

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

Skysong Innovations, LLC,)	
)	
<i>Plaintiff,</i>)	
)	
v.)	C.A. No. 2:25-cv-00098
)	
Fortinet, Inc.,)	JURY TRIAL DEMANDED
)	
<i>Defendant.</i>)	
)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Skysong Innovations, LLC (“Skysong”) alleges against Defendant Fortinet, Inc. (“Fortinet” or “Defendant”) the following:

NATURE OF THE CASE

1. This is a civil action for infringement of U.S. Patent No. 10,313,385 (the “385 Patent”), U.S. Patent No. 11,275,900 (the “900 Patent”), U.S. Patent No. 11,775,831 (the “831 Patent”), and U.S. Patent No. 11,892,897 (the “897 Patent” and collectively, the “Asserted Patents”) arising under the Patent Laws of the United States, 35 U.S.C. §§ 271 *et seq.*

THE PARTIES

2. Plaintiff Skysong is a private nonprofit and the exclusive intellectual property management and technology transfer organization for Arizona State University (“ASU”). Skysong works with ASU faculty, researchers, and technology industry partners to translate ASU innovations into broad societal impact. Skysong’s goal is the rapid and wide dissemination of intellectual property and inventions created by ASU to the marketplace.¹

¹ See <https://skysonginnovations.com/>; <https://skysonginnovations.com/about/>.

3. ASU’s charter, which is literally carved in stone on its Tempe campus, reads: “ASU is a comprehensive public research university, measured not by whom it excludes, but by whom it includes and how they succeed; advancing research and discovery of public value; and assuming fundamental responsibility for the economic, social, cultural and overall health of the communities it serves.”² Founded in 1885 as Territorial Normal School by the 13th Arizona Territorial Legislature, ASU is the State of Arizona’s largest university, with its largest campus located in Tempe, Arizona. ASU offers more than 400 academic undergraduate programs and majors led by expert faculty in highly ranked colleges and schools. ASU has over 183,000 enrolled students, of which more than 18,000 were veteran or military-affiliated students during fall 2024.³ For example, U.S. News & World Report rates 84 ASU degree programs in the top 25 in the country, including 38 programs ranked in the nation’s top 10.⁴ A member of the Association of American Universities (comprising the country’s leading research universities), ASU has over 400 faculty members elected to the National Academies of Science, with five of its faculty receiving the Nobel Prize. ASU has held the No. 1 ranking for innovation ten years in a row and is ranked in the top 10 worldwide among universities granted U.S. patents according to the National Academy of

² <https://www.asu.edu/about/charter-mission>.

³ <https://www.asu.edu/about/facts-and-figures>.

⁴ <https://www.asu.edu/about/facts-and-figures>.

Inventors.⁵ In addition, ASU is ranked No. 2 in the country for employability among public universities; it is one of Arizona's largest employers with more than 18,500 employees.⁶

4. Each of the Asserted Patents is assigned to Skysong. Skysong is the exclusive owner of all rights, title, and interest in and to the Asserted Patents, and has the right to bring this suit to recover damages for any current or past infringement of the Asserted Patents.

5. On information and belief, Fortinet is a Delaware corporation with a regular and established place of business in this District at 6735 Salt Cedar Way, Frisco, TX 75034.⁷ Upon information and belief, Fortinet does business in Texas and in this District, directly or through intermediaries. Fortinet is registered to do business in the State of Texas and has been since at least November 24, 2009.

6. Fortinet provides various products and solutions for network security, cloud infrastructure, endpoint security, and security operations, without authorization, that implement patented technologies invented by ASU. Fortinet's infringing products and services include, but are not limited to, Fortinet's integrated platform—the Fortinet Security Fabric, including certain integrated tools and products such as FortiGuard, FortiRecon, and FortiGate, as well as prior versions and functionalities that are the same or essentially same as that described herein (collectively, "Fortinet Security Fabric" or the "Accused Products").

⁵<https://news.asu.edu/20240923-university-news-asu-no-1-innovation-10-years-us-news-world-report-ranking#:~:text=University%20news-,A%20decade%20strong%3A%20ASU%20takes%20top%20spot%20in%20innovation,10th%20year%20in%20a%20row&text=For%20the%2010th%20year%20in,rankings%20earned%20by%20the%20university;https://academyofinventors.org/wp-content/uploads/2024/02/2023-Top-100-Worldwide.pdf;https://news.asu.edu/20240219-university-news-asu-ranked-no-9-worldwide-us-patents-2023>.

⁶<https://cfo.asu.edu/working-at-asu#:~:text=ASU%20is%20one%20of%20Arizona's,which%20starts%20with%20its%20employees>.

⁷<https://www.fortinet.com/corporate/about-us/global-offices#NA>.

JURISDICTION AND VENUE

7. This is an action for patent infringement arising under the Patent Laws of the United States, including 35 U.S.C. §§ 271 *et seq.* This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

8. This Court has personal jurisdiction over Fortinet. On information and belief, Fortinet regularly conducts business in the State of Texas and in this District, which includes operating systems, using software, and/or providing services and/or engaging in activities in Texas and in this District that infringe one or more claims of the Asserted Patents in this forum, as well as inducing others to infringe in this District.

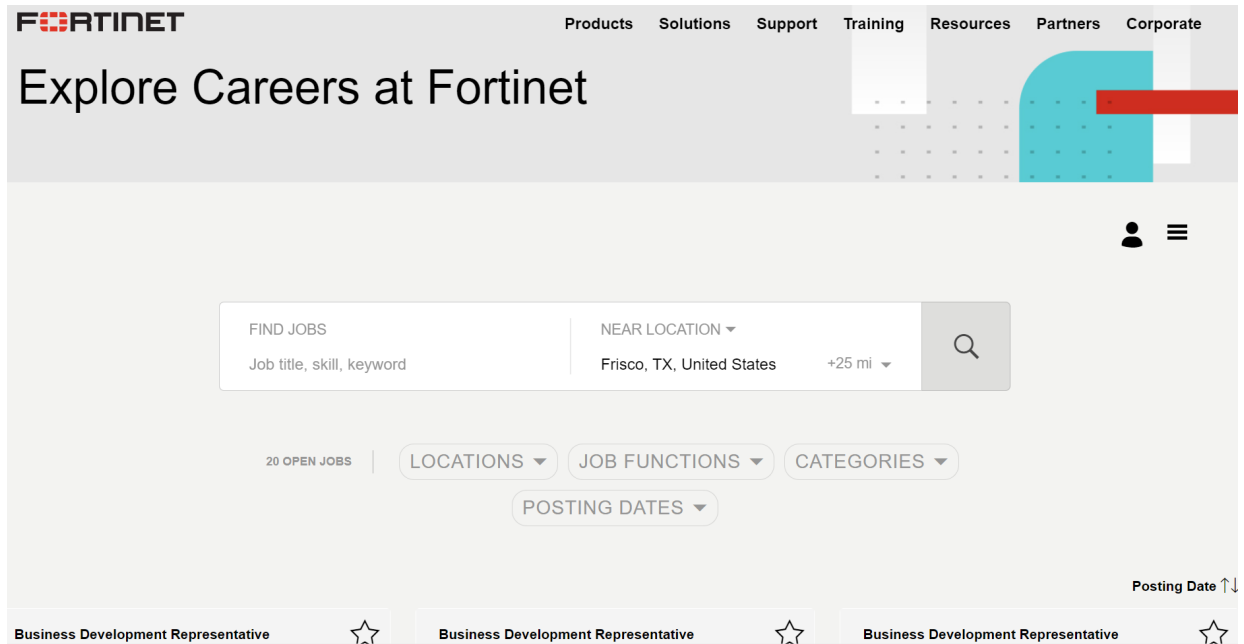
9. Fortinet has also, directly and through its extensive network of partnerships, including with local service providers, purposefully and voluntarily placed the Accused Products that practice the methods claimed in the Asserted Patents into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District.

10. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c), and 28 U.S.C. § 1400(b). Fortinet has a regular and established place of business in this District, including in Collin County located at 6735 Salt Cedar Wy, Frisco, TX 75034, and is deemed to reside in this District.⁸ On information and belief, Fortinet has regular and systematic contacts within this District and has committed acts of infringement within this District.

11. On information and belief, Fortinet has hundreds of employees in this District, including executives, senior and mid-level officials, managerial staff, and first level positions in engineering, sales, marketing, customer service, and finance.

⁸<https://www.fortinet.com/corporate/about-us/global-offices#NA>.

12. On information and belief, Fortinet's employees located in this District may have relevant information, including information concerning the products and services Fortinet provides, including the Accused Products, and how those products operate. Fortinet also currently lists at least 20 open positions, including business development representatives, regional account managers, inside sales representatives, and engineers, in Frisco and Plano, Texas.⁹



13. Fortinet has committed acts of infringement within this District. For example, on information and belief, Fortinet uses the Accused Products in this District in manners that practice the Asserted Patents, including by testing the Accused Products and by using the Accused Products at its offices in this District.

14. On information and belief, Fortinet makes, uses, advertises, offers for sale, and/or sells the Accused Products that practice the Asserted Patents in the State of Texas and in this

⁹https://edel.fa.us2.oraclecloud.com/hcmUI/CandidateExperience/en/sites/CX_2001/requisitions?lastSelectedFacet=LOCATIONS&location=Frisco%2C+TX%2C+United+States&locationId=300000003078877&locationLevel=city&mode=location&radius=25&radiusUnit=MI&selectedLocationsFacet=300000003028044.

District directly and/or through its partnerships with businesses in the State of Texas and in this District.

15. On information and belief, Fortinet sells, offers for sale, advertises, makes, installs, and/or otherwise provides the Accused Products, the use of which infringe the Asserted Patents in this District and the State of Texas. Fortinet performs these acts directly and/or through its partnerships with other entities.¹⁰

16. On information and belief, Fortinet also uses a network of partners, which comprises re-sellers, managed service providers and cybersecurity experts to provide the Accused Products and implementation of services for the Accused Products to its customers in this District. Each of these partners sells, offers for sale, and/or installs the Accused Products.

17. Fortinet engages in activities that infringe the Asserted Patents (directly or indirectly) within this District. For example, Fortinet's operation and use of the Accused Products within this District infringe (directly or indirectly) the Asserted Patents.

18. Fortinet also infringes (directly or indirectly) the Asserted Patents by providing services in connection with the Accused Products including installing, maintaining, supporting, operating, providing instructions, and/or advertising the Accused Products within this District. End-users and partner customers infringe the Asserted Patents by installing and operating the Accused Products, which perform the claimed methods in the Asserted Patents within this District.

