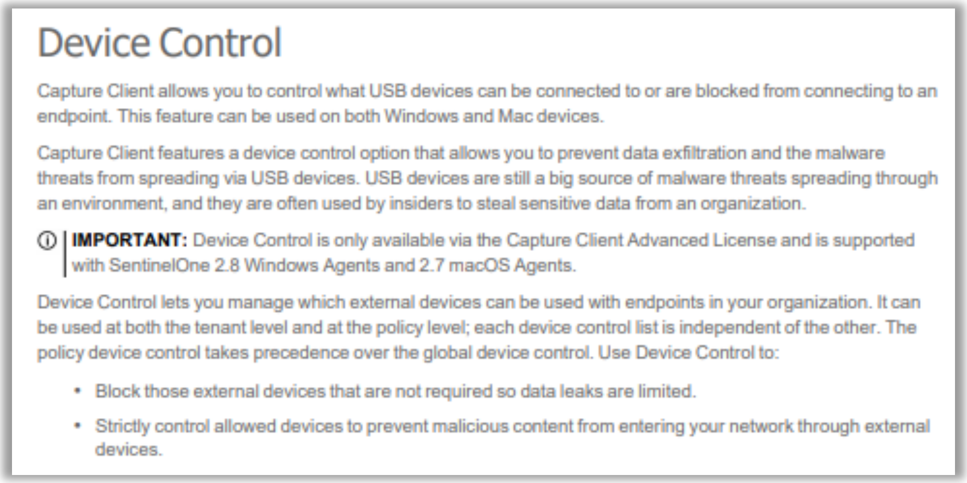
1. Navigate to **Policies > Exclusions**.
2. Select the **File Types** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down list.
5. Enter the `File Type`.
6. Add a `Description`.
7. Click the **Add** button to save the exclusion.

Browsers

You can exclude a specific web browser from being checked for malicious content.

To exclude a specific browser:

1. Navigate to **Policies > Exclusions**.
2. Select the **Browsers** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down menu.
5. Select a **Browser** type from the drop-down list.
6. Add a `Description`.
7. Click **Add** to save the exclusion.



Device Control

Capture Client allows you to control what USB devices can be connected to or are blocked from connecting to an endpoint. This feature can be used on both Windows and Mac devices.

Capture Client features a device control option that allows you to prevent data exfiltration and the malware threats from spreading via USB devices. USB devices are still a big source of malware threats spreading through an environment, and they are often used by insiders to steal sensitive data from an organization.

ⓘ **IMPORTANT:** Device Control is only available via the Capture Client Advanced License and is supported with SentinelOne 2.8 Windows Agents and 2.7 macOS Agents.

Device Control lets you manage which external devices can be used with endpoints in your organization. It can be used at both the tenant level and at the policy level; each device control list is independent of the other. The policy device control takes precedence over the global device control. Use Device Control to:

- Block those external devices that are not required so data leaks are limited.
- Strictly control allowed devices to prevent malicious content from entering your network through external devices.

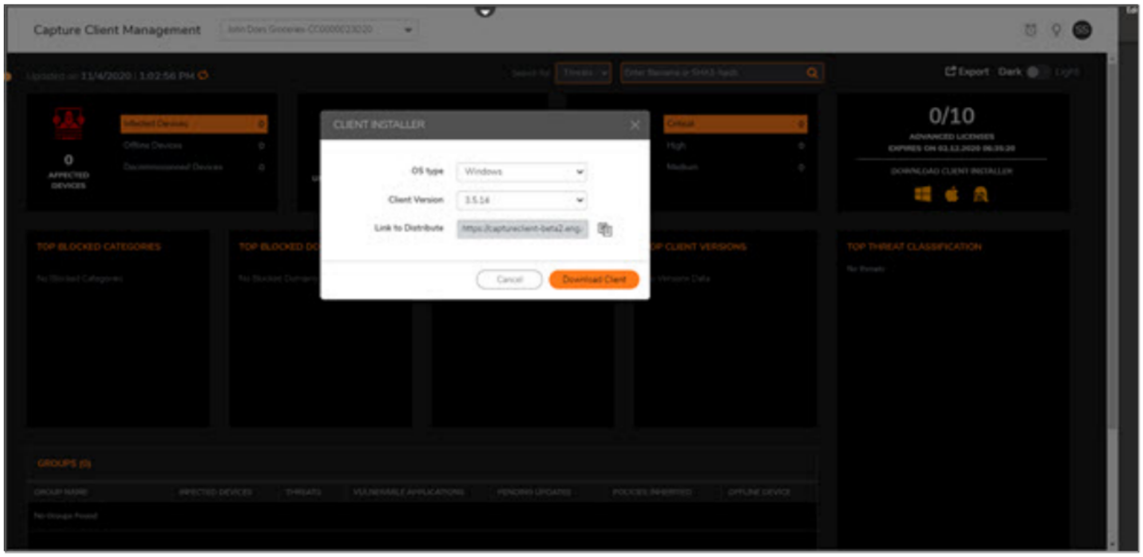
[162]

159. Every ’918 Accused Product practices configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions. For example, Capture Client is a software service downloaded on the endpoint for monitoring the endpoint.

[162] https://www.sonicwall.com/techdocs/pdf/capture_client-protecting_assets.pdf, at 10-22.

Pre-Configured Client Installation

The Dashboard provides access to the **Download** links that can be used to download the clients for each OS type with choices for versions. We always recommend installing the latest General Release version. You can also copy the link to distribute the client via custom installation scripts or third-party platforms like software deployment tools and Remote Monitoring & Management tools.

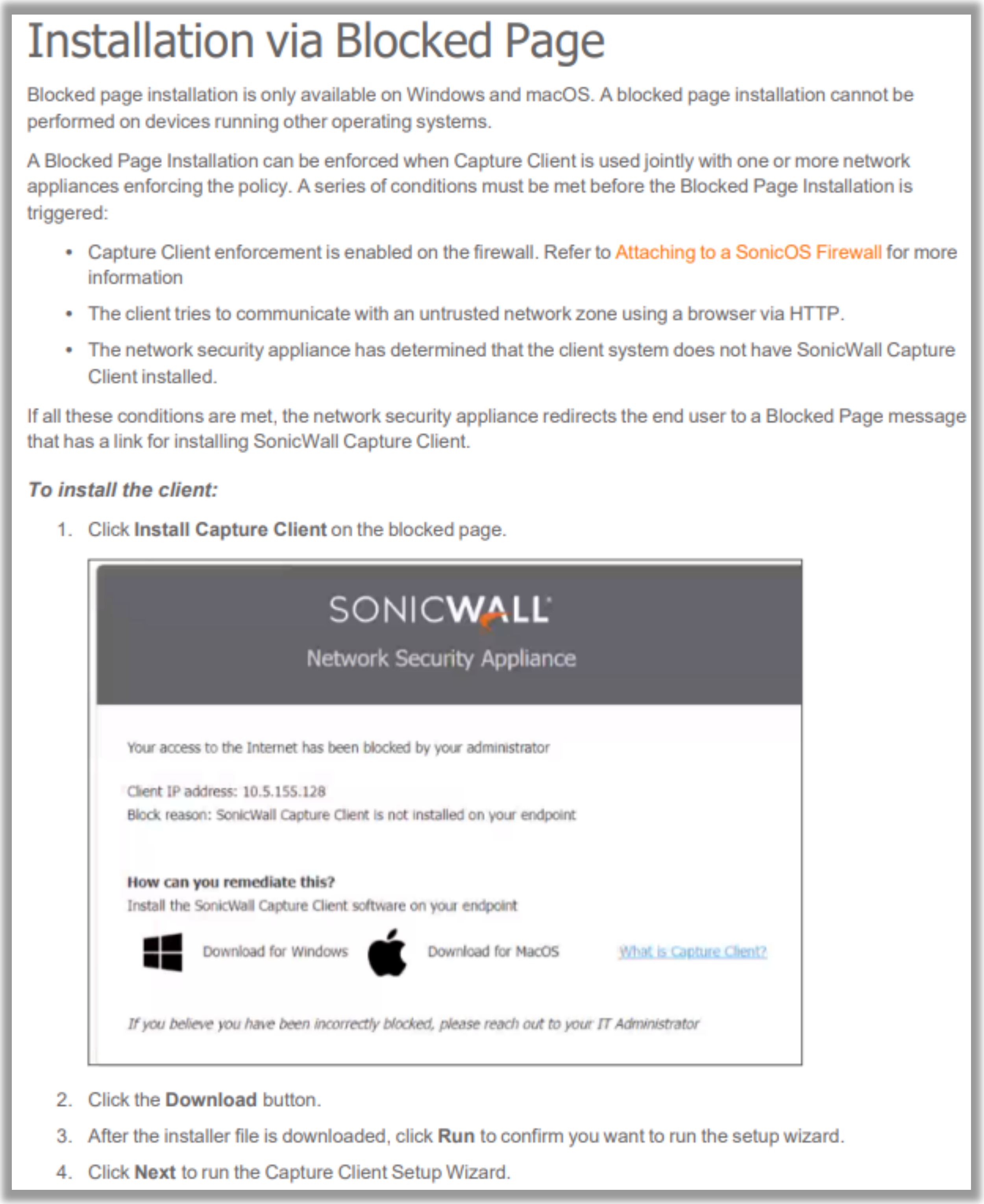


OS type: Windows

Client Version: 3.5.14

Link to Distribute: https://captureclient-beta2.eng

The clients downloaded this are pre-configured with licensing details for your tenant and end users are not prompted to enter any information as part of the installation process.



Installation via Blocked Page

Blocked page installation is only available on Windows and macOS. A blocked page installation cannot be performed on devices running other operating systems.

A Blocked Page Installation can be enforced when Capture Client is used jointly with one or more network appliances enforcing the policy. A series of conditions must be met before the Blocked Page Installation is triggered:

- Capture Client enforcement is enabled on the firewall. Refer to Attaching to a SonicOS Firewall for more information
- The client tries to communicate with an untrusted network zone using a browser via HTTP.
- The network security appliance has determined that the client system does not have SonicWall Capture Client installed.

If all these conditions are met, the network security appliance redirects the end user to a Blocked Page message that has a link for installing SonicWall Capture Client.

To install the client:

1. Click **Install Capture Client** on the blocked page.

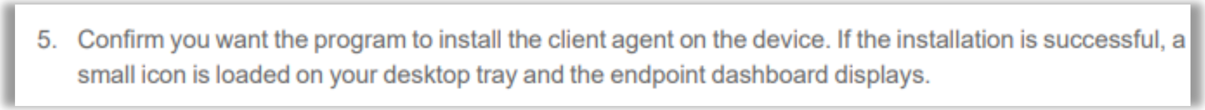
Your access to the Internet has been blocked by your administrator

Client IP address: 10.5.155.128
Block reason: SonicWall Capture Client is not installed on your endpoint

How can you remediate this?
Install the SonicWall Capture Client software on your endpoint

If you believe you have been incorrectly blocked, please reach out to your IT Administrator

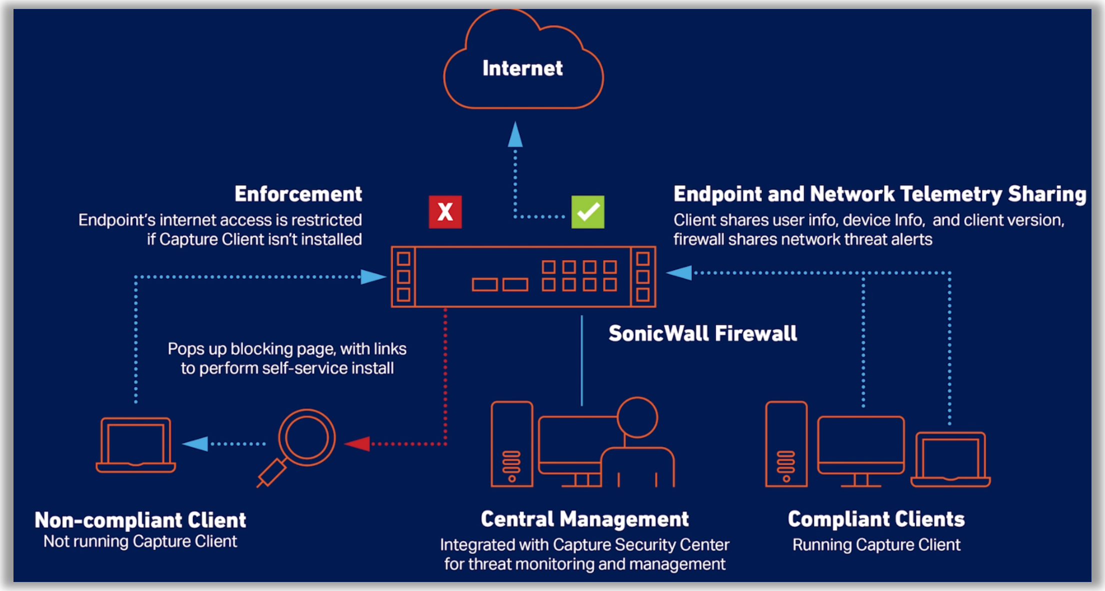
2. Click the **Download** button.
3. After the installer file is downloaded, click **Run** to confirm you want to run the setup wizard.
4. Click **Next** to run the Capture Client Setup Wizard.



5. Confirm you want the program to install the client agent on the device. If the installation is successful, a small icon is loaded on your desktop tray and the endpoint dashboard displays.

[163]

160. Every ’918 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint. For example, Capture Client provides endpoint telemetry sharing, including user info, device info, and client version and monitors the endpoint for new threats in order to “generate reports of the state of your environment and endpoints.”



Internet

Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts

SonicWall Firewall

Pops up blocking page, with links to perform self-service install

Non-compliant Client
Not running Capture Client

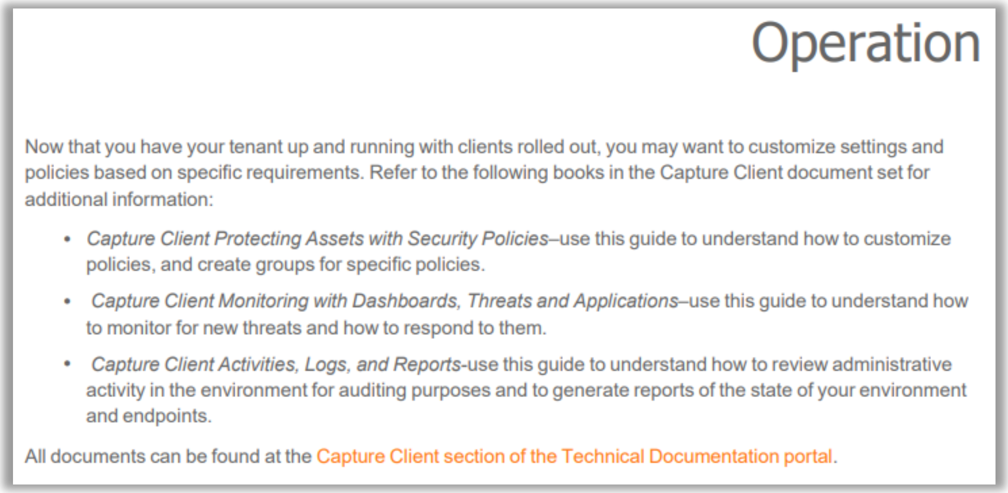
Central Management
Integrated with Capture Security Center for threat monitoring and management

Compliant Clients
Running Capture Client

[164]

[163] https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 22-24.

[164] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112



Operation

Now that you have your tenant up and running with clients rolled out, you may want to customize settings and policies based on specific requirements. Refer to the following books in the Capture Client document set for additional information:

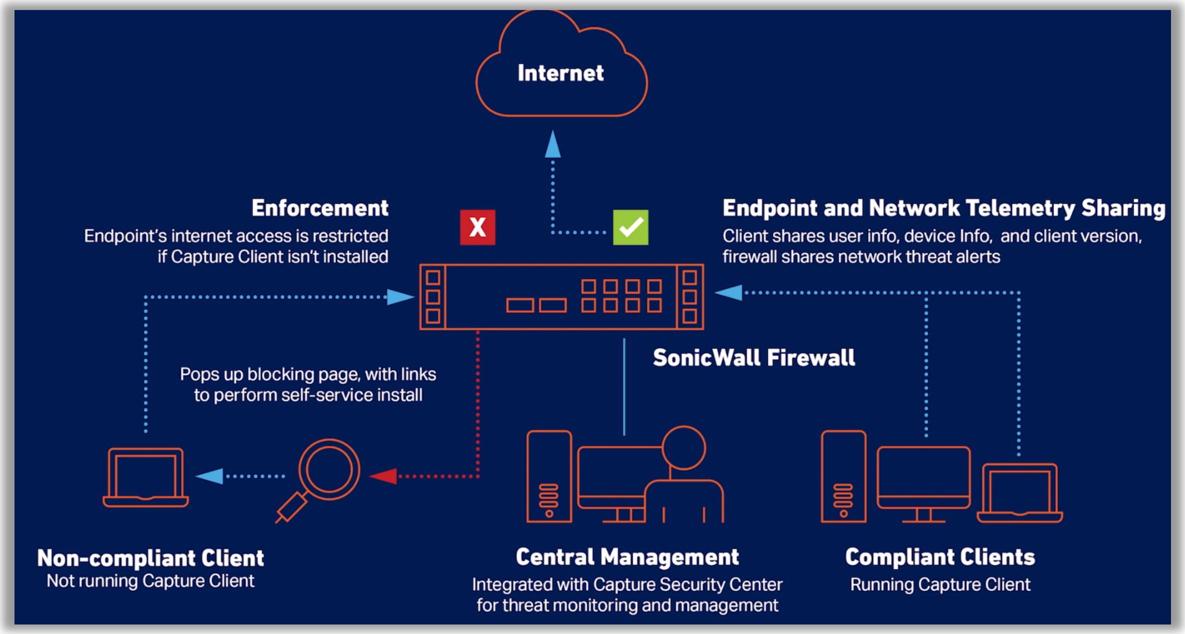
- *Capture Client Protecting Assets with Security Policies*–use this guide to understand how to customize policies, and create groups for specific policies.
- *Capture Client Monitoring with Dashboards, Threats and Applications*–use this guide to understand how to monitor for new threats and how to respond to them.
- *Capture Client Activities, Logs, and Reports*-use this guide to understand how to review administrative activity in the environment for auditing purposes and to generate reports of the state of your environment and endpoints.

All documents can be found at the Capture Client section of the Technical Documentation portal.

[165]

161. Every ’918 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store. For example, Capture Client determines a compliance state of the endpoint based on whether the monitored status information meets the compliances policies that are managed at the cloud-based management console. For further example, a basic policy is whether Capture Client is running on the endpoint. If so, the endpoint is compliant; if not, the endpoint is not compliant.

[165] https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 27.



Internet

Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts

SonicWall Firewall

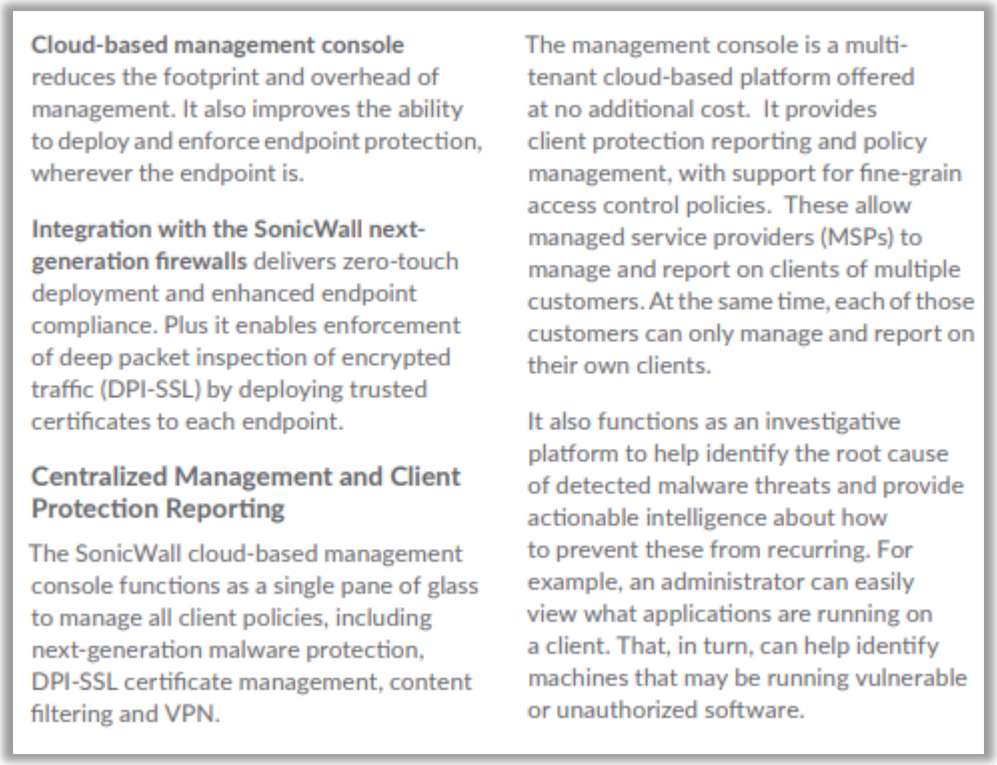
Pops up blocking page, with links to perform self-service install

Non-compliant Client
Not running Capture Client

Central Management
Integrated with Capture Security Center for threat monitoring and management

Compliant Clients
Running Capture Client

[166]



Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

Centralized Management and Client Protection Reporting

The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

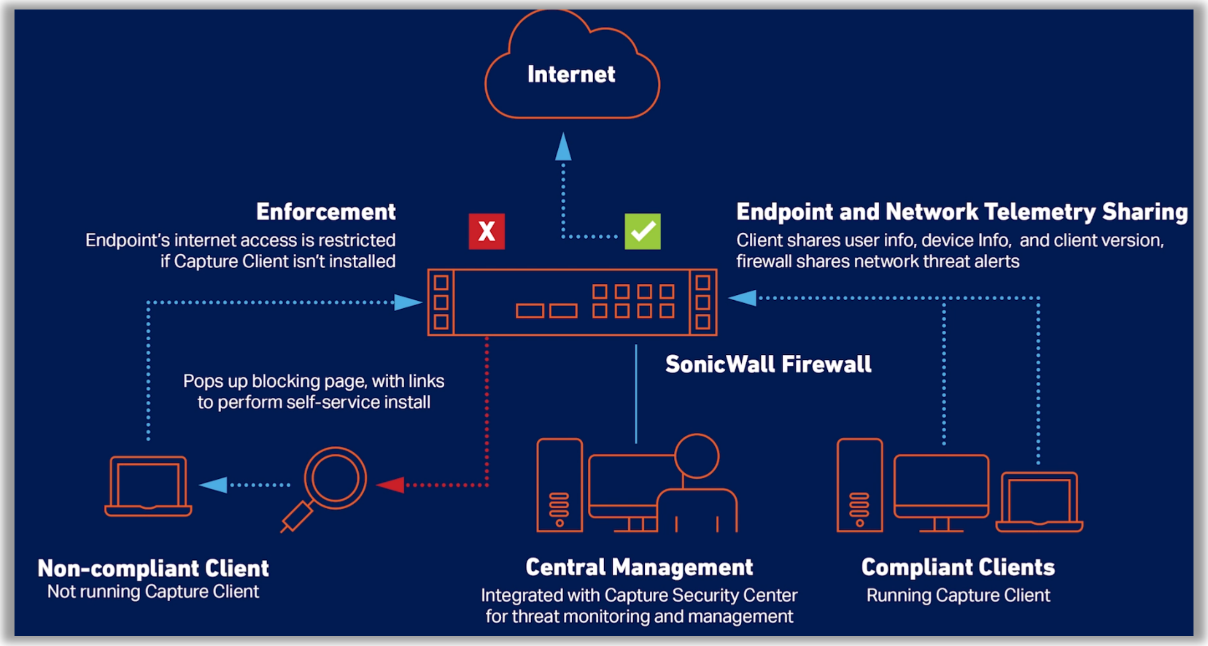
It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.

[167]

[166] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[167] https://www.sonicwall.com/medialibrary/pt/datasheet/sonicwall-capture-client.pdf

162. Every ’918 Accused Product authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state. For example, if an endpoint is not compliant by having downloaded the Capture Client, an identified action is that Internet access may be blocked (i.e., authorizing access by the endpoint to a computing resource on the network)._



Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts

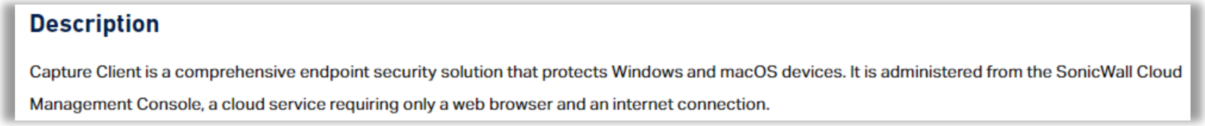
Pops up blocking page, with links to perform self-service install

Non-compliant Client
Not running Capture Client

Central Management
Integrated with Capture Security Center for threat monitoring and management

Compliant Clients
Running Capture Client

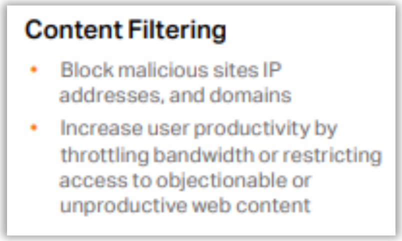
[168]



Description

Capture Client is a comprehensive endpoint security solution that protects Windows and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection.

[169]



Content Filtering

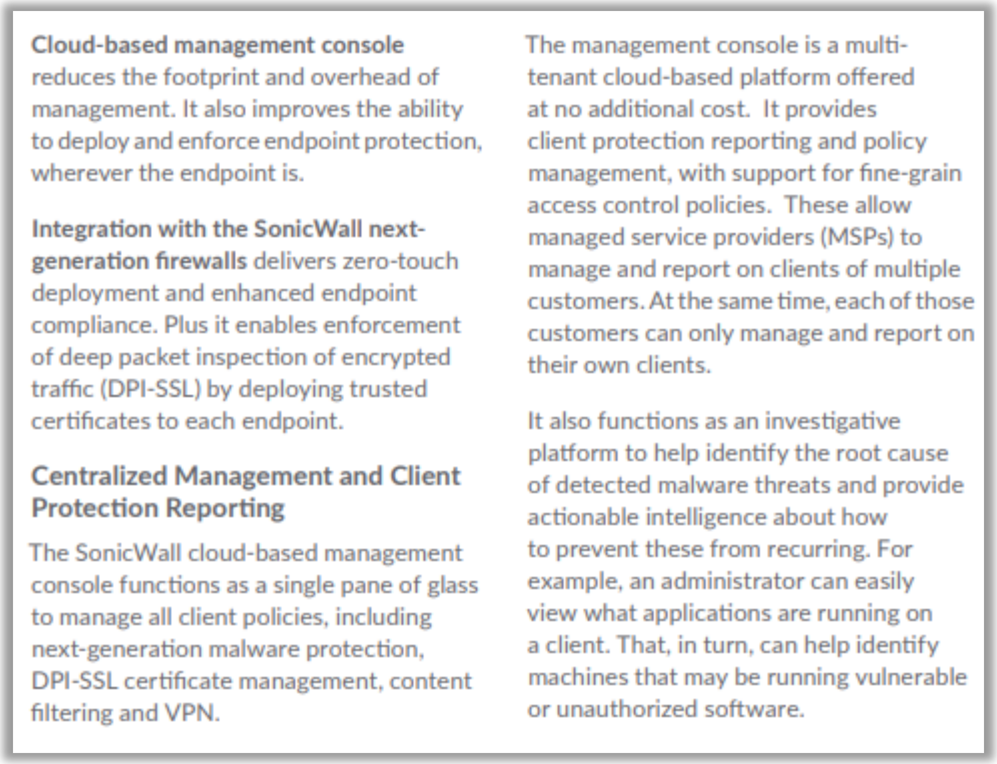
- Block malicious sites IP addresses, and domains
- Increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content

[170]

[168] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[169] https://www.sonicwall.com/support/knowledge-base/capture-client-system-requirements/210512075820480/

[170] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.



Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

Centralized Management and Client Protection Reporting

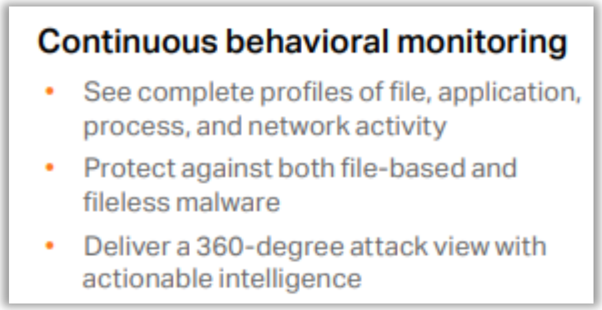
The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.

[171]

163. Every ’918 Accused Product continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes. For example, Capture Client performs continuous behavioral monitoring and “continuously monitors for suspicious activity” so that access may be restricted to computing resources if the compliance state of the endpoint changes (e.g., “increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content”).



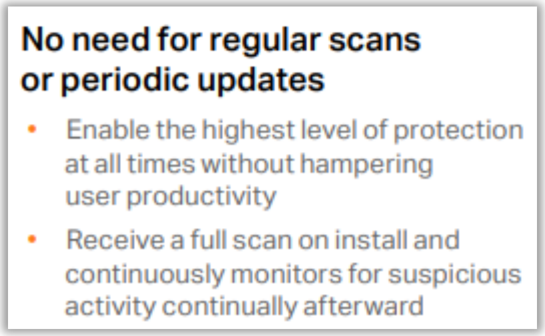
Continuous behavioral monitoring

- See complete profiles of file, application, process, and network activity
- Protect against both file-based and fileless malware
- Deliver a 360-degree attack view with actionable intelligence

[172]

[171] https://www.sonicwall.com/medialibrary/pt/datasheet/sonicwall-capture-client.pdf

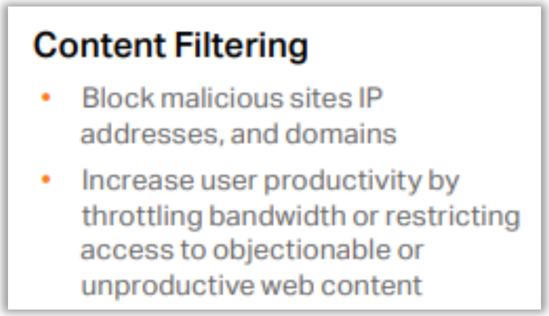
[172] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.



No need for regular scans or periodic updates

- Enable the highest level of protection at all times without hampering user productivity
- Receive a full scan on install and continuously monitors for suspicious activity continually afterward

[173]



Content Filtering

- Block malicious sites IP addresses, and domains
- Increase user productivity by throttling bandwidth or restricting access to objectionable or unproductive web content

[174]

164. Defendant has and continues to directly infringe one or more claims of the ’918 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

165. Defendant has and continues to indirectly infringe one or more claims of the ’918 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’918 Accused Products.

166. Defendant has and continues to indirectly infringe one or more claims of the ’918 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing

[173] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.
[174] https://www.sonicwall.com/medialibrary/en/datasheet/sonicwall-capture-client.pdf, at 2.

into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’918 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’918 Patent by providing these products to customers and end-users for use in an infringing manner.

167. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’918 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing manner, including at least though its SonicWall Technical Documentation,[175] Video Tutorials,[176] SonicWall University,[177] and Customer Service[178] websites.

168. Defendant has and continues to indirectly infringe one or more claims of the ’918 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’918 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls or Capture Client. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’918 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-

[175] https://www.sonicwall.com/support/technical-documentation/?language=English

[176] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[177] https://www.sonicwall.com/partners/sonicwall-university/

[178] https://www.sonicwall.com/support/contact-support/customer-service/

infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’918 Patent but remained willfully blind to the infringing nature of others’ actions.

169. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’918 Patent in an amount to be proved at trial.

170. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’918 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

171. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’918 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’918 Patent. Upon information and belief, Defendant had actual knowledge of the ’918 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’9183 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

COUNT IX
(Infringement of the ’997 Patent)

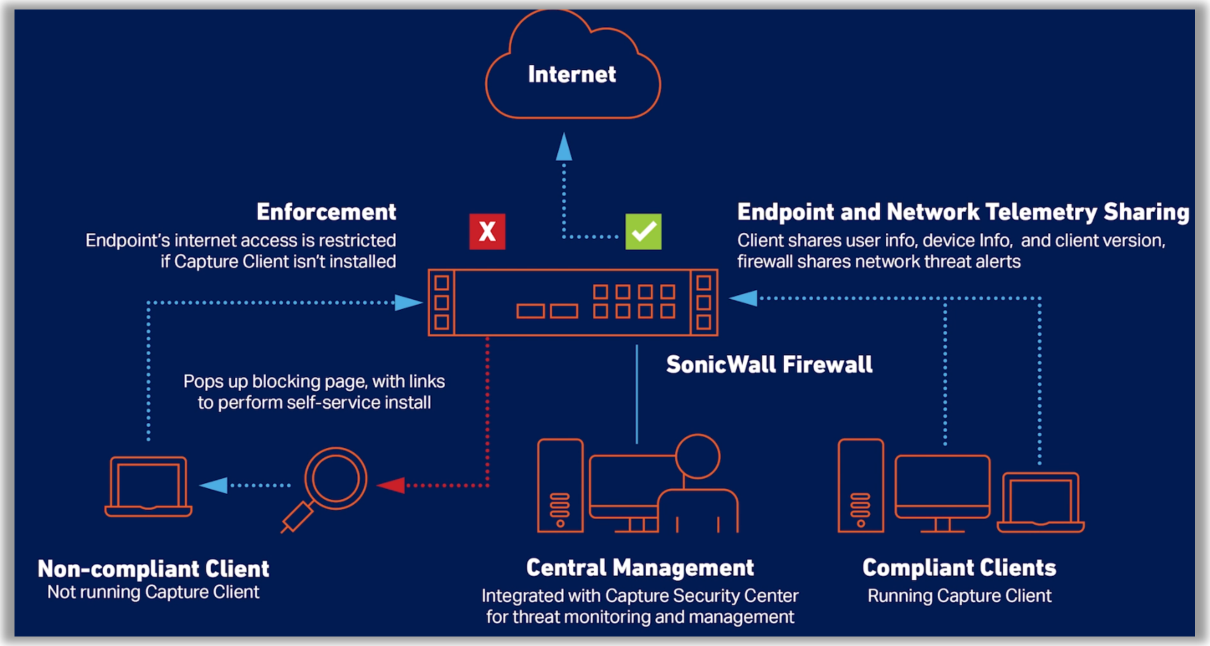
172. Paragraphs 1 through 30 are incorporated by reference as if fully set forth herein.

173. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’997 Patent.

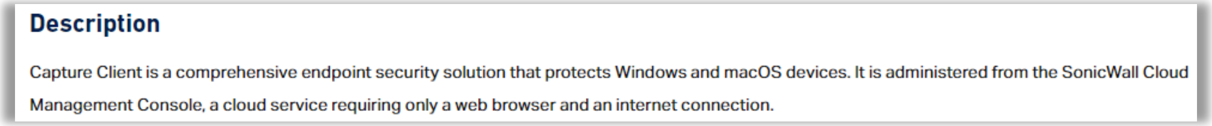
174. Defendant has and continues to directly infringe the ’997 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’997 Patent. Such products include at least SonicWall Capture Client alone, or in combination with SonicWall’s SOHO / TZ Series Firewalls (including at least TZ670, TZ570/TZ570P/TZ570W, TZ470/TZ470W, TZ370/TZ370W, TZ270/TZ270W, TZ600/TZ600P, TZ500/TZ500W, TZ400/TZ400W, TZ350/TZ350W, TZ300/TZ300P/TZ300W, and SOHO 250/SOHO 250W), NSa Series Firewalls (including at least NSa 6700, NSa 5700, NSa 4700, NSa 3700, NSa 2700, NSa 9650, NSa 9450, NSa 9250, NSa 6650, NSa 5650, NSa 4650, NSa 3650, and NSa 2650), NSsp Series Firewalls (including at least NSsp 15700, NSsp 13700, NSsp 11700, NSsp 10700, NSsp 12800, and NSsp 12400), NSv Series Firewalls (including at least NSv 870, NSv 470, and NSv 270) (the “’997 Accused Products”) which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing

system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.

175. Every ’997 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies. For example, Capture Client “is administered from the SonicWall Cloud Management Console” (e.g., a computing system remote from the endpoint), “a cloud service requiring only a web browser and an internet connection.


Internet
Enforcement
Endpoint’s internet access is restricted if Capture Client isn’t installed
X
✓
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center for threat monitoring and management
Compliant Clients
Running Capture Client

[179]



Description

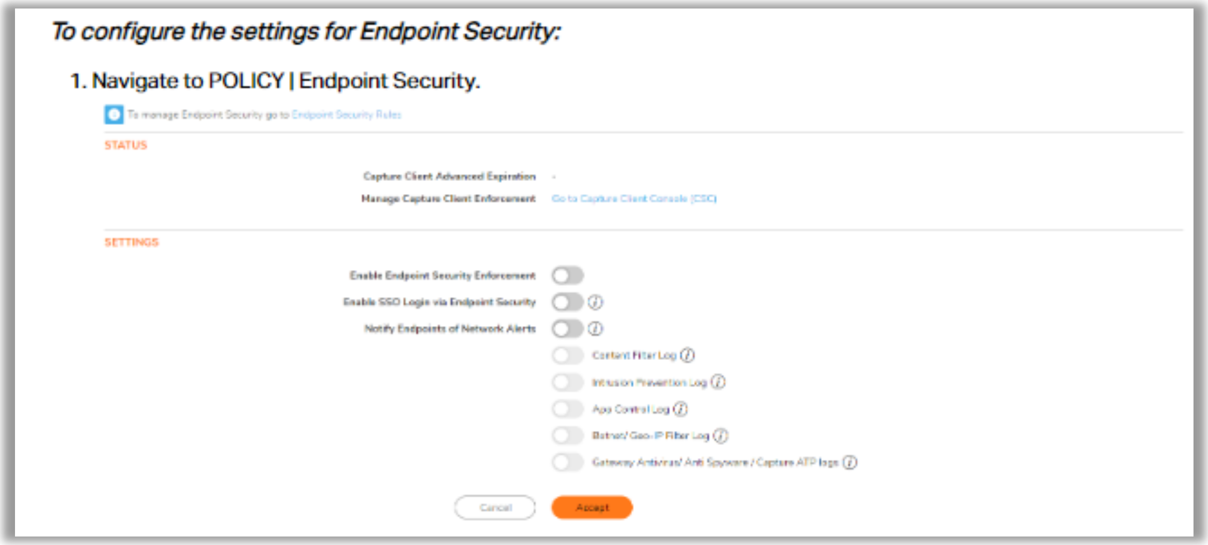
Capture Client is a comprehensive endpoint security solution that protects Windows and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection.

[180]

[179] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[180] https://www.sonicwall.com/support/knowledge-base/capture-client-system-requirements/210512075820480/

176. Every ’997 Accused Product practices maintaining the plurality of policies in a data store on the computing system. For example, Capture Client allows the storage of various endpoint security policies: “POLICY | Endpoint Security.” These policies can later be managed through the Capture Client Console, indicating that they are stored on the computing system.



To configure the settings for Endpoint Security:

1. Navigate to POLICY | Endpoint Security.

To manage Endpoint Security go to Endpoint Security Rules

STATUS

Capture Client Advanced Expiration -

Manage Capture Client Enforcement Go to Capture Client Console (CSC)

SETTINGS

Enable Endpoint Security Enforcement ○

Enable SSO Login via Endpoint Security ○

Notify Endpoints of Network Alerts ○

○ Content Filter Log

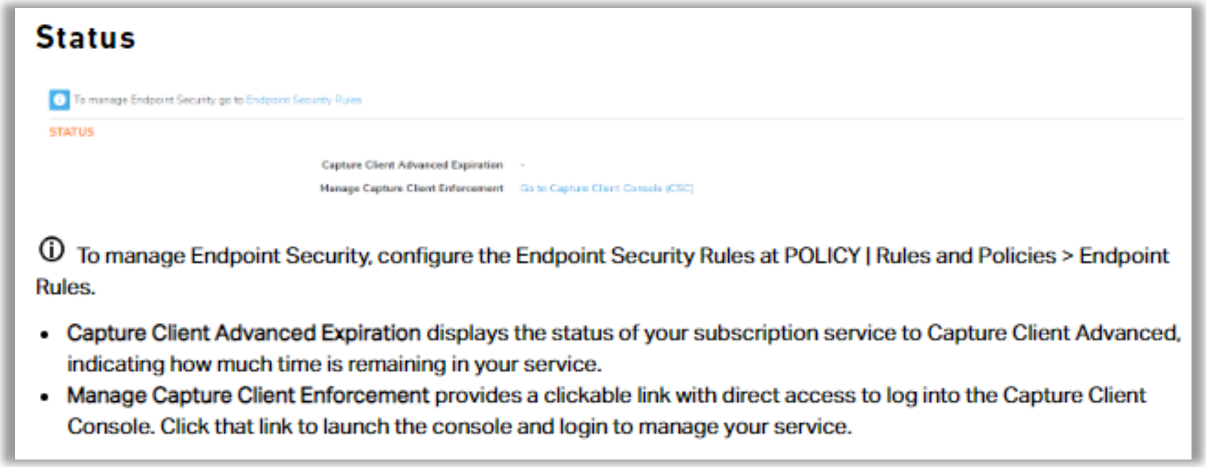
○ Intrusion Prevention Log

○ App Control Log

○ Botnet/ Geo-IP Filter Log

○ Gateway Antivirus/ Anti Spyware / Capture ATP logs

[181]



Status

To manage Endpoint Security go to Endpoint Security Rules

STATUS

Capture Client Advanced Expiration -

Manage Capture Client Enforcement Go to Capture Client Console (CSC)

ⓘ To manage Endpoint Security, configure the Endpoint Security Rules at POLICY | Rules and Policies > Endpoint Rules.

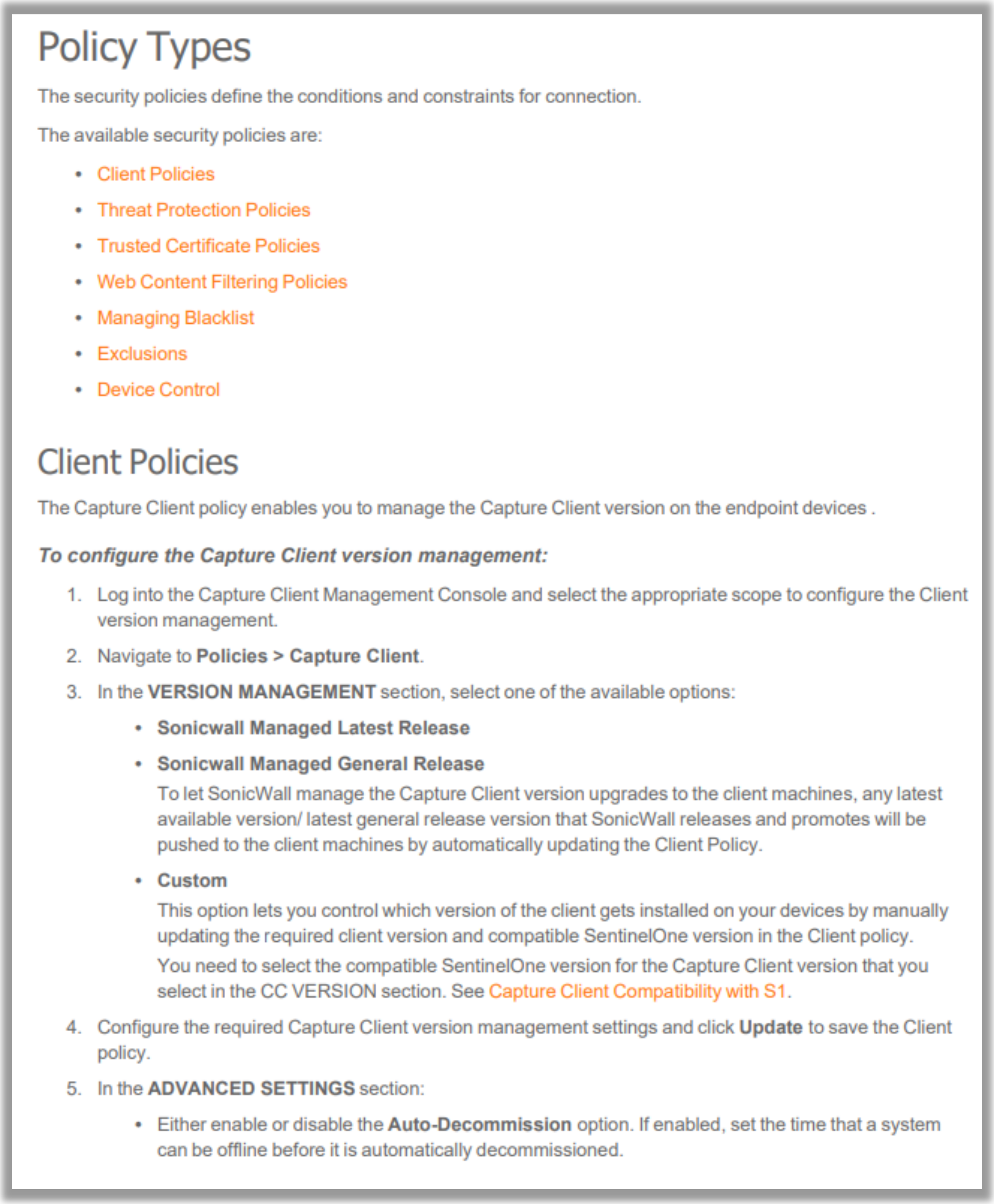
- **Capture Client Advanced Expiration** displays the status of your subscription service to Capture Client Advanced, indicating how much time is remaining in your service.
- **Manage Capture Client Enforcement** provides a clickable link with direct access to log into the Capture Client Console. Click that link to launch the console and login to manage your service.

[182]

[181] https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-endpoint_security/Content/endpoint-security.htm/

[182] https://www.sonicwall.com/support/technical-documentation/docs/sonicos-7-0-0-0-endpoint_security/Content/endpoint-security-status.htm/

177. Every ’997 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Capture Client identifies, from the plurality of policies, operating conditions (*e.g.*, threats and suspicious activities) on the endpoint to monitor in order to determine mitigation mode: Detect, Protect, or Capture ATP.



Policy Types

The security policies define the conditions and constraints for connection.

The available security policies are:

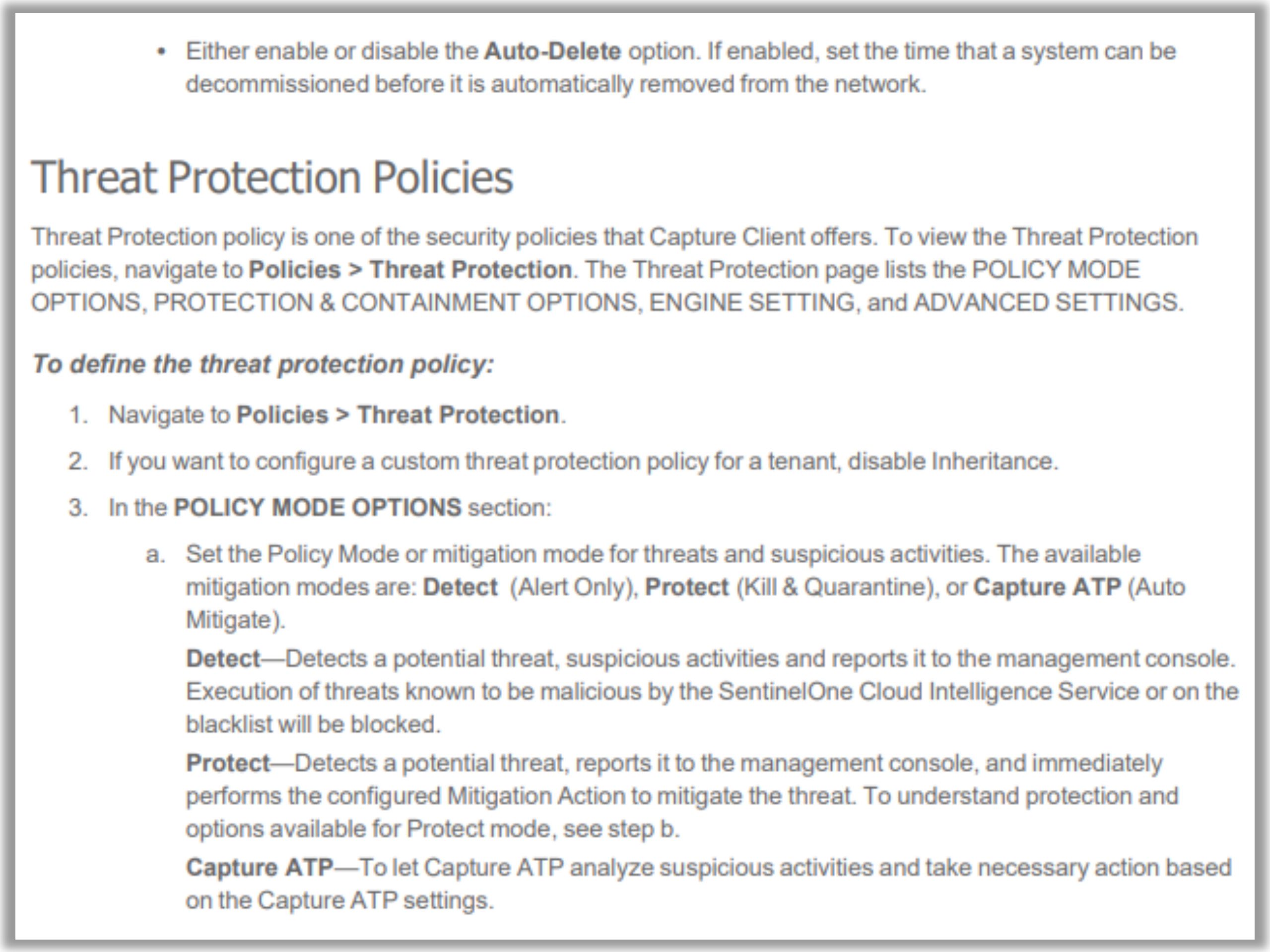
- Client Policies
- Threat Protection Policies
- Trusted Certificate Policies
- Web Content Filtering Policies
- Managing Blacklist
- Exclusions
- Device Control

Client Policies

The Capture Client policy enables you to manage the Capture Client version on the endpoint devices .

To configure the Capture Client version management:

1. Log into the Capture Client Management Console and select the appropriate scope to configure the Client version management.
2. Navigate to **Policies > Capture Client**.
3. In the **VERSION MANAGEMENT** section, select one of the available options:
    - **Sonicwall Managed Latest Release**
    - **Sonicwall Managed General Release**
      To let SonicWall manage the Capture Client version upgrades to the client machines, any latest available version/ latest general release version that SonicWall releases and promotes will be pushed to the client machines by automatically updating the Client Policy.
    - **Custom**
      This option lets you control which version of the client gets installed on your devices by manually updating the required client version and compatible SentinelOne version in the Client policy.
      You need to select the compatible SentinelOne version for the Capture Client version that you select in the CC VERSION section. See Capture Client Compatibility with S1.
4. Configure the required Capture Client version management settings and click **Update** to save the Client policy.
5. In the **ADVANCED SETTINGS** section:
    - Either enable or disable the **Auto-Decommission** option. If enabled, set the time that a system can be offline before it is automatically decommissioned.



- Either enable or disable the **Auto-Delete** option. If enabled, set the time that a system can be decommissioned before it is automatically removed from the network.

Threat Protection Policies

Threat Protection policy is one of the security policies that Capture Client offers. To view the Threat Protection policies, navigate to **Policies > Threat Protection**. The Threat Protection page lists the POLICY MODE OPTIONS, PROTECTION & CONTAINMENT OPTIONS, ENGINE SETTING, and ADVANCED SETTINGS.

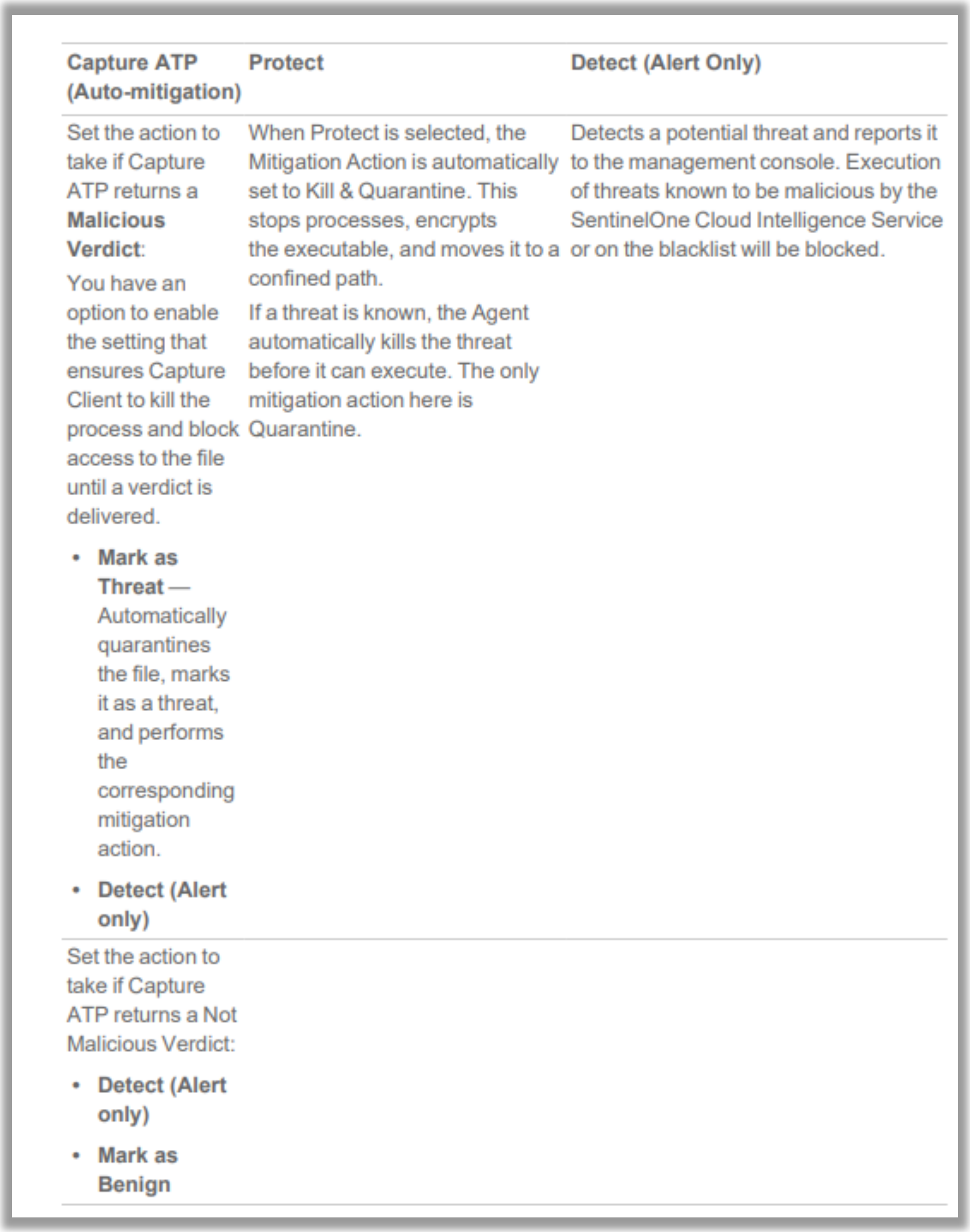
To define the threat protection policy:

1. Navigate to **Policies > Threat Protection**.
2. If you want to configure a custom threat protection policy for a tenant, disable Inheritance.
3. In the **POLICY MODE OPTIONS** section:
   a. Set the Policy Mode or mitigation mode for threats and suspicious activities. The available mitigation modes are: **Detect** (Alert Only), **Protect** (Kill & Quarantine), or **Capture ATP** (Auto Mitigate).

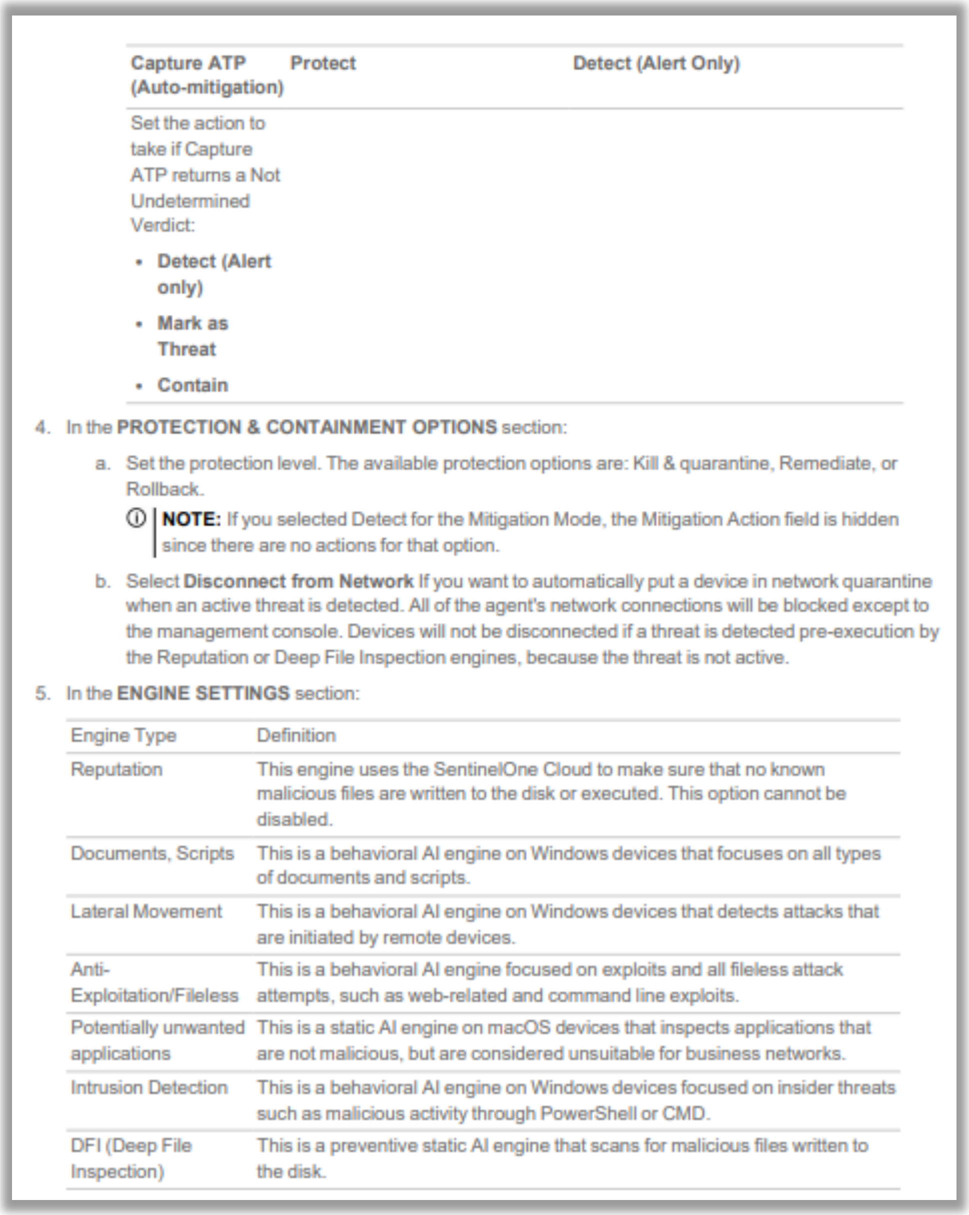
      Detect—Detects a potential threat, suspicious activities and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.

      Protect—Detects a potential threat, reports it to the management console, and immediately performs the configured Mitigation Action to mitigate the threat. To understand protection and options available for Protect mode, see step b.

      Capture ATP—To let Capture ATP analyze suspicious activities and take necessary action based on the Capture ATP settings.



Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a **Malicious Verdict**: You have an option to enable the setting that ensures Capture Client to kill the process and block access to the file until a verdict is delivered. • **Mark as Threat** — Automatically quarantines the file, marks it as a threat, and performs the corresponding mitigation action. • **Detect (Alert only)**	When Protect is selected, the Mitigation Action is automatically set to Kill & Quarantine. This stops processes, encrypts the executable, and moves it to a confined path. If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action here is Quarantine.	Detects a potential threat and reports it to the management console. Execution of threats known to be malicious by the SentinelOne Cloud Intelligence Service or on the blacklist will be blocked.
Set the action to take if Capture ATP returns a Not Malicious Verdict: • **Detect (Alert only)** • **Mark as Benign**		



Capture ATP (Auto-mitigation)	Protect	Detect (Alert Only)
Set the action to take if Capture ATP returns a Not Undetermined Verdict: • **Detect (Alert only)** • **Mark as Threat** • **Contain**		

4. In the **PROTECTION & CONTAINMENT OPTIONS** section:

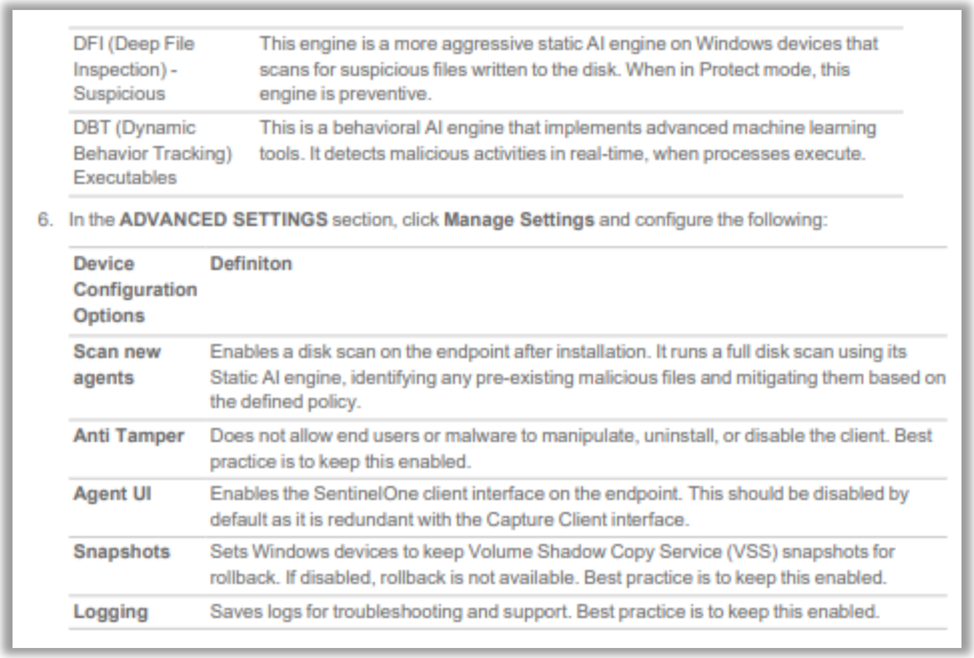
   a. Set the protection level. The available protection options are: Kill & quarantine, Remediate, or Rollback.

   ⓘ **NOTE:** If you selected Detect for the Mitigation Mode, the Mitigation Action field is hidden since there are no actions for that option.

   b. Select **Disconnect from Network** If you want to automatically put a device in network quarantine when an active threat is detected. All of the agent's network connections will be blocked except to the management console. Devices will not be disconnected if a threat is detected pre-execution by the Reputation or Deep File Inspection engines, because the threat is not active.

5. In the **ENGINE SETTINGS** section:

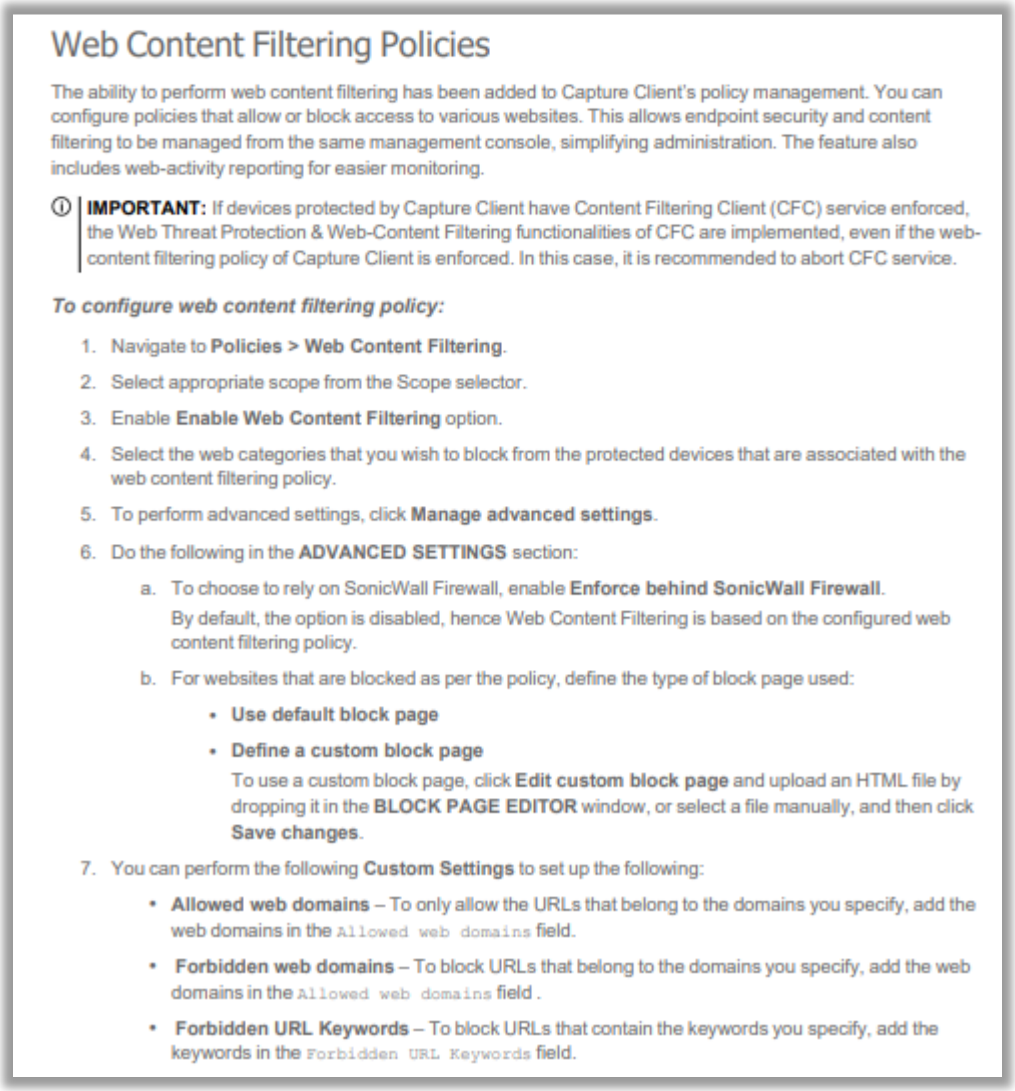
Engine Type	Definition
Reputation	This engine uses the SentinelOne Cloud to make sure that no known malicious files are written to the disk or executed. This option cannot be disabled.
Documents, Scripts	This is a behavioral AI engine on Windows devices that focuses on all types of documents and scripts.
Lateral Movement	This is a behavioral AI engine on Windows devices that detects attacks that are initiated by remote devices.
Anti-Exploitation/Fileless	This is a behavioral AI engine focused on exploits and all fileless attack attempts, such as web-related and command line exploits.
Potentially unwanted applications	This is a static AI engine on macOS devices that inspects applications that are not malicious, but are considered unsuitable for business networks.
Intrusion Detection	This is a behavioral AI engine on Windows devices focused on insider threats such as malicious activity through PowerShell or CMD.
DFI (Deep File Inspection)	This is a preventive static AI engine that scans for malicious files written to the disk.



DFI (Deep File Inspection) - Suspicious	This engine is a more aggressive static AI engine on Windows devices that scans for suspicious files written to the disk. When in Protect mode, this engine is preventive.
DBT (Dynamic Behavior Tracking) Executables	This is a behavioral AI engine that implements advanced machine learning tools. It detects malicious activities in real-time, when processes execute.

6. In the **ADVANCED SETTINGS** section, click **Manage Settings** and configure the following:

Device Configuration Options	Definiton
Scan new agents	Enables a disk scan on the endpoint after installation. It runs a full disk scan using its Static AI engine, identifying any pre-existing malicious files and mitigating them based on the defined policy.
Anti Tamper	Does not allow end users or malware to manipulate, uninstall, or disable the client. Best practice is to keep this enabled.
Agent UI	Enables the SentinelOne client interface on the endpoint. This should be disabled by default as it is redundant with the Capture Client interface.
Snapshots	Sets Windows devices to keep Volume Shadow Copy Service (VSS) snapshots for rollback. If disabled, rollback is not available. Best practice is to keep this enabled.
Logging	Saves logs for troubleshooting and support. Best practice is to keep this enabled.



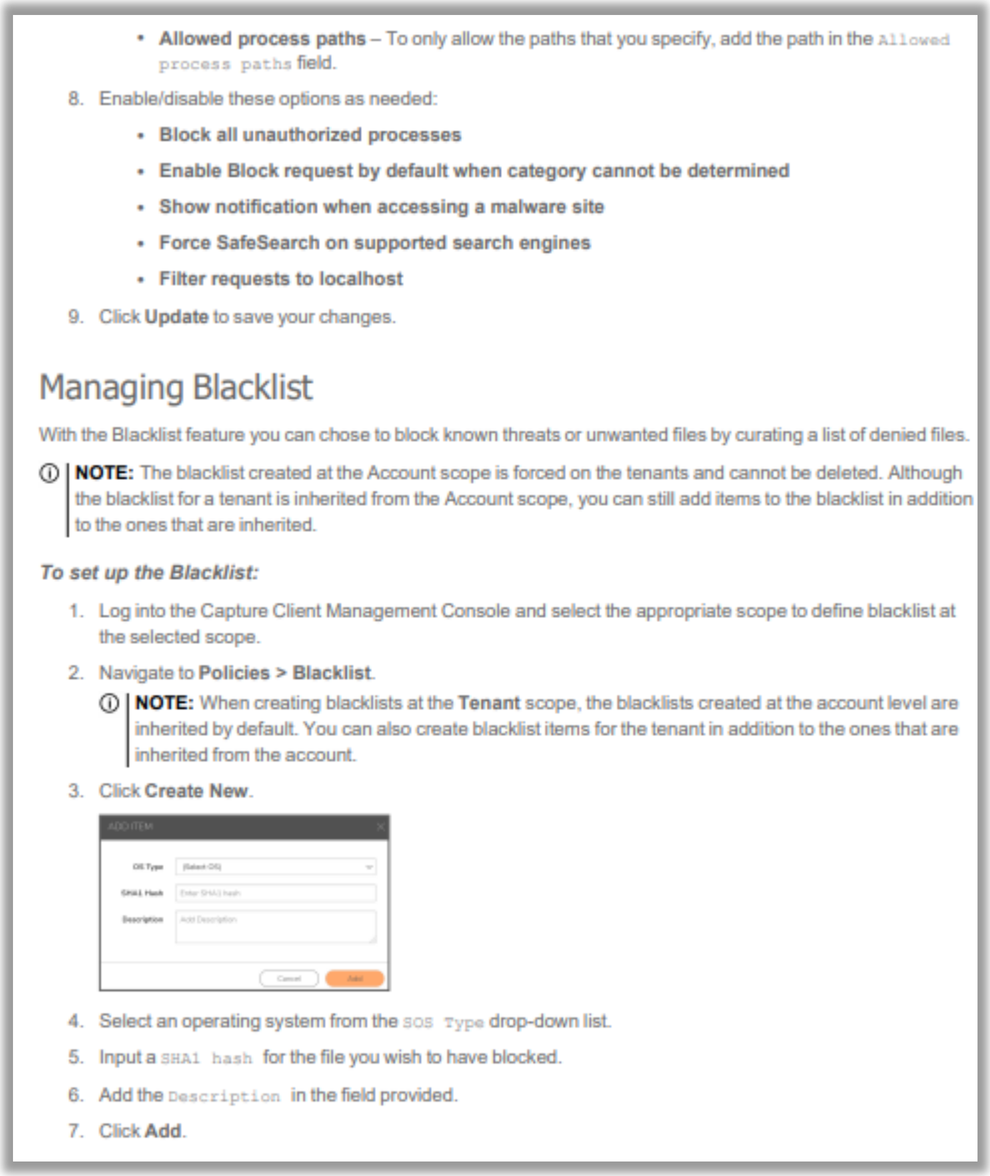
Web Content Filtering Policies

The ability to perform web content filtering has been added to Capture Client's policy management. You can configure policies that allow or block access to various websites. This allows endpoint security and content filtering to be managed from the same management console, simplifying administration. The feature also includes web-activity reporting for easier monitoring.

ⓘ **IMPORTANT:** If devices protected by Capture Client have Content Filtering Client (CFC) service enforced, the Web Threat Protection & Web-Content Filtering functionalities of CFC are implemented, even if the web-content filtering policy of Capture Client is enforced. In this case, it is recommended to abort CFC service.

To configure web content filtering policy:

1. Navigate to **Policies > Web Content Filtering**.
2. Select appropriate scope from the Scope selector.
3. Enable **Enable Web Content Filtering** option.
4. Select the web categories that you wish to block from the protected devices that are associated with the web content filtering policy.
5. To perform advanced settings, click **Manage advanced settings**.
6. Do the following in the **ADVANCED SETTINGS** section:
   a. To choose to rely on SonicWall Firewall, enable **Enforce behind SonicWall Firewall**.
      By default, the option is disabled, hence Web Content Filtering is based on the configured web content filtering policy.
   b. For websites that are blocked as per the policy, define the type of block page used:
      - **Use default block page**
      - **Define a custom block page**
        To use a custom block page, click **Edit custom block page** and upload an HTML file by dropping it in the **BLOCK PAGE EDITOR** window, or select a file manually, and then click **Save changes**.
7. You can perform the following **Custom Settings** to set up the following:
   - **Allowed web domains** – To only allow the URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field.
   - **Forbidden web domains** – To block URLs that belong to the domains you specify, add the web domains in the `Allowed web domains` field .
   - **Forbidden URL Keywords** – To block URLs that contain the keywords you specify, add the keywords in the `Forbidden URL Keywords` field.



- **Allowed process paths** – To only allow the paths that you specify, add the path in the `Allowed process paths` field.

8. Enable/disable these options as needed:
    - **Block all unauthorized processes**
    - **Enable Block request by default when category cannot be determined**
    - **Show notification when accessing a malware site**
    - **Force SafeSearch on supported search engines**
    - **Filter requests to localhost**
9. Click **Update** to save your changes.

Managing Blacklist

With the Blacklist feature you can chose to block known threats or unwanted files by curating a list of denied files.

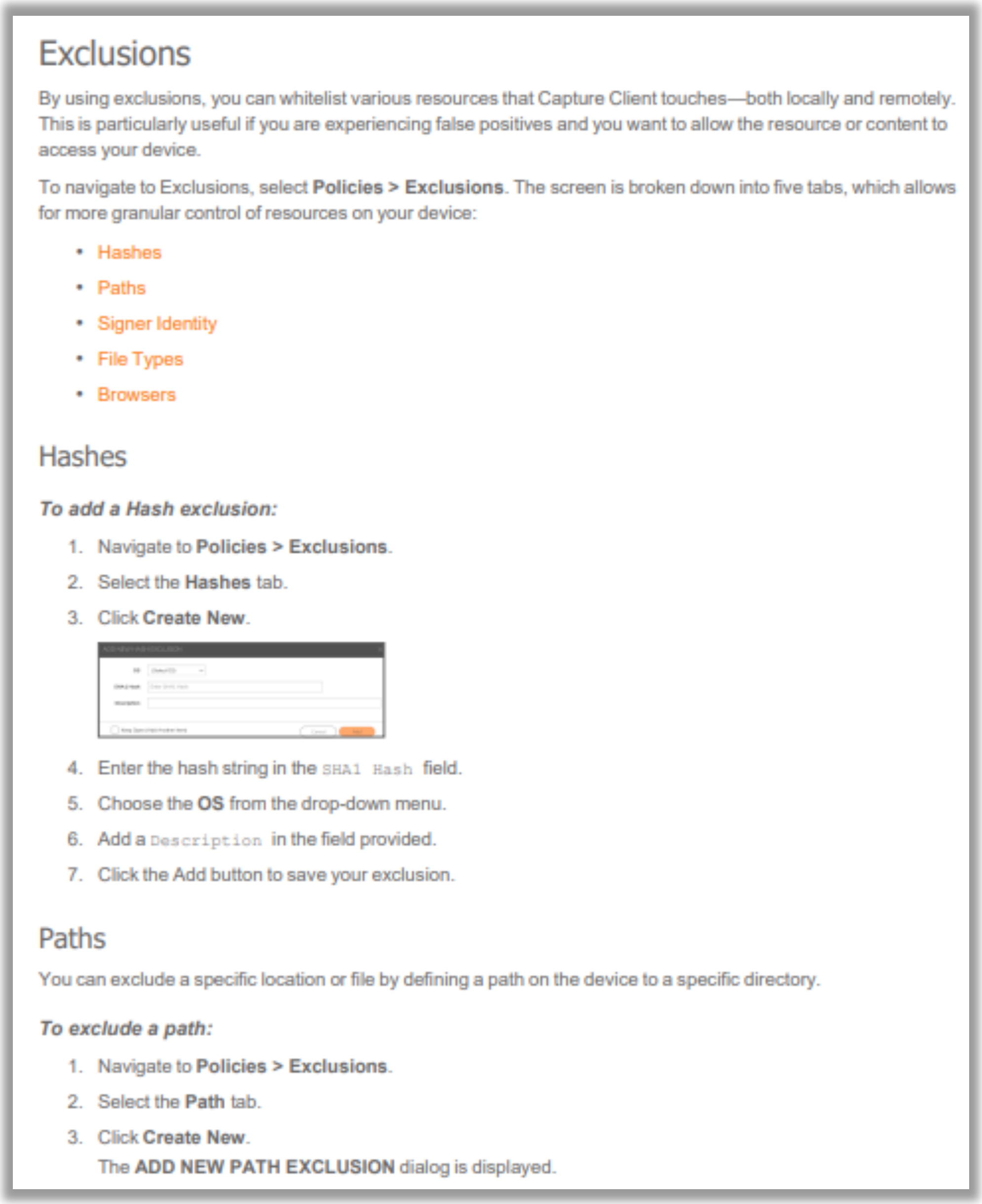
ⓘ **NOTE:** The blacklist created at the Account scope is forced on the tenants and cannot be deleted. Although the blacklist for a tenant is inherited from the Account scope, you can still add items to the blacklist in addition to the ones that are inherited.

To set up the Blacklist:

1. Log into the Capture Client Management Console and select the appropriate scope to define blacklist at the selected scope.
2. Navigate to **Policies > Blacklist**.

    ⓘ **NOTE:** When creating blacklists at the **Tenant** scope, the blacklists created at the account level are inherited by default. You can also create blacklist items for the tenant in addition to the ones that are inherited from the account.
3. Click **Create New**.

4. Select an operating system from the `SOS Type` drop-down list.
5. Input a `SHA1 hash` for the file you wish to have blocked.
6. Add the `Description` in the field provided.
7. Click **Add**.



Exclusions

By using exclusions, you can whitelist various resources that Capture Client touches—both locally and remotely. This is particularly useful if you are experiencing false positives and you want to allow the resource or content to access your device.

To navigate to Exclusions, select **Policies > Exclusions**. The screen is broken down into five tabs, which allows for more granular control of resources on your device:

- Hashes
- Paths
- Signer Identity
- File Types
- Browsers

Hashes

To add a Hash exclusion:

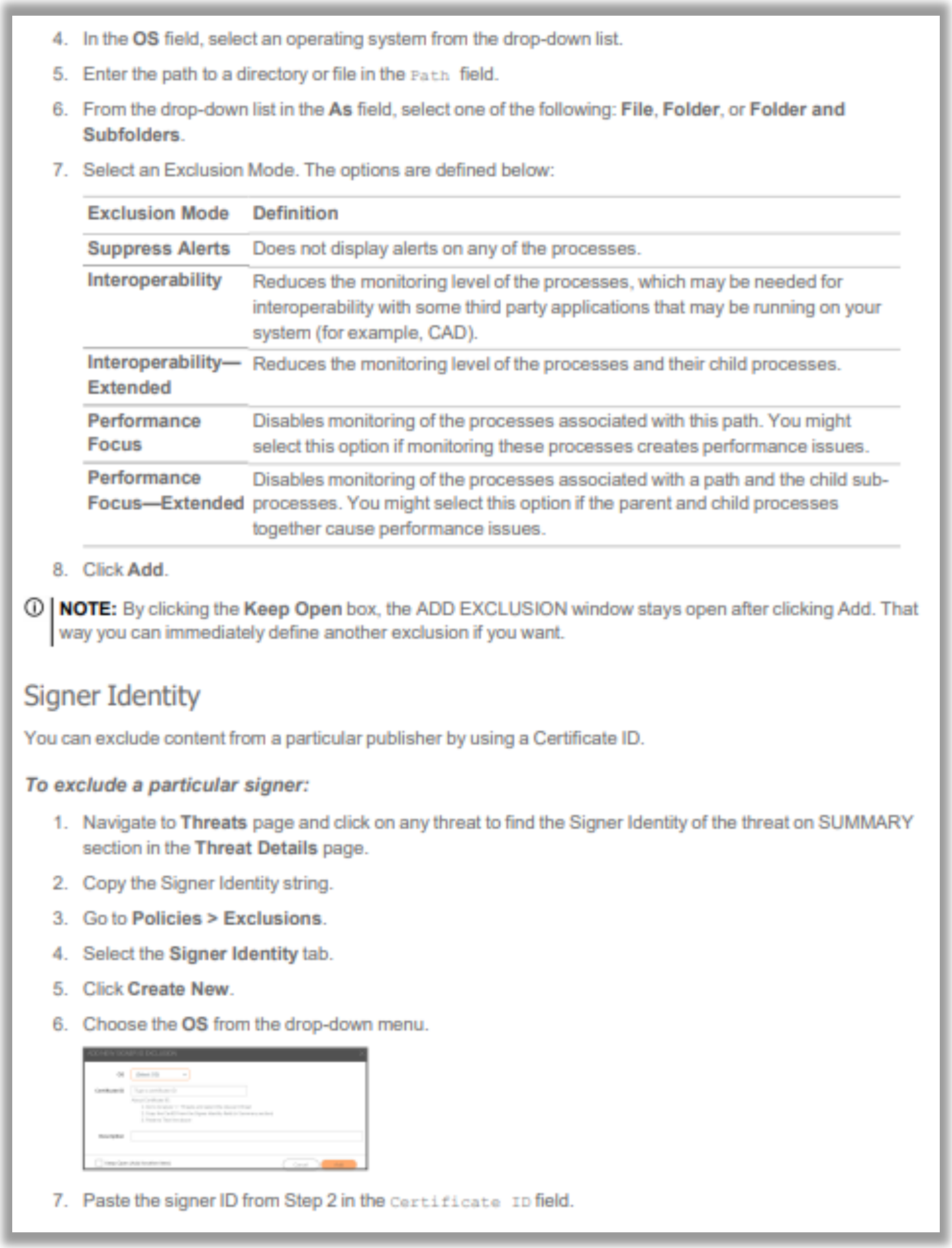
1. Navigate to **Policies > Exclusions**.
2. Select the **Hashes** tab.
3. Click **Create New**.
4. Enter the hash string in the `SHA1 Hash` field.
5. Choose the **OS** from the drop-down menu.
6. Add a `Description` in the field provided.
7. Click the Add button to save your exclusion.

Paths

You can exclude a specific location or file by defining a path on the device to a specific directory.

To exclude a path:

1. Navigate to **Policies > Exclusions**.
2. Select the **Path** tab.
3. Click **Create New**.
   The **ADD NEW PATH EXCLUSION** dialog is displayed.



4. In the **OS** field, select an operating system from the drop-down list.
5. Enter the path to a directory or file in the `Path` field.
6. From the drop-down list in the **As** field, select one of the following: **File**, **Folder**, or **Folder and Subfolders**.
7. Select an Exclusion Mode. The options are defined below:

Exclusion Mode	Definition
Suppress Alerts	Does not display alerts on any of the processes.
Interoperability	Reduces the monitoring level of the processes, which may be needed for interoperability with some third party applications that may be running on your system (for example, CAD).
Interoperability—Extended	Reduces the monitoring level of the processes and their child processes.
Performance Focus	Disables monitoring of the processes associated with this path. You might select this option if monitoring these processes creates performance issues.
Performance Focus—Extended	Disables monitoring of the processes associated with a path and the child sub-processes. You might select this option if the parent and child processes together cause performance issues.

8. Click **Add**.

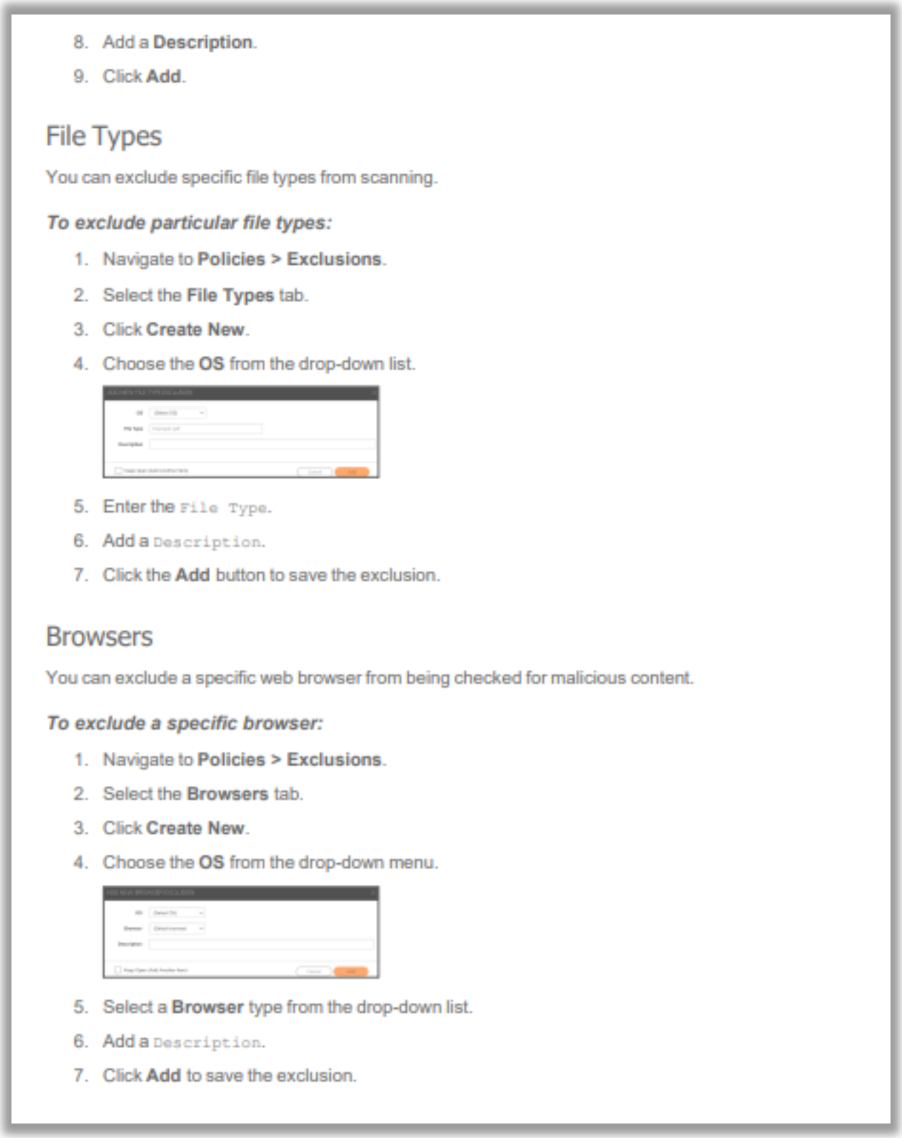
ⓘ **NOTE:** By clicking the **Keep Open** box, the ADD EXCLUSION window stays open after clicking Add. That way you can immediately define another exclusion if you want.

Signer Identity

You can exclude content from a particular publisher by using a Certificate ID.

To exclude a particular signer:

1. Navigate to **Threats** page and click on any threat to find the Signer Identity of the threat on SUMMARY section in the **Threat Details** page.
2. Copy the Signer Identity string.
3. Go to **Policies > Exclusions**.
4. Select the **Signer Identity** tab.
5. Click **Create New**.
6. Choose the **OS** from the drop-down menu.
7. Paste the signer ID from Step 2 in the `Certificate ID` field.



8. Add a **Description**.
9. Click **Add**.

File Types

You can exclude specific file types from scanning.

To exclude particular file types:

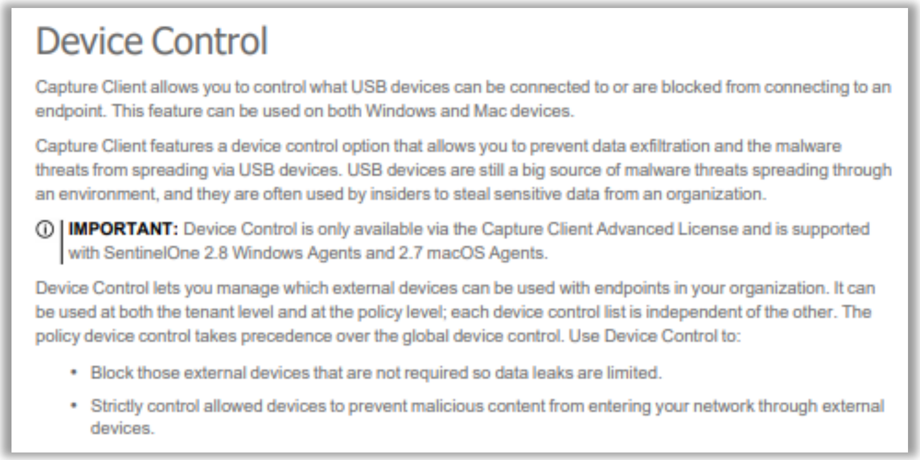
1. Navigate to **Policies > Exclusions**.
2. Select the **File Types** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down list.
5. Enter the `File Type`.
6. Add a `Description`.
7. Click the **Add** button to save the exclusion.

Browsers

You can exclude a specific web browser from being checked for malicious content.

To exclude a specific browser:

1. Navigate to **Policies > Exclusions**.
2. Select the **Browsers** tab.
3. Click **Create New**.
4. Choose the **OS** from the drop-down menu.
5. Select a **Browser** type from the drop-down list.
6. Add a `Description`.
7. Click **Add** to save the exclusion.



Device Control

Capture Client allows you to control what USB devices can be connected to or are blocked from connecting to an endpoint. This feature can be used on both Windows and Mac devices.

Capture Client features a device control option that allows you to prevent data exfiltration and the malware threats from spreading via USB devices. USB devices are still a big source of malware threats spreading through an environment, and they are often used by insiders to steal sensitive data from an organization.

ⓘ **IMPORTANT:** Device Control is only available via the Capture Client Advanced License and is supported with SentinelOne 2.8 Windows Agents and 2.7 macOS Agents.

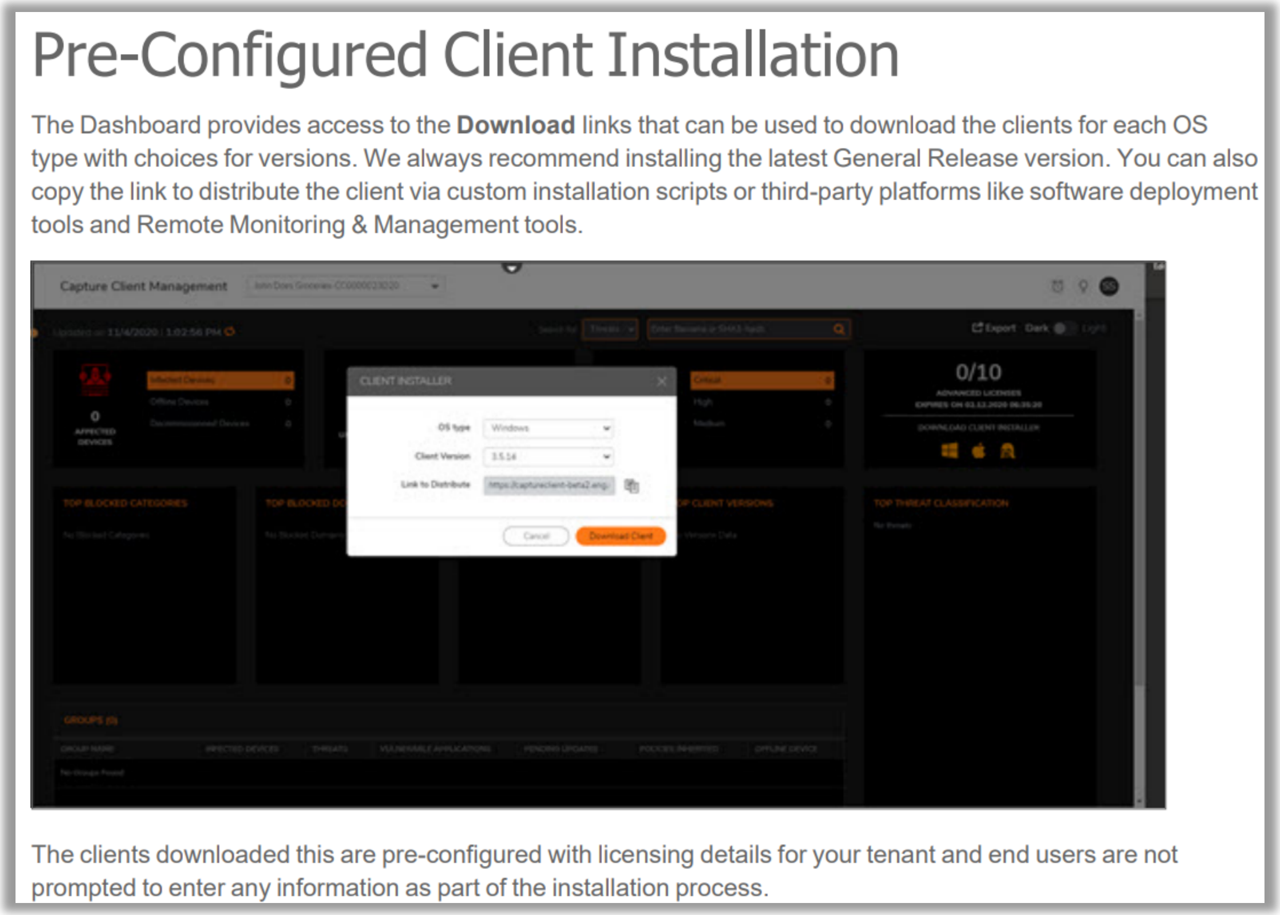
Device Control lets you manage which external devices can be used with endpoints in your organization. It can be used at both the tenant level and at the policy level; each device control list is independent of the other. The policy device control takes precedence over the global device control. Use Device Control to:

- Block those external devices that are not required so data leaks are limited.
- Strictly control allowed devices to prevent malicious content from entering your network through external devices.

[183]

[183] https://www.sonicwall.com/techdocs/pdf/capture_client-protecting_assets.pdf, at 10-22.

178. Every ’997 Accused Product practices configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions. For example, Capture Client is a software service downloaded on the endpoint for monitoring the endpoint.



Pre-Configured Client Installation

The Dashboard provides access to the **Download** links that can be used to download the clients for each OS type with choices for versions. We always recommend installing the latest General Release version. You can also copy the link to distribute the client via custom installation scripts or third-party platforms like software deployment tools and Remote Monitoring & Management tools.

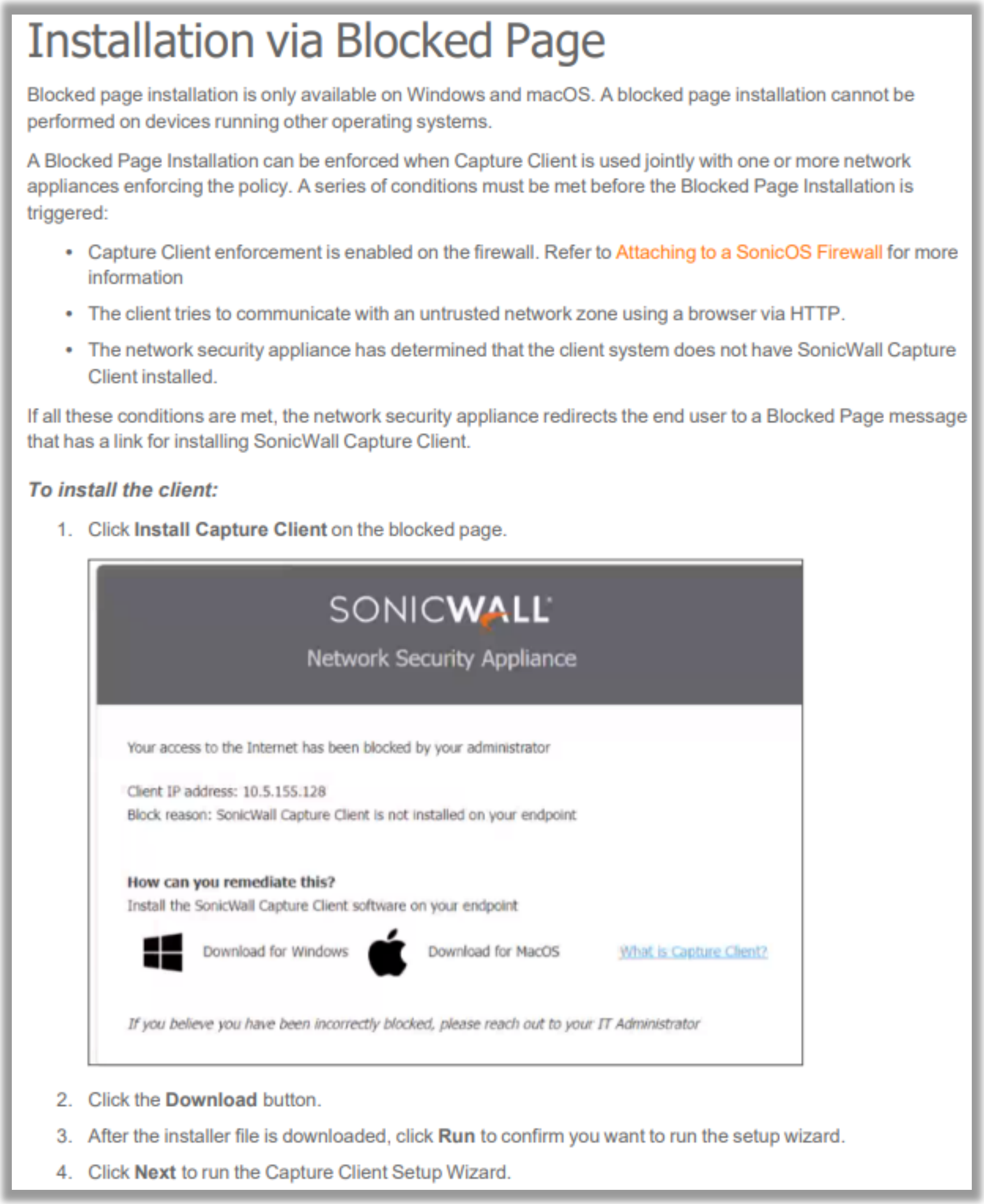
CLIENT INSTALLER

OS type: Windows

Client Version: 3.5.14

Link to Distribute: https://captureclient-beta2.eng...

The clients downloaded this are pre-configured with licensing details for your tenant and end users are not prompted to enter any information as part of the installation process.



Installation via Blocked Page

Blocked page installation is only available on Windows and macOS. A blocked page installation cannot be performed on devices running other operating systems.

A Blocked Page Installation can be enforced when Capture Client is used jointly with one or more network appliances enforcing the policy. A series of conditions must be met before the Blocked Page Installation is triggered:

- Capture Client enforcement is enabled on the firewall. Refer to Attaching to a SonicOS Firewall for more information
- The client tries to communicate with an untrusted network zone using a browser via HTTP.
- The network security appliance has determined that the client system does not have SonicWall Capture Client installed.

If all these conditions are met, the network security appliance redirects the end user to a Blocked Page message that has a link for installing SonicWall Capture Client.

To install the client:

1. Click **Install Capture Client** on the blocked page.

SONICWALL

Network Security Appliance

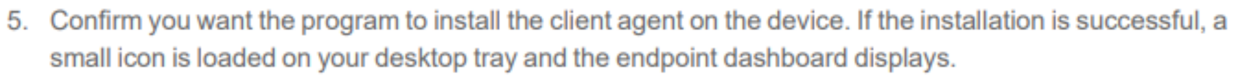
Your access to the Internet has been blocked by your administrator

Client IP address: 10.5.155.128
Block reason: SonicWall Capture Client is not installed on your endpoint

How can you remediate this?
Install the SonicWall Capture Client software on your endpoint

If you believe you have been incorrectly blocked, please reach out to your IT Administrator

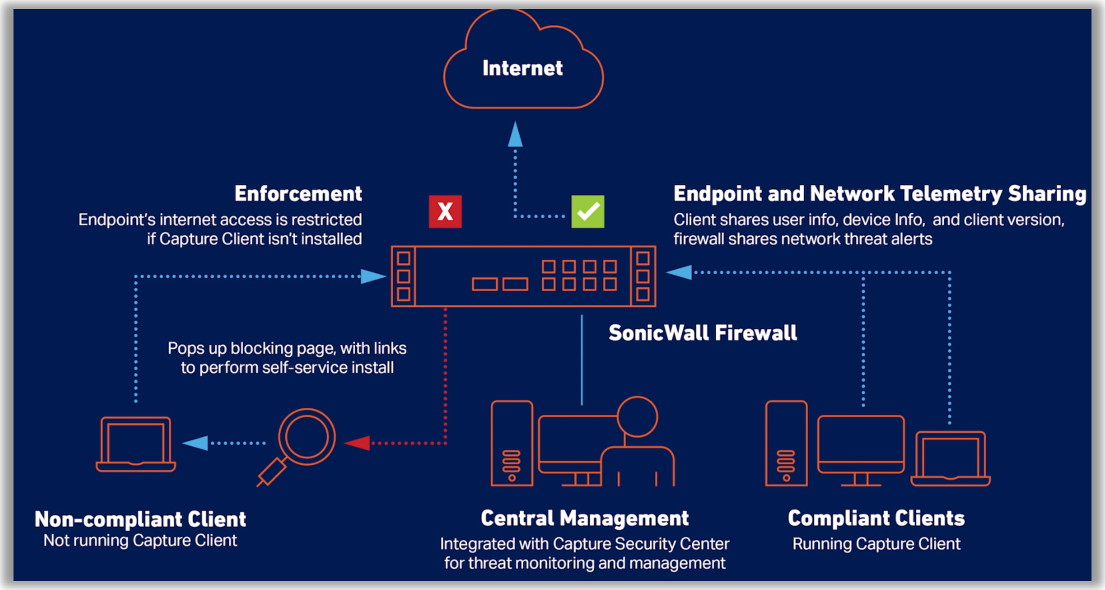
2. Click the **Download** button.
3. After the installer file is downloaded, click **Run** to confirm you want to run the setup wizard.
4. Click **Next** to run the Capture Client Setup Wizard.



5. Confirm you want the program to install the client agent on the device. If the installation is successful, a small icon is loaded on your desktop tray and the endpoint dashboard displays.

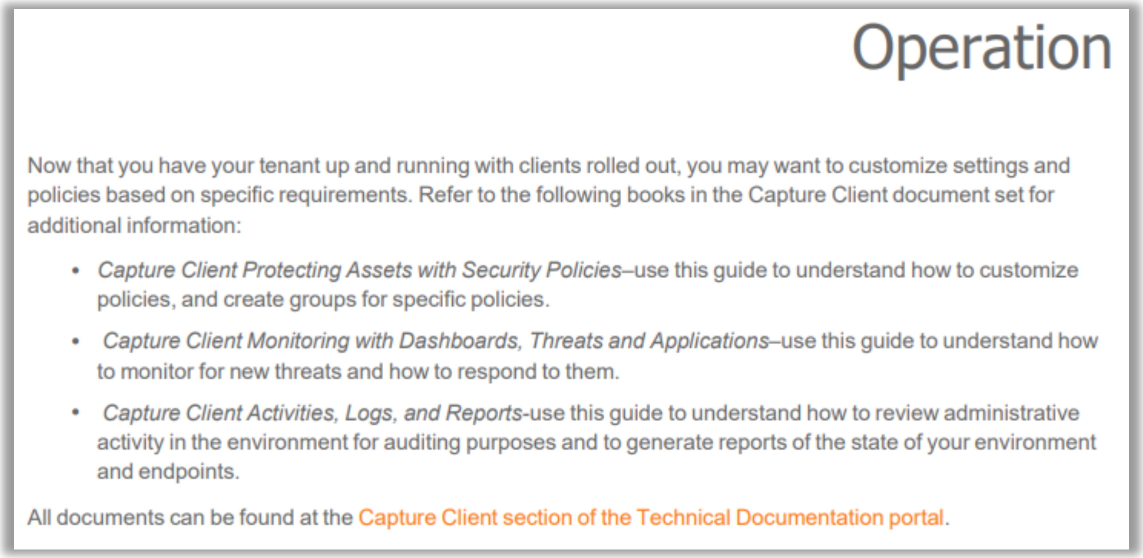
https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 22-24.

179. Every ’997 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services. For example, Capture Client provides endpoint telemetry sharing, including user info, device info, and client version and monitors the endpoint for new threats in order to “generate reports of the state of your environment and endpoints.”


Internet
Enforcement
Endpoint's internet access is restricted
if Capture Client isn't installed
X
✓
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version,
firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links
to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center
for threat monitoring and management
Compliant Clients
Running Capture Client

[184]

[184] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112



Operation

Now that you have your tenant up and running with clients rolled out, you may want to customize settings and policies based on specific requirements. Refer to the following books in the Capture Client document set for additional information:

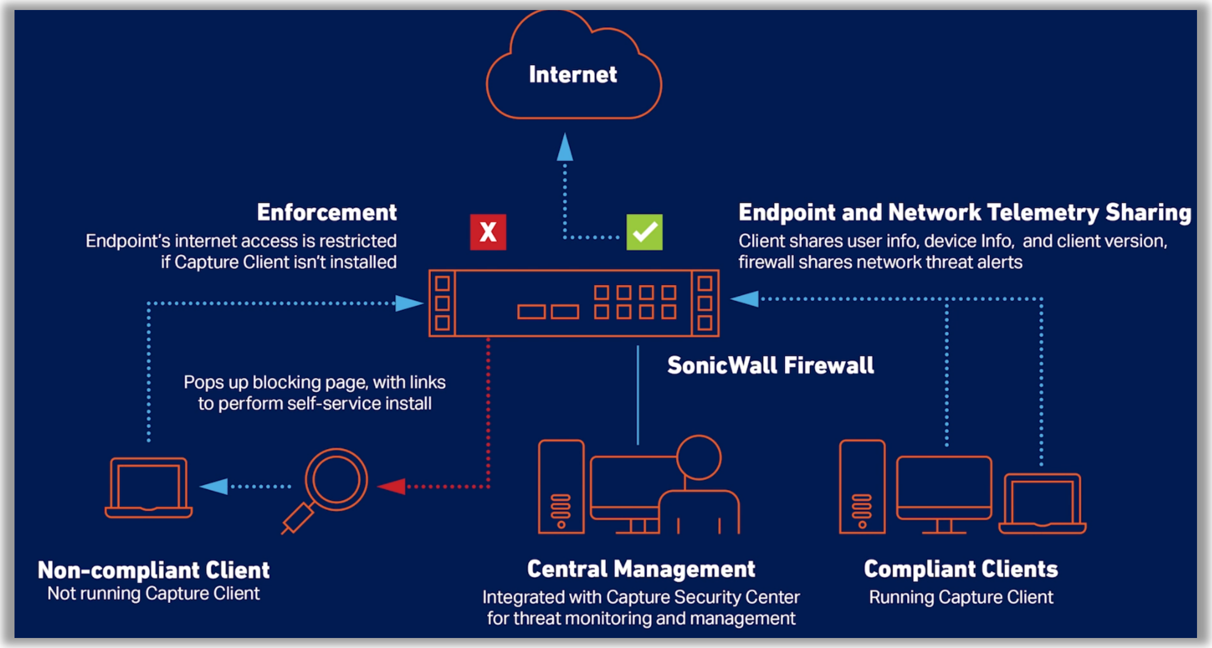
- *Capture Client Protecting Assets with Security Policies*–use this guide to understand how to customize policies, and create groups for specific policies.
- *Capture Client Monitoring with Dashboards, Threats and Applications*–use this guide to understand how to monitor for new threats and how to respond to them.
- *Capture Client Activities, Logs, and Reports*-use this guide to understand how to review administrative activity in the environment for auditing purposes and to generate reports of the state of your environment and endpoints.

All documents can be found at the Capture Client section of the Technical Documentation portal.

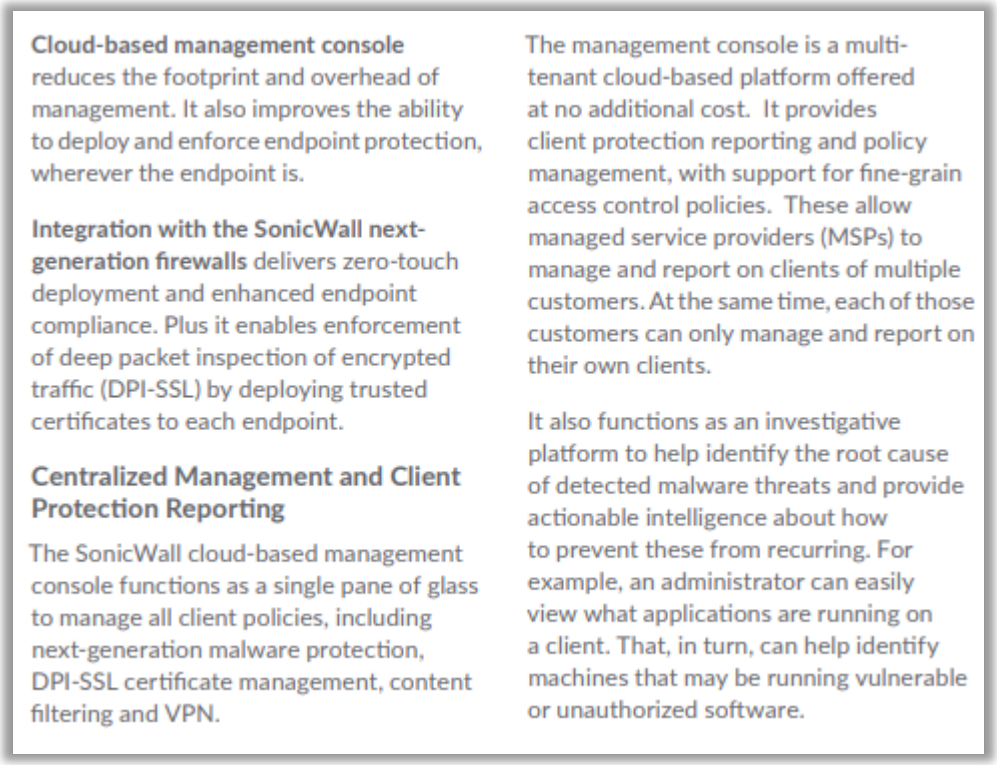
[185]

180. Every ’997 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, Capture Client determines a compliance state of the endpoint based on whether the monitored status information meets the compliances policies that are managed at the cloud-based management console. For further example, a basic policy is whether Capture Client is running on the endpoint. If so, the endpoint is compliant; if not, the endpoint is not compliant.

[185] https://www.sonicwall.com/techdocs/pdf/capture_client-getting_started.pdf, at 27.


Internet
Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed
Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts
SonicWall Firewall
Pops up blocking page, with links to perform self-service install
Non-compliant Client
Not running Capture Client
Central Management
Integrated with Capture Security Center for threat monitoring and management
Compliant Clients
Running Capture Client

[186]



Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

Centralized Management and Client Protection Reporting

The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

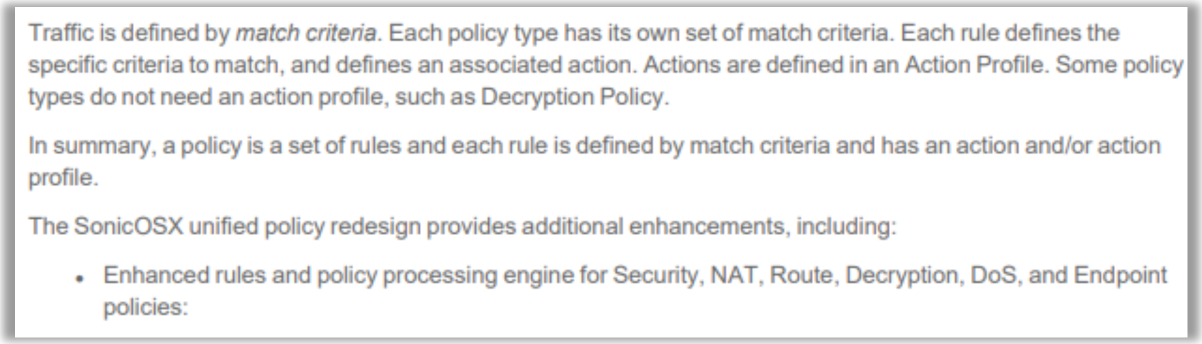
It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.

[187]

[186] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

[187] https://www.sonicwall.com/medialibrary/pt/datasheet/sonicwall-capture-client.pdf

181. Every ’997 Accused Product practices initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. For example, Capture Client can initiate actions since “each rule is defined by match criteria and has an action and/or action profile.” In one example, if an endpoint is not compliant by having downloaded the Capture Client, an identified action is that Internet access may be blocked.



Traffic is defined by *match criteria*. Each policy type has its own set of match criteria. Each rule defines the specific criteria to match, and defines an associated action. Actions are defined in an Action Profile. Some policy types do not need an action profile, such as Decryption Policy.

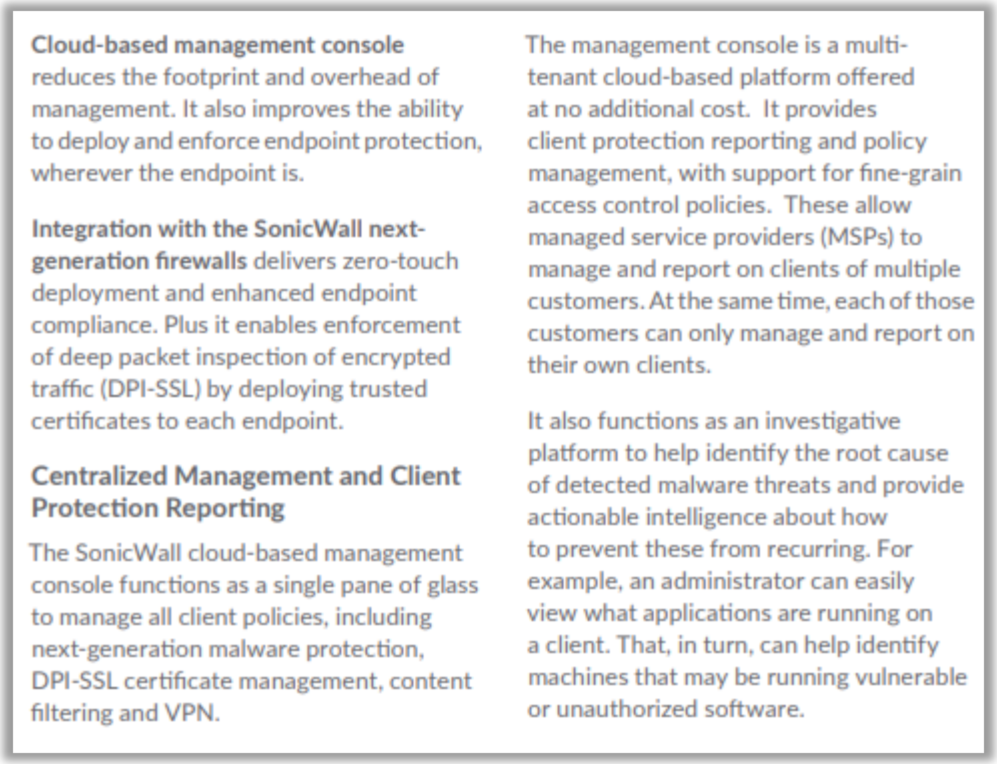
In summary, a policy is a set of rules and each rule is defined by match criteria and has an action and/or action profile.

The SonicOSX unified policy redesign provides additional enhancements, including:

- Enhanced rules and policy processing engine for Security, NAT, Route, Decryption, DoS, and Endpoint policies:

[188]

[188] https://www.sonicwall.com/techdocs/pdf/sonicos-7-0-about.pdf, at 51.



Cloud-based management console reduces the footprint and overhead of management. It also improves the ability to deploy and enforce endpoint protection, wherever the endpoint is.

Integration with the SonicWall next-generation firewalls delivers zero-touch deployment and enhanced endpoint compliance. Plus it enables enforcement of deep packet inspection of encrypted traffic (DPI-SSL) by deploying trusted certificates to each endpoint.

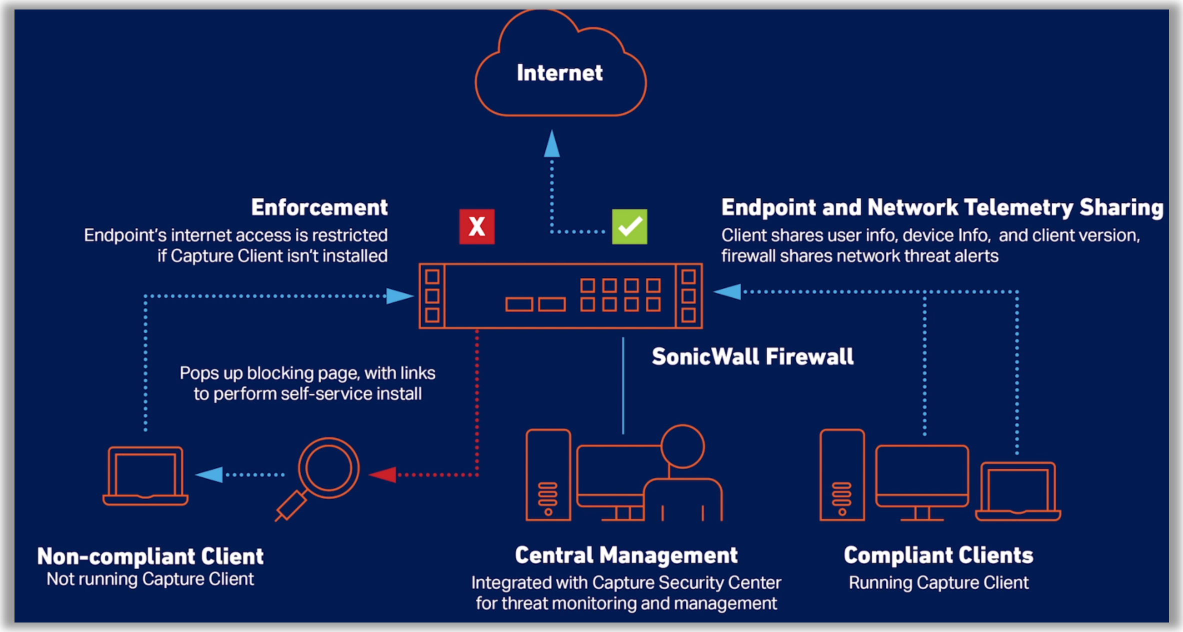
Centralized Management and Client Protection Reporting

The SonicWall cloud-based management console functions as a single pane of glass to manage all client policies, including next-generation malware protection, DPI-SSL certificate management, content filtering and VPN.

The management console is a multi-tenant cloud-based platform offered at no additional cost. It provides client protection reporting and policy management, with support for fine-grain access control policies. These allow managed service providers (MSPs) to manage and report on clients of multiple customers. At the same time, each of those customers can only manage and report on their own clients.

It also functions as an investigative platform to help identify the root cause of detected malware threats and provide actionable intelligence about how to prevent these from recurring. For example, an administrator can easily view what applications are running on a client. That, in turn, can help identify machines that may be running vulnerable or unauthorized software.

[189]



Internet

Enforcement
Endpoint's internet access is restricted if Capture Client isn't installed

Endpoint and Network Telemetry Sharing
Client shares user info, device Info, and client version, firewall shares network threat alerts

SonicWall Firewall

Pops up blocking page, with links to perform self-service install

Non-compliant Client
Not running Capture Client

Central Management
Integrated with Capture Security Center for threat monitoring and management

Compliant Clients
Running Capture Client

[190]

[189] https://www.sonicwall.com/medialibrary/pt/datasheet/sonicwall-capture-client.pdf

[190] https://players.brightcove.net/5380177764001/3xb8sfQmL_default/index.html?videoId=6315400218112

182. Defendant has and continues to directly infringe one or more claims of the ’997 Patent, including claim 1, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing the infringing Accused Products into the United States without authority and in violation of 35 U.S.C. § 271.

183. Defendant has and continues to indirectly infringe one or more claims of the ’997 Patent by knowingly and intentionally inducing others, including SonicWall customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’997 Accused Products.

184. Defendant has and continues to indirectly infringe one or more claims of the ’997 Patent including, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the ’997 Patent at least as of the date of this Complaint against SonicWall, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’997 Patent by providing these products to customers and end-users for use in an infringing manner.

185. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’997 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information, product manuals, documentation, and support which instruct customers and end-users how to use the Accused Products in an infringing

manner, including at least though its SonicWall Technical Documentation,[191] Video Tutorials,[192] SonicWall University,[193] and Customer Service[194] websites.

186. Defendant has and continues to indirectly infringe one or more claims of the ’997 Patent by contributing to the direct infringement, either literally or under the doctrine of equivalents, by others, including end-users, by making, using, offering to sell, selling, and/or importing into the United States the Accused Products, with the knowledge that, at least as of the date of this Complaint, the Accused Products contain components that constitute a material part of the inventions claimed in the ’997 Patent. Such components include, for example, SonicWall’s network security appliances such as firewalls or Capture Client, that integrate with Sonicwall Capture ATP. Defendant knows that these components are especially made or especially adapted for use in an infringement of the ’997 Patent and that these components are not a staple article or commodity of commerce suitable for substantial non-infringing use. Alternatively, Defendant believed there was a high probability that others would infringe the ’997 Patent but remained willfully blind to the infringing nature of others’ actions.

187. Taasera has suffered damages as a result of Defendant’s direct and indirect infringement of the ’997 Patent in an amount to be proved at trial.

188. Taasera has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’997 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

189. On information and belief, Defendant acted egregiously and with willful misconduct in that its actions constituted direct or indirect infringement of a valid patent, and this was either

[191] https://www.sonicwall.com/support/technical-documentation/?language=English

[192] https://www.sonicwall.com/support/video-tutorials/#t=All&sort=relevancy&numberOfResults=12

[193] https://www.sonicwall.com/partners/sonicwall-university/

[194] https://www.sonicwall.com/support/contact-support/customer-service/

known or so obvious that Defendant should have known about it. Defendant continues to infringe the ’997 patent by making, using, selling, offering for sale and/or importing in the United States the Accused Products and by inducing the direct infringing use, sale, offer for sale, and importation of the Accused Products by others, in reckless disregard of Taasera’s patent rights. Defendant has committed and continues to commit acts of infringement that Defendant actually knew or should have known constituted an unjustifiably high risk of infringement of at least one valid and enforceable claim of the ’997 Patent. Upon information and belief, Defendant had actual knowledge of the ’997 Patent from related prior litigations accusing products with similar network and endpoint security functionalities involving direct competitors of Defendant. Defendant’s infringement of the ’997 Patent has been and continues to be willful, entitling Taasera to an award of treble damages, reasonable attorney fees, and costs in bringing this action under 35 U.S.C. §§ 284 and 285.

PRAYER FOR RELIEF

WHEREFORE, Taasera prays for judgment and relief as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate Taasera for Defendant’s infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. A judgment and order requiring Defendant to pay Taasera treble damages and pre-judgment interest under 35 U.S.C. § 284 as a result of, inter alia, Defendant’s willful and deliberate infringement of the Asserted Patents;

e. Entry of judgment declaring that this case is exceptional and awarding Taasera its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

f. Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38 and Civil Local Rule 3-6, Taasera demands a jury trial on all issues and claims so triable.

DATED: February 7, 2024

Respectfully submitted,

By: */s/ Benjamin T. Wang*
Benjamin T. Wang

FABRICANT LLP
Alfred R. Fabricant
ffabricant@fabricantllp.com
Peter Lambrianakos
plambrianakos@fabricantllp.com
Vincent J. Rubino, III
vrubino@fabricantllp.com
Joseph Mercadante
jmercadante@fabricantllp.com
411 Theodore Fremd Avenue, Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Benjamin T. Wang (CA SBN 228712)
bwang@raklaw.com
Minna Y. Chan (CA SBN 305941)
mchan@raklaw.com
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, California 90025
23 Telephone: (310) 826-7474
Facsimile (310) 826-9226

Attorneys for Plaintiff
Taasera Licensing LLC