UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPEN TEXT, INC.,	)	
Plaintiffs,	)	
v.	)	Civil Action No. 6:22-cv-00342
FORCEPOINT LLC,	)	JURY TRIAL DEMANDED
Defendant.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Webroot, Inc., ("Webroot") and Open Text, Inc., ("OpenText") (collectively "Plaintiffs") allege against Forcepoint LLC ("Forcepoint" or "Defendant") the following:

1. This case involves patented technologies that helped to revolutionize and have become widely adopted in, the fields of malware detection, network security, and endpoint protection. Endpoint protection involves securing endpoints or entry points of end-user devices (*e.g.*, desktops, laptops, mobile devices, etc.) on a network or in a cloud from cybersecurity threats, like malware.

2. Before Plaintiffs' patented technologies, security platforms typically relied on signatures (*i.e.*, unique identifiers) of computer objects (*e.g.*, computer programs) that were analyzed and identified as "bad" by teams of threat researchers. This approach required antivirus companies to employ hundreds to thousands of threat analysts to review individual programs and determine if they posed a threat.

3. The "bad" programs identified by researchers were compiled into a library and uploaded to an antivirus software program installed on each endpoint device. To detect threats, a

resource intensive “virus scan” of each endpoint device was conducted. These virus scans could take hours to complete and substantially impact productivity and performance.

4. Despite substantial investments in resources and time, the conventional systems still were unable to identify and prevent emerging (“zero-day”) threats from new or unknown malware. New threats persisted and were free to wreak havoc until a team of threat analysts could identify each one and upload these newly identified threats to an update of the “bad” program library. The updated “bad” program library, including signatures to identify new threats as well as old, then had to be disseminated to all of the endpoint computers, which required time and resource consuming downloads of the entire signature library to every computer each time an update was provided.

5. By the early-to-mid 2000s, new threats escalated as network connectivity became widespread, and programs that mutate slightly with each new copy (polymorphic programs) appeared. These events, and others, rendered the traditional signature-based virus scan systems entirely ineffective for these modern environments.

6. Plaintiffs’ patented technology helped transform the way malware detection and network security is conducted, reducing, and often even eliminating the shortcomings that plagued signature-based endpoint security products that relied on human analysts.

7. Instead of relying on human analysts, Plaintiffs’ patented technology enabled the automatic and real-time analysis, identification, and neutralization of previously unknown threats, including new and emerging malware, as well as advanced polymorphic programs.

8. Plaintiffs’ patented technology uses information about the computer objects being executed—including, for example, information about the object’s behavior and information collected from across a network—along with machine learning technology and novel system

architectures—to provide security systems that are effective in identifying and blocking new security threats in real-time in real-world, commercial systems.

9. Plaintiffs' patented technology further includes new architectures that efficiently and effectively distribute workloads across the network, new techniques for enabling safe and secure browsing even of potentially malicious websites, advanced identification, and classification of potentially harmful Internet resources, among other technologies.

10. Plaintiffs' patented technology makes the new security platforms and techniques better at detecting malware by for example reducing false positives/negatives and enabling the identification and mitigation of new and emerging threats in near real-time. These improvements are accomplished while at the same time reducing the resource demands on the endpoint computers and network appliances.

11. Plaintiff Webroot has implemented this patented technology in its security products like Webroot SecureAnywhere AntiVirus, which identifies and neutralizes unknown and undesirable computer objects in the wild in real-time.

12. Over the years, Plaintiff Webroot has also received numerous accolades and awards for its products and services. For example, Webroot has received 22 PC Magazine Editor's Choice Awards, including "Best AntiVirus and Security Suite 2021." That same year, Webroot also received the Expert Insights Best-of-Endpoint Security award.

13. Plaintiffs currently own more than 70 patents describing and claiming these various security innovations, including U.S. Patent No. 8,726,389 (the "'389 Patent"), U.S. Patent No. 10,599,844 (the "'844 Patent"), U.S. Patent No. 8,438,386 (the "'386 Patent"), U.S. Patent No. 9,413,721 (the "'721 Patent"), and U.S. Patent No. 10,025,928 (the "'928 Patent") (Exhibits 1 – 5, respectively).

14. Plaintiffs’ patented technology represents such a vast improvement on the traditional malware detection and network security systems that it has become a widely adopted and accepted approach to providing endpoint security in real-time.

15. Defendant Forcepoint is a direct competitor of Plaintiffs and provides security software that, without authorization, implements Plaintiffs’ patented technologies. Forcepoint’s infringing security products and services include, but are not limited to, Forcepoint’s Next-Generation Firewall, Web Appliance or Secure Web Gateway, Web Security, Forcepoint One, Advanced Classification Engine, Threat Seeker Intelligence, Advance Malware Detection, and Remote Browser Isolation, as well as products that include any of the above products or modules, or that include the same functionality described herein (collectively, “Accused Products”).

16. Plaintiffs bring this action to seek damages for and to ultimately stop Defendant’s continued infringement of Plaintiffs’ patents, including in particular the ’389, ’844, ’386, ’721, and ’928 Patents (collectively the “Asserted Patents”). As a result of Forcepoint’s unlawful competition in this District and elsewhere in the United States, Plaintiffs have lost sales and profits and suffered irreparable harm, including lost market share and goodwill.

NATURE OF THE CASE

17. Plaintiffs brings claims under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*, for the infringement of the Asserted Patents. Defendant has infringed and continue to infringe each of the Asserted Patents under at least 35 U.S.C. §§271(a), 271(b) and 271(c).

THE PARTIES

18. Plaintiff Webroot, Inc., is the owner by assignment of each of the Asserted Patents.

19. Webroot has launched multiple cybersecurity products incorporating its patented technology, including for example Webroot SecureAnywhere and Evasion Shield.

20. Webroot is a registered business in Texas with multiple customers in this District. Webroot also partners with several entities in this District to resell, distribute, install, and consult on Webroot's products.

21. Plaintiff Open Text Inc. holds an exclusive license to the Asserted Patents. OpenText is registered to do business in the State of Texas.

22. OpenText is a Delaware corporation and maintains three business offices in the state of Texas, two of which are located in this District, including one in Austin and another in San Antonio. Over 60 employees work in OpenText's Austin office, including employees in engineering, customer support, legal and compliance teams, IT, and corporate development. The Austin office also hosts an OpenText data center. OpenText is in the computer systems design and services industry. OpenText sells and services software in the United States.

23. Defendant Forcepoint LLC is a Delaware limited liability company with a principal place of business in this District at 10900 Stonelake Blvd #350, Austin, TX 78759. Forcepoint is registered to do business in the State of Texas

<u>JURISDICTION & VENUE</u>

24. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*. The Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

25. This Court has personal jurisdiction over Forcepoint because Forcepoint's principal place of business is located in the State of Texas and because Forcepoint regularly conducts business in the State of Texas and in this District, including operating systems, using software, providing services, and/or engaging in activities in Texas and in this District that infringe one or more claims of the Asserted Patents

26. Defendant Forcepoint has, either directly and through its extensive network of

partnerships including those with local IT service providers, purposely and voluntarily placed its infringing products and/or provided services into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, as detailed below. (*See, e.g.*, Forcepoint, *Find a Partner*, https://www.forcepoint.com/partners/find-a-partner.)

27. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because Forcepoint resides in this District, has a regular and established place of business in this District, and has committed acts of infringement within this District.

28. On information and belief, Forcepoint has employees in this District that have relevant knowledge regarding the Accused Products, including for example how they are marketed and sold to customers, what additional services are provided to customers based on the Accused Products, and how the products operate.

29. Forcepoint's operations in this District include client outreach and sales for each of the Accused Products. Forcepoint also provides technical support to partners and customers located in this District, including from its office in this District.

30. On information and belief, Forcepoint uses and/or tests the Accused Products in this District, including at its office in this District.

31. Forcepoint further sells, offers for sale, advertises, makes, installs, maintains, and/or otherwise provides security software, appliances, and services, including the Accused Products, the use of which infringes the Asserted Patents in this District. Forcepoint performs these infringing acts directly in this District.

32. Forcepoint also performs these infringing acts through other entities such as resellers, managed service provides, and cybersecurity experts located in this District, including for example, through its "partners." (Forcepoint, *Find a Partner*,

https://www.forcepoint.com/partners/find-a-partner.)

33. As further detailed below, Defendant engages in activities within this judicial district that infringe (directly or indirectly) the Asserted Patents, either literally or under the doctrine equivalents, including the provision of, use, operation, sales, offering for sale, installation, maintenance, and advertising of the Accused Products. Forcepoint also infringes (directly or indirectly) the Asserted Patents by using, offering for sale, selling, installing, maintaining, operating, providing instructions, and/or advertising the Accused Products within this District, either literally or under the doctrine of equivalents.

34. End-users and partner customers infringe the Asserted Patents at least by using and operating, in whole and in part, the Accused Products with this District.

35. Defendant Forcepoint encourages and induces third parties including partners and customers to use the Accused Products in an infringing way at least by making Forcepoint's security software, appliances, and services available for download or purchase, widely advertising those products and services, providing instructions for using, installing, and maintaining those products, providing technical support to users, and/or engaging in activities that aid and abet infringement of the Asserted Patents by end-users. (*See, e.g.*, Forcepoint, *Welcome to Forcepoint Hub*, https://support.forcepoint.com/s/login/ ?ec=302&startURL=%2Fs%2F.)

36. Defendant Forcepoint also contributes to the infringement of its customers and end users of the Accused Products by offering to sell or selling with the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, the Accused Products and the example functionality discussed below

have no substantial non-infringing uses but instead are specifically designed to practice the Asserted Patents.

37. Defendant's infringement adversely impacts Plaintiffs and their employees who live in this district, as well as Plaintiffs' partners and customers who live and work in and around this judicial district. On information and belief, Defendant actively targets and offers Accused Products to customers served by Plaintiffs, including in particular customers/end-users in this District.

PLAINTIFFS' PATENTED INNOVATIONS

38. Plaintiff Webroot, and its predecessors were all pioneers and leading innovators in developing and providing modern end point security protection, including "community-based" signatureless threat detection process using AI-driven behavior analysis across the entire network to provide "zero-day" protection against unknown threats.

39. The Asserted Patents discussed below capture technology, features, and processes that reflect these and other innovations, and improve on traditional anti-Malware and network security systems.

U.S. Patent No. 8,726,389

40. The '389 Patent generally discloses and claims systems and processes related to real-time and advanced classification techniques. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '389 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the '389 Patent.

41. The '389 Patent is entitled "Methods and Apparatus for Dealing with Malware," was filed on July 8, 2012, and was duly and legally issued by the United States Patent Office on May 13, 2014. The '389 Patent claims priority to Foreign Application No. 0513375.6 (GB), filed

on June 30, 2005. A true and correct copy of the ’389 Patent is attached as Exhibit 1.

42. Malware detection systems in use at the time the ’389 Patent was filed identified malware by maintaining a database of signatures identifying known bad objects (*i.e.*, malware). The signature for an object was conventionally made by creating a hash or checksum corresponding to the object file, which uniquely identifies that object. The signature of each object was then compared to the database to look up whether it matches known malware.

43. If the signature of the object is not found in the database, it is assumed safe or alternatively, the whole file is sent for further investigation by a human analyst. The process of further investigation was typically carried out manually or “semimanually” by subjecting the file to detailed analysis, for example by emulation or interpretation, which can take days given the human involvement that is typically required. (*See, e.g.,* Exhibit 1, ’389 Patent, 2:9-17.)

44. This approach had significant drawbacks, including that it required considerable effort by the providers of such systems to identify and analyze new malware and generate signatures of objects that are found to be bad after human analysis. Large vendors of anti-malware packages typically employed *thousands* of human analysts to identify and analyze objects and keep the database of signatures of bad objects reasonably up to date.

45. However, as the volume of network traffic increases, the task of keeping up with identifying suspect objects and investigating whether or not they are bad becomes practically impossible. It can take days to subject a suspicious file to detailed analysis given the human involvement, and a considerable period of time elapses before a new file is classified as safe or as malware. Thus, the human analysis introduces a time delay where users are exposed and unprotected from the risks posed by previously unidentified malware. (*See* Exhibit 1, ’389 Patent, 2:9-23, 2:63-67.)

46. By contrast, the methods and systems disclosed and claimed in the ’389 Patent perform automatic, sophisticated review (*e.g.*, “pattern analysis”) of the actual attributes of a software object or process and the behavior engaged in by, or associated with, that object or process on computers connected to a network.

47. This review enables a determination of “the nature of the object,” (*e.g.*, whether it is malicious or not based on review of the object, its behaviors or the activities associated with the object), without requiring a detailed manual analysis of the code of the object itself or relying exclusively on whether it has a signature that matches an extensive database of known malicious “signatures.” (*See* Exhibit 1, ’389 Patent, 3:14-24.) This provides a significant improvement to the operation of the computer network because monitoring behavior or other information about the object or process, rather than code or signature matching, allows the system to rapidly determine the nature of the object (*e.g.*, malware), without requiring a detailed manual analysis of the code of the object itself as in conventional anti-virus software. (*See* Exhibit 1, ’389 Patent, 3:14-24.)

48. The approaches in the ’389 Patent are generally focused on receiving *information about the behavior* of objects or processes on remote computers at a base computer. This information is analyzed automatically by, for example, mapping the behavior and attributes of objects known across the community in order to identify suspicious behavior and to identify malware at an early stage. (*See* Exhibit 1, ’389 Patent, 11:5-26.) This approach allows, among other advantages, the number of human analysts needed to be massively reduced. It also improves the computer network by reducing the latency involved with identifying new threats and responding to objects exhibiting new, potentially malevolent behavior.

49. The techniques disclosed and claimed in the ’389 Patent is necessarily rooted in computer technology—in other words, the identification of malicious computer code in computer

networks is fundamentally and inextricably a problem experienced with computer technology and networks—and addresses this fundamental computer technology problem with a computer technology solution. Furthermore, the ’389 patent improves the technical functioning of the computer network using techniques—such as analyzing behavioral information about or associated with computer objects and processes—to improve network security by identifying malware more quickly and with less resources. These technical improvements address identified weaknesses in conventional systems and processes. (*See*, *e.g.*, Exhibit 1, ’389 Patent, 3:14-24.)

50. In particular, the ’389 Patent describes and claims deploying an unconventional “event” based model that classifies a particular object as malicious or safe by analyzing real-time data sent by remote computers on the events, or actions, that a particular software “object,” and other objects deemed similar to it, initiate or perform on those computers. (*See* Exhibit 1, ’389 Patent, 3:14-55.) This information is collected from across the network, correlated and used for subsequent comparisons to new or unknown computer objects to identify relationships between the correlated data and the new or unknown computer objects. The objects may be classified as malware based on this comparison.

51. Through continuous aggregate analysis of events involving computer objects as they occur across networks, the methods and systems described and claimed in the ’389 Patent maintain up-to-date information about computer objects (including malicious objects) seen across the network, identify relationships between those previously identified objects and any new or unknown objects, and make malware determinations based on those relationships. “For example, a new object that purports to be a version of notepad.exe can have its behavior compared with the behav[io]r of one or more other objects that are also known as notepad.exe … In this way, new patterns of behav[io]r can be identified for the new object.” (*Id.* at 10:58-65.)

52. The methods and systems described and claimed in the ’389 Patent can rapidly determine “the nature of the object,” (*e.g.*, whether it is malicious or not) based on information such as the behavior of the object or effects the object has, without requiring “detailed analysis of the object itself as such” (manually reviewing the object’s code) or reliance on matching an extensive database of known malicious “signatures.” (*Id.* at 3:14-24.)

53. The ’389 Patent describes and claims systems and methods that necessarily address issues unique to computer networks and computer network operation; namely the identification of “bad” software (*e.g.*, malware, viruses, etc.). This patent provides unique network security enhancement that solves the technical problem of rapidly identifying newly arising and emerging malware by reviewing information about the object and processes (*e.g.,* the behaviors and events associated with software objects and processes running on computers within the network).

54. The systems and methods described and claimed in the ’389 Patent improve the operation of computer networks by identifying malicious objects in real-time and taking action to remove or eliminate the threat posed by the malware object or process once it has been identified. The described and claimed techniques provide a technological solution to a technological problem—the inability of conventional code or signature matching solutions to identify new or unknown malware objects or processes at or near the runtime of the objects or processes themselves without the extensive delay and resource use associated with traditional systems.

U.S. Patent No. 10,599,844

55. The ’844 Patent is entitled “Automatic Threat Detection of Executable Files Based on Static Data Analysis,” was filed May 12, 2015 and was duly and legally issued by the USPTO on March 24, 2020. A true and correct copy of the ’844 Patent is attached as Exhibit 2. Plaintiff

Webroot owns by assignment the entire right, title, and interest in and to the ’844 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’844 Patent.

56. The ’844 Patent addresses and improves upon conventional approaches to malware detection in computer networks and computer network operation. Every day, an uncountable number of new executable files are created and distributed across computer networks. Many of those files are unknown, and malicious. It is, thus, vital to accurately and immediately diagnose those files for any potential threat, while also efficiently using resources (*e.g.*, processing power). (*See* Exhibit 2, ’844 Patent, 1:7-13.)

57. Conventional approaches for diagnosing potential malware threats were costly and time consuming, making it difficult to realistically address zero-day threats for all of the files entering a system. These “[a]pproaches to detecting threats typically focus[ed] on finding malicious code blocks within a file and analyzing the behavior of the file.” (*See* Exhibit 2, ’844 Patent, 2:15-17.) Encrypted files would be decrypted then disassembled to extract the code for analysis, typically by traditional anti-virus software based on signature matching. (*Id.* at 2:15-20) If the code was malware, investigating its behavior involved running the code on the system, which put the system at risk. (*Id.* at 2:20-23.)

58. Another approach for protecting against potential threats from unknown executable files involved wavelet decomposition to determine software entropy. (*See* ’844 Patent Prosecution History, April 24, 2019 Applicant Remarks, at 8.) Wavelet decomposition is a process where an original image is decomposed into a sequence of new images, usually called wavelet planes. (*Id.*) In this method, each data file in a set of data files is split into random, non-overlapping file chunks of a fixed length. (*Id.*) Those file chunks are then represented as an entropy time-series, which measures the time it takes for each chunk to decompose. (*Id.*) Said differently, this approach

measured how much time it took a data file to decompose. (*Id.*) Once the file decomposition rate, or entropy time-series, had been calculated, that rate would be compared to decomposition rates of "known bad" files to identify files that contain malware. (*Id.* at 9.) This process required significant computing resources—typically taking hours to complete—and was not sufficiently accurate in identifying malware.