19. Fortinet encourages and induces its customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its products and services available on its website, widely advertises those products and services, provides applications that

¹⁰See <https://partnerportal.fortinet.com/directory/search?l=United+States&st=Texas>.

allow partners and users to access those products and services, provides instructions for installing, and maintaining those products, and provides technical support to users.¹¹

PLAINTIFF'S PATENTED INNOVATIONS

20. The '385 Patent, titled "Systems and methods for data driven game theoretic cyber threat mitigation," was filed on November 28, 2016, and duly and legally issued by the USPTO on June 4, 2019. The '385 Patent claims priority to U.S. Provisional Application No. 62/261,200, which was filed on November 30, 2015. A true and correct copy of the '385 Patent is attached hereto as Exhibit 1.

21. The named inventors of the '385 Patent are Paulo Shakarian, John Robertson, Jana Shakarian, Vivin Paliath, and Amanda Thart.

22. The '385 Patent "relates to a security game framework, and in particular to a data-driven security game framework that models an attacker based on exploit market data actively mined from the 'darknet' or other overlay communication networks to develop strategies for the defender." (Exhibit 1, '385 Patent, 1:15-20.) At the time of the filing of the '385 Patent, "there d[id] not appear to be a game theoretic approach to host-based defense where the activities of the attacker are informed from an 'un-conventional' source (information not directly related to the defender's system) specifically information from darknet markets in this case." (*Id.* at 2:26-31.) To address these shortcomings, the '385 Patent "introduce[d] a rigorous and thoroughly analyzed framework for addressing penetration testing that is fed with real - world exploit market data, mined from the darknet." (*Id.* at 3:4-7.) In one embodiment, the '385 Patent employs a new security game frame-work "designed to model an attacker with access to exploit markets and a defender of information technology infrastructure; theoretical analysis of the framework leading to the

¹¹See <https://www.fortinet.com/corporate/about-us/contact-us>.

development of algorithms to find near - optimal strategies for both players; and an implementation of the system and the results of a thorough suite of experiments on real-world data.” (*Id.* at 3:8-15.)

23. Each claim in the '385 Patent recites an independent invention. Neither claim 8, nor any other individual claim is representative of all claims in the '385 Patent.

24. The '385 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

25. The '900 Patent, titled “Systems and methods for automatically assigning one or more labels to discussion topics shown in online forums on the dark web,” was filed on May 7, 2019, and duly and legally issued by the USPTO on March 15, 2022. The '900 Patent claims priority to U.S. Provisional Application No. 62/668,878, which was filed on May 9, 2018. A true and correct copy of the '900 Patent is attached hereto as Exhibit 2.

26. The named inventors of the '900 Patent are Revanth Patil, Paulo Shakarian, Ashkan Aleali, and Ericsson Marin.

27. The '900 Patent covers “systems and methods for automatically assigning one or more labels or tags related to various discussion forum topics on the dark web or deep web” (Exhibit 2, '900 Patent, 1:17-20). Malicious users of the internet seek “online platforms for illegal activities such as credit card fraud, identity theft, leaks of sensitive information and sharing hacking information” (*Id.* at 1:25-27). The dark web and deep web have “emerged in the last decade and contributed to the achievement of those criminal tasks” (*Id.* at 1:27-30). The '900 Patent addresses the issue of the lack of efficient labelling and classification of information found on the “deep web that is not indexed by web search engines” (*Id.* at 1:63-64), as “[c]urrent technologies use learning models and techniques that do not address the issues of labeled data

scarcity, nor do they address imbalanced data classes in the training set. Training sets are labeled by hand, which is a time-consuming and typically un-scalable process.” (*Id.* at 2:10-15). To address these shortcomings, the ’900 Patent claims techniques “includ[ing] an inventive computer-implemented system [...] that involves automatically assigning one or more labels (tags), in a hierarchical structure, to discussion topics seen” in deep-web forums (*Id.* at 3:10-14).

28. Each claim in the ’900 Patent recites an independent invention. Neither claim 12, nor any other individual claim is representative of all claims in the ’900 Patent.

29. The ’900 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

30. The ’831 Patent, titled “Cascaded computing for convolutional neural networks,” was filed on January 13, 2023, and duly and legally issued by the USPTO on October 3, 2023. The ’831 Patent is a continuation of U.S. Patent Application No. 16/335,775 filed on March 22, 2019, which is a U.S. National Stage Application under 35 USC § 371 and claims the benefit of International Patent Application No. PCT/US2017/052736 filed on September 21, 2017, which claims priority to U.S. Provisional Patent Application No. 62/399,753 filed on September 26, 2016. A true and correct copy of the ’831 Patent is attached hereto as Exhibit 3.

31. The named inventors of the ’831 Patent are Jae-sun Seo and Minkyu Kim.

32. The ’831 Patent is directed to techniques for “for efficiently reducing the amount of total computation in CNNs without affecting the output result or classification accuracy.” (Exhibit 3, ’831 Patent, 1:33-36). “Convolutional Neural Networks (CNNs) have gained popularity in many computer vision applications (image, video, speech, etc.), because of their ability to train and classify with high accuracy. Due to multiple layers of convolution and pooling operations that are compute-/memory-intensive, it is difficult to perform real-time classification with low power

consumption on today's computing systems.” (*Id.* at 1:22-29). To address these shortcomings, the ’831 Patent claims innovative techniques that “can be embodied in methods that include actions of: in one or more layers of a convolutional neural network (CNN), performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs) for each of a plurality of data sets; examining a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present among the first set of values; responsive to identifying the maximum value, performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value; and propagating the full precision computation of the value to a subsequent layer of the CNN.” (*Id.* at 1:37-50).

33. Each claim in the ’831 Patent recites an independent invention. Neither claim 1, nor any other individual claim is representative of all claims in the ’831 Patent.

34. The ’831 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

35. The ’897 Patent, titled “Systems and methods for predicting which software vulnerabilities will be exploited by malicious hackers to prioritize for patching,” was filed on October 26, 2018, and duly and legally issued by the USPTO on February 6, 2024. The ’897 Patent claims priority to U.S. Provisional Application No. 62/581,123, which was filed on November 3, 2017. A true and correct copy of the ’897 Patent is attached hereto as Exhibit 4.

36. The named inventors of the ’897 Patent are Paulo Shakarian, Mohammed Almukaynizi, Jana Shakarian, Eric Nunes, Krishna Dharaiya, Manoj Balasubramaniam Senguttuvan, and Alexander Grimm.

37. The ’897 Patent “relates to assessing the likelihood of exploitation of software vulnerabilities, and in particular to systems and methods for predicting which software

vulnerabilities will be exploited by malicious hackers and hence prioritized by patching.” (Exhibit 4, ’897 Patent, 1:24-28). Prior to the ’897 Patent, “current methods for prioritizing patching vulnerabilities appear to fall short.” (*Id.* at 1:48-49). For example, prior-art methods: over-reported “vulnerabilities as severe and will be exploited to be on the side of caution”; were “not an effective predictor of vulnerabilities being exploited”; and “were limited to single sites that provided a relatively small number of predictions” (*Id.* at 1:45-2:7). To overcome such issues, the inventions in the ’897 Patent marshals “machine learning models described herein in predicting exploits in the wild” (*Id.* at 3:55-56) drawing upon “a variety of data sources or data feeds” (*Id.* at 3:27-29) to analyze exploited vulnerabilities. For instance, it further “leverages machine learning techniques on features derived from the social network of users participating in darkweb/deepweb (DW) forums, as well as features derived from the National Vulnerability Database.” (*Id.* at 4:20-23).

38. Each claim in the ’897 Patent recites an independent invention. Neither claim 1, nor any other individual claim is representative of all claims in the ’897 Patent.

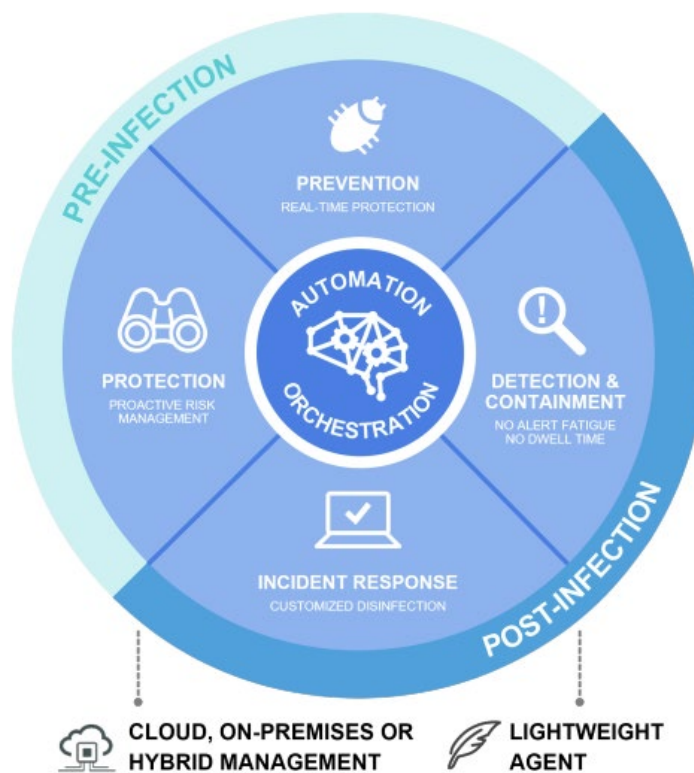
39. The ’897 Patent is valid and enforceable and enjoys a statutory presumption of validity pursuant to 35 U.S.C. § 282.

THE ACCUSED PRODUCTS

40. Fortinet offers, sells, and uses several products that provide and implement malware detection and endpoint protection platforms for individuals and enterprises and incorporate Plaintiff’s patented technologies. Those products include the Fortinet Security Fabric, which spans secure networking, unified Secure Access Service Edge (“SASE”) and AI-driven security operations (“SecOps”) and links different security sensors and tools together to collect, coordinate,

and respond to malicious behavior in real time.¹² Fortinet Security Fabric can be used to coordinate the behavior of Fortinet products including FortiEDR and FortiDLP.

41. For example, FortiEDR, which is part of the SecOps platform, “identifies and stops breaches in real time automatically and efficiently with a lightweight agent.”¹³



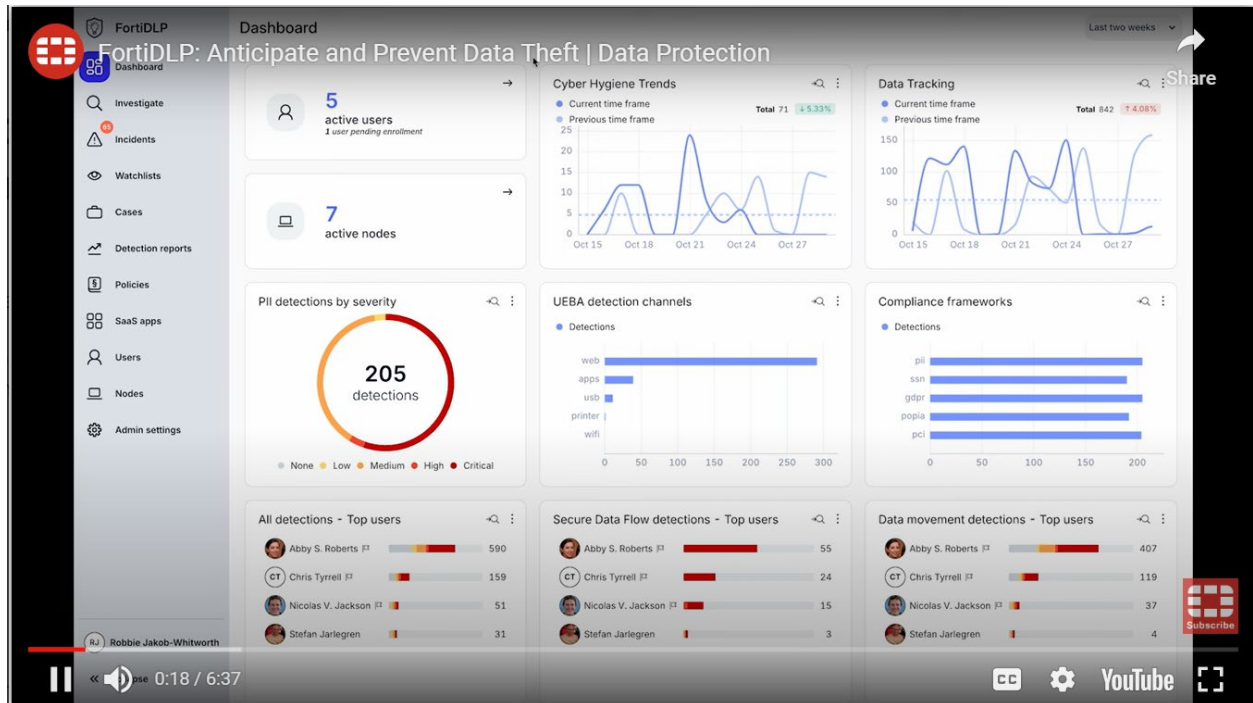
42. Similarly, FortiDLP is a “cloud-native endpoint data protection solution that helps ... anticipate and prevent data leaks” and “detect behavior-related insider risks.”¹⁴ “FortiDLP’s

¹²<https://investor.fortinet.com/static-files/10e4e7f5-4b07-4285-975e-c406d407325a> (2024 Form 10-K); <https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/339062/fortinet-security-fabric>.

¹³<https://www.fortinet.com/products/endpoint-security/fortiedr>; <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf>.

¹⁴<https://www.fortinet.com/products/fortidlp>.

scalable, lightweight agent collects and records data regardless of network connection and location.”¹⁵



FIRST CAUSE OF ACTION (INFRINGEMENT OF THE '385 PATENT)

43. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

44. Fortinet is not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the '385 Patent.

45. Fortinet has infringed and continues to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the '385 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of Fortinet Security Fabric such as FortiGuard,

¹⁵<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortidlp.pdf>

at least when used for their ordinary and customary purposes, practice each element of at least claim 8 of the '385 Patent as demonstrated below.

46. For example, claim 8 of the '385 Patent recites:

A method for improving a computing device, the method comprising:

accessing data comprising dark net information associated with a computer system;

obtaining a set of exploits from the dark net information, the set of exploits configured to bypass a security feature of the computer system;

applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities;

creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system, wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system;

analyzing an application associated with the set of exploits on the computer system to detect a particular vulnerability of the constraint set of vulnerabilities of the computer system; and

altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack..

47. As illustrated in the example below,¹⁶ Fortinet Security Fabric performs each step of the method of claim 8 of the '385 Patent. To the extent that the preamble of claim 8 is limiting, Fortinet Security Fabric implements a *method for improving a computing device*. Fortinet Security Fabric is designed to protect computer systems from attacks and comprises a comprehensive technology stack that includes signature-based detection, heuristic and behavior-based detection, and AI- and ML-driven analysis. The integration of these components and capabilities within Fortinet's offerings practices this claim element.

¹⁶The following examples are illustrative only and not intended to limit Plaintiff's right to supplement or modify its allegations regarding the exemplary products or to allege that other Fortinet products infringe the '385 Patent.

Proven Protection Against the Latest Threats

FortiGuard AntiVirus leverages a comprehensive technology stack that includes signature-based detection, heuristic and behavior-based detection, and AI- and ML-driven analysis.

The subscription service protects your network, endpoints, and cloud deployments from a wide range of malware. It attaches to many Fortinet products including FortiGate Next-Generation Firewalls (NGFWs), FortiMail, FortiWeb, FortiClient, and FortiSandbox.

17

48. For instance, Fortinet states its system monitors worldwide attack using global network sensors.

AI-Powered Threat Intelligence for an Evolving Digital World

As cyber threats continue to grow and evolve, so does the need for innovative solutions and reliable threat intelligence. Using millions of global network sensors, FortiGuard Labs monitors the worldwide attack surface and employs artificial intelligence (AI) to mine that data for new threats, ensuring you are prepared for what's coming.

18

About This Report and FortiRecon

This FortiGuard Labs Darknet Trends Report leveraged the Fortinet [FortiRecon](#) service to provide a deep dive into what adversaries are seeing, doing, and planning, enabling organizations to better understand the threats posed by the growth of criminal forums and markets operating on the darknet. The report covers global, regional, and industry/sector threat landscape perspectives as well as protection recommendations for IT and OT organizations for darknet activity observed during Q2 2022.

19

¹⁷<https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/antivirus>.

¹⁸<https://www.fortinet.com/fortiguard/labs>.

¹⁹<https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/report-threat-intelligence-q2.pdf>.

1. Executive Summary

Lurking in the shadows of the internet, there is a hidden, fast-growing threat of adversaries using newfound ways of committing crimes for their financial, political, or reputational gain. FortGuard Labs, leveraging the FortiRecon service, tracks these cybercriminals and their activities to protect organizations from imminent threats. This report presents an overview and related data of the cybercrime trends we witnessed during Q2 2022.

20

49. As another example, Fortinet employs a platform where the incoming data is processed according to instructions set by its platform.

FORTINET

ORDERING GUIDE

FortiSandbox and FortiGuard Sandbox Service

Available in

- Hardware Appliance
- VM Appliance
- Public Cloud
- Fortinet-Hosted

Purpose-built advanced AI Engine provides verdicts **10x** faster and **3x** detection and accuracy.

FortiSandbox, powered by the FortiGuard Advanced AI engine, is designed specifically for detecting unknown malware and phishing threats. It seamlessly integrates with existing security infrastructures, providing automated protection for both IT and OT environments. Additionally, it supports SOC teams with threat analysis and daily operations.

The new **FortiSandbox Universal VM** is an all-in-one license that supports any type of sandboxing VM, including Windows, Linux, Android, Custom, Cloud, and OT Simulator VMs. It offers the flexibility to choose and expand VM capacity, whether deployed on-premise or in the cloud.

FortiSandbox is offered on various cloud services and on-premise appliances. Choose which of the following solutions best fit your organizational needs:

- **Sandbox as-a-service (SaaS):** subscription services for FortiGate (and Fortinet Security Fabric devices) to support either:
 - **Detection:** out-of-band sandboxing, alerting, reporting, and log enrichment for SOC response.
 - **Detection and Prevention:** prioritized and high capacity to support inline sandboxing plus SOCaaS log ingestion.
- **SOC Augmentation:** Various form factors to support SOC teams in detection, prevention, and providing threat insights and hunting capabilities:
 - **Platform-as-a-Service (PaaS):** a Fortinet-hosted Cloud subscription service with dedicated VM resource.
 - **Public Cloud:** cloud-based FortiSandbox on Azure/AWS/OCI/GCP cloud.
 - **Dedicated Appliance:** on-premise physical or virtual appliance with predictable response time.

21

²⁰<https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/report-threat-intelligence-q2.pdf>.

²¹<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortisandbox.pdf>.

50. Fortinet Security Fabric performs a method that includes *accessing data comprising dark net information associated with a computer system*. For instance, Fortinet Security Fabric accesses data through network connections, specifically obtaining dark net information associated with a computer systems via FortiRecon. FortiRecon also actively monitors and collects data from dark web sources.

Go Beyond Pure Threat Intel Feeds with FortiRecon Dark Web Monitoring

FortiRecon ACI uses a powerful combination of artificial intelligence, machine learning, and HUMINT. FortiGuard Labs' cybersecurity experts provide unrivaled, organization-specific and expertly curated dark web, open source, and technical threat intel, including threat actor insights, and past/potential ransomware attacks on your organization or supply chain vendors. The experts enhance the offering with guidance on prioritizing remediation efforts, and also detect evidence of attacks in process. With this type of info, it is exceedingly easier to act fast and remediate threats quickly.

22

About This Report and FortiRecon

This FortiGuard Labs Darknet Trends Report leveraged the Fortinet [FortiRecon](#) service to provide a deep dive into what adversaries are seeing, doing, and planning, enabling organizations to better understand the threats posed by the growth of criminal forums and markets operating on the darknet. The report covers global, regional, and industry/sector threat landscape perspectives as well as protection recommendations for IT and OT organizations for darknet activity observed during Q2 2022.

23

1. Executive Summary

Lurking in the shadows of the internet, there is a hidden, fast-growing threat of adversaries using newfound ways of committing crimes for their financial, political, or reputational gain. FortGuard Labs, leveraging the FortiRecon service, tracks these cybercriminals and their activities to protect organizations from imminent threats. This report presents an overview and related data of the cybercrime trends we witnessed during Q2 2022.

24

²²<https://www.fortinet.com/products/fortirecon>.

²³<https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/report-threat-intelligence-q2.pdf>.

²⁴<https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/report-threat-intelligence-q2.pdf>.

51. Fortinet Security Fabric performs a method that includes *obtaining a set of exploits from the dark net information, the set of exploits configured to bypass a security feature of the computer system*. As previously discussed, and with further evidence shown below, FortiRecon obtains exploits from dark net through its monitoring of the dark net as part of Fortinet’s counter adversary operations.

Cybercriminals gravitate to the darknet because of its anonymity and lack of accountability. For the same reason, many adversaries are now starting to use instant messaging apps, such as Telegram, Tox, QQ, WeChat, and Discord. Others may use Threema or Jabber to offer a Tor redirection.

These platforms provide numerous features, including end-to-end encryption and auto-deleted messages, making tracking more difficult. Messaging apps are also being used to place bids on marketplace orders and host chat groups known as “channels” to send messages to an unlimited number of anonymous subscribers. Responses to group messages can be private encrypted conversations about illicit job offers, stolen documents, or hacking tools. The safer threat actors feel they can communicate, the more likely they are to share these tools and cybercrime opportunities—and the harder they’ll be to track.

Below is a summary of darknet activities observed by the FortiGuard Labs using the FortiRecon team service during Q2 2022:

- Financial services was the most targeted industry sector, followed by manufacturing, government, and technology.
- The Top Victim organizations operate in North America, followed by South Asia, Western Europe, and East Asia.
- FortiGuard Labs promoted 24 threat actors to be credible, meaning they had been sufficiently observed and their activity confirmed for the reports to be treated as genuine.
- Rising ransomware activity was observed, where the operators of LockBit ransomware were particularly active, naming 252 victims and outperforming all other ransomware groups.

25

²⁵<https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/report-threat-intelligence-q2.pdf>.

NOV 21, 2024 SEVERITY: CRITICAL

Palo Alto Networks Management Interface Attack

Type: Attack

What is the Palo Alto Networks Management Interface Attack?
Palo Alto Networks has recently disclosed two zero-day vulnerabilities, CVE-2024-0012 and CVE-2024-9474, affecting the PAN-OS Firewall and other products. Both flaws, which are actively being exploited in the wild, affect the management web interface and have been added to CISA's Known Exploited Vulnerabilities Catalog (KEV).

What is the FortiGuard Labs analysis?
FortiGuard Labs has observed numerous attack attempts targeting the Palo Alto PAN-OS vulnerabilities. Successful exploitation allows attackers to bypass authentication and gain administrator privileges without any user interaction and the attackers may then perform administrative actions, change configuration, and further exploit other vulnerabilities. The FortiGuard team recommends users apply the vendor's fix, follow any additional mitigation steps provided, and always follow industry best practices for deployment of such devices.

26

52. Fortinet Security Fabric performs a method that includes *applying an exploit function which takes the set of exploits as input and returns a set of vulnerabilities*. Specifically, FortiGuard Labs, uses hardware capabilities to detect complex attack techniques. In addition, FortiRecon provides actionable external attack surface intelligence on exposed assets, threat actor activity, and their tools, and tactics. This shows that Fortinet Security Fabric performs actions that involve applying an exploit function that takes the set of exploits as input and returns a set of vulnerabilities.

²⁶<https://www.fortinet.com/fortiguard/labs>.

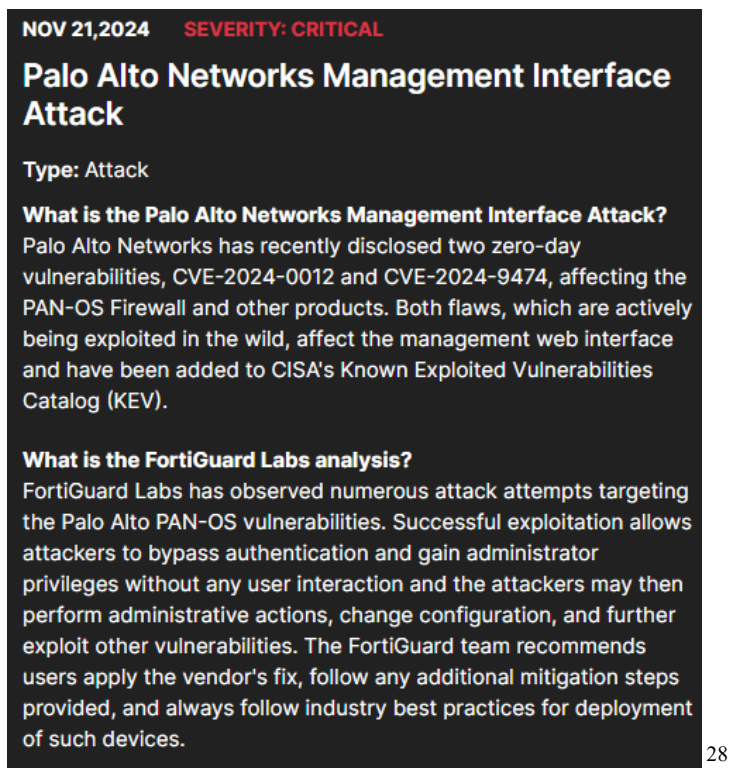
About This Report and FortiRecon

This FortiGuard Labs Darknet Trends Report leveraged the Fortinet [FortiRecon](#) service to provide a deep dive into what adversaries are seeing, doing, and planning, enabling organizations to better understand the threats posed by the growth of criminal forums and markets operating on the darknet. The report covers global, regional, and industry/sector threat landscape perspectives as well as protection recommendations for IT and OT organizations for darknet activity observed during Q2 2022.

[FortiRecon](#) is Fortinet's Digital Risk Protection (DRP) service. This SaaS-based service combines three powerful technologies and services—External Attack Surface Management, Brand Protection, and Adversary Centric Intelligence—to protect critical digital assets and data from external threats. By looking into open web, social media, mobile app stores, the dark web, and deep web sources, FortiRecon provides organization-specific, expert-curated, and actionable external attack surface intelligence on exposed assets, threat actor activity, and their tools, and tactics. The service also identifies brand infringement and monitors ransomware data leaks to proactively help remediate and execute takedowns on an organization's behalf.

27

²⁷<https://www.fortinet.com/content/dam/fortinet/assets/intelligence-reports/report-threat-intelligence-q2.pdf>.



53. Fortinet Security Fabric performs a method that includes *creating a constraint set of vulnerabilities of the computer system from the set of vulnerabilities comprising a minimum set of dependencies to operate the computer system, wherein application of the set of exploits on the computer system comprises determining the effect of the set of exploits on the constraint set of vulnerabilities of the computer system.* For instance, FortiSandbox executes submitted files and URLs within a controlled environment mimicking real world end user scenarios.

²⁸<https://www.fortinet.com/fortiguard/labs>.

How does Fortinet detect and protect against Palo Alto Networks Management Interface Attack?

- To detect and block any traffic targeting the vulnerabilities, the FortiGuard IPS Service is available.
- To automatically detect and respond to advanced threats such as 0-day or unknown malware, behavior-based detection through FortiSandbox and FortiXDR is available.
- To detect and respond to the attack, the FortiGuard Outbreak Detection Service provides an automatic event handler and reports through FortiAnalyzer.
- Automated Threat Hunting with Indicators of Compromise (IoC) Service is available through FortiAnalyzer, FortiSIEM, and FortiSOAR.

29

Threat Coverage: How FortiSandbox protects against unknown JavaScript malware

Introduction

FortiSandbox seamlessly integrates with various Security Fabric platform products, offering a straightforward approach to safeguarding against breaches. Upon detecting malicious code, FortiSandbox promptly responds by assigning risk ratings and instantly sharing local intelligence with Fortinet Security Fabric, Fabric-Ready Partners, and other security solutions.

This article highlights how FortiSandbox detects and captures the behavior of an obfuscated zero-day JavaScript sample. Upon execution, the original sample triggers the download of another JavaScript file, which plays a critical role as it contains commands and additional code aimed at establishing a connection and awaiting a response from a Command and Control (C2) server. This two-step approach showcases a sophisticated malware delivery and underscores the covert nature of the malicious activities orchestrated by threat actors. FortiSandbox executes submitted files and URLs within a controlled environment mimicking real world end user scenarios.

All the information in this article was gathered from the Job detail report generated by FortiSandbox.

30

54. Fortinet Security Fabric performs actions that involve *analyzing an application associated with the set of exploits on the computer system to detect a particular vulnerability of the constraint set of vulnerabilities of the computer system*. Specifically, Fortinet Security Fabric conducts detailed examinations of how exploits are applied to systems and identifies specific vulnerabilities that could be exploited by adversaries.

²⁹<https://www.fortinet.com/fortiguard/labs>.

³⁰<https://community.fortinet.com/t5/FortiSandbox/Threat-Coverage-How-FortiSandbox-protects-against-unknown/ta-p/305208>.

Threat Coverage: How FortiSandbox protects against unknown JavaScript malware

Introduction

FortiSandbox seamlessly integrates with various Security Fabric platform products, offering a straightforward approach to safeguarding against breaches. Upon detecting malicious code, FortiSandbox promptly responds by assigning risk ratings and instantly sharing local intelligence with Fortinet Security Fabric, Fabric-Ready Partners, and other security solutions.

This article highlights how FortiSandbox detects and captures the behavior of an obfuscated zero-day JavaScript sample. Upon execution, the original sample triggers the download of another JavaScript file, which plays a critical role as it contains commands and additional code aimed at establishing a connection and awaiting a response from a Command and Control (C2) server. This two-step approach showcases a sophisticated malware delivery and underscores the covert nature of the malicious activities orchestrated by threat actors. FortiSandbox executes submitted files and URLs within a controlled environment mimicking real world end user scenarios.

All the information in this article was gathered from the Job detail report generated by FortiSandbox.

31

³¹<https://community.fortinet.com/t5/FortiSandbox/Threat-Coverage-How-FortiSandbox-protects-against-unknown/ta-p/305208>.

NOV 21, 2024 SEVERITY: CRITICAL

Palo Alto Networks Management Interface Attack

Type: Attack

What is the Palo Alto Networks Management Interface Attack?
Palo Alto Networks has recently disclosed two zero-day vulnerabilities, CVE-2024-0012 and CVE-2024-9474, affecting the PAN-OS Firewall and other products. Both flaws, which are actively being exploited in the wild, affect the management web interface and have been added to CISA's Known Exploited Vulnerabilities Catalog (KEV).

What is the FortiGuard Labs analysis?
FortiGuard Labs has observed numerous attack attempts targeting the Palo Alto PAN-OS vulnerabilities. Successful exploitation allows attackers to bypass authentication and gain administrator privileges without any user interaction and the attackers may then perform administrative actions, change configuration, and further exploit other vulnerabilities. The FortiGuard team recommends users apply the vendor's fix, follow any additional mitigation steps provided, and always follow industry best practices for deployment of such devices.

32

55. Fortinet Security Fabric performs a method that includes *altering a configuration of the computer system in response to the analysis of the application of the set of exploits to reduce potential damage of a cyberattack*. For instance, Fortinet Security Fabric implements configuration changes based on the intelligence gathered to protect systems against identified threats.

³²<https://www.fortinet.com/fortiguard/labs>.

Threat Coverage: How FortiSandbox protects against unknown JavaScript malware

Introduction

FortiSandbox seamlessly integrates with various Security Fabric platform products, offering a straightforward approach to safeguarding against breaches. Upon detecting malicious code, FortiSandbox promptly responds by assigning risk ratings and instantly sharing local intelligence with Fortinet Security Fabric, Fabric-Ready Partners, and other security solutions.

This article highlights how FortiSandbox detects and captures the behavior of an obfuscated zero-day JavaScript sample. Upon execution, the original sample triggers the download of another JavaScript file, which plays a critical role as it contains commands and additional code aimed at establishing a connection and awaiting a response from a Command and Control (C2) server. This two-step approach showcases a sophisticated malware delivery and underscores the covert nature of the malicious activities orchestrated by threat actors. FortiSandbox executes submitted files and URLs within a controlled environment mimicking real world end user scenarios.

All the information in this article was gathered from the Job detail report generated by FortiSandbox.

33

NOV 21, 2024 SEVERITY: CRITICAL

Palo Alto Networks Management Interface Attack

Type: Attack

What is the Palo Alto Networks Management Interface Attack?

Palo Alto Networks has recently disclosed two zero-day vulnerabilities, CVE-2024-0012 and CVE-2024-9474, affecting the PAN-OS Firewall and other products. Both flaws, which are actively being exploited in the wild, affect the management web interface and have been added to CISA's Known Exploited Vulnerabilities Catalog (KEV).

What is the FortiGuard Labs analysis?

FortiGuard Labs has observed numerous attack attempts targeting the Palo Alto PAN-OS vulnerabilities. Successful exploitation allows attackers to bypass authentication and gain administrator privileges without any user interaction and the attackers may then perform administrative actions, change configuration, and further exploit other vulnerabilities. The FortiGuard team recommends users apply the vendor's fix, follow any additional mitigation steps provided, and always follow industry best practices for deployment of such devices.

34

³³<https://community.fortinet.com/t5/FortiSandbox/Threat-Coverage-How-FortiSandbox-protects-against-unknown/ta-p/305208>.

³⁴<https://www.fortinet.com/fortiguard/labs>.

Threat Mitigation

FortiSandbox uniquely integrates with various products through the Security Fabric platform that automates your breach protection strategy with an incredibly simple setup. Once malicious code is identified, FortiSandbox will return risk ratings and the local intelligence is shared in real time with Fortinet, Fabric-Ready Partners, and third-party security solutions to mitigate and immunize against new advanced threats. The local intelligence can optionally be shared with the FortiGuard Labs, to help protect organizations globally. The diagram following describes the automated mitigation process flow.

35

56. Fortinet is and has been aware of the '385 Patent and its coverage of the Accused Products since at least the filing of this Complaint.

57. Fortinet's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '385 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

58. Fortinet has actively induced and is actively inducing infringement of at least claim 1 of the '385 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Fortinet encourages and induces customers to use the Accused Products in a manner that infringes claim 1 of the '385 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

59. Fortinet encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

³⁵<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf>.

60. Fortinet further encourages and induces its customers to infringe at least claim 1 of the '385 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products in the United States.³⁶

61. For example, on information and belief, Fortinet shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. On further information and belief, Fortinet also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.³⁷

62. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Products remain operational for each customer through ongoing technical support, on information and belief, Fortinet and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '385 Patent.

63. Plaintiff has suffered and continues to suffer damages as a result of Fortinet's infringement of the '900 Patent. Fortinet is therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Fortinet's infringement, but no less than a reasonable royalty.

³⁶ <https://www.fortinet.com/products>; https://www.fortinet.com/resources/ordering-guides?document_type=ordering-guide&q=ordering%20guide.

³⁷ <https://www.fortinet.com/support/product-downloads>; <https://www.fortinet.com/demo-center>; <https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>; <https://www.fortinet.com/resources>; <https://www.fortinet.com/corporate/about-us/contact-us>.

64. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '385 Patent.

65. On information and belief, despite Fortinet's knowledge of the Asserted Patents and Plaintiff's patented technology, Fortinet made the deliberate decision to sell products and services that it knew infringe the Asserted Patents. Fortinet's continued infringement of the '385 Patent with knowledge of the '385 Patent constitutes willful infringement.

**SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE '900 PATENT)**

66. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

67. Fortinet is not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the '900 Patent.

68. Fortinet has infringed and continues to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the '900 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 12 of the '900 Patent.

69. Claim 12 of the '900 Patent recites:

A method, comprising:
configuring a processor for executing operations including:
accessing data associated with a deep web forum, the data defining a topic for classification;
extracting a set of features from the data as inputs for a machine classifier; and
apply a machine classifier to the set of features to generate a prediction list of tags for classifying the topic, wherein the prediction list includes a prediction probability value for each tag of the plurality of tags; and

adding all parent tags associated with a tag of the plurality of tags to the prediction list based on a comparison between the prediction probability value for the tag and a first predetermined threshold value.

70. For instance, Fortinet Security Fabric performs a method that includes *configuring a processor for executing operations*. For example, FortiGuard datacenters make use of FortiGate ASIC processors.

FortiGate® - High performance Network Security Platform

- ASIC-Powered Performance**
 FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.
- High speed and Flexible Connectivity**
 The FortiGate product family offers a variety of interfaces for today's network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.
- Broad Product Offerings**
 The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises, to high-end platforms for service providers and data centers.

38

71. Fortinet Security Fabric performs a method that includes *accessing data associated with a deep web forum, the data defining a topic for classification*. For instance, Fortinet Security Fabric includes FortiGuard Labs Threat Intelligence, which classifies criminal activities it detects while monitoring the darknet, also referred to as dark web, “a part or division of the deep web than can be accessed only with special software.” The data obtained about criminal activities is submitted to “automation tools to scan, process, mine and correlate this data.”

FortiGuard Labs Threat Intelligence Resources

At FortiGuard Labs, we use threat intelligence to better understand the techniques, malicious software, and potential targets that threat actors are considering attacking. Our threat intelligence is curated from many different sources, including (but certainly not limited to) millions of global network sensors, as well as multiple honeypots, cybersecurity reports, and intelligence shared between security professionals, security vendors, government organizations, and private partnerships.

With over 100 billion indicators of compromise, or IOCs, observed every day, threat hunters at FortiGuard Labs also employ a variety of automation tools to scan, process, mine, and correlate this data. This includes multiple internal machine learning techniques and our patented AI threat collection and correlation system, using big data analytics and elastic search clusters, writing Yara rules, and sometimes just relying on a close relationship with our customers and other security professionals who participate in the community submissions of threats.

³⁸<https://community.fortinet.com/tpykb84852/attachments/tpykb84852/techforum/1890/1/INSID E-WF-DAT-R1-201508.pdf>

In those cases where we identify malware connecting to specific sites for command and control, we also add the URLs and IPs (if it makes sense) to the malicious software categories on our web, **DNS**, and IP reputation filters.

39

Dark Web vs Deep Web

The deep web is an internet section that is not indexed by web crawlers or search engines, and the dark web is a part or division of the deep web that can be accessed only with special software. Although the former is used mainly for legitimate daily online activities, the latter is more anonymous and known as a haven for illegal transactions.

Here are other key differences between the dark web and the deep web:

1. To access the deep web, you need a password, whereas to access the dark web, you need to use Tor Project or a similar browser.
2. The deep web has a much broader scope compared to the dark web, covering a range of content that is not accessible by search engines.

Four Features Of Dark Web Monitoring

Here are some of the features of dark web monitoring:

1. Threat intelligence

Dark web monitoring tools map out useful sections of the dark web and determine important sources of threat intelligence—data or knowledge that allows you to mitigate or prevent **hacking**. With a dark web monitoring tool, you can subscribe to a feed of threat intelligence without the need to hire an expert to seek out, aggregate, and analyze it manually.

40

72. As a further example, FortiGuard collects information from deep-web forums and malware marketplaces that define various *topics for classification*, such as different kinds of malware: “remote access trojans, botnets for sale (such as the Zeus botnet), and crypto currency malware.” For instance, each kind of malware may form a sub-topic (*tag*) to a broader topic of

³⁹<https://www.fortinet.com/blog/threat-research/how-threat-researchers-leverage-darknet-to-stay-ahead-of-cyber-threats>

⁴⁰<https://www.fortinet.com/resources/cyberglossary/dark-web-monitoring>

malware (a *parent tag*). Relevant topics are automatically collected. “While we no longer manually search these sites, we do set up crawlers, APIs, or other access methods permitted by the websites that host the data to search for specific keywords and phrases.”⁴¹

In other words, I could give you all the forums, marketplaces, and TOR sites I visit; however, unless you already have techniques (or can develop them), these websites won't be useful because of the amount of information that has to be searched through and separated to make that information actionable.

While we no longer manually search these sites, we do set up crawlers, APIs, or other access methods permitted by the websites that host the data to search for specific keywords and phrases. And because of the shifting threat landscape, we have to refine our searches continuously. Many of these techniques are custom developed, and therefore not commonly available to the average user. And even then, we still have to contend with things such as CAPTCHA logins, two-factor authentication, and automated lockouts. And to complicate things further, some of these sites are explicitly looking for IPs connecting from known cybersecurity organizations or researchers, and will actively block them and lock them out.

Darknet Marketplaces

Another question I am often asked is, “What are some of the things we find on attacker/hacker forums, such as the Darknet's infamous onion sites?”

Let's start with the Darknet marketplaces. This is an underground version of e-commerce sites, where you can browse and purchase goods and services. The majority of the listings are generally related to narcotics. However, when we browse the software or malware sections of these sites, we often come across new data. Using the screenshots below, you can see such items as remote access trojans, botnets for sale (such as the Zeus botnet), and crypto currency malware.

WARNING: Do not trade outside of market like Telegram, Wickr or any other chats, we cannot protect you from scamming, always buy on the market you are protected by Escrow system.

★ Zeus Bot ★ Botnet & GUIDE 2020 ★
 #516 | Sold by: YMarker | Category: Software & Malware - Botnets & Malware | Offer since: Nov 17, 2019

Views: 9473 | Origin Country: Worldwide
 Purchase: 131 | Ships To: Worldwide
 Ends: Never | Quantity left: Unlimited
 Offer class: Digital | Payment type: Escrow

★★★★★ - 8 reviews (100.00%)

Instant Delivery (empty notes) - 1 day - USD +0.00 / Order

Price: 0.00075 BTC \$7.00

Qty: 1

Notice: found auto-dispatch on this offer good for you

42

73. Fortinet Security Fabric performs a method that includes *extracting a set of features from the data as inputs for a machine classifier*. For example, FortiRecon's “Adversary Centric Intelligence” (“ACI”) uses machine-learning and artificial-intelligence tools to monitor and classify deep-web information about potential threats.

⁴¹ <https://www.fortinet.com/blog/threat-research/how-threat-researchers-leverage-darknet-to-stay-ahead-of-cyber-threats>

⁴² <https://www.fortinet.com/blog/threat-research/how-threat-researchers-leverage-darknet-to-stay-ahead-of-cyber-threats>



Go Beyond Pure Threat Intel Feeds with FortiRecon Dark Web Monitoring

FortiRecon ACI uses a powerful combination of artificial intelligence, machine learning, and HUMINT. FortiGuard Labs' cybersecurity experts provide unrivaled, organization-specific and expertly curated dark web, open source, and technical threat intel, including threat actor insights, and past/potential ransomware attacks on your organization or supply chain vendors. The experts enhance the offering with guidance on prioritizing remediation efforts, and also detect evidence of attacks in process. With this type of info, it is exceedingly easier to act fast and remediate threats quickly.

43

74. The machine-learning algorithms (e.g., *machine classifier*) used by FortiRecon ACI employ “feature vectors” to process large volumes of data collected from deep-web sources (e.g., *a set of features from the data as inputs*).

Feature vector

This refers to a set of more than one numerical feature. It is used as an input, entered into the machine-learning model to generate predictions and to train the system.

Training

When an algorithm examines a set of data and finds patterns, the system is being “trained” and the resulting output is the machine-learning model.

Prediction

After the machine-learning model has been trained, it can receive an input and then provide a prediction regarding the output.

Target (Label)

The target is the value the machine-learning model is charged with predicting.

⁴³<https://www.fortinet.com/products/fortirecon>

How does machine learning work?

Machine learning algorithms process large volumes of data, seeking patterns that may not be obvious to human analysts. The patterns are detected by computing statistical measurements like weighted averages. Machine learning depends on vector and tensor (or matrix) algorithms. The probabilistic results may be stored in special data structures that allow easy lookup.

44

75. Fortinet Security Fabric performs a method that *appl[ies] a machine classifier to the set of features to generate a prediction list of tags for classifying the topic, wherein the prediction list includes a prediction probability value for each tag of the plurality of tags.* For instance, FortiGuard uses machine learning to classify information from deep web “Hacker Sites/Forums” and other websites into categories and derive from them indicators of compromise indicating a prediction of topics associated with a cybersecurity threat.

Fortiguard Labs collects indicators of compromise (IOCs) by a variety of methods. Following are some examples:

Machine Learning

ML techniques are used to capture IOCs (indicators of compromise) such as malicious IP addresses, domains and urls.

Global Sensors

Millions of sensors deployed around the globe consisting of participating customer devices, honeypots and deception decoys pick up early signals of compromise in the global cyber space.

Web Crawlers

Fortinet propriety web crawler armed with Artificial Intelligence crawl the Internet looking for malicious sites.

Hacker Sites/Forums

Troll the underground/darknet to uncover zero-day threat events.

45

⁴⁴<https://www.fortinet.com/resources/cyberglossary/what-is-machine-learning>

⁴⁵<https://www.fortiguard.com/services/ioc>

How Does Fortinet Use AI and ML-Driven Cybersecurity?

The big change in the malware industry that triggered the need for AI was heuristics and adaptive malware. We went almost overnight from a volume of malware that could be handled manually to a situation with exponential growth in the number of samples. We had to adapt and take advantage of artificial intelligence and machine learning to support our malware analysts.

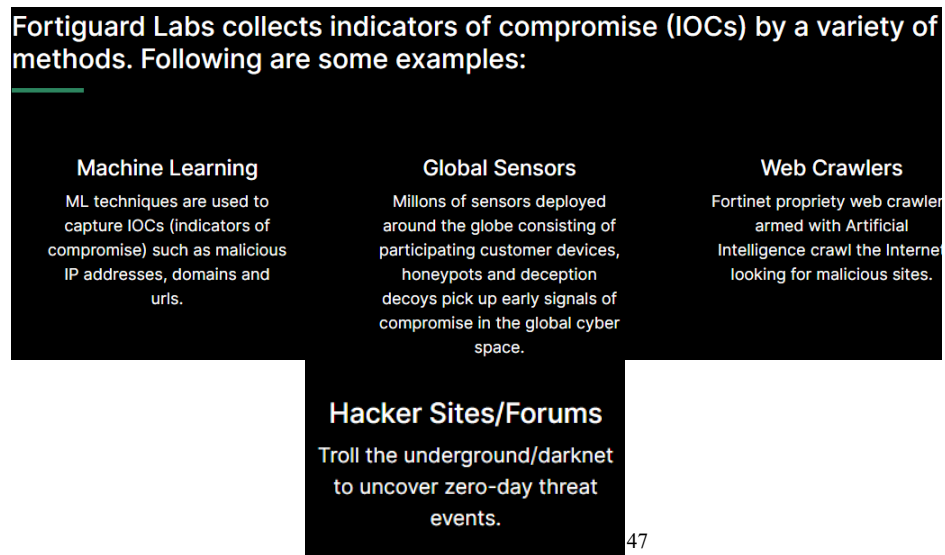
Fortinet has been in the AI business for more than a decade. At a high level, Fortinet uses artificial intelligence and machine learning in multiple areas:

Predict

ML/AI is particularly good at drawing relationships and making predictions. An example is comparing two infections' "DNA" and tracing the source of a problem. This is a more advanced application of AI, as prediction has a time element—meaning you can tell ahead of time what will happen. Based on the historical data points, trending, etc., it is possible to predict what might happen to your network.

46

76. Finally, Fortinet Security Fabric performs a method step of *adding all parent tags associated with a tag of the plurality of tags to the prediction list based on a comparison between the prediction probability value for the tag and a first predetermined threshold value*. For instance, FortiGuard machine-learning tools correlate information from deep-web "Hacker Sites/Forums" with other sources such as "Global Sensors" and "Web Crawlers" to apply all relevant categorizations to the information (e.g., *add all parent tags*).



47

⁴⁶AI (Artificial Intelligence) and Machine Learning in the Cybersecurity Battle | Fortinet Blog

⁴⁷<https://www.fortiguard.com/services/ioc>

How Does Fortinet Use AI and ML-Driven Cybersecurity?

The big change in the malware industry that triggered the need for AI was heuristics and adaptive malware. We went almost overnight from a volume of malware that could be handled manually to a situation with exponential growth in the number of samples. We had to adapt and take advantage of artificial intelligence and machine learning to support our malware analysts.

Fortinet has been in the AI business for more than a decade. At a high level, Fortinet uses artificial intelligence and machine learning in multiple areas:

Predict

ML/AI is particularly good at drawing relationships and making predictions. An example is comparing two infections' "DNA" and tracing the source of a problem. This is a more advanced application of AI, as prediction has a time element—meaning you can tell ahead of time what will happen. Based on the historical data points, trending, etc., it is possible to predict what might happen to your network.

48

77. Fortinet is and has been aware of the '900 Patent and its coverage of the Accused Products since at least the filing of this Complaint.

78. Fortinet's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 12 of the '900 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

79. Fortinet has actively induced and is actively inducing infringement of at least claim 12 of the '900 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Fortinet encourages and induces customers to use the Accused Products in a manner that infringes claim 12 of the '900 Patent at least by offering and providing software that performs a method that infringes claim 12 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

⁴⁸AI (Artificial Intelligence) and Machine Learning in the Cybersecurity Battle | Fortinet Blog

80. Fortinet encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

81. Fortinet further encourages and induces its customers to infringe at least claim 12 of the '900 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products in the United States.⁴⁹

82. For example, on information and belief, Fortinet shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. On further information and belief, Fortinet also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.⁵⁰

83. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Products remain operational for each customer through ongoing technical support, on information and belief, Fortinet and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '900 Patent.

⁴⁹ <https://www.fortinet.com/products>; https://www.fortinet.com/resources/ordering-guides?document_type=ordering-guide&q=ordering%20guide.

⁵⁰ <https://www.fortinet.com/support/product-downloads>; <https://www.fortinet.com/demo-center>; <https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>; <https://www.fortinet.com/resources>; <https://www.fortinet.com/corporate/about-us/contact-us>.

84. Plaintiff has suffered and continues to suffer damages as a result of Fortinet's infringement of the '900 Patent. Fortinet is therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Fortinet's infringement, but no less than a reasonable royalty.

85. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '900 Patent.

86. On information and belief, despite Fortinet's knowledge of the Asserted Patents and Plaintiff's patented technology, Fortinet made the deliberate decision to sell products and services that it knew infringe the Asserted Patents. Fortinet's continued infringement of the '900 Patent with knowledge of the '900 Patent constitutes willful infringement.

**THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE '831 PATENT)**

87. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

88. Fortinet is not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the '831 Patent.

89. Fortinet has infringed and continues to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the '831 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '831 Patent.

90. Claim 1 of the '831 Patent recites:

One or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations comprising:

in one or more layers of a convolutional neural network (CNN), performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs) for each of a plurality of data sets;

examining a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present among the first set of values;

responsive to identifying the maximum value, performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value; and

propagating the full precision computation of the value to a subsequent layer of the CNN.

91. For instance, to the extent that the preamble is limiting, the Accused Products embody *one or more non-transitory computer-readable storage media storing instructions which, when executed by at least one processor, cause the at least one processor to perform operations*. For example, the Accused Products include FortiRecon, which “continuously monitors and identifies internet-facing unmanaged, vulnerable, and misconfigured assets, security certificate issues, leaked credentials, and vulnerable internal assets.” Furthermore, the Accused Products include processors, such as FortiGuard Labs’ integration of “processors (e.g., SPU, vSPU)” and “memory” within Fortinet’s systems, which “facilitates the execution of essential operations”, including AI-powered threat detection, cryptographic security, and real-time protection against cyber threats.

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet’s layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

**State-of-the-art
unparalleled performance
with Fortinet's patented
SPU and vSPU processors**

51

92. The Accused Products embody a non-transitory storage media whose instructions include *in one or more layers of a convolutional neural network (CNN), performing a first iteration that includes computing a value based on a first set of most significant bits (MSBs) for each of a plurality of data sets*. For instance, FortiGuard AI uses machine learning which may include convolutional neural networks.

- FortiGuard AI is a self-evolving threat detection system that uses machine learning and continuous training to autonomously collect, analyze, and classify threats with a high degree of accuracy and at machine speed.
- FortiGuard AI is integrated into Fortinet's threat intelligence services platform to power all of the advanced threat detection capabilities that FortiGuard services share across the Security Fabric.
- Fortinet also announced new User Entity and Behavioral Analysis (UEBA) capabilities, and the launch of FortiGuard Threat Intelligence Service (TIS) as an enterprise service offering.

52

93. The Accused Products embody a non-transitory storage media whose instructions include *examining a first set of values computed for the plurality of data sets in the first iteration to determine whether a maximum value is present among the first set of values*. For instance, FortiRecon implements “multiple internal machine learning techniques” to “scan, process, mine, and correlate” data collected from “millions of global network sensors, as well as multiple honeypots, cybersecurity reports, and intelligence”, which can be enhanced by the analysis of a plurality of data sets in accordance with the claim.

⁵¹<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf>

⁵²<https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2018/fortiguard-ai-delivers-proactive-threat-detection>

FortiGuard Labs Threat Intelligence Resources

At FortiGuard Labs, we use threat intelligence to better understand the techniques, **malicious software**, and potential targets that threat actors are considering attacking. Our threat intelligence is curated from many different sources, including (but certainly not limited to) millions of global network sensors, as well as multiple honeypots, cybersecurity reports, and intelligence shared between security professionals, security vendors, government organizations, and private partnerships.

With over 100 billion indicators of compromise, or IOCs, observed every day, threat hunters at FortiGuard Labs also employ a variety of automation tools to scan, process, mine, and correlate this data. This includes multiple internal machine learning techniques and our patented **AI** threat collection and correlation system, using big data analytics and elastic search clusters, writing Yara rules, and sometimes just relying on a close relationship with our customers and other security professionals who participate in the community submissions of threats.

In those cases where we identify malware connecting to specific sites for command and control, we also add the URLs and IPs (if it makes sense) to the malicious software categories on our web, **DNS**, and IP reputation filters.

⁵³

94. The Accused Products embody a non-transitory storage media whose instructions include *responsive to identifying the maximum value, performing a full precision computation of the value for a data set, of the plurality of data sets, that exhibited the maximum value*. For instance, the Accused Products include AI and machine-learning tools configured to “scale” and “enhance” Fortinet’s accurate analysis of millions of data points to detect and predict cybersecurity threats.

⁵³<https://www.fortinet.com/blog/threat-research/how-threat-researchers-leverage-darknet-to-stay-ahead-of-cyber-threats>

How Does Fortinet Use AI and ML-Driven Cybersecurity?

The big change in the malware industry that triggered the need for AI was heuristics and adaptive malware. We went almost overnight from a volume of malware that could be handled manually to a situation with exponential growth in the number of samples. We had to adapt and take advantage of artificial intelligence and machine learning to support our malware analysts.

Fortinet has been in the AI business for more than a decade. At a high level, Fortinet uses artificial intelligence and machine learning in multiple areas:

Scale

One of the first use cases 10 years ago was the advent of the virtual **FortiGuard** threat analyst. The huge growth in samples meant that analysts could no longer handle the volumes of samples they were receiving, so we created an artificial neural network (ANN) for sub-second sample classification. Over six generations of this solution, this grew into **FortiAI**, which analyzes millions of samples per day with near-perfect accuracy—a task that would normally require thousands of human analysts.

Enhance

An ML use case is a great way to enhance traditional security solutions. Some examples are:

- Adding ML analysis of malicious vectors in **FortiSandbox**
- ML-enabled AV engine in **FortiOS**
- Widely adopt ML in other solutions such as **FortiWeb**, **FortiGuard Security Services**, and many more. This enables better and more accurate detections of malicious activities or anomalies for our customers. In this area, innovation is key.

Predict

ML/AI is particularly good at drawing relationships and making predictions. An example is comparing two infections' "DNA" and tracing the source of a problem. This is a more advanced application of AI, as prediction has a time element—meaning you can tell ahead of time what will happen. Based on the historical data points, trending, etc., it is possible to predict what might happen to your network.

Reduce time to detect

Fortinet pushes the physical limit to "sub-second" detection of malicious code, enabling SecOps solutions to integrate with our flagship **FortiGate NGFW** for *inline blocking*, stopping patient zero. While reducing the time to detect from minutes to sub-second might not sound significant, it's crucial when a major, widespread outbreak occurs. Customers should have the ability to react quickly to threat actors.

54

95. The Accused Products embody a non-transitory storage media whose instructions include *propagating the full precision computation of the value to a subsequent layer of the CNN*. For instance, as discussed above, the Accused Products use multiple machine-learning techniques to scale and enhance threat analysis when predicting and detecting malicious code or other activities, which may include *propagating a full precision computation* in accordance with this claim limitation.

96. Fortinet is and has been aware of the '831 Patent and its coverage of the Accused Products since at least the filing of this Complaint.

⁵⁴<https://www.fortinet.com/blog/business-and-technology/battle-ai-ml-cybersecurity-world>

97. Fortinet's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '831 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

98. Fortinet has actively induced and is actively inducing infringement of at least claim 1 of the '831 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Fortinet encourages and induces customers to use the Accused Products in a manner that infringes claim 1 of the '831 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

99. Fortinet encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

100. Fortinet further encourages and induces its customers to infringe at least claim 1 of the '831 Patent: 1) by making its security services available on its website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products in the United States.⁵⁵

⁵⁵ <https://www.fortinet.com/products>; https://www.fortinet.com/resources/ordering-guides?document_type=ordering-guide&q=ordering%20guide.

101. For example, on information and belief, Fortinet shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. On further information and belief, Fortinet also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.⁵⁶

102. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Products remain operational for each customer through ongoing technical support, on information and belief, Fortinet and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '831 Patent.

103. Plaintiff has suffered and continues to suffer damages as a result of Fortinet's infringement of the '831 Patent. Fortinet is therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Fortinet's infringement, but no less than a reasonable royalty.

104. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '831 Patent.

105. On information and belief, despite Fortinet's knowledge of the Asserted Patents and Plaintiff's patented technology, Fortinet made the deliberate decision to sell products and services

⁵⁶ <https://www.fortinet.com/support/product-downloads>; <https://www.fortinet.com/demo-center>; <https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>; <https://www.fortinet.com/resources>; <https://www.fortinet.com/corporate/about-us/contact-us>.

that it knew infringe the Asserted Patents. Fortinet's continued infringement of the '831 Patent with knowledge of the '831 Patent constitutes willful infringement.

**FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE '897 PATENT)**

106. Plaintiff incorporates and realleges all of the above paragraphs as though fully set forth herein.

107. Fortinet is not licensed (expressly or impliedly) or otherwise authorized to make, use, offer for sale, or sell any products or services that embody the inventions of the '897 Patent.

108. Fortinet has infringed and continues to infringe, either literally and/or under the doctrine of equivalents, one or more claims of the '897 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '897 Patent.

109. Claim 1 of the '897 Patent recites:

A method for assessing a likelihood of exploitation of software vulnerabilities, comprising:

utilizing a processor in operable communication with at least one memory for storing instructions that are executed by the processor to perform operations, including:

accessing a plurality of datasets associated with a predetermined set of data sources, the plurality of datasets including training data comprising hacker communications;

accessing features from the plurality of datasets that include measures computed from social connections of users posting hacking-related content

applying learning algorithms to the training data to generate classification models that are configured to predict class labels defining a likelihood of exploitation of respective software vulnerabilities;

accessing one or more features associated with a software vulnerability; and

computing, by applying the one or more features to the classification model, a class label defining one or more values defining a likelihood of exploitation associated

with the software vulnerability, wherein the likelihood of exploitation predicts an actual exploitation of the respective software vulnerabilities before disclosure based on the hacker communications from the training data.

110. For instance, to the extent that the preamble is limiting, Fortinet Security Fabric implements a *method for assessing a likelihood of exploitation of software vulnerabilities*. For example, Fortinet Security Fabric includes FortiRecon, which “continuously monitors and identifies internet-facing unmanaged, vulnerable, and misconfigured assets, security certificate issues, leaked credentials, and vulnerable internal assets.” (E.g., *software vulnerabilities*). FortiRecon serves to “prioritize remediations and proactively optimize defenses based on risk exposure, potential and current attacks on software vendors, vulnerabilities exploited in the wild, and more” (e.g., *assessing a likelihood of exploitation of software vulnerabilities*).⁵⁷



Avoid Blind Spots in Security Monitoring with FortiRecon ASM

FortiRecon alerts on external and internal weak points that attackers can exploit to access your network and move laterally. It continuously monitors and identifies internet-facing unmanaged, vulnerable, and misconfigured assets, security certificate issues, leaked credentials, and vulnerable internal assets. This helps you gain control over all assets. You can prioritize remediations and proactively optimize defenses based on risk exposure, potential and current attacks on software vendors, vulnerabilities exploited in the wild, and more.

Watch Now »

111. As another example, Fortinet Security Fabric comprises “Threat Intelligence,” including the use of “multiple internal machine learning techniques and our patented AI threat collection and correlation system, using big data analytics and elastic search clusters” to “better understand the techniques, malicious software, and potential targets that threat actors are considering attacking.” (E.g., *assessing a likelihood of exploitation of software vulnerabilities*).

⁵⁷<https://www.fortinet.com/products/fortirecon>

FortiGuard Labs Threat Intelligence Resources

At **FortiGuard Labs**, we use threat intelligence to better understand the techniques, **malicious software**, and potential targets that threat actors are considering attacking. Our threat intelligence is curated from many different sources, including (but certainly not limited to) millions of global network sensors, as well as multiple honeypots, cybersecurity reports, and intelligence shared between security professionals, security vendors, government organizations, and private partnerships.

With over 100 billion indicators of compromise, or IOCs, observed every day, threat hunters at FortiGuard Labs also employ a variety of automation tools to scan, process, mine, and correlate this data. This includes multiple internal machine learning techniques and our patented **AI** threat collection and correlation system, using big data analytics and elastic search clusters, writing Yara rules, and sometimes just relying on a close relationship with our customers and other security professionals who participate in the community submissions of threats.

In those cases where we identify malware connecting to specific sites for command and control, we also add the URLs and IPs (if it makes sense) to the malicious software categories on our web, **DNS**, and IP reputation filters.

58

112. As a further example, FortiGuard Labs provides information on the likelihood of exploitation of software vulnerabilities by participating in the “EPSS (Exploit Prediction Scoring System.” By training the EPSS model, FortiGuard Labs provides “estimates [of] the likelihood of a vulnerability being exploited in the wild.”

Fortinet also provided data sets to help train the model for the **Exploit Prediction Scoring System** (EPSS) project and FortiGuard Labs has been an active participant. EPSS is an open model for predicting the likelihood that a vulnerability will be exploited in the wild. Coupled with the TTP (tactics, techniques, and procedures) data we are providing through the Threat Intelligence Insider, we’re building the future of cybersecurity protections and decision making.

59

113. Fortinet Security Fabric performs a method that includes *utilizing a processor in operable communication with at least one memory for storing instructions that are executed by the processor to perform operations*. For instance, FortiGuard Labs drives Fortinet's products with advanced threat intelligence and machine learning capabilities. The integration of “processors (e.g., SPU, vSPU)” and “memory” within Fortinet's systems “facilitates the execution of essential operations”, including AI-powered threat detection, cryptographic security, and real-time protection against cyber threats.

⁵⁸<https://www.fortinet.com/blog/threat-research/how-threat-researchers-leverage-darknet-to-stay-ahead-of-cyber-threats>

⁵⁹<https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss>


FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet’s layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

**State-of-the-art
unparalleled performance**
with Fortinet’s patented
SPU and vSPU processors

60

114. Fortinet Security Fabric performs a method that includes *accessing a plurality of datasets associated with a predetermined set of data sources, the plurality of datasets including training data comprising hacker communications*. For instance, FortiRecon accesses various “threat sources” (e.g., *a plurality of datasets associated with a predetermined set of data sources*) by monitoring “dark web discourse” and “forum” sources comprising data from criminal forums and discussions on the dark web (e.g., *training data comprising hacker communications*), as well as “Pastebin” and “OSINT” sources.



**FAR-REACHING
THREAT SOURCES**
Discovers
current/potential threats
with dark web, Pastebin,
forum, market, and OSINT
monitoring by FortiGuard
Labs experts

61

⁶⁰<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-400f-series.pdf>

⁶¹<https://www.fortinet.com/products/fortirecon>

Dark Web Discourse

The 2H 2023 Global Threat Landscape Report also includes findings from FortiRecon, which give a glimpse into the discourse between threat actors on dark web forums, marketplaces, Telegram channels, and other sources. Some of the findings include:

- Threat actors discussed targeting organizations within the finance industry most often, followed by the business services and education sectors.
- More than 3,000 data breaches were shared on prominent dark web forums.
- 221 vulnerabilities were actively discussed on the darknet, while 237 vulnerabilities were discussed on Telegram channels.
- Over 850,000 payment cards were advertised for sale.

62

115. Fortinet Security Fabric performs a method that includes *accessing features from the plurality of datasets that include measures computed from social connections of users posting hacking-related content*. For instance, FortiRecon “monitors and reports on vulnerabilities and exploits being actively discussed on the dark web and open source.”⁶³ Furthermore, FortiRecon is stated to “glimpse into the discourse between threat actors on dark web forums, marketplaces, Telegram channels, and other sources.”⁶⁴

Vulnerability intelligence and prioritization

Monitors and reports on vulnerabilities and exploits being actively used and discussed on the dark web and open source. FortiRecon re-rates vulnerability scores based on scan results, wide usage, CVEs, and CVSS, for effective remediation prioritization.

Ransomware intelligence

OSINT cyber threats intel

Helps you stay up to date with information on current cyber threats or events published on open source platforms, for example, social media and GitHub repositories.

Data leakage intel

Alerts on leaked credentials and data related to your organization

65

116. Fortinet Security Fabric performs a method that includes *applying learning algorithms to the training data to generate classification models that are configured to predict class labels defining a likelihood of exploitation of respective software vulnerabilities*. For instance, FortiRecon “uses a powerful combination of artificial intelligence, machine learning and

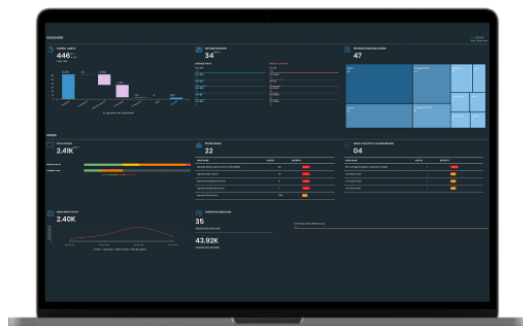
⁶²<https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-threat-research-finds-cybercriminals-are-exploiting-new-industry-vulnerabilities-faster>

⁶³<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortirecon.pdf>

⁶⁴<https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-threat-research-finds-cybercriminals-are-exploiting-new-industry-vulnerabilities-faster>

⁶⁵<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortirecon.pdf>

HUMINT” to conduct its dark-web monitoring and process threat intelligence (e.g., *applying learning algorithms to the training data to generate classification models*).



Go Beyond Pure Threat Intel Feeds with FortiRecon Dark Web Monitoring

FortiRecon ACI uses a powerful combination of artificial intelligence, machine learning, and HUMINT. FortiGuard Labs' cybersecurity experts provide unrivaled, organization-specific and expertly curated dark web, open source, and technical threat intel, including threat actor insights, and past/potential ransomware attacks on your organization or supply chain vendors. The experts enhance the offering with guidance on prioritizing remediation efforts, and also detect evidence of attacks in process. With this type of info, it is exceedingly easier to act fast and remediate threats quickly.

66

117. Furthermore, FortiRecon “monitors and reports on vulnerabilities and exploits being actively used” (e.g. *configured to predict class labels defining a likelihood of exploitation of respective software vulnerabilities*).

118. As another example, Fortinet Security Fabric contributes to the training of the EPSS machine-learning “predictive model”. The model is “used in combination with vulnerability metadata to predict future exploitation activity.” It generates a score (e.g., a *class label*) to predict the likelihood of software vulnerability exploitation.

As can be seen, any EPSS deployment must first go through a training phase, where it is given historical vulnerability data and daily exploitation activity to develop and refine its predictive model. Once established, the predictive model can then be used in combination with vulnerability metadata on a daily basis to predict future exploitation activity.

The resulting EPSS score can be used for such things as prioritizing which software to patch based on a threshold, with the advantage of requiring organizations to patch fewer vulnerabilities compared to using a patching strategy based solely on a CVSS ranking. There is too much math involved to describe the process here, but you can go to this site to learn more (<https://www.first.org/epss/model>). But the takeaway is that organizations that properly deploy and train EPSS will need to patch fewer vulnerabilities than they would have using the classic CVSS strategy while maintaining the same level of protection.

You are warned, though. EPSS should never be treated as a risk score. Other factors, such as how accessible vulnerable assets are to attackers, the type of weakness a vulnerability presents, the asset's purpose and value, etc., are all factors to consider when prioritizing which vulnerabilities should be addressed. Fortunately, those factors are typically contained in the string vector of the CVSS score.

67

119. Fortinet Security Fabric performs a method that includes *accessing one or more features associated with a software vulnerability*. For instance, FortiRecon’s Adversary Centric

⁶⁶<https://www.fortinet.com/products/fortirecon>

⁶⁷<https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss>

Intelligence module provides “curated dark web [...] threat intelligence” (e.g., *features associated with a software vulnerability*).

FortiRecon Adversary Centric Intelligence

Leverages FortiGuard Threat Research teams to provide organization-specific and expertly curated dark web, open source, and technical threat intelligence, including threat actor insights, past and potential ransomware attacks on your organization or your supply chain vendors, to enable security professionals to better prepare for potential attacks, proactively assess risks, and adjust security posture accordingly.

68

120. Furthermore, FortiRecon accesses specific “vulnerability intelligence” drawn from its collection of dark-web hacker discussions and other sources “to help prioritize vulnerability patching.”⁶⁹

121. Fortinet Security Fabric performs a method that includes *computing, by applying the one or more features to the classification model, a class label defining one or more values defining a likelihood of exploitation associated with the software vulnerability, wherein the likelihood of exploitation predicts an actual exploitation of the respective software vulnerabilities before disclosure based on the hacker communications from the training data*. For instance, FortiRecon uses FortiGuard Threat Intelligence to collect and process hacker information through machine-learning classifying tools (discussed, *supra*), and obtain “targeted, curated intelligence to provide an early warning of any malicious activity targeted to the organization.” (E.g., *wherein the likelihood of exploitation predicts an actual exploitation [...] before disclosure based on the hacker communications from the training data*).

⁶⁸<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortirecon.pdf>

⁶⁹<https://docs.fortinet.com/document/fortirecon/24.3.0/user-guide/019955/vulnerability-intelligence>

FortiRecon scans the organization's attack surface and identifies risks to assets across both external and internal domains while FortiGuard Threat Intelligence delivers early warning of risks to the organization through targeted, curated intelligence to provide an early warning of any malicious activity targeted to the organization.

⁷⁰

122. Fortinet is and has been aware of the '897 Patent and its coverage of the Accused Products since at least the filing of this Complaint.

123. Fortinet's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '897 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services.

124. Fortinet has actively induced and is actively inducing infringement of at least claim 1 of the '897 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Fortinet encourages and induces customers to use the Accused Products in a manner that infringes claim 1 of the '897 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

125. Fortinet encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways.

126. Fortinet further encourages and induces its customers to infringe at least claim 1 of the '897 Patent: 1) by making its security services available on its website, providing applications

⁷⁰<https://docs.fortinet.com/document/fortirecon/24.3.0/user-guide/897693/introduction>.

that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products in the United States.⁷¹

127. For example, on information and belief, Fortinet shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. On further information and belief, Fortinet also provides customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner.⁷²

128. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Products remain operational for each customer through ongoing technical support, on information and belief, Fortinet and/or its partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '897 Patent.

129. Plaintiff has suffered and continues to suffer damages as a result of Fortinet's infringement of the '897 Patent. Fortinet is therefore liable to Plaintiff under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiff for Fortinet's infringement, but no less than a reasonable royalty.

⁷¹ <https://www.fortinet.com/products>; https://www.fortinet.com/resources/ordering-guides?document_type=ordering-guide&q=ordering%20guide.

⁷² <https://www.fortinet.com/support/product-downloads>; <https://www.fortinet.com/demo-center>; <https://community.fortinet.com/t5/Knowledge-Base/ct-p/knowledgebase>; <https://www.fortinet.com/resources>; <https://www.fortinet.com/corporate/about-us/contact-us>.

130. Plaintiff, its predecessors-in-interest, and/or any licensees have satisfied all statutory obligations required to collect pre-filing damages for the full period allowed by law for infringement of the '897 Patent.

131. On information and belief, despite Fortinet's knowledge of the Asserted Patents and Plaintiff's patented technology, Fortinet made the deliberate decision to sell products and services that it knew infringe the Asserted Patents. Fortinet's continued infringement of the '897 Patent with knowledge of the '897 Patent constitutes willful infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

- A. That this Court adjudge and decree that Defendant has been, and is currently, infringing each of the Asserted Patents;
- B. That this Court award damages to Plaintiff to compensate it for Defendant's past infringement of the Asserted Patents, through the date of trial in this action, and damages for future infringement of the Asserted Patents, through the expiration dates of the Asserted Patents;
- C. That this Court award pre- and post-judgment interest on such damages to Plaintiff;
- D. That this Court order an accounting of damages incurred by Plaintiff from six years prior to the date this lawsuit was filed through the entry of a final, non-appealable judgment;
- E. That this Court determine that this patent infringement case is exceptional and award Plaintiff its costs and attorneys' fees incurred in this action;
- F. That this Court award increased damages under 35 U.S.C. § 284; and
- G. That this Court award such other and further relief as the Court deems just and equitable.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff respectfully requests a trial by jury on all issues so triable.

DATED: January 31, 2025

By: /s/ Cecil E. Key
Cecil E. Key
Jay P. Kesan (*pro hac vice to be filed*)
KEY KESAN DALLMANN PLLC
1050 Connecticut Avenue, N.W. Suite 500
Washington, DC 20036
Telephone: (202)772-1100
jay.kesan@kkd-law.com
cecil.key@kkd-law.com

Attorneys for Plaintiff
Skysong Innovations, LLC