59. The '844 Patent significantly improved upon and addressed shortcomings associated with these prior approaches. The '844 Patent describes and claims methods and systems that detect threats in executable files without the need to decrypt or unpack those executable files by extracting "static data points inside of the executable file", generating "feature vectors" from those static data points, selectively turning on or off features of the feature vector, and then evaluating the feature vector to determine if the file is malicious. (*See, e.g.,* Exhibit 2, '844 Patent, 1:20-21; cl. 1.) The described systems and methods enable accurate and efficient identification of malware without the need to distinguish between encrypted files and non-encrypted files (*id.* at 6:58-59), thereby significantly increasing efficiency and reducing processing resources required to analyze each potentially malicious computer object. By using this unconventional approach to determine whether a file executable on a computer poses a threat, the '844 Patent improves on the operation of the computer network associated with the computer by enhancing security, including by increasing detection of new threats, reducing the error rates in identifying suspicious files, and improving efficiency in detecting malicious files. (*See* Exhibit 2, '844 Patent, 2:46-56.)

60. The '844 Patent describes and claims techniques that employ a learning classifier (*e.g.*, a machine-learning classifier) to determine whether an executable file is malicious, for example by using the classifier to classify data into subgroups and identify and analyze specific data points to which those subgroups correspond. (*See* Exhibit 2, '844 Patent, 4:33-41, 7:40-8:1.)

The described and claimed techniques also selectively turn on or off features for evaluation by the learning classifier. (*See id*. at 7:57-66.) Doing so accelerates analysis and reduces false positives by testing those features of a file likely to be relevant to a determination of its maliciousness. For example, the learning classifier "may detect that the file does not contain 'legal information'," such as "timestamp data, licensing information, copyright information, etc." (*See id.* at 7:66-8:5.) In this example, given the lack of legal protection information in the file, the learning classifier would "adaptively check" the file for additional features that might be indicative of a threat," while "turn[ing] off," and thus not use processing time unnecessarily checking features related to an evaluation of "legal information." (*Id*. at 8:5-10.)

61. Second, the '844 Patent describes and claims techniques that use character strings extracted from within the executable file to generate a feature vector and then evaluate that feature vector using support vector processing to classify executable files. (*See* Exhibit 2, '844 Patent, 9:2-11.) The classifier provides, for example, the ability to leverage the indicia of "benign" files, which use "meaningful words" in certain data fields, versus "malicious" files, which leave such fields empty or full of "random characters," to build meaningful feature vectors that are analyzed to make faster and more identifications of malware (*See, e.g.,* Exhibit 2, '844 Patent, 9:2-18.)

62. The '844 Patent is thus directed to specific solutions to problems necessarily rooted in computer technology, namely, the determination whether a file executable on a computer poses a threat. The '844 Patent improved upon the accuracy and efficiency of malware detection. (*See* Exhibit 2, '844 Patent, 2:15-45.)

63. By using some or all of the unconventional techniques described above to determine whether a file executable on a computer poses a threat, the '844 Patent addresses a problem necessarily involving computers and improves upon the operation of computer networks.

In particular, the ’844 Patent achieves a number of technical advantages over conventional approaches to malware detection including, for example:

- enhanced security protection including automatic detection of threats, reduction, or minimization of error rates in identification and marking of suspicious behavior or files (*e.g.*, cut down on the number of false positives),
- ability to adapt over time to continuously and quickly detect new threats or potentially unwanted files/applications,
- improved efficiency in detection of malicious files, and
- improved usability and interaction for users by eliminating the need to continuously check for security threats.

(*See* Exhibit 2, ’844 Patent, 2:15-57.)

<u>U.S. Patent No. 8,438,386</u>

64. U.S. Patent No. 8,438,386, entitled “System and Method for Developing a Risk Profile for an Internet Service,” was filed on February 21, 2010, and claims priority to two provisional applications, application numbers 61/171,264 and 61/241,389, filed on April 21, 2009 and September 10, 2009 respectively. The United States Patent Office duly and legally issued the ’386 Patent on May 7, 2013. A true and correct copy of the ’386 Patent is attached as Exhibit 3. Plaintiff Open Text owns by assignment the entire right, title, and interest in and to the ’386 patent. Open Text has granted Plaintiff Webroot an exclusive license to the ’386 patent.

65. The ’386 Patent generally is directed to a method for controlling access to an Internet resource by determining that resource’s reputation and risk. The ’386 Patent discloses and claims inventive techniques that significantly improve on prior art tools for preventing access to Internet resources. Preventing access to computer network resources is, by its very nature,

necessarily rooted in computer technology and overcomes a problem specific to computer networks (namely, problems arising with accessing malicious Internet resources).

66. Before the filing of the ’386 Patent, conventional methods for preventing users from accessing malicious code on webpages involved “‘Content Filtering’ or “Security solutions, such as antivirus products.” (Exhibit 3, ’386 Patent, 1:30-46.) Content filtering is where “Web sites are organized into categories and requests for Web content are matched against per-category policies and either allowed or blocked.” (*Id.* at 1:30-40.) Security solutions like anti-virus products, by contrast, “examine file or Web page content to discover known patterns or signatures that represent security threats to users, computers, or corporate networks. These focus not on the subject matter of a site but look for viruses and other ‘malware that are currently infecting the site.’” (*Id.* at 1:41-46.) These approaches, however, are reactive rather than predictive; for example, they focus on “accessing known infected sites” and “identif[ying] and distribut[ing]” signatures of known malware. (*Id.* at 1:46-50.)

67. Unlike these prior art systems (*e.g.*, signature matching systems) which cannot predictively prevent access, the ’386 Patent improved on prior-art security solutions by assigning risk profiles to internet resources that have not been previously characterized before granting or allowing access. (*Id.* at 1:23-24.) The patent explains that a “predictive security assessment for an Internet resource is provided based on known facts about the Internet resource, which is more secure than relying only on knowledge of previously experienced security attacks.” (*Id.* at 9:42-45.) Techniques described in the ’386 Patent system include the use of samples of internet resources that have varying degrees of risk and, using a reputational model, predicts an internet resource’s relative degree of risk. (*Id.* at 4:34-36.)

68. For example, the methods and systems described and claimed in the ’386 Patent system may predict the relative degree of risk by generating a reputation index based on factors that include location, behavior and legitimacy. (*Id.* at 6:10-25.) When an end-user of a Local Area Network (“LAN”) transmits a request for an internet resource, the system analyzes the “reputation index” for the requested resource and determines whether the reputation index is at or above a threshold value established for the LAN before granting or denying access to the resource. (*Id.* at 1:26.) In doing so, behavioral and other information about the internet resource may be used to proactively block or allow access, as opposed to systems that employ a reactive approach that relies on, for example, signature matching.

69. By assessing an internet resource’s risk in a predictive way—*e.g.*, before infections are isolated and signatures are identified and distributed—a technological solution that addresses weaknesses in prior systems is provided. As the ’386 Patent explains, “[a] predictive security assessment for an Internet resource is provided . . . , which is more secure than relying only on knowledge of previously experienced security attacks.” (*Id.* at 9:42-45.) In other words, systems and methods described in the ’386 Patent can protect against threats from internet resources that have not been previously characterized as malicious or included in pre-existing signature files.

70. The techniques described and claimed in the ’386 Patent solve problems in the field of computers and network security. As discussed above, traditional virus detection methods focused on reactive approaches—blocking web resources that included signatures of known viruses or malware, and internet resource management tools were limited to categorically blocking certain types of web resources. These limitations in prior systems were overcome by, for example, predicting the potential risk that requested internet resources presented to a user’s computing device and the network on which the user was operating. Whereas categorically blocking websites

of a certain type or websites that were infected with known signatures of viruses and malware left systems vulnerable to unknowns, assessing the "reputation" of an internet resource based on, for example, location, legitimacy and/or behavioral factors, the '386 Patent provided methods and systems that effectively and efficiently determined whether to block or allow a user's access to a web resource in a predictive manner. These approaches can address zero-day threats in an efficient and effective way. Moreover, the specific factors and combinations of factors described and claimed in the '386 Patent (*e.g.*, "country of an internet protocol address block," "top-level domain," and "script block count") are necessarily rooted in computer technology to overcome a problem specifically arising in the realm of computer networks. (*See, e.g.,* Exhibit 3, '386 Patent, cl. 1.) The '386 Patent system improves on prior, manual, and reactive approaches with an unconventional, automated, and predictive approach that improves computer functionality.

<u>U.S. Patent No. 9,413,721</u>

71. The '721 Patent is entitled "Methods and Apparatus for Dealing with Malware," was filed on February 13, 2012, and duly and legally issued by the United States Patent Office on February 5, 2013. A true and correct copy of the '721 Patent is attached as Exhibit 4. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '721 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the '721 Patent.

72. The systems and methods described and claimed in the '721 Patent are directed to improved techniques for detecting and classifying malware, a technological problem fundamentally and inextricably associated with computer technology and computer networks. The '721 Patent explains that prior anti-malware products used signature matching to detect malware, either locally or at a central server. (Exhibit 4, '721 Patent, 1:37-2:14.) The local anti-malware product suffered from delays in identifying new malware threats and obtaining signatures for them

so they could be blocked. (*Id.* at 1:37-55.) Central servers stored signatures in the cloud. (*Id.* at 56-57.) But only signature or very basic information was sent to the central server for matching. (*Id.* at 1:67-2:2.) If the object was unknown, a copy had to be sent to the central server for investigation by a human, a time consuming and laborious task. (*Id.* at 2:5-7.) In a network environment, it was unrealistic for a human to investigate each new object due to the high volume of incursions that take place over a network. (*Id.* at 2:7-10.) Thus, under these approaches, "malevolent objects may escape investigation and detection for considerable periods of time." (*Id.* at 2:10-13.)

73. To address these shortcomings, the '721 Patent describes and claims unconventional, novel distributed system architectures, such as remote computers that may be allocated to "threat" servers, with "central" servers sitting behind them. (Exhibit 4, '721 Patent, 9:16-57.) These enhanced computer architectures provide a technical solution to the technical problem of detecting and classifying malware in a computer network environment, thus improving network security while identifying and classifying malware threats in real-time without delays engendered by use of human analysts. (*See*, *e.g.*, Exhibit 4, '721 Patent, 1:60-2:7.)

74. In particular, the '721 Patent describes and claims embodiments that may include three-tiered architectures of remote computers, threat servers, and a central server that provides a technical enhancement to the computer network itself (improving upon the two-tiered architectures of traditional systems having only remote computers and a central server) by enabling the central server to keep, for example, a master list "of all data objects, their metadata and behaviour seen on all of the remote computers" and propagate it back to the threat servers. (Exhibit 4, '721 Patent 12:28-54.) This novel network architecture improves the operation of the computer network over traditional networks because, for example and as described in the '721 Patent, "[t]his scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a

conventional scheme." (*Id.* at 12:55-57.)

75. Further, "by being able to query and analyze the collective view of an object, i.e., its metadata and behaviours, across all agents [] that have seen it, a more informed view can be derived, whether by human or computer, of the object. In addition, it is possible to cross-group objects based on any of their criteria, i.e. metadata and behaviour." (*Id.* at 18:17-22.) Thus, embodiments enable better malware identification than conventional systems (*e.g.*, using human analysis) in addition to providing an efficiency benefit. The patent explicitly notes that "the work in processing the raw data [] is too large of a task to be practical for a human operator to complete." (*Id.* at 18:50-52.)

76. The systems and methods described and claimed in the '721 Patent provide further technical improvements. For example, the information collected at the central server may include additional information about the object being classified as well as a count associated with the number of times that the first computer object has been seen to the central server. (*Id.* at cl. 1.) As explained above, using information about the object (such as behavior information) being classified, embodiments described and claimed in the '721 Patent provide an approach that is more effective than traditional code or signature matching techniques for classifying objects as malicious. (*Id.* at 1:54-2:14.)

77. Prior methods of classifying malware had technical drawbacks when used on a distributed network. For example, a distributed network that required each server to maintain rules for determining what is malware required each server to deal with huge amounts of largely common data. (Exhibit 4, '721 Patent, 12:20-24.) It was also generally impractical to store the required data on each server because, for example, there were problems determining whether or not the data—which is both massive and constantly changing—is common and up-to-date in real-

time. (*Id.* at 12:24-27.) The three-tiered architectures described and claimed in embodiments of the ’721 Patent provide a technical solution for distributed computer networks by, *inter alia*, reducing the workload across the network. (*Id.* at 12:28-59.)

78. Accordingly, the ’721 Patent discloses and claims, among other things, an unconventional technological solution to the inherently computer-network centric technical issue of identifying malware in computer systems. The solutions implemented by the ’721 Patent provides a specific and substantial improvement over prior malware classification systems, for example by introducing novel computer network architecture elements combined in an unconventional manner. These approaches improve the function and working of malware detection services by, for example, utilizing multiple threat servers and central servers and performing the analysis and communication carried out by each type of server in an unconventional and efficient manner. These elements and their combination represent a marked improvement in the functioning of computer systems utilized to identify and detect malware in computers networks.

U.S. Patent No. 10,025,928

79. U.S. Patent No. 10,025,928 (“the ’928 Patent”) entitled “Proactive Browser Content Analysis” was filed on October 3, 2012, claims priority to provisional application 61/542,693 filed October 3, 2011, and was duly and legally issued by the United States Patent Office on July 17, 2018. A true and correct copy of the ’928 Patent is attached as Exhibit 5. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’928 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’928 Patent.

80. The ’928 Patent sets forth techniques for, *inter alia*, “controlling pestware or malware or other undesirable or unwanted applications and/or instructions.” (’928 Patent, 1:19-21.) The ’928 Patent describes and claims methods and systems that guard against malware by, for

example, intercepting browser engine requests and modifying data received from the web server for rendering and display by the browser engine. The ’928 Patent warns that “source[s] of malware … end up or [are] strategically placed at [a] webserver … [so that] the malware source 106 may generate a malware object in a variety of forms including in a scripting language.” (’928 Patent, 3:21-26.)

81. In one embodiment, the ’928 Patent describes a protection agent 116, which “ha[s] full control over what the browser engine 118 ‘sees.’” (’928 Patent, 4:6-10, 4:21-22.) Protection agent 116 intercepts the browser’s requests for web content. (’928 Patent, 4:9.) “[I]f the request does not appear to be a request for malicious content,” then protection agent 116 forwards the request to the web server and, in return, “receives [the requested] content … from the website.” (’928 Patent, 6:19-22.) After receiving the web content, protection agent 116 analyzes the webpage for threats. For example, “all the links in the webpage, all the pictures in the webpage, and any scripts in the webpage … at a low level of granularity.” (’928 Patent, 6:51-54.) If a threat is found in the webpage action may be taken. For example, “[I]f a malicious script is found, it may be commented out [changed, enhanced, and removed] before the content is handed to the browser engine.” (’928 Patent, 6:54-58.) “[A]fter performing all of its processing, removing, and/or adding any code as needed, the protection agent feeds the HTML content back to the browser engine” as if the browser engine were “‘speaking to an actual web server.” (’928 Patent, 4:14-21.)

82. The ’928 Patent provides technical benefits that improve the functioning of the computer system, including enabling safer browsing without affecting the browsing experience. For example, the protection agent can analyze webpages for any signs of malware and delete any instances found. The web browser seamlessly may communicate with a protection agent in such a way that the browser receives communications from the protection agent as if the protection agent

were the web server. In addition, methods and systems claimed in the ’928 Patent provided technical benefits that improve the performance of computer systems. For example, while prior methods simply made high-level modifications to the content after it had been displayed through a Browser Helper Object,” embodiments of the ’928 Patent may modify the content at the protocol level, requiring “virtually no performance overhead.” In fact, in addition to there being virtually no performance overhead, “in many cases, there is actually a performance improvement.” (’928 Patent, 4:49-55.)

83. The systems and methods described and claimed in the ’928 Patent are fundamentally rooted in computer technology—in fact, they are processes only performed within a networked computer environment. The techniques described in the ’928 Patent address problems necessarily rooted in computer technology. For example, the ’928 Patent guards against computer malware distributed through webpages accessed over a computer network, a problem affecting internet traffic.

84. The ’928 Patent further describes and claims unconventional techniques for guarding against malware. For example, the ’928 Patent describes embodiments that annotate instances of possible malware—*e.g.*, when the protection agent assembles and modifies the webpage. While prior methods, for example, simply “make high-level modifications to the content after it has been displayed through a Browser Helper Object,” the described and claimed methods may do so at the protocol level, which requires “virtually no performance overhead.” (’928 Patent, 4:49-55.) Moreover, by modifying the webpage at the protocol level, embodiments of the ’928 Patent offer a novel means to prevent malware from ever reaching a user’s browser, without the need to account for differences between browsers. For example, the ’928 Patent explains:

> [M]odifying content at the [protocol] level … is very different than the prior approaches … [after] a page has already been parsed and rendered by a browser

> engine. This prior approach is problematic because it allows the browser engine to potentially execute malicious scripts or perform malicious actions while … parsing and rendering the code. And in addition, because the annotations are added after rending, the annotation process must account for the rendering differences (e.g., differences in how and where content is displayed) that different browsers (e.g., Firefox, Safari, Chrome, Internet Explorer, etc.) exhibit."

('928 Patent, 7:11-20.)

ACCUSED PRODUCTS

85. Forcepoint's products that practice one or more claims of the Asserted Patents include, but are not necessarily limited to, Forcepoint's Next-Generation Firewall, Web Appliance, Web Security or Secure Web Gateway, Advanced Classification Engine, Threat Seeker Intelligence, Advance Malware Detection, Forcepoint One, and Remote Browser Isolation, as well as products that include any of the above products or modules, or that include the same functionality described herein.

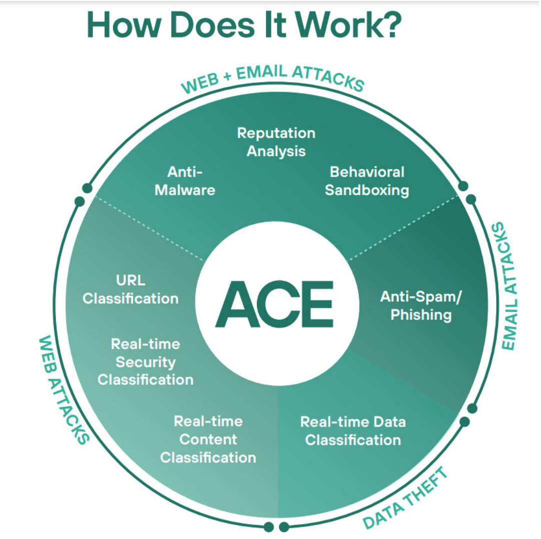
86. Forcepoint's Next-Generation Firewall ("NGFW") is an SD-WAN network device that provides Forcepoint's customers with "consistent security, performance, and operations across physical, virtual, and cloud systems." Forcepoint's NGFW provides application-layer exfiltration protection, "selectively and automatically whitelist[ing] or blacklist[ing] network traffic originating from applications on PCs, laptops, servers, file shares, and other endpoint devices based on highly granular endpoint contextual data." (*See* https://www.forcepoint.com/sites/default/files/resources/datasheets/datasheet_forcepoint_ngfw_en_0_0.pdf.)

87. Forcepoint's Web Appliances "are preconfigured to eliminate vulnerabilities from unnecessary software, open ports, default logins, and more, easing your deployment and enhancing your security." (Forcepoint, *Appliance*, https://www.forcepoint.com/appliance.) They are designed "to simplify the deployment of redundant, load-balanced clusters, increasing the

throughput of your implementation." (https://www.forcepoint.com/appliance.)

88. Forcepoint's Web Security (or Secure Web Gateway, "SWG"), which on information and belief is offered as a standalone product or as part of Forcepoint One, is a product that "provides robust protection through content aware defenses and cloud app discovery and monitoring, reducing risks to sensitive data for both on premise and mobile users." (*See, e.g.*, Forcepoint, *Forcepoint Web Security*, https://forcepoint.drift.click/brochure_secure_web_gateway.) Forcepoint Web Security employs Forcepoint's Advanced Classification Engine ("ACE") as the decision engine that identifies the nature and format of the digital artifacts being analyzed. (*See* https://forcepoint.drift.click/brochure_secure_web_gateway.) Forcepoint Web Security additionally employs Forcepoint's ThreatSeeker Intelligence to provide real-time security updates that block advanced threats, malware, phishing attacks, lures, and scams.

89. Forcepoint's ACE is a suite of cyber threat prevention and detection analytics embedded in Forcepoint products. (*See* Forcepoint, *Forcepoint Advanced Classification Engine (ACE)*, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.) As shown in the picture below, ACE combines many different threat analysis approaches into one detection engine.

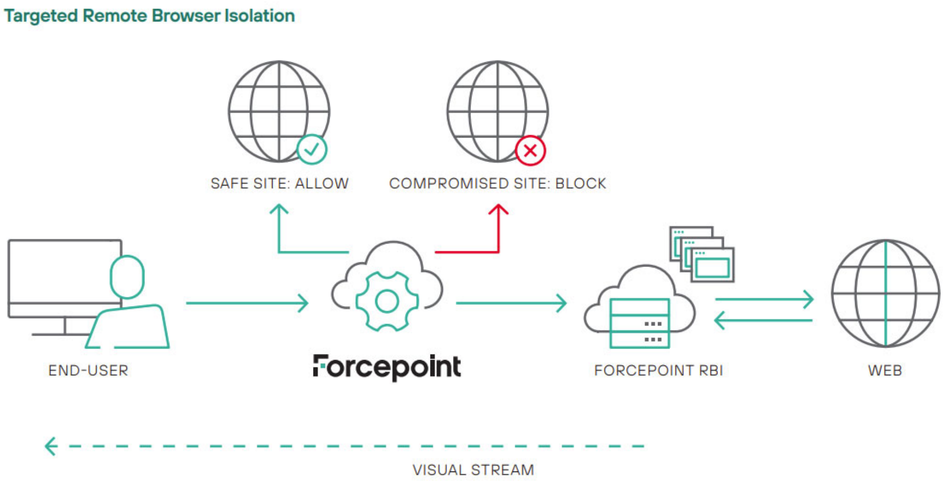


(*See* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.) Using these various methods, Forcepoint's ACE provides "detailed, real-time categorization of content to enable a rich picture of the content surrounding cyber behavior." (*See* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.)

90. Forcepoint's ThreatSeeker Intelligence is responsible for collecting and aggregating threat data, using ACE to analyze the data. (*See* https://forcepoint.drift.click/brochure_secure_web_gateway.) ThreatSeeker Intelligence provides Forcepoint's products with "the core collective security intelligence." (*See* https://forcepoint.drift.click/brochure_secure_web_gateway.)

91. Forcepoint's Advance Malware Detection ("AMD") provides visualized malware reporting. Using Advanced Malware Detection, system administrators can view their threat exposure with detailed correlated incident information. (*See* Forcepoint, *Advanced Malware Detection*, https://www.forcepoint.com/product/advanced-malware-detection.)

92. Forcepoint's Remote Browser Isolation "provides users with safe access to uncategorized sites and known bad sites when necessary by using Forcepoint Web Security with Remote Browser Isolation." By isolating the browser from the end user's desktop, Forcepoint's Remote Browser Isolation prevents threats from reaching the user's browser.



(*See* Forcepoint, *Remote Browser Isolation*, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution-brief-remote-browser-isolation-en_0_0_0_0_0_0_0_0_0_0_0_0_0_0.pdf.)

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE '389 Patent)

93. Webroot realleges and incorporates by reference the allegations of the preceding paragraphs of this Complaint.

94. Forcepoint has infringed and continues to infringe one or more claims of the '389 Patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including products that include features such as Forcepoint's Advanced Classification Engine and ThreatSeeker Intelligence, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '389 Patent as demonstrated below.

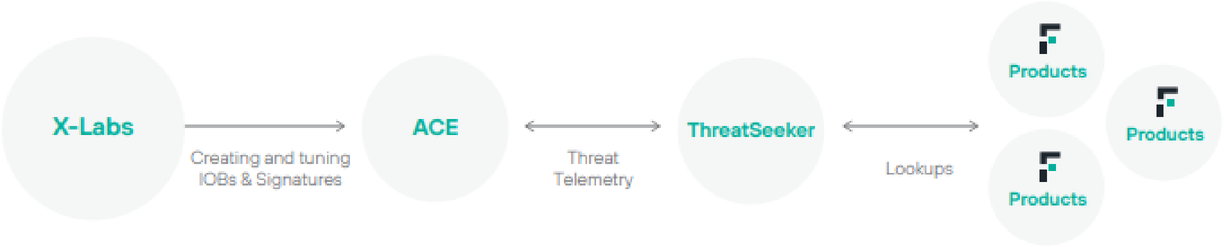
95. For example, claim 1 of the '389 Patent recites:

> a method of classifying a computer object as malware, the method comprising:

> at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> storing, at the base computer, said data received from the first and second remote computers;
>
> correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;
>
> comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and
>
> classifying, by the base computer, the computer object as malware on the basis of said comparison.

96. To the extent the preamble is limiting, the Accused Products perform *a method of classifying a computer object as malware*. For example, Forcepoint's Advanced Classification Engine ("ACE") in combination with Forcepoint's ThreatSeeker Intelligence "identif[ies] malware, phishing, spam, and other risks to [an] enterprise." (*See* Forcepoint, *Forcepoint Advanced Classification Engine (ACE) Solution Brief*, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.)

97. The Accused Products perform a method that includes the step of *at a base computer, receiving data about a computer object from a first [and second] remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed*. Forcepoint's ThreatSeeker Intelligence resides on a base computer and receives threat data about computer objects from multiple remote computers. For example, "ThreatSeeker Intelligence aggregates threat intel from ACE engines, firewalls, and endpoints deployed around the world to provide telemetry back to those devices." (*See* Forcepoint, *Forcepoint Advanced Classification Engine (ACE) Solution Brief*, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.) The figure below illustrates how ThreatSeeker receives information from Forcepoint products.



(*See* Forcepoint, *Forcepoint Advanced Classification Engine (ACE) Solution Brief*, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.)

98. ThreatSeeker Intelligence also receives "threat telemetry" and "threat intelligence," which includes collecting content from "web pages, documents, executable, scripts, streaming,

media, emails, mobile applications, and other Internet traffic," as well as information from Forcepoint's Advanced Classification Engine (ACE). For example, "ACE inspects traffic content and usage patterns using up to eight different defense assessment areas for identifying malware, phishing, spam, and other risks" to provide threat data including behavioral information. (*Id.*)

99. Moreover, as explained above, Forcepoint's ThreatSeeker Intelligence aggregates data from sources of information, including endpoints, firewalls, and Threatpoint's ACE. That information about the object is used to detect threats. For example, ACE assesses objects according to identifying information from their code, *i.e.,* scripts and iframe tags, url classification of websites, and how data is structured. This information is provided to the ThreatSeeker Intelligence, which "allow[s] threat intelligence [to,] from one attack vector[,] … influence analytics applied to another attack vector." (*See* Forcepoint, *Forcepoint Advanced Classification Engine (ACE) Solution Brief,* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_ brief_ forcepoint_ace_en.pdf.)

100. The Accused Products perform a method that includes *storing, at the base computer, said data received from the first and second remote computers*. As explained above, "Forcepoint's ThreatSeeker Intelligence aggregates threat intel from ACE engines, firewalls, and endpoints." (*Id.*) Aggregating threat intelligence and telemetry involves and includes storing the information. For example, data collected is further stored and analyzed by Forcepoint X-Labs. "ThreatSeeker informs ACE with directly actionable updates by continually collecting content and new trends, and this data allows X-Labs researchers to further optimize data models and analytics on an ongoing basis." (*Id.*)

101. The Accused Products perform a method that includes *correlating, by the base computer, at least a portion of the data about the computer object received from the first remote*

computer to at least a portion of the data about the computer object received from the second remote computer. As explained above, Forcepoint's ThreatSeeker Intelligence aggregates data from endpoints, firewalls, and Threatpoint's ACE. That aggregated information is then correlated so that the information may be used, for example, to assist in identifying zero-day threats as well as threats identified by other sources. For example, Forcepoint's ACE, in connection with Forcepoint's ThreatSeeker Intelligence, performs file analysis such that "[o]bserved behavior is correlated with known threats to provide valuable information for even zero-day threats, all in real time." (*See* Forcepoint, *Cybersecurity Intelligence (CSI) Tools*, https://www.forcepoint.com/services/cybersecurity-intelligence-csi-tools.) This "allow[s] threat intelligence gained from one attack vector to influence analytics applied to another attack vector." (*See* Forcepoint, *Forcepoint Advanced Classification Engine (ACE) Solution Brief,* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint _ace_en.pdf.)

102. The Accused Products perform a method that includes *comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities*. As explained above, Forcepoint ACE, in connection with Forcepoint's ThreatSeeker Intelligence, correlates intelligence and telemetry from attacks and compares that correlated information to new and previously identified threats for analysis, including on information and belief, to determine relationships between the correlated data and any potential threats (other objects or entities) "to detect previously unknown malware." For example, Forcepoint advertises that its ACE shares what it learns, "allowing threat intelligence gained from one attack vector to influence analytics applied to another attack vector." (*See* Forcepoint,

Forcepoint Advanced Classification Engine (ACE) Solution Brief, https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_ace_en.pdf.)

103. Moreover, Forcepoint's ACE, in connection with Forcepoint's ThreatSeeker Intelligence, performs file analysis such that "[o]bserved behavior is correlated with known threats to provide valuable information for even zero-day threats, all in real time." (*See* Forcepoint, *Cybersecurity Intelligence (CSI) Tools*, https://www.forcepoint.com/services/cybersecurity-intelligence-csi-tools.)

104. The Accused Products perform a method that includes *classifying, by the base computer, the computer object as malware on the basis of said comparison*. As explained above, Forcepoint's ThreatSeeker Intelligence, alone or in combination with Forcepoint's ACE, "identif[ies] malware, phishing, spam, and other risks to [an] enterprise." (*Id.*)

105. Each claim in the '389 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '389 Patent.

106. Forcepoint has been aware of the '389 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '389 Patent, including on its web site, since at least July 2020.

107. Forcepoint directly infringes at least claim 1 of the '389 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Forcepoint performs a method in an infringing manner as described above by running the Accused Products to protect its own computer and network operations. On information and belief, the Forcepoint performs a method in an infringing manner in testing the operation of the Accused Products and corresponding systems. As another example, Forcepoint performs each

of the method steps when providing or administering services to third parties, customers, and partners using the Accused Products.

108. Forcepoint's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '389 Patent, literally or under the doctrine of equivalents, at least by performing the claimed methods when using the Accused Products and corresponding systems and services, as described above.

109. Forcepoint actively induced and is actively inducing infringement of at least claim 1 of the '389 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, Forcepoint encourages and induces customers to use Forcepoint's security software and appliances in a manner that infringes claim 1 of the '389 Patent by at least offering and providing software and appliances that perform a method that infringes claim 1 when installed and operated by the customer, and by activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of its Accused Products and services in the United States. (*See, e.g.*, Forcepoint, Administrator Help: Forcepoint Web Security, http://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf; Forcepoint, *Installation Guide: Advanced Malware Detection*, *https://www.websense.com/content/support/library/amd-op/v10/install/manager-install.pdf*.)

110. Forcepoint encourages, instructs, directs, and/or requires third parties—including its partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

111. Forcepoint further encourages and induces its customers to infringe claim 1 of the '389 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. (*See* Forcepoint, Administrator Help: Forcepoint Web Security, http://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf.)

112. For example, on information and belief, Forcepoint shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the software and systems as described above, including at least customers and partners. (*See* Forcepoint, *Installation Guide: Advanced Malware Detection*, *https://www.websense.com/content/support/library/amd-op/v10/install/manager-install.pdf*.). On further information and belief, Forcepoint also provides customer service or technical support to purchasers of the Accused Products and corresponding system and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner.

113. Forcepoint and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. (*See* Forcepoint, Administrator Help: Forcepoint Web Security, http://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf.) On information and belief, each customer enters into a contractual relationship with Forcepoint and/or its partners that obligates each customer to perform certain actions as a condition to use the Accused Products. Further, in order to receive the benefit of Forcepoint's and/or its partners' continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '389 Patent. Further, as the entity that provides

installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Forcepoint 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 '389 Patent.

114. Forcepoint also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the '389 Patent.

115. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Forcepoint. For example, on information and belief, Forcepoint directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Forcepoint further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method steps of at least claim 1 of the '389 Patent.

116. Plaintiffs have suffered and continues to suffer damages, including lost profits, as a result of Defendant's infringement of the '389 Patent. Defendant is therefore liable to Plaintiffs

under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant's infringement, but no less than a reasonable royalty.

117. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant from infringing the '389 Patent. On information and belief, Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

118. Defendant's infringement of the '389 Patent, is knowing and willful. Defendant acquired actual knowledge of the '389 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the '389 Patent from at least the date Plaintiffs marked its products with the '389 Patent and/or provided notice of the '389 Patent on its website.

119. On information and belief, despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant's continued infringement of the '389 Patent with knowledge of the '389 Patent constitutes willful infringement.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE '844 PATENT)

120. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

121. Forcepoint has infringed and continues to infringe one or more claims of the '844 Patent in violation of 35 U.S.C. § 271 in this judicial District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Forcepoint Advanced Malware Detection Appliance (as well as any other products that

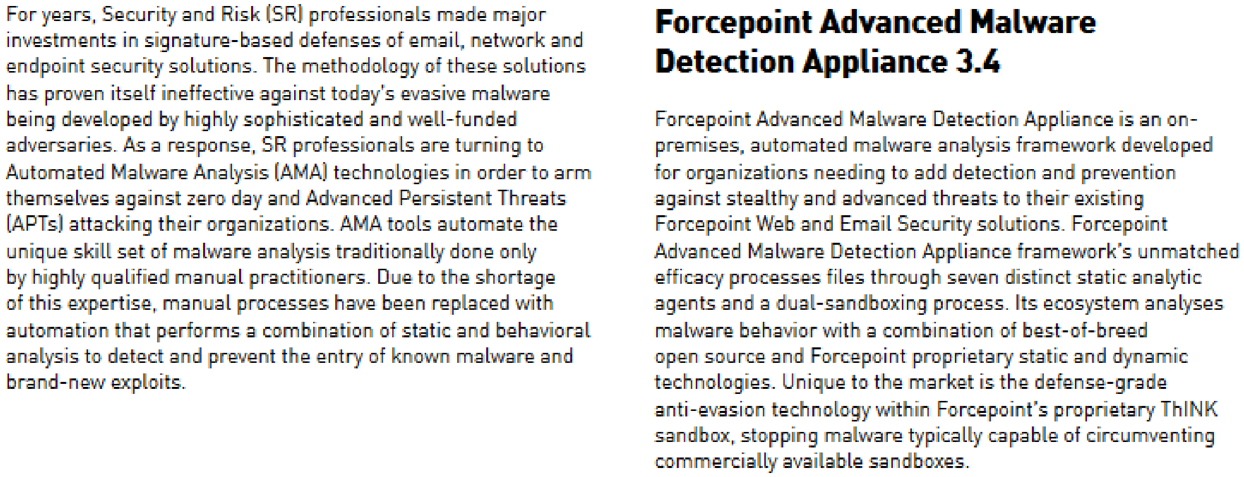
include the features described below), when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '844 Patent, as demonstrated below.

122. Claim 1 of the '844 Patent recites:

> 1. A computer-implemented method comprising:
>
> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;
>
> generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and
>
> wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and
>
> evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

123. The Accused Products perform each element of the method of claim 1 of the '844 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform a *computer-implemented method*, as further explained below. For example, the Accused Products "perform[] a combination of static and behavioral analysis to detect and prevent the entry of known malware and brand-new exploits." The "Forcepoint Advanced Malware Detection Appliance is an on-premises, automated malware analysis framework developed for organizations needing to add detection and prevention against stealthy and advanced threats to their existing Forcepoint Web and Email Security solutions" including processing "files through seven distinct static analytic agents and a dual-sandboxing process." The Accused Products perform an analysis that includes integrating and using static analysis, including by integrating and using its partner Cylance's static analysis, in which "files are put through a four-phase machine learning process (collection,

extraction, learning & classification) in milliseconds with extreme accuracy." On information and belief, this analysis includes the use of "models" that are "deliver[ed]" to the appliance and then used to "predict whether a file is valid or malicious."



For years, Security and Risk (SR) professionals made major investments in signature-based defenses of email, network and endpoint security solutions. The methodology of these solutions has proven itself ineffective against today's evasive malware being developed by highly sophisticated and well-funded adversaries. As a response, SR professionals are turning to Automated Malware Analysis (AMA) technologies in order to arm themselves against zero day and Advanced Persistent Threats (APTs) attacking their organizations. AMA tools automate the unique skill set of malware analysis traditionally done only by highly qualified manual practitioners. Due to the shortage of this expertise, manual processes have been replaced with automation that performs a combination of static and behavioral analysis to detect and prevent the entry of known malware and brand-new exploits.

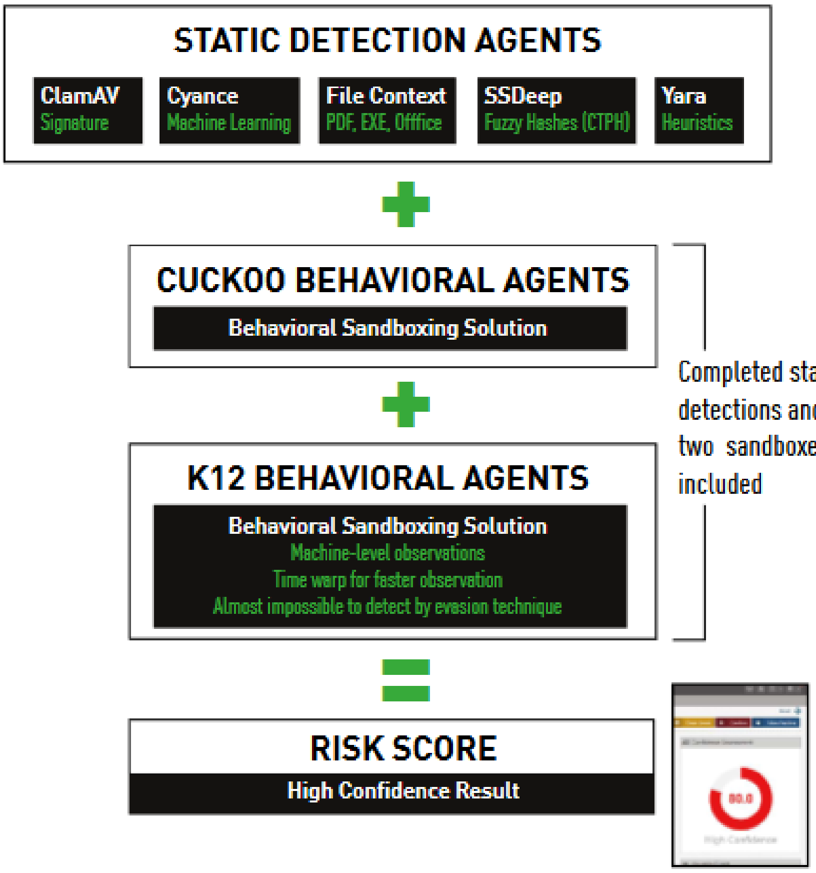
Forcepoint Advanced Malware Detection Appliance 3.4

Forcepoint Advanced Malware Detection Appliance is an on-premises, automated malware analysis framework developed for organizations needing to add detection and prevention against stealthy and advanced threats to their existing Forcepoint Web and Email Security solutions. Forcepoint Advanced Malware Detection Appliance framework's unmatched efficacy processes files through seven distinct static analytic agents and a dual-sandboxing process. Its ecosystem analyses malware behavior with a combination of best-of-breed open source and Forcepoint proprietary static and dynamic technologies. Unique to the market is the defense-grade anti-evasion technology within Forcepoint's proprietary ThINK sandbox, stopping malware typically capable of circumventing commercially available sandboxes.

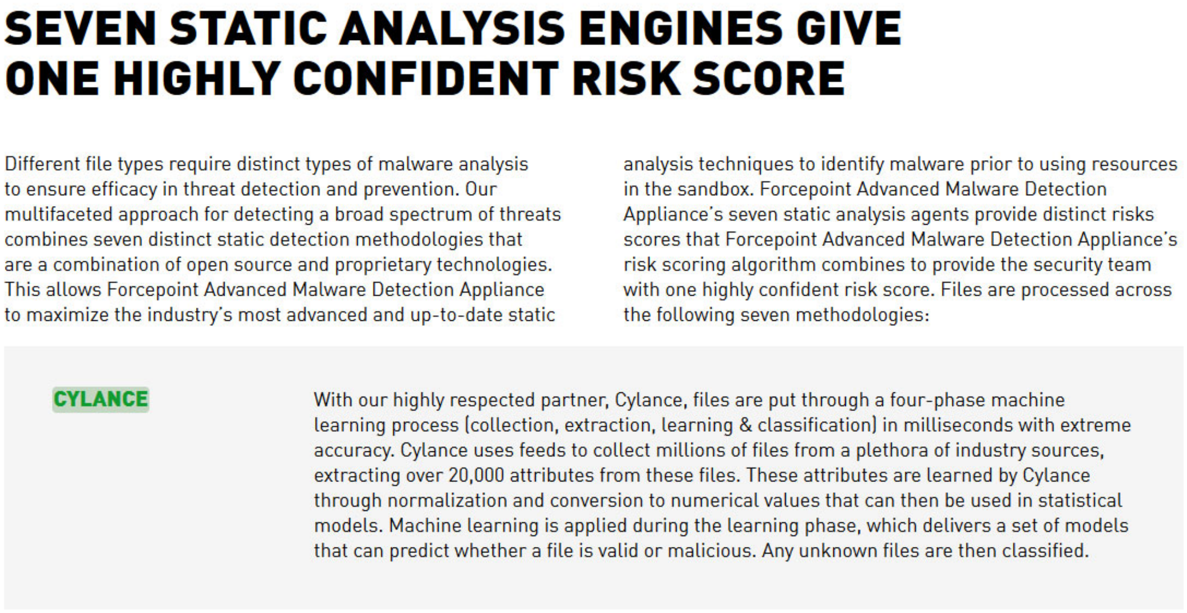
(*See* https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf at page 2.)

FORCEPOINT ADVANCED MALWARE DETECTION APPLIANCE DETECTION FRAMEWOR

FIG 1: Extensive ecosystem that leverages the best-of-breed open source and proprietary technology available today.



(*See* https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf at page 3.)



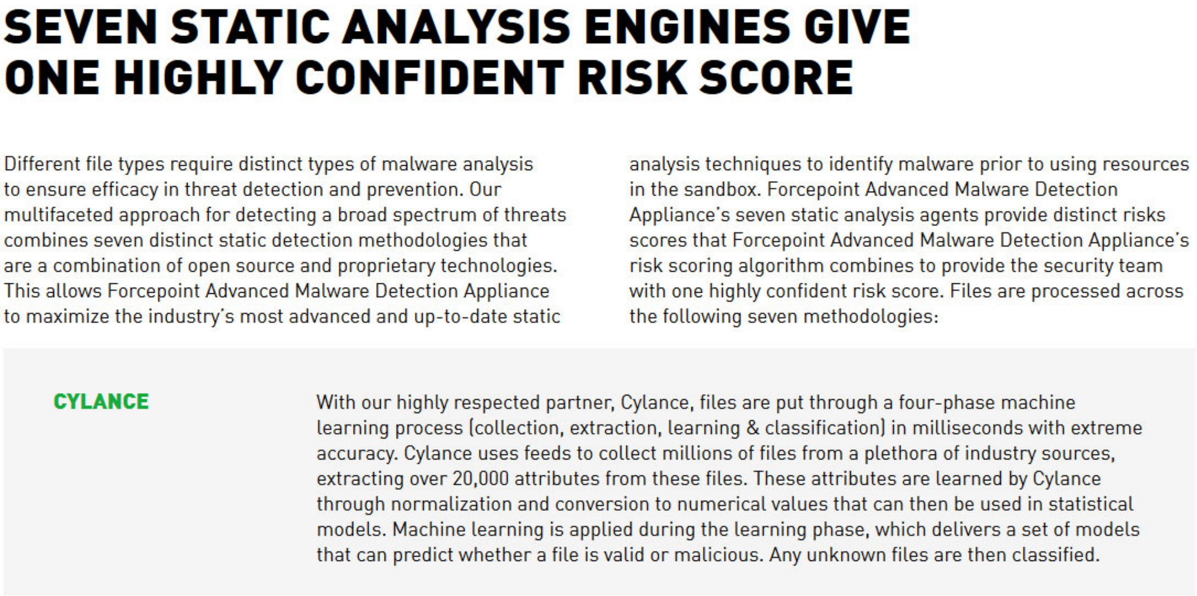
SEVEN STATIC ANALYSIS ENGINES GIVE ONE HIGHLY CONFIDENT RISK SCORE

Different file types require distinct types of malware analysis to ensure efficacy in threat detection and prevention. Our multifaceted approach for detecting a broad spectrum of threats combines seven distinct static detection methodologies that are a combination of open source and proprietary technologies. This allows Forcepoint Advanced Malware Detection Appliance to maximize the industry's most advanced and up-to-date static analysis techniques to identify malware prior to using resources in the sandbox. Forcepoint Advanced Malware Detection Appliance's seven static analysis agents provide distinct risks scores that Forcepoint Advanced Malware Detection Appliance's risk scoring algorithm combines to provide the security team with one highly confident risk score. Files are processed across the following seven methodologies:

CYLANCE	With our highly respected partner, Cylance, files are put through a four-phase machine learning process (collection, extraction, learning & classification) in milliseconds with extreme accuracy. Cylance uses feeds to collect millions of files from a plethora of industry sources, extracting over 20,000 attributes from these files. These attributes are learned by Cylance through normalization and conversion to numerical values that can then be used in statistical models. Machine learning is applied during the learning phase, which delivers a set of models that can predict whether a file is valid or malicious. Any unknown files are then classified.

(*See* https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf at page 4.)

124. The Accused Products perform a method that includes *extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file*. For example, the Accused Products use "seven distinct static detection methodologies" including Cylance's static analysis, in which "files are put through a four-phase machine learning process (collection, extraction, learning & classification) in milliseconds with extreme accuracy."



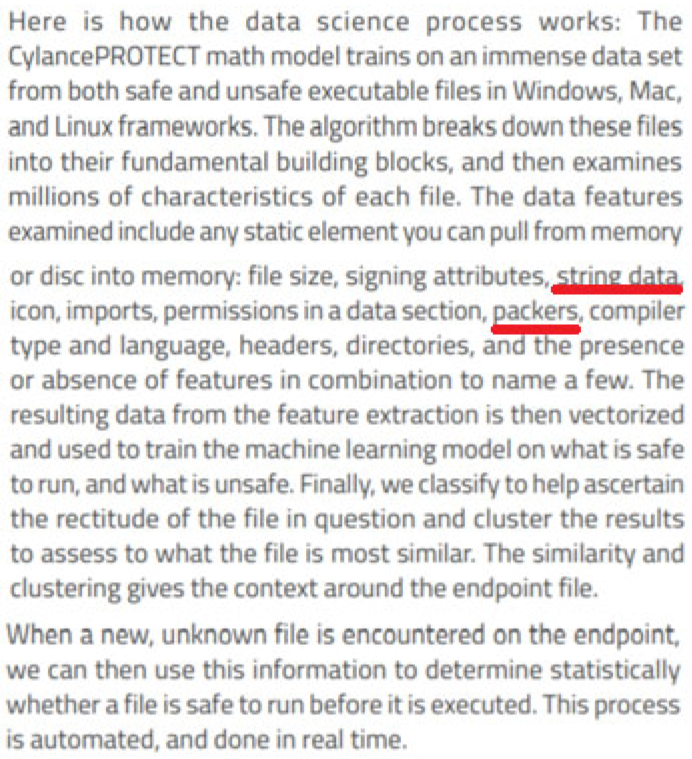
SEVEN STATIC ANALYSIS ENGINES GIVE ONE HIGHLY CONFIDENT RISK SCORE

Different file types require distinct types of malware analysis to ensure efficacy in threat detection and prevention. Our multifaceted approach for detecting a broad spectrum of threats combines seven distinct static detection methodologies that are a combination of open source and proprietary technologies. This allows Forcepoint Advanced Malware Detection Appliance to maximize the industry's most advanced and up-to-date static analysis techniques to identify malware prior to using resources in the sandbox. Forcepoint Advanced Malware Detection Appliance's seven static analysis agents provide distinct risks scores that Forcepoint Advanced Malware Detection Appliance's risk scoring algorithm combines to provide the security team with one highly confident risk score. Files are processed across the following seven methodologies:

CYLANCE

With our highly respected partner, Cylance, files are put through a four-phase machine learning process (collection, extraction, learning & classification) in milliseconds with extreme accuracy. Cylance uses feeds to collect millions of files from a plethora of industry sources, extracting over 20,000 attributes from these files. These attributes are learned by Cylance through normalization and conversion to numerical values that can then be used in statistical models. Machine learning is applied during the learning phase, which delivers a set of models that can predict whether a file is valid or malicious. Any unknown files are then classified.

125. The Accused Products implement Cylance's static analysis—*e.g.* through the use of a set of models delivered to the appliance. That analysis examines data features that include "any static element you can pull from memory or disc into memory: file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and the presence or absence of features in combination." Further, "[w]hen a new, unknown file is encountered on the endpoint, we can then use this information to determine statistically whether a file is safe to run before it is executed."

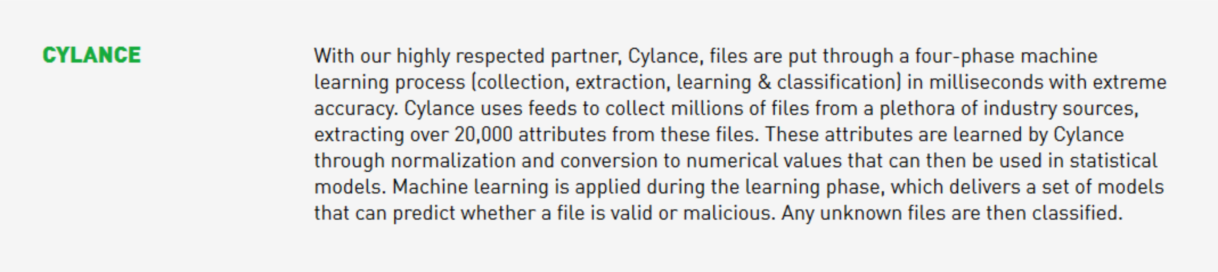


Here is how the data science process works: The CylancePROTECT math model trains on an immense data set from both safe and unsafe executable files in Windows, Mac, and Linux frameworks. The algorithm breaks down these files into their fundamental building blocks, and then examines millions of characteristics of each file. The data features examined include any static element you can pull from memory or disc into memory: file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and the presence or absence of features in combination to name a few. The resulting data from the feature extraction is then vectorized and used to train the machine learning model on what is safe to run, and what is unsafe. Finally, we classify to help ascertain the rectitude of the file in question and cluster the results to assess to what the file is most similar. The similarity and clustering gives the context around the endpoint file.

When a new, unknown file is encountered on the endpoint, we can then use this information to determine statistically whether a file is safe to run before it is executed. This process is automated, and done in real time.

(*See* https://www.blackberry.com/content/dam/cylance/documents/pdf/pdf-feature-focus-protect-malware-control.pdf at page 02; *see also,* blackberry.com/us/en/products/unified-endpoint-security/cylance-is-now-blackberry ("Cylance is now part of Blackberry Cybersecurity").)

126. The Accused Products perform a method that includes *generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points*. As explained above, the Accused Products implement Cylance's static analysis in which "files are put through a four-phase machine learning process (collection, extraction, learning & classification)." "Machine learning is applied during the learning phase, which delivers a set of models that can predict whether a file is valid or malicious. Any unknown files are then classified."

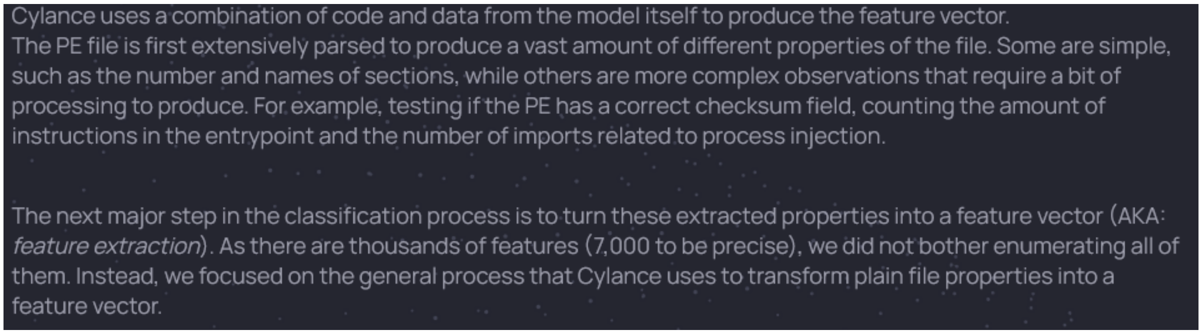


CYLANCE

With our highly respected partner, Cylance, files are put through a four-phase machine learning process (collection, extraction, learning & classification) in milliseconds with extreme accuracy. Cylance uses feeds to collect millions of files from a plethora of industry sources, extracting over 20,000 attributes from these files. These attributes are learned by Cylance through normalization and conversion to numerical values that can then be used in statistical models. Machine learning is applied during the learning phase, which delivers a set of models that can predict whether a file is valid or malicious. Any unknown files are then classified.

(*See* https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf.)

127. Additionally, the resulting data "from the feature extraction is . . . vectorized and used to train the machine learning." On information and belief, Cylance's static analysis similarly generates a feature vector from the static data points during the classification process. (*See* https://www.blackberry.com/content/dam/cylance/documents/pdf/pdf-feature-focus-protect-malware-control.pdf at page 02.) For example, the Accused Products, implementing the Cylance static analysis, uses "any static element you can pull from memory or disc into memory: file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and the presence or absence of features in combination." During the classification process, the Accused Products generate a "feature vector" using "extracted properties" from the file:

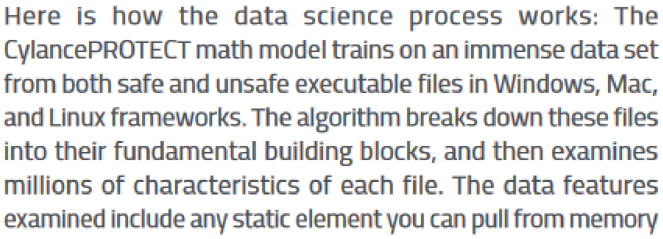


Cylance uses a combination of code and data from the model itself to produce the feature vector.
The PE file is first extensively parsed to produce a vast amount of different properties of the file. Some are simple, such as the number and names of sections, while others are more complex observations that require a bit of processing to produce. For example, testing if the PE has a correct checksum field, counting the amount of instructions in the entrypoint and the number of imports related to process injection.

The next major step in the classification process is to turn these extracted properties into a feature vector (AKA: *feature extraction*). As there are thousands of features (7,000 to be precise), we did not bother enumerating all of them. Instead, we focused on the general process that Cylance uses to transform plain file properties into a feature vector.

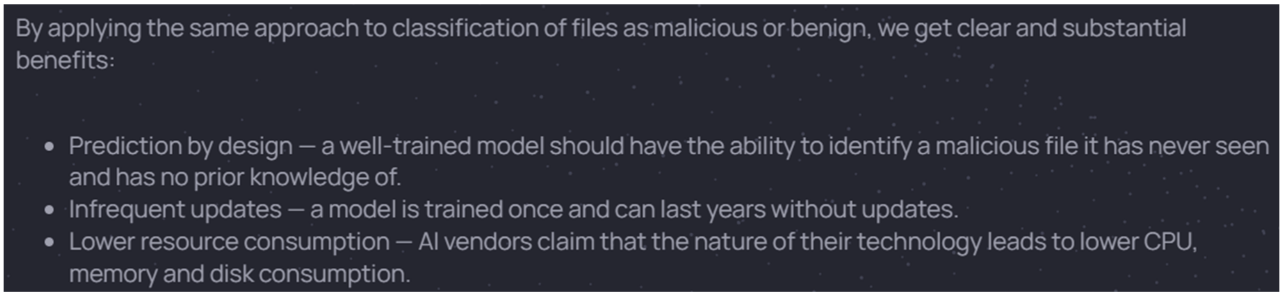
(*See* https://skylightcyber.com/2019/07/18/cylance-i-kill-you/.)

128. As explained above, the Accused Products implement Cylance's static analysis (*e.g.*, through the use of a set of models provided to the appliance), which uses a "math model [that] trains on an immense data set from both safe and unsafe executable files in Windows, Mac, and Linux frameworks. The algorithm breaks down these files into their fundamental building blocks, and then examines millions of characteristics of each file."



Here is how the data science process works: The CylancePROTECT math model trains on an immense data set from both safe and unsafe executable files in Windows, Mac, and Linux frameworks. The algorithm breaks down these files into their fundamental building blocks, and then examines millions of characteristics of each file. The data features examined include any static element you can pull from memory

(*See* https://www.blackberry.com/content/dam/cylance/documents/pdf/pdf-feature-focus-protect-malware-control.pdf.)



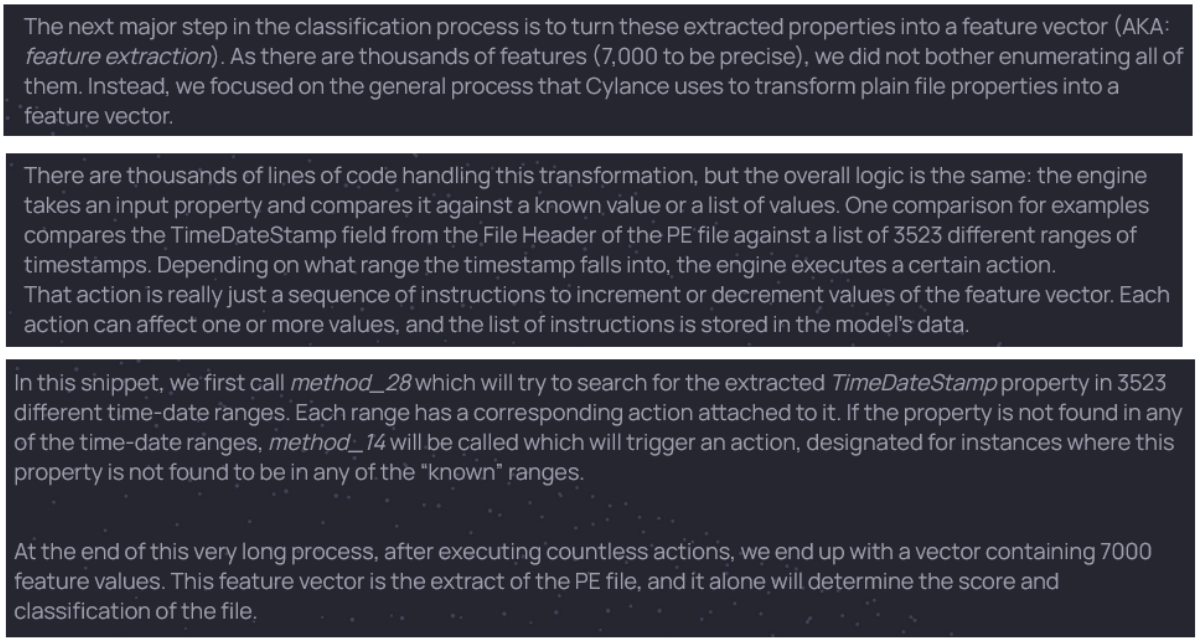
By applying the same approach to classification of files as malicious or benign, we get clear and substantial benefits:

- Prediction by design — a well-trained model should have the ability to identify a malicious file it has never seen and has no prior knowledge of.
- Infrequent updates — a model is trained once and can last years without updates.
- Lower resource consumption — AI vendors claim that the nature of their technology leads to lower CPU, memory and disk consumption.

(*See* https://skylightcyber.com/2019/07/18/cylance-i-kill-you/ at page 04.)

129. The Accused Products perform a method that includes *wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range*. As explained above, the Accused Products implement Cylance's static analysis as part of the classification process. When that occurs "extracted properties" are turned "into a feature vector." On information and belief, there "are thousands of lines of code handling this transformation, but the overall logic is the same: the engine takes an input property and compares

it against a known value or a list of values. One comparison for examples compares the TimeDateStamp field from the File Header of the PE file against a list of 3523 different ranges of timestamps. Depending on what range the timestamp falls into, the engine executes a certain action. That action is really just a sequence of instructions to increment or decrement values of the feature vector. Each action can affect one or more values, and the list of instructions is stored in the model's data."



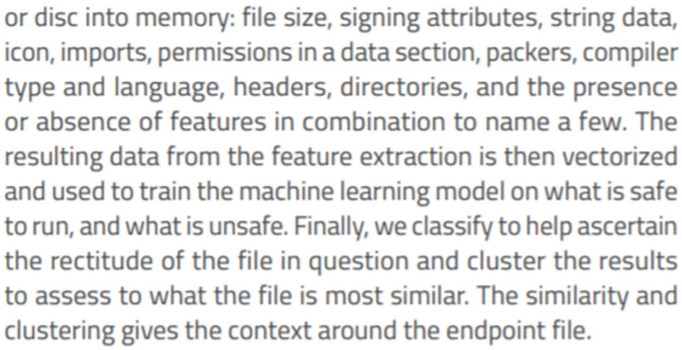
The next major step in the classification process is to turn these extracted properties into a feature vector (AKA: *feature extraction*). As there are thousands of features (7,000 to be precise), we did not bother enumerating all of them. Instead, we focused on the general process that Cylance uses to transform plain file properties into a feature vector.

There are thousands of lines of code handling this transformation, but the overall logic is the same: the engine takes an input property and compares it against a known value or a list of values. One comparison for examples compares the TimeDateStamp field from the File Header of the PE file against a list of 3523 different ranges of timestamps. Depending on what range the timestamp falls into, the engine executes a certain action. That action is really just a sequence of instructions to increment or decrement values of the feature vector. Each action can affect one or more values, and the list of instructions is stored in the model's data.

In this snippet, we first call *method_28* which will try to search for the extracted *TimeDateStamp* property in 3523 different time-date ranges. Each range has a corresponding action attached to it. If the property is not found in any of the time-date ranges, *method_14* will be called which will trigger an action, designated for instances where this property is not found to be in any of the "known" ranges.

At the end of this very long process, after executing countless actions, we end up with a vector containing 7000 feature values. This feature vector is the extract of the PE file, and it alone will determine the score and classification of the file.

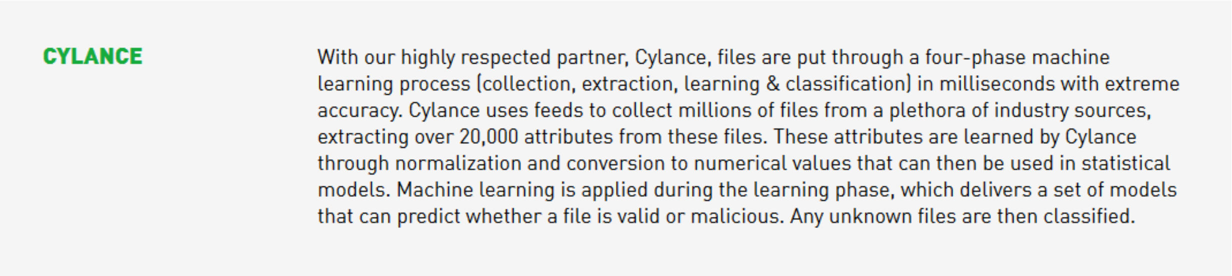
(*See* https://skylightcyber.com/2019/07/18/cylance-i-kill-you/.)



or disc into memory: file size, signing attributes, string data, icon, imports, permissions in a data section, packers, compiler type and language, headers, directories, and the presence or absence of features in combination to name a few. The resulting data from the feature extraction is then vectorized and used to train the machine learning model on what is safe to run, and what is unsafe. Finally, we classify to help ascertain the rectitude of the file in question and cluster the results to assess to what the file is most similar. The similarity and clustering gives the context around the endpoint file.

(*See* https://www.blackberry.com/content/dam/cylance/documents/pdf/pdf-feature-focus-protect-malware-control.pdf at page 02.)

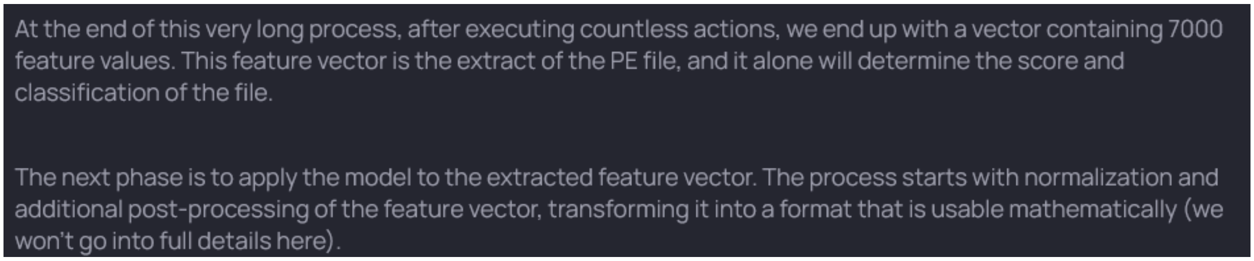
130. The Accused Products perform a method that includes *evaluating the feature vector using support vector processing to determine whether the executable file is harmful*. As explained above, the Accused Products use Cylance's static analysis in which "files are put through a four-phase machine learning process (collection, extraction, learning & classification)" and "[m]achine learning is applied during the learning phase, which delivers a set of models that can predict whether a file is valid or malicious. Any unknown files are then classified." When Forcepoint uses Cylance's static analysis, the "feature vector" is used to "determine the score and classification of the file" by "apply[ing] the model to the extracted feature vector."



CYLANCE

With our highly respected partner, Cylance, files are put through a four-phase machine learning process (collection, extraction, learning & classification) in milliseconds with extreme accuracy. Cylance uses feeds to collect millions of files from a plethora of industry sources, extracting over 20,000 attributes from these files. These attributes are learned by Cylance through normalization and conversion to numerical values that can then be used in statistical models. Machine learning is applied during the learning phase, which delivers a set of models that can predict whether a file is valid or malicious. Any unknown files are then classified.

(*See* https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf.)



At the end of this very long process, after executing countless actions, we end up with a vector containing 7000 feature values. This feature vector is the extract of the PE file, and it alone will determine the score and classification of the file.

The next phase is to apply the model to the extracted feature vector. The process starts with normalization and additional post-processing of the feature vector, transforming it into a format that is usable mathematically (we won't go into full details here).

(*See* https://skylightcyber.com/2019/07/18/cylance-i-kill-you/.)

131. Each claim in the '844 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '844 Patent.

132. Defendant has been aware of the ’844 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the ’844 Patent, including on their web site, since at least July 2020.

133. Defendant directly infringes at least claim 1 of the ’844 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendant performs the claimed method in an infringing manner as described above by running the Accused Products to protect their own computer and network operations. On information and belief, Defendant also performs the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendant performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

134. Defendant’s partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’844 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

135. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’844 Patent with specific intent to induce infringement and/or with willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers to use the Accused Products in a manner that infringes claim 1 of the ’844 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 activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of its Accused Products, including Forcepoint’s Advanced Malware Detection Appliance in the United

States. (*See, e.g.*, Forcepoint, *Installation Guide: Advanced Malware Detection*, *https://www.websense.com/content/support/library/amd-op/v10/install/manager-install.pdf*.)

136. Defendant encourages, instructs, directs, and/or requires third parties—including its partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

137. Defendant further encourages and induces its customers to infringe claim 1 of the ’844 Patent: 1) by making the Accused Products and related 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 and services in the United States. (*See* Forcepoint, *Installation Guide: Advanced Malware Detection*, https://www.websense.com/content/support/library/amd-op/v10/install/manager-install.pdf.)

138. For example, on information and belief, Defendant shares instructions, guides, and manuals, which advertise and instruct third parties on how to use the Accused Products as described above, including at least its customers and partners. (*See* Forcepoint, *Installation Guide: Advanced Malware Detection*, https://www.websense.com/content/support/library/amd-op/v10/install/manager-install.pdf; NGFW 6.7 Online Help, https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.7.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.) On further information and belief, Defendant 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. (*See* NGFW 6.7 Online Help,

https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.7.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.)

139. Defendant and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendant and/or one of its partners, which obligates each customer to perform certain actions in order to use the Accused Products. Further, in order to receive the benefit of Defendant's and/or Defendant's partners continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '844 Patent. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendant 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 '844 Patent.

140. Defendant also contributes to the infringement of its partner, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation, practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the '844 Patent.

141. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Forcepoint. Defendant also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’844 Patent.

142. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Defendant. For example, on information and belief, Defendant directs and/or controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Defendant further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’844 Patent.

143. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’844 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

144. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant from infringing the ’844 Patent.

145. Defendant’s infringement of the ’844 Patent is knowing and willful. On information and belief, Defendant had actual knowledge of the ’844 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the ’844 Patent from at least the date Plaintiffs marked their products with the ’844 Patent and/or provided notice of the ’844 Patent on their website.

146. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Forcepoint. For example, on information and belief, Forcepoint directs and controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Forcepoint further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method steps of at least claim 1 of the ’844 Patent.

147. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’844 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

148. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant from infringing the ’844 Patent. Plaintiffs have lost potential customers,

business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

149. Defendant's infringement of the '844 Patent is knowing and willful. Defendant acquired actual knowledge of the '844 Patent when Plaintiffs filed this lawsuit and had constructive knowledge of the '844 Patent from at least the date Plaintiffs marked its products with the '844 Patent and/or provided notice of the '844 Patent on its website.

150. On information and belief, despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that it knew infringe these patents. Defendant's continued infringement of the '844 Patent with knowledge of the '844 Patent constitutes willful infringement.

151. Despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that it knew infringe these patents. Defendant's continued infringement of the '844 Patent with knowledge of the '844 Patent constitutes willful infringement.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE '386 PATENT)

152. Webroot realleges and incorporates by reference the allegations of the preceding paragraphs of this Complaint.

153. Forcepoint has infringed and continues to infringe one or more claims of the '386 patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including for example products such as Forcepoint's Web Security software that include features such as Forcepoint's Advanced Classification Engine (ACE) and ThreatSeeker Intelligence that, when

used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’386 Patent, as demonstrated below.

154. For example, claim 1 of the ’386 patent recites:

> 1. A method for controlling access to an Internet resource, the method comprising:
>
> transmitting a request for an Internet resource from an Internet-enabled client application from a client-side device of a local area network, the Internet resource residing at a first server;
>
> receiving the request for the Internet resource at a security appliance of the local area network prior to transmission of the request over the Internet;
>
> determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network, the reputation index generated from a reputation vector for the Internet resource, the reputation vector comprising a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations and location, wherein the location factor of the plurality of factors for the reputation vector comprises two or more of: country of domain registration, country of service hosting and country of an internet protocol address block, wherein the legitimacy factor of the plurality of factors for the reputation vector comprises two or more of: age of a domain registration, popularity rank, internet protocol address, number of hosts, top-level domain, and wherein the behavior factor of the plurality of factors for the reputation vector comprises at least one of: plurality of run-time behaviors, script block count, picture count, immediate redirect and response latency; and
>
> transmitting a decision transmission to the Internet-enabled client application of the client-side device, the decision transmission allowing or denying access to the Internet resource.

155. To the extent the preamble is construed to be limiting, the Accused Products perform a method that includes “*controlling access to an Internet resource*.” For example, Forcepoint’s Web Security, using Forcepoint’s ThreatSeeker Intelligence, “provides content-aware web security reputation intelligence that enables customers to manage access to suspicious

websites." (*See* Forcepoint, *Master Database URL Categories*, https://www.forcepoint.com/product/feature/master-database-url-categories.)

156. The Accused Products perform a method that includes "*transmitting a request for an Internet resource from an Internet-enabled client application from a client-side device of a local area network, the Internet resource residing at a first server* [*and*] *receiving the request for the Internet resource at a security appliance of the local area network prior to transmission of the request over the Internet*." For example, Forcepoint's Secure Web Gateway includes a Proxy (SSL) for "in-line inspection of all web traffic [to] ensure[] maximum security efficiency." (*See* Forcepoint, *Forcepoint Web Security: Forcepoint's Cloud and On-Premises Web Security*, https://forcepoint.drift.click/brochure_secure_web_gateway.)

157. The Accused Products perform a method that includes "*determining if a reputation index for the Internet resource is at or above a threshold value established for the local area network, the reputation index generated from a reputation vector for the Internet resource*." For example, Forcepoint's Advanced Classification Engine ("ACE"), which runs analytics on many of Forcepoint's offerings including "Forcepoint Web Security, Forcepoint Email Security, Forcepoint Next Generation Firewall (NGFW), and Forcepoint DLP (Data Loss Prevention)," outputs a composite score for determining whether a resource is malware based on each of ACE's eight defense assessment areas. Forcepoint's literature explains that "ACE defense assessment contributes a risk score and contextual information to the composite scoring algorithms, which then calculates overall risk and consider patterns that may indicate the presence of a threat." (*See* Websense, *Websense ACE (Advanced Classification Engine)* at 7, https://bluekarmasecurity.net/wp-content/uploads/2014/09/Websense-ACE-Advanced-Classification-Engine_whitepaper.pdf.) "An overall composite score is determined and passed

back to the submitting security applications (Forcepoint Email Security or Forcepoint Web Security) to take action." (Forcepoint, *Forcepoint Advanced Malware Detection Appliance* 7, https://www.forcepoint.com/sites/default/files/resources/files/brochure_forcepoint_advanced_malware_detection_appliance_en.pdf.) Additionally, "ACE considers more than twenty different characteristics in its URL/IP reputation analysis by including attributes such as traffic volumes, DNS registration details and the autonomous system number (ASN)." (*See* https://bluekarmasecurity.net/wp-content/uploads/2014/09/Websense-ACE-Advanced-Classification-Engine_whitepaper.pdf at page 6.)

158. The combination of reputation factors analyzed includes *a plurality of factors for the Internet resource comprising security history, legitimacy, behavior, associations, and location*. Regarding *security history*, Forcepoint's ThreatSeeker Intelligence analyzes, for example, a website's reputation for "contain[ing] suspicious content." (*See* https://www.forcepoint.com/product/feature/master-database-url-categories.) Regarding *legitimacy*, Forcepoint ThreatSeeker Intelligence analyzes, for example, a website's reputation for being Newly Registered: "[s]ites whose domain name was registered recently." (*Id.*) Regarding *behavior*, Forcepoint ThreatSeeker Intelligence analyzes, for example, a website's reputation for "camouflage[ing] [its] true nature or … include[ing] elements suggesting latent malicious intent." (*Id.*) Regarding *associations*, Forcepoint ThreatSeeker Intelligence analyzes, for example, a website's reputation for "hosting known and potential exploit code." Regarding *location*, for example, Forcepoint's ACE considers "DNS registration details" and ThreatSeeker Intelligence analyzes a website's reputation for "mask[ing] [its] identity using Dynamic DNS services, often associated with advanced persistent threats (APTs)." (*Id.*)

159. On information and belief, the reputation analysis of *the location factor comprises two or more of: country of domain registration, country of service hosting and country of an internet protocol address block*. For example, "ACE considers more than twenty different characteristics in its URL/IP reputation analysis … including … DNS registration details and the autonomous system number (ASN), thereby going beyond legacy reputation systems..." (*See, e.g.,* https://bluekarmasecurity.net/wp-content/uploads/2014/09/Websense-ACE-Advanced-Classification-Engine_whitepaper.pdf at page 6.) ACE additionally analyzes a website's reputation for masking its identity using a Dynamic DNS service, which requires knowledge of the website's true identity. (*See* https://www.forcepoint.com/product/feature/master-database-url-categories.) The website's true identity includes where the website's domain is registered. Additionally, the website's full URL address includes the country of the internet protocol, for example .us, .uk, etc.

160. The reputation analysis of *the legitimacy factor … comprises two or more of: age of a domain registration, popularity rank, internet protocol address, number of hosts, or top-level domain.* For example, ThreatSeeker Intelligence analyzes a website's reputation for being Newly Registered: "[s]ites whose domain name was registered recently." (*See* https://www.forcepoint.com/product/feature/master-database-url-categories (navigate to and select "Web Security Reputation").) ThreatSeeker Intelligence also analyzes a website's reputation based on protocol address such as "Private IP Addresses: IP addresses defined in RFC 1918 'Address Allocation for Private Intranets.'" (*Id.* (navigate to and select "Baseline Categories").) Further, as discussed above, ThreatSeeker Intelligence analyzes a website's full URL address, which includes the top-level domain of the internet protocol, for example .com, co.uk, .ru, etc.

161. The reputation analysis of *the behavior factor … comprises at least one of: plurality of run-time behaviors, script block count, picture count, immediate redirect and response latency*. For example, ThreatSeeker Intelligence analyzes a website's reputation for a plurality of run-time behaviors including websites that encrypt using custom encryption methods for the outbound network transmissions and websites that "record all keystrokes, and … send those keystrokes … to an external party." (*See* https://www.forcepoint.com/product/feature/master-database-url-categories (navigate to and select "Forcepoint Security Filtering".) ThreatSeeker Intelligence also analyzes a website's "malicious URL Redirection." (*See* https://bluekarmasecurity.net/wp-content/uploads/2014/09/Websense-ACE-Advanced-Classification-Engine_whitepaper.pdf at page 10.)

162. Each claim in the '386 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '386 Patent.

163. Forcepoint has been aware of the '386 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '386 Patent, including on its web site, since at least July 2020.

164. Forcepoint directly infringes at least claim 1 of the '386 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Forcepoint performs a method in an infringing manner as described above by running the Accused Products to protect its own computer and network operations. On information and belief, the Forcepoint performs a method in an infringing manner in testing the operation of the Accused Products and corresponding systems. As another example, Forcepoint performs each of the method steps when providing or administering services to third parties, customers, and partners using the Accused Products.

165. Forcepoint's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '386 Patent, literally or under the doctrine of equivalents, at least by performing the claimed methods when using the Accused Products and corresponding systems and services, as described above.

166. Forcepoint actively induced and is actively inducing infringement of at least claim 1 of the '386 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, Forcepoint encourages and induces customers to use its security software in a manner that infringes claim 1 of the '386 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 activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of its Accused Products, including Forcepoint Web Security software, SaaS model, and services in the United States. (*See, e.g.*, Forcepoint, *Administrator Help: Forcepoint Web Security*, http://www.websense.com/content/support/library/ web/v85/web_help/web_help.pdf.)

167. Forcepoint 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, as described above.

168. Forcepoint further encourages and induces its customers to infringe claim 1 of the '386 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, including Web Security software, SaaS model, and services in the United States. (*See* Forcepoint, *Installation Guide:*

Forcepoint Web Security, http://www.websense.com/content/support/library/web/v85/install/websec_install_full.pdf.)

169. For example, on information and belief, Forcepoint 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. (*See* Forcepoint, *Administrator Help: Forcepoint Web Security*, http://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf.) On further information and belief, Forcepoint also provides customer service or technical support to purchasers of the Accused Products and corresponding system and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id.*)

170. Forcepoint and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Forcepoint and/or a Forcepoint partner, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Forcepoint's and/or its partner's continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '386 Patent. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Forcepoint and/or its partners establish the manner and timing of each customer's performance of activities that infringe the '386 Patent.

171. Forcepoint also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’386 Patent.

172. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Forcepoint. For example, on information and belief, Forcepoint directs and/or controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Forcepoint further directs and/or controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method steps of at least claim 1 of the ‘386 Patent.

173. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’386 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

174. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant from infringing the ’386 Patent. On information and belief, Plaintiffs

have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

175. Defendant's infringement of the '386 Patent is knowing and willful. On information and belief, Defendant had actual knowledge of the '386 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the '386 Patent from at least the date Plaintiffs marked its products with the '386 Patent and/or provided notice of the '386 Patent on its website.

176. On information and belief, despite Defendant's knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant's continued infringement of the '386 Patent with knowledge of the '386 Patent constitutes willful infringement.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE '721 PATENT)

177. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

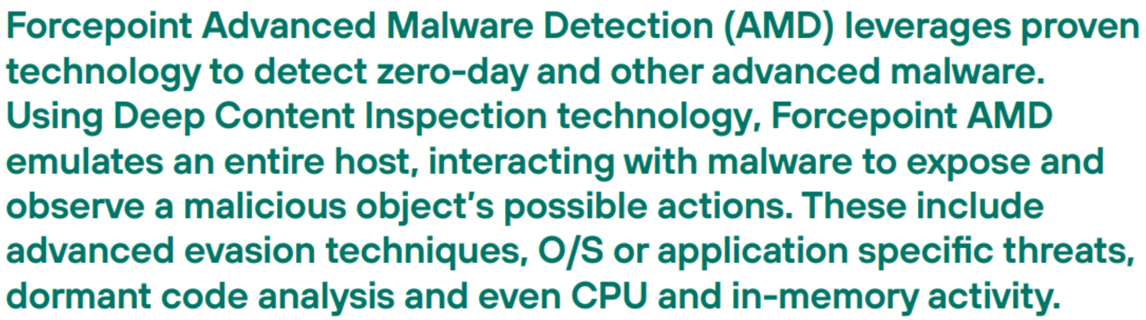
178. Forcepoint has infringed and continues to infringe one or more claims of the '721 patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including for example Forcepoint's Advanced Malware Detection Systems and systems that incorporate it, such as Next Generation Firewall solutions, when used for their ordinary and customary purposes, practice each element of at least claim 1 the '721 Patent as demonstrated below.

179. For example, claim 1 of the '721 patent recites:

> A method of classifying a computer object as malware, the method comprising:
>
> receiving, at a first threat server, details of a first computer object

> from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object;
>
> determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server;
>
> receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen;
>
> storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen;
>
> providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer;
>
> increasing a count associated with a number of times that the first computer object has been seen, and providing the increased count associated with the number of times that the first computer object has been seen to the central server; and
>
> receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.

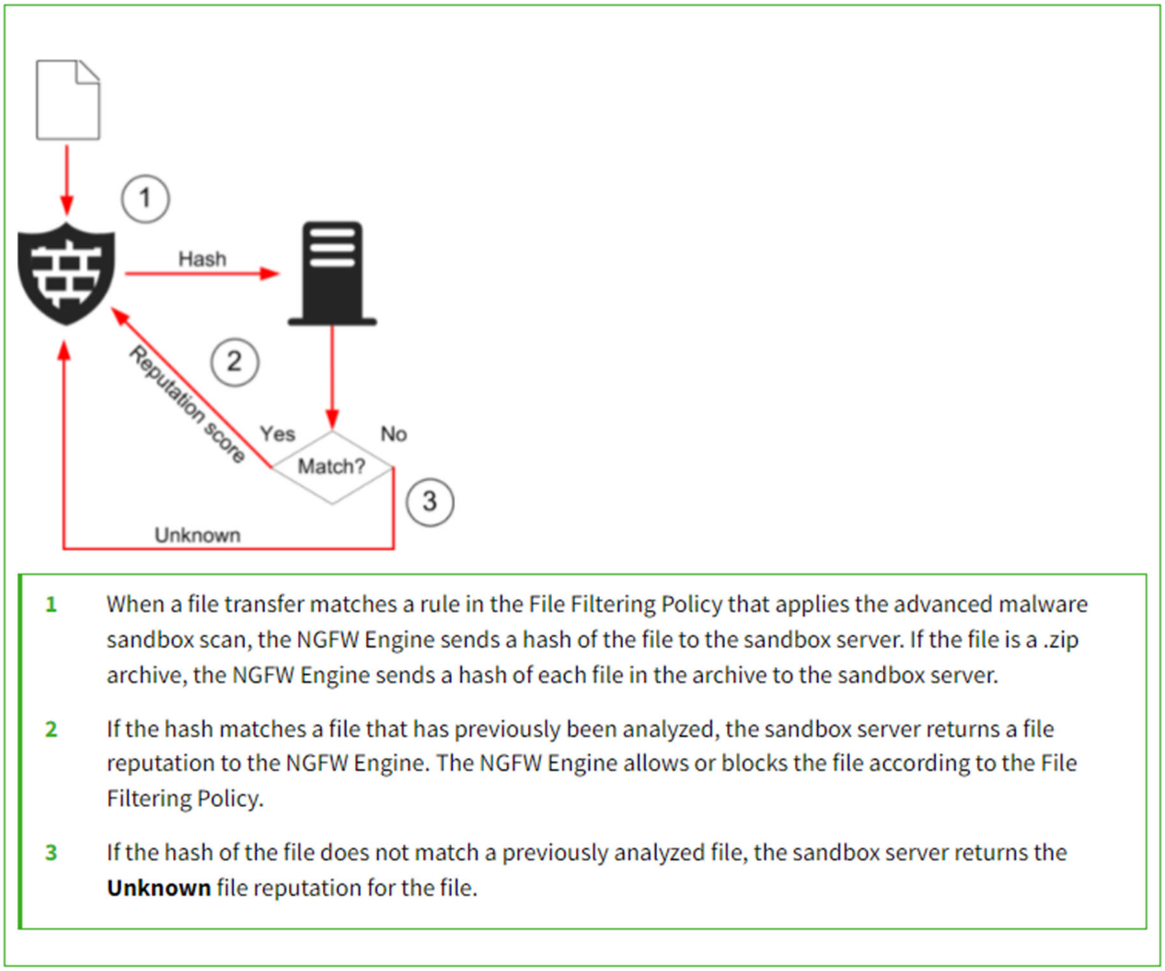
180. To the extent the preamble is construed as limiting, the Accused Products perform *a method of classifying a computer object as malware*. For example, the Forcepoint Advanced Malware Detection systems and Next Generation Firewall solutions detect "zero-day and other advanced malware."



Forcepoint Advanced Malware Detection (AMD) leverages proven technology to detect zero-day and other advanced malware. Using Deep Content Inspection technology, Forcepoint AMD emulates an entire host, interacting with malware to expose and observe a malicious object's possible actions. These include advanced evasion techniques, O/S or application specific threats, dormant code analysis and even CPU and in-memory activity.

(*See* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution_brief_forcepoint_advanced_malware_detection_en.pdf; https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-DA3B3807-18E1-482B-A5E8-A8BD468E5BB0.html.)

181. The Accused Products perform a method that includes *receiving, at a first threat server, details of a first computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object*. For example, in systems using Forcepoint Advanced Malware Detection and Forcepoint Next Generation Firewall solution, when the Forcepoint File Filtering Policy detects a suspicious file, the Forcepoint NGFW (next generation firewall) Engine sends a hash of the file to a sandbox server; at least the hash uniquely identifies the file object.



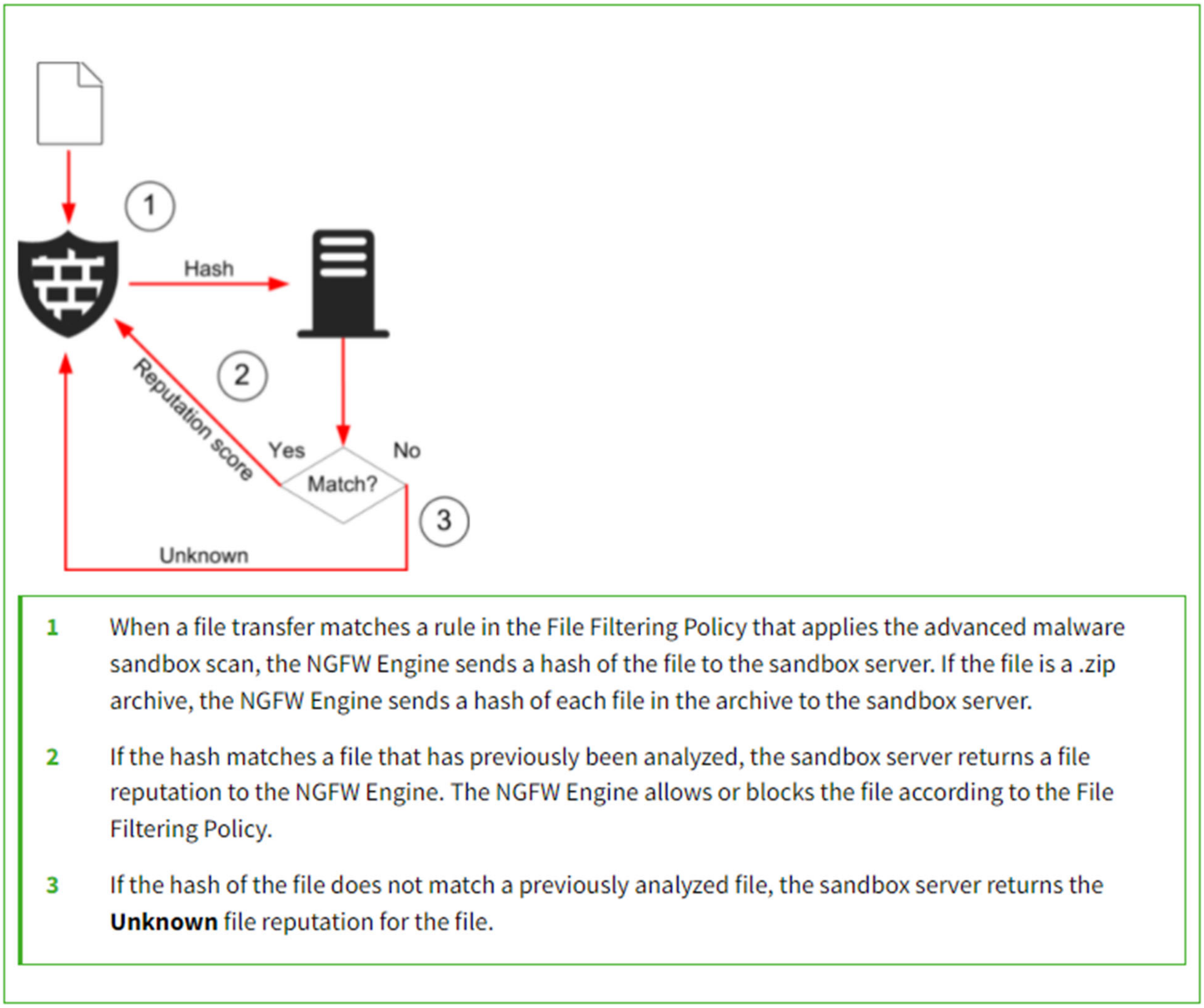
1 When a file transfer matches a rule in the File Filtering Policy that applies the advanced malware sandbox scan, the NGFW Engine sends a hash of the file to the sandbox server. If the file is a .zip archive, the NGFW Engine sends a hash of each file in the archive to the sandbox server.

2 If the hash matches a file that has previously been analyzed, the sandbox server returns a file reputation to the NGFW Engine. The NGFW Engine allows or blocks the file according to the File Filtering Policy.

3 If the hash of the file does not match a previously analyzed file, the sandbox server returns the **Unknown** file reputation for the file.

(*See* https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.)

182. The Accused Products perform a method that includes the step of *determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server*. For example, the sandbox server compares the file hash to a database of hashes of files that have been previously seen to determine whether the hash matches a "previously analyzed file" that has previously been identified.



1 When a file transfer matches a rule in the File Filtering Policy that applies the advanced malware sandbox scan, the NGFW Engine sends a hash of the file to the sandbox server. If the file is a .zip archive, the NGFW Engine sends a hash of each file in the archive to the sandbox server.

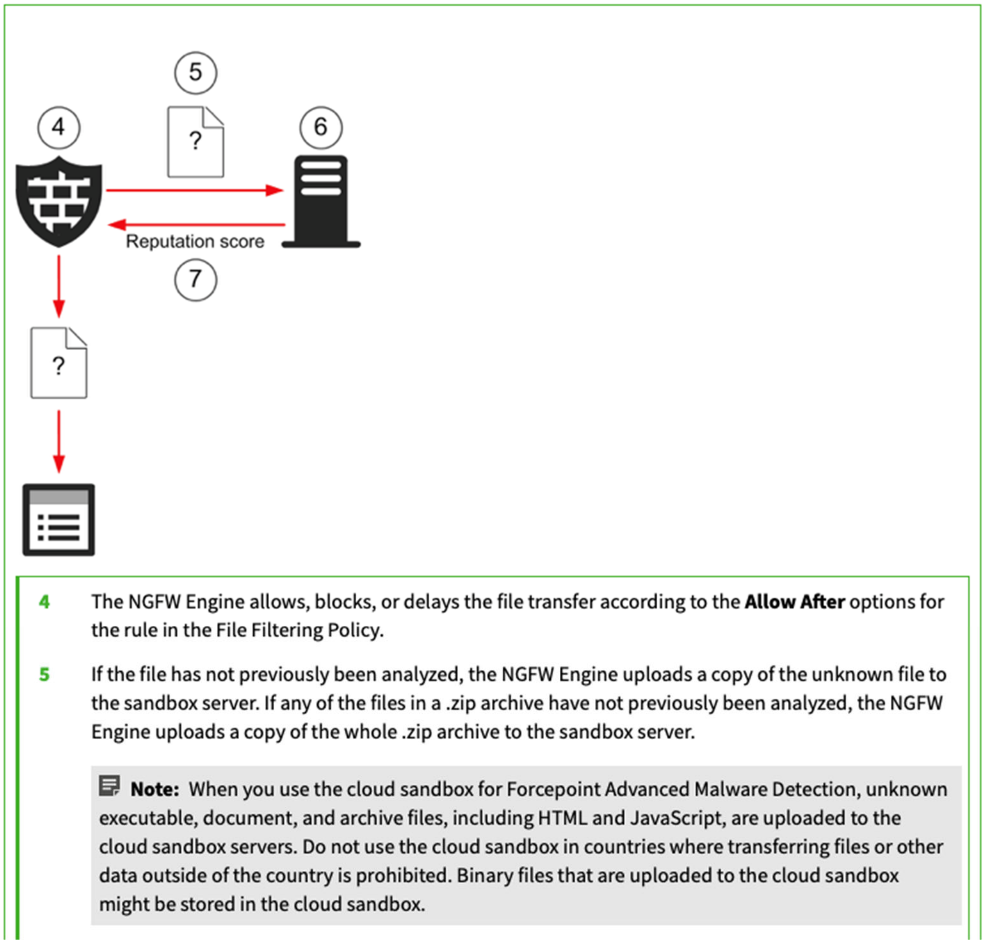
2 If the hash matches a file that has previously been analyzed, the sandbox server returns a file reputation to the NGFW Engine. The NGFW Engine allows or blocks the file according to the File Filtering Policy.

3 If the hash of the file does not match a previously analyzed file, the sandbox server returns the **Unknown** file reputation for the file.

(*See* https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.)

183. The Accused Products perform a method that includes *receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen* and *storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen*. For example, if the suspect file has not been previously analyzed by the sandbox server, the NGFW Engine uploads a copy of the file to the sandbox server. The NFGW Engine also receives

information about whether a file was compressed (.zip) and if so what files/objects were inside the archive, and whether a file object is a "document, [or] archive files, including HTML and JavaScript." Indeed, Forcepoint sends "threat intelligence updates containing the characteristics, behaviors and associated IOCs of every malicious object curated and analyzed within the global service." On information and belief, this information is stored in a database.

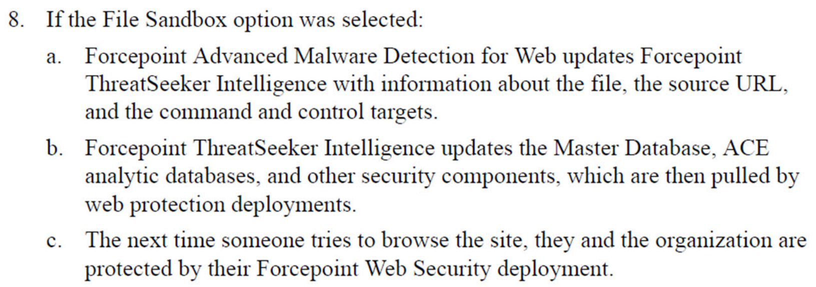


4 The NGFW Engine allows, blocks, or delays the file transfer according to the **Allow After** options for the rule in the File Filtering Policy.

5 If the file has not previously been analyzed, the NGFW Engine uploads a copy of the unknown file to the sandbox server. If any of the files in a .zip archive have not previously been analyzed, the NGFW Engine uploads a copy of the whole .zip archive to the sandbox server.

> **Note:** When you use the cloud sandbox for Forcepoint Advanced Malware Detection, unknown executable, document, and archive files, including HTML and JavaScript, are uploaded to the cloud sandbox servers. Do not use the cloud sandbox in countries where transferring files or other data outside of the country is prohibited. Binary files that are uploaded to the cloud sandbox might be stored in the cloud sandbox.

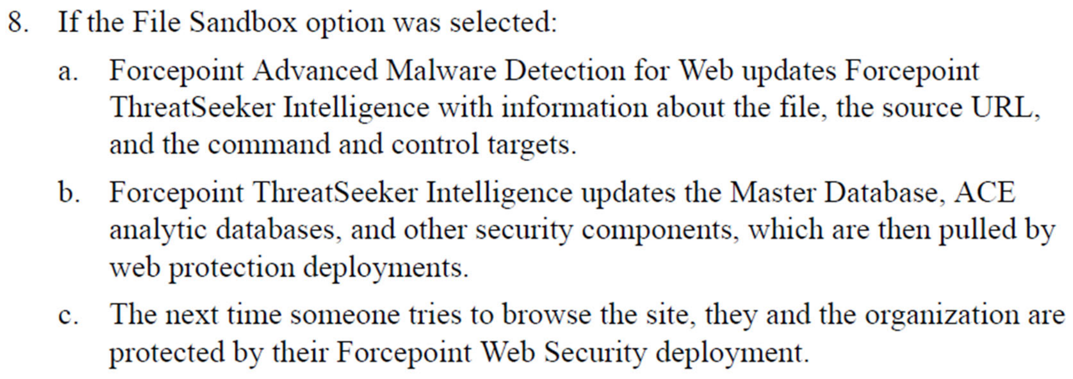
(*See* https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.)



8. If the File Sandbox option was selected:
   a. Forcepoint Advanced Malware Detection for Web updates Forcepoint ThreatSeeker Intelligence with information about the file, the source URL, and the command and control targets.
   b. Forcepoint ThreatSeeker Intelligence updates the Master Database, ACE analytic databases, and other security components, which are then pulled by web protection deployments.
   c. The next time someone tries to browse the site, they and the organization are protected by their Forcepoint Web Security deployment.

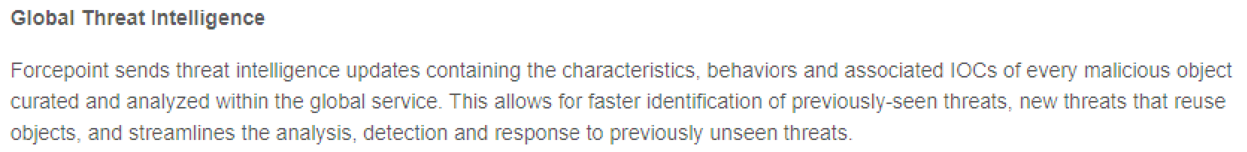
(*See* https://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf at page 107.)

184. The Accused Products perform a method that includes *providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer*. For example, Forcepoint Advanced Malware Detection and the NGFW send information about the file, the source URL, and the command-and-control targets to Forcepoint ThreatSeeker Intelligence, which updates the Master Database, as well as ACE analytic databases and other security components. Moreover, as discussed above, hashes (signatures) of files are also transmitted. Indeed, Forcepoint sends "threat intelligence updates containing the characteristics, behaviors and associated IOCs of every malicious object curated and analyzed within the global service."



8. If the File Sandbox option was selected:
   a. Forcepoint Advanced Malware Detection for Web updates Forcepoint ThreatSeeker Intelligence with information about the file, the source URL, and the command and control targets.
   b. Forcepoint ThreatSeeker Intelligence updates the Master Database, ACE analytic databases, and other security components, which are then pulled by web protection deployments.
   c. The next time someone tries to browse the site, they and the organization are protected by their Forcepoint Web Security deployment.

(*See* https://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf at page 107.)

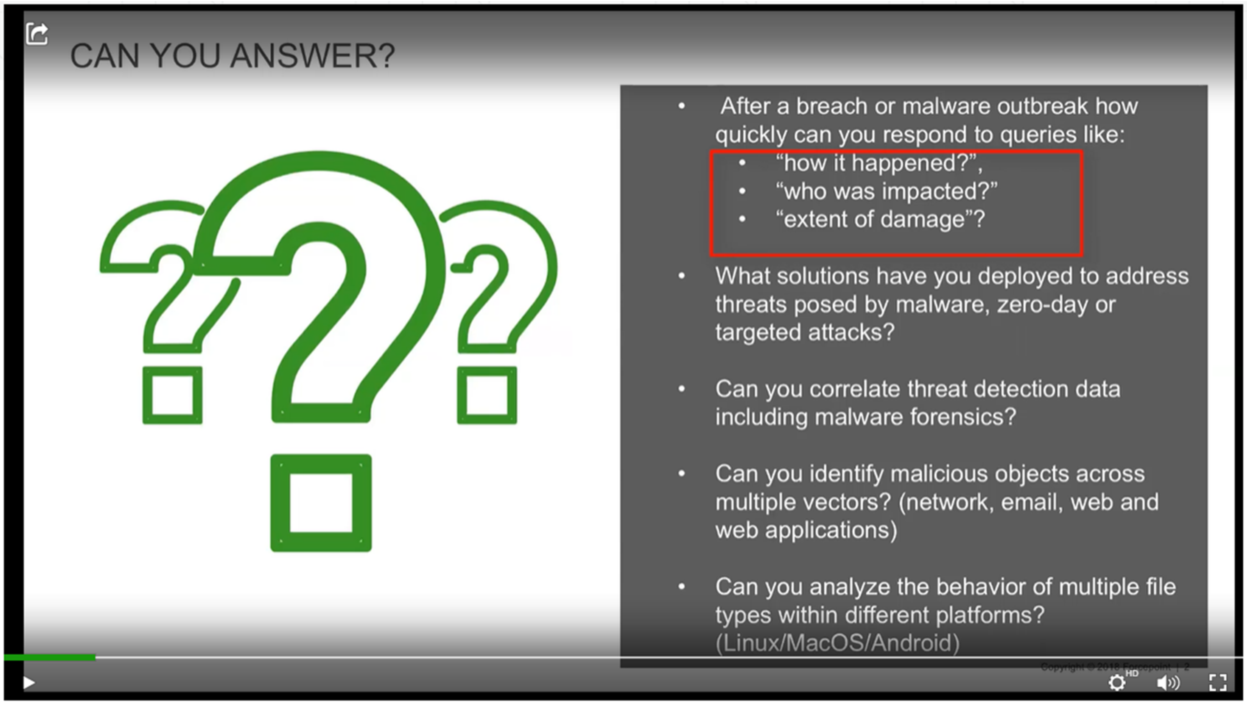


Global Threat Intelligence

Forcepoint sends threat intelligence updates containing the characteristics, behaviors and associated IOCs of every malicious object curated and analyzed within the global service. This allows for faster identification of previously-seen threats, new threats that reuse objects, and streamlines the analysis, detection and response to previously unseen threats.

(*See* https://roi4cio.com/catalog/en/product/forcepoint-advanced-malware-detection.)

185. The Accused Products perform a method that includes *increasing a count associated with a number of times that the first computer object has been seen, and providing the increased count associated with the number of times that the first computer object has been seen to the central server*. On information and belief, Forcepoint Advanced Malware Detection and the NGFW systems keep a count of how many times a malicious file has been encountered. For example, Forcepoint AMD is able to determine how many people have encountered a malicious file across a user group.



CAN YOU ANSWER?

- After a breach or malware outbreak how quickly can you respond to queries like:
  - "how it happened?",
  - "who was impacted?"
  - "extent of damage"?
- What solutions have you deployed to address threats posed by malware, zero-day or targeted attacks?
- Can you correlate threat detection data including malware forensics?
- Can you identify malicious objects across multiple vectors? (network, email, web and web applications)
- Can you analyze the behavior of multiple file types within different platforms? (Linux/MacOS/Android)

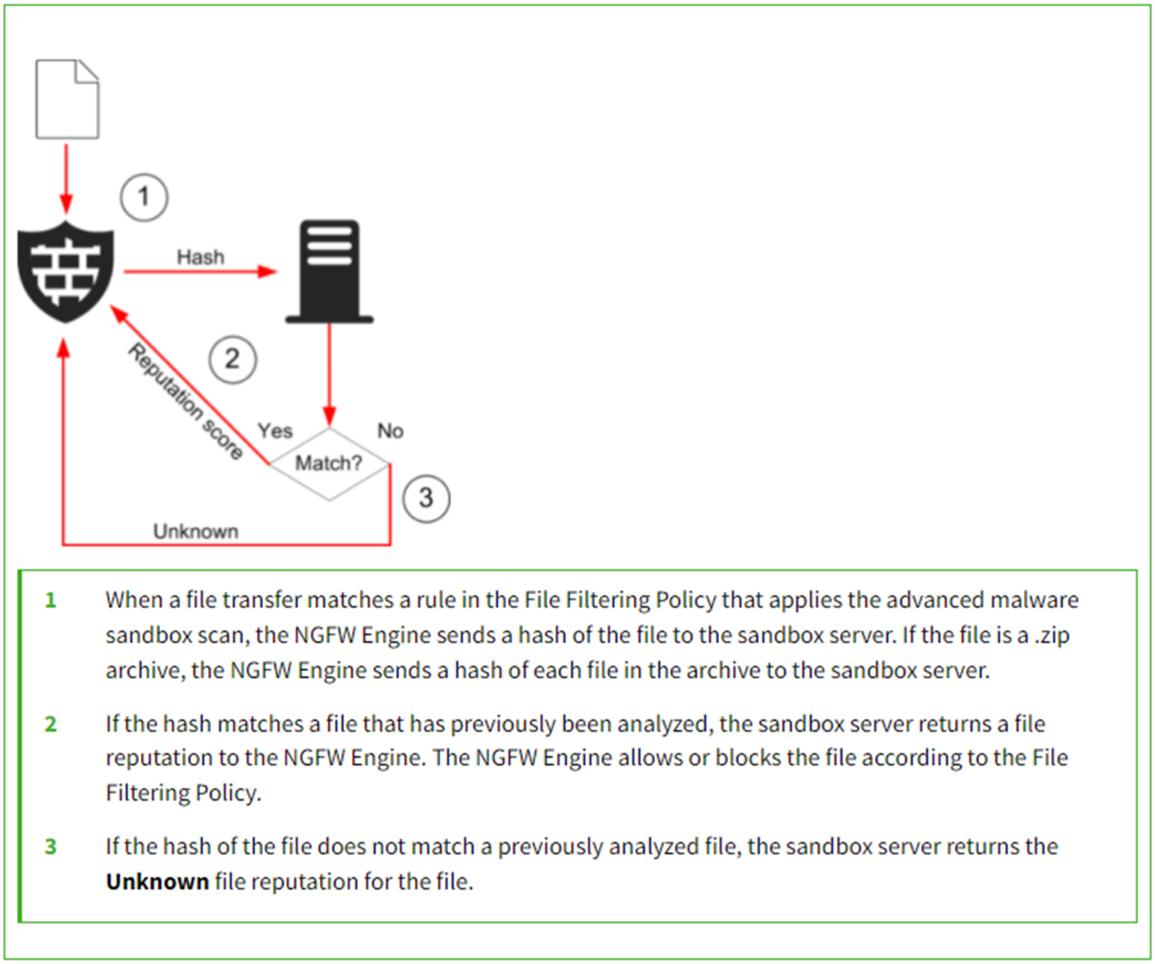
(*See* https://www.forcepoint.com/form/thank-you-your-interest-webcast?form_id=1427&resource=18566&category=webcasts.)

186. In addition, on information and belief, the Accused Products such as Forcepoint Advanced Malware Detection and NGFW solutions log information about network activity and trends are stored in one or more databases. For example, "the Log Database can store trend data to enable presentation reporting on Internet activity trends. When trend reporting is enabled, the ETL database job (see Web protection reporting database jobs, page 452) adds daily trend data to the catalog database, and the trend job runs nightly to store weekly, monthly, and yearly trend information. The Log Database also stores statistical data (like bandwidth and count) for browsers, operating system platforms, and user agent strings to enable application reporting." (*See* https://www.websense.com/content/support/library/ web/v85/web_help/web_help.pdf at pages 460-461.)

187. The Accused Products perform a method that includes *receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.* On information and belief, the file's hash and reputation is distributed to all sandbox servers such that the sandboxes can return reputation results. (https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.9.0/GUID-41D85576-7C24-4BA8-8605-710F52790CD8.html ("When the analysis is complete, the sandbox server sends an updated file reputation to the NGFW Engine. The updated file reputation is cached on the NGFW Engine that requested the scan and stored on the sandbox server"); https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.7.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.)

188. This enables, for example, the sandbox server to compare the file hash to a database

of hashes of files that have been previously seen to determine whether the hash matches a "previously analyzed file" that has previously been identified. In addition, as explained above, information about the file, uploaded by Forcepoint ThreatSeeker Intelligence to the Master Database, ACE analytics databases, and other security components, are further disseminated to other web protection deployments.

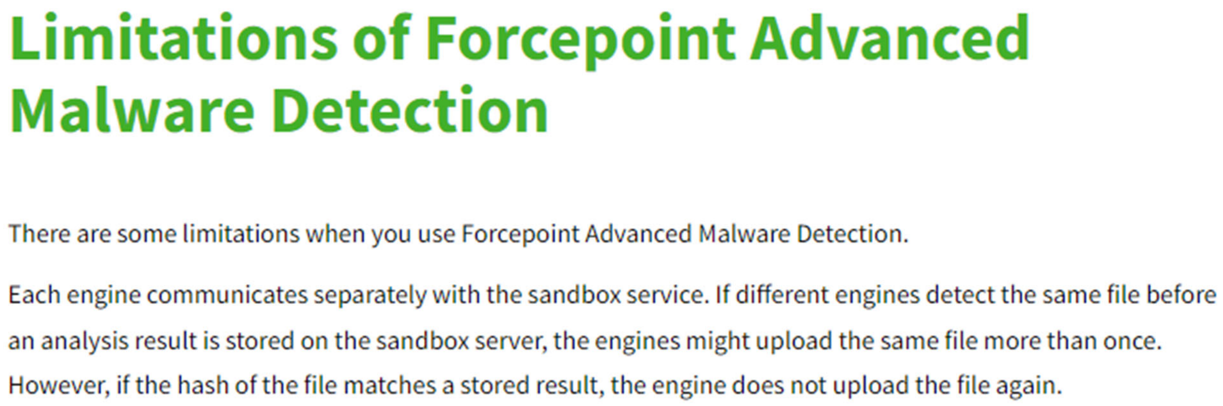


1 When a file transfer matches a rule in the File Filtering Policy that applies the advanced malware sandbox scan, the NGFW Engine sends a hash of the file to the sandbox server. If the file is a .zip archive, the NGFW Engine sends a hash of each file in the archive to the sandbox server.

2 If the hash matches a file that has previously been analyzed, the sandbox server returns a file reputation to the NGFW Engine. The NGFW Engine allows or blocks the file according to the File Filtering Policy.

3 If the hash of the file does not match a previously analyzed file, the sandbox server returns the **Unknown** file reputation for the file.

(*See* https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-EECA15DA-9B8A-4C2F-9C42-D53516ADC19E.html.)

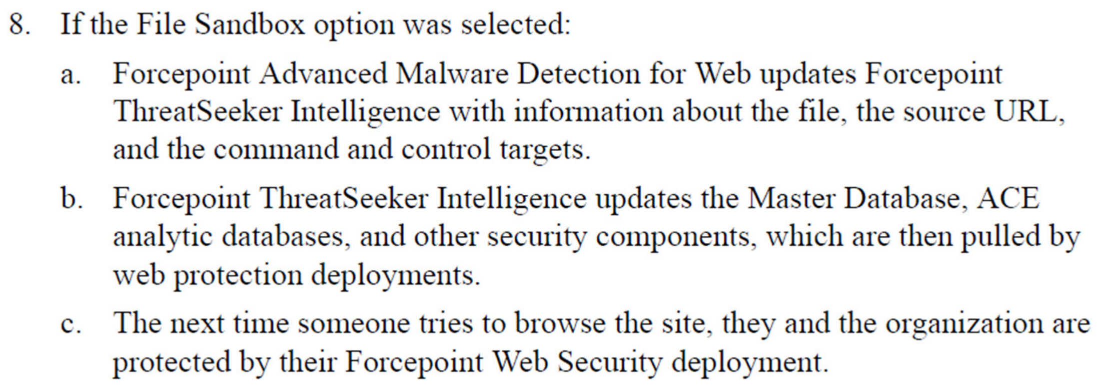


Limitations of Forcepoint Advanced Malware Detection

There are some limitations when you use Forcepoint Advanced Malware Detection.

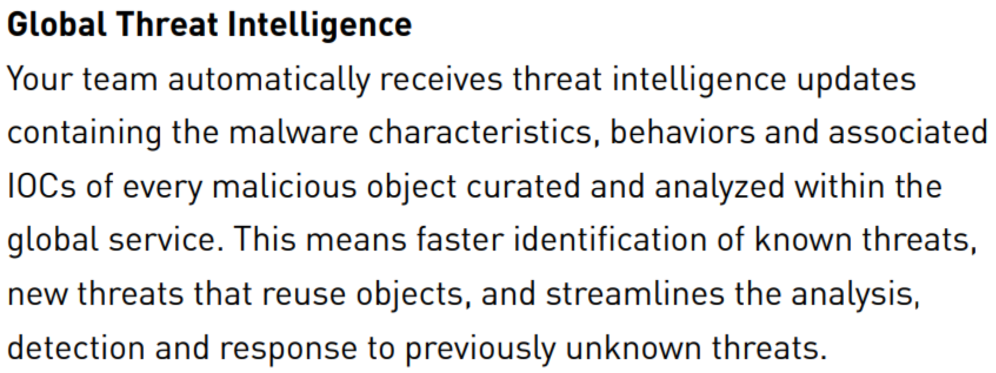
Each engine communicates separately with the sandbox service. If different engines detect the same file before an analysis result is stored on the sandbox server, the engines might upload the same file more than once. However, if the hash of the file matches a stored result, the engine does not upload the file again.

(*See* https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.5.0/GUID-222054A1-AAC3-4153-8F8C-47E17903EA70.html.)



8. If the File Sandbox option was selected:
   a. Forcepoint Advanced Malware Detection for Web updates Forcepoint ThreatSeeker Intelligence with information about the file, the source URL, and the command and control targets.
   b. Forcepoint ThreatSeeker Intelligence updates the Master Database, ACE analytic databases, and other security components, which are then pulled by web protection deployments.
   c. The next time someone tries to browse the site, they and the organization are protected by their Forcepoint Web Security deployment.

(*See* https://www.websense.com/content/support/library/web/v85/web_help/web_help.pdf, at page 107.)



Global Threat Intelligence

Your team automatically receives threat intelligence updates containing the malware characteristics, behaviors and associated IOCs of every malicious object curated and analyzed within the global service. This means faster identification of known threats, new threats that reuse objects, and streamlines the analysis, detection and response to previously unknown threats.

(*See* https://www.forcepoint.com/sites/default/files/resources/files/datasheet_advanced_malware_detection_en.pdf.)

189. Each claim in the ’721 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’721 Patent.

190. Forcepoint has been aware of the ’721 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the ’721 Patent, including on its web site, since at least July 2020.

191. Forcepoint directly infringes at least claim 1 of the ’721 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Forcepoint performs a method in an infringing manner as described above by running the Accused Products to protect its own computer and network operations. On information and belief, the Forcepoint performs a method in an infringing manner in testing the operation of the Accused Products and corresponding systems. As another example, Forcepoint performs each of the method steps when providing or administering services to third parties, customers, and partners using the Accused Products.

192. Forcepoint’s partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’721 Patent, literally or under the doctrine of equivalents, at least by performing the claimed methods when using the Accused Products and corresponding systems and services, as described above.

193. Forcepoint actively induced and is actively inducing infringement of at least claim 1 of the ’721 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, Forcepoint encourages and induces customers to use Forcepoint’s security software in a manner that infringes claim 1 of the ’721 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 activities

relating to selling, marketing, advertising, promotion, installation, support, and distribution of its Accused Products in the United States. (*See* Forcepoint, *Next Generation Firewall Installation Guide*, https://www.websense.com/content/support/library/ngfw/v67/install/ngfw_670_ig_a_en-us.pdf.)

194. Forcepoint 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, as described above.

195. Forcepoint further encourages and induces its customers to infringe claim 1 of the ’721 Patent: 1) by making the Accused Products and related 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, including the Next-Generation Firewall defense, software, SaaS model, and services in the United States. (*See* Forcepoint, *Next Generation Firewall Installation Guide*, https://www.websense.com/ content/support/library/ngfw/v67/install/ngfw_670_ig_a_en-us.pdf.)

196. For example, on information and belief, Forcepoint 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. (*See* Forcepoint, *Next Generation Firewall Installation Guide*, https://www.websense.com/content/support/library/ngfw/v67/install/ngfw_670_ig_a_en-us.pdf.) On further information and belief, Forcepoint also provides customer service or technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id.*)

197. Forcepoint and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Forcepoint and/or its partners, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Forcepoint's and/or its partner's continued technical support and their specialized knowledge and guidance with respect to operation of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '721 Patent. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Forcepoint 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 '721 Patent.

198. Forcepoint also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the '721 Patent.

199. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Forcepoint. For example, on information and belief, Forcepoint directs and/or controls the activities or actions of its partners in connection with

the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Forcepoint further directs and/or controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method steps of at least claim 1 of the ‘721 Patent.

200. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’721 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendant’s infringement, but no less than a reasonable royalty.

201. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant from infringing the ’721 Patent. On information and belief, Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

202. Defendant’s infringement of the ’721 Patent is knowing and willful. Defendant acquired actual knowledge of the ’721 Patent when Plaintiffs filed this lawsuit and had constructive knowledge of the ’721 Patent from at least the date Plaintiffs marked its products with the ’721 Patent and/or provided notice of the ’721 Patent on its website.

203. On information and belief, despite Defendant’s knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant’s continued infringement of the ’250 Patent with knowledge of the ’721 Patent constitutes willful infringement.

FIFTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’928 Patent)

204. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

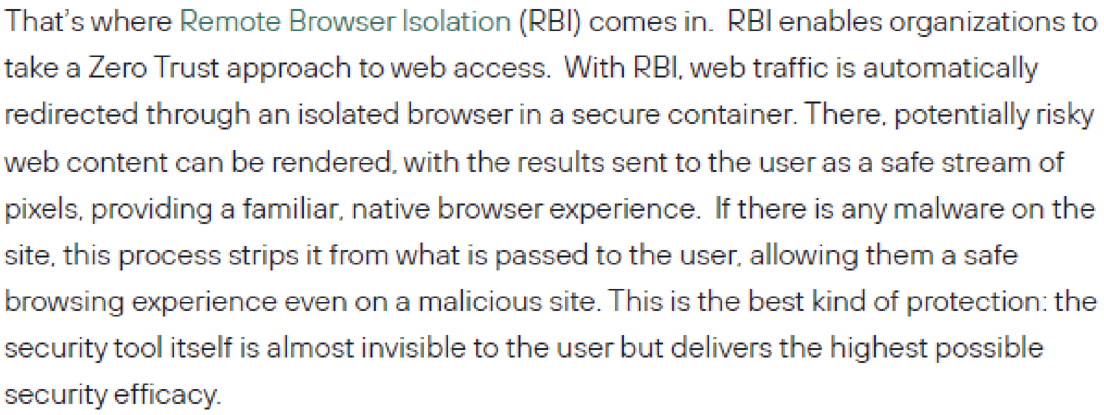
205. Forcepoint has infringed and continues to infringe one or more claims of the ’928 Patent in violation of 35 U.S.C. § 271 in this judicial district and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, for example Forcepoint’s Remote Browser Isolation and related software and services, such as Ericom Shield Zero Trust and Cyberinc’s Isla Smart Isolation feature incorporated therein (“Remote Browser” or “RBI”) that, when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’928 Patent as demonstrated below.

206. For example, claim 1 of the ’928 Patent recites:

> 1. A content analysis and malware prevention method comprising:
>
> intercepting, by a protection agent, a request from a web browser;
>
> determining, by the protection agent, whether the request is associated with known malicious content;
>
> when the request is associated with known malicious content, blocking, by the protection agent, the request; and
>
> when the request is not associated with known malicious content:
>
> sending, by the protection agent, the request to one or more web servers
>
> receiving, at the protection agent on a remote computer, web content from the one or more web servers, wherein web content comprises data for assembling a web page, and wherein the web content is received in response to the request;
>
> identifying, by the protection agent, a malware threat within the web content;
>
> in response to identifying the malware threat, modifying, by the protection

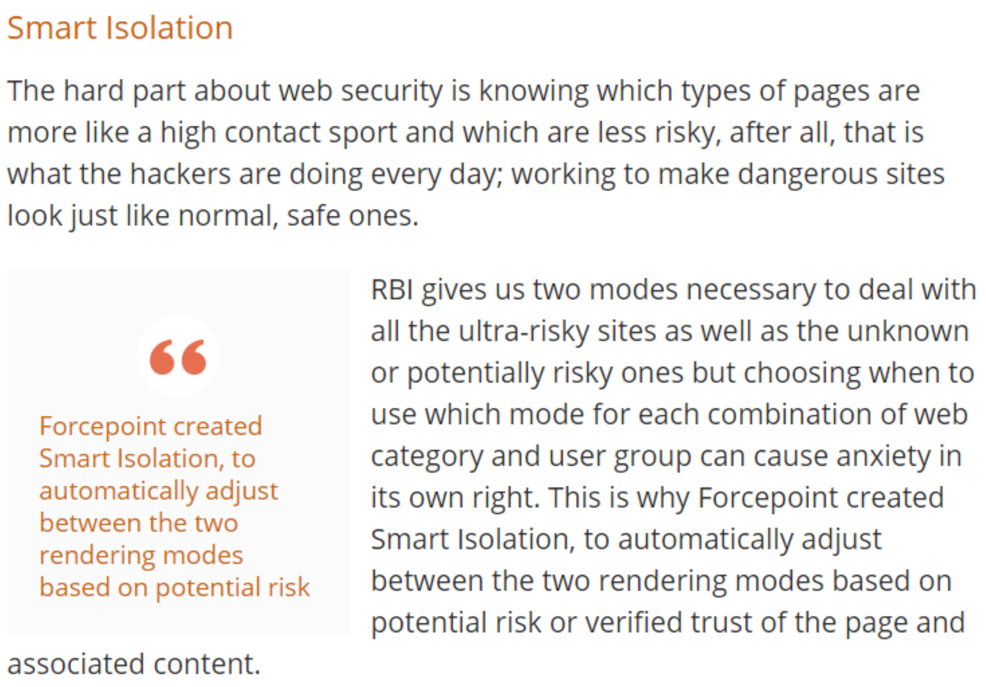
> agent, the web content, wherein modifying the web content comprises modifying the web content at protocol level to remove the malware threat from the web content;
>
> assembling, by the protection agent, a modified version of the web page, wherein the modified web page is assembled using the modified web content, and wherein the modified version of the web page does not comprise the malware threat; and
>
> providing, by the protection agent, the modified version of the web page to the web browser application on the remote computer for rendering and display.

207. To the extent the preamble is construed to be limiting, the Accused Products perform *a content analysis and malware prevention method*. For example, Forcepoint's RBI "gives us two modes necessary to deal with all the ultra-risky sites as well as the unknown or potentially risky ones": "Secure Streaming "and "Secure Rendering." RBI "automatically adjust[s] between the two rendering modes based on potential risk or verified trust of the page and associated content." The Accused Products thereby "provide[] malware protection against ransomware" as well as "zero-day threats." Indeed, "[i]f there is any malware on the site, this process strips it from what is passed to the user, allowing them a safe browsing experience even on a malicious site."



That's where Remote Browser Isolation (RBI) comes in. RBI enables organizations to take a Zero Trust approach to web access. With RBI, web traffic is automatically redirected through an isolated browser in a secure container. There, potentially risky web content can be rendered, with the results sent to the user as a safe stream of pixels, providing a familiar, native browser experience. If there is any malware on the site, this process strips it from what is passed to the user, allowing them a safe browsing experience even on a malicious site. This is the best kind of protection: the security tool itself is almost invisible to the user but delivers the highest possible security efficacy.

(*See* https://www.forcepoint.com/blog/insights/remote-browser-isolation-higher-level-web-security at page 01.)



Smart Isolation

The hard part about web security is knowing which types of pages are more like a high contact sport and which are less risky, after all, that is what the hackers are doing every day; working to make dangerous sites look just like normal, safe ones.

RBI gives us two modes necessary to deal with all the ultra-risky sites as well as the unknown or potentially risky ones but choosing when to use which mode for each combination of web category and user group can cause anxiety in its own right. This is why Forcepoint created Smart Isolation, to automatically adjust between the two rendering modes based on potential risk or verified trust of the page and associated content.

> “ Forcepoint created Smart Isolation, to automatically adjust between the two rendering modes based on potential risk

(*See* https://www.sourcesecurity.com/news/forcepoint-launches-industry-smart-remote-browser-co-1642591598-ga-npr.1642592193.html?ref=nav at page 02.)

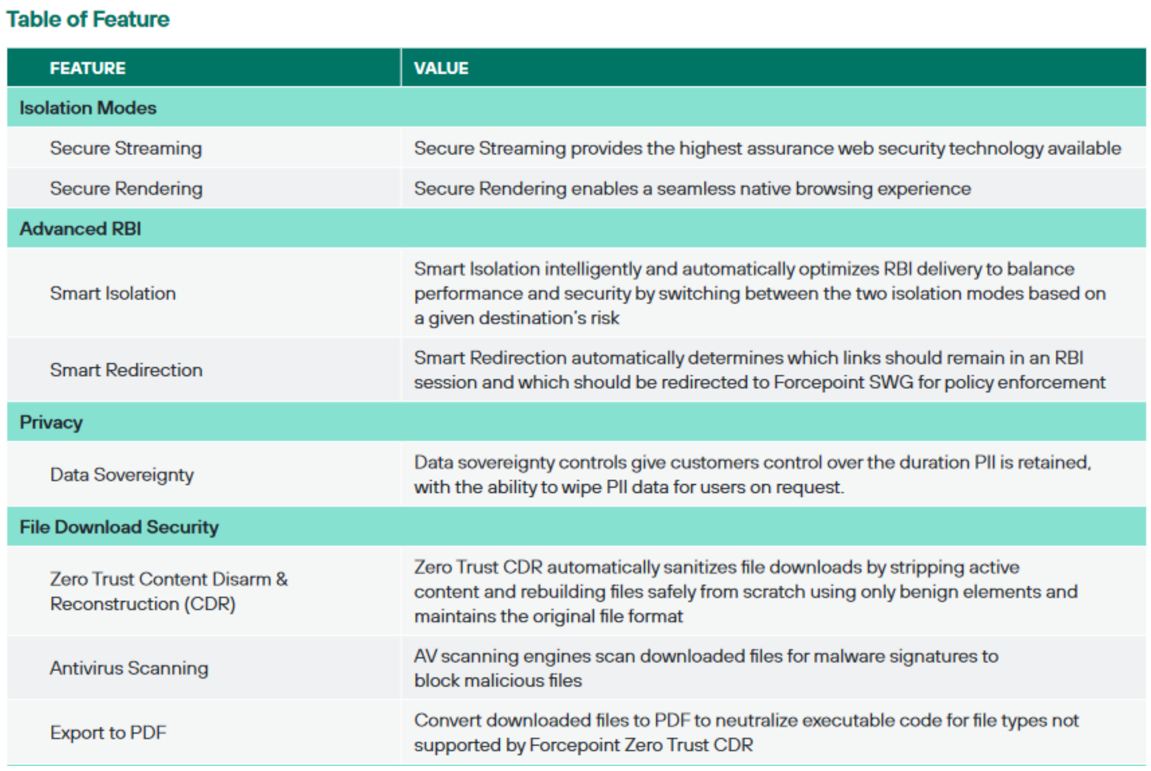
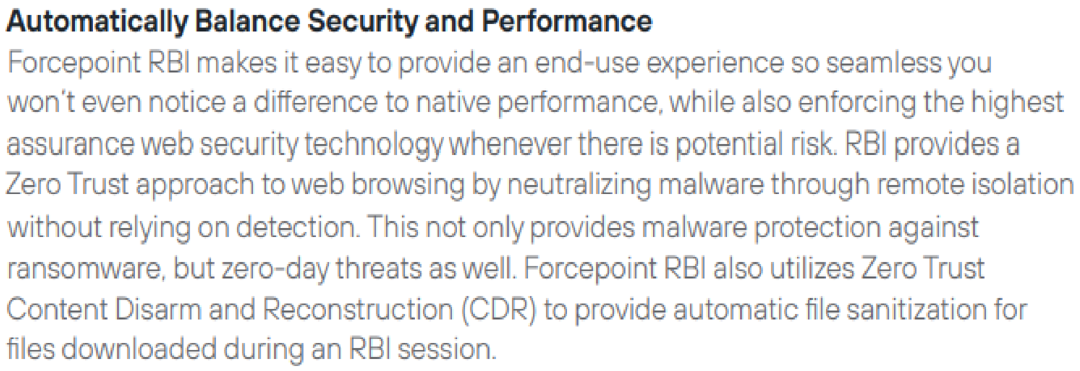


Table of Feature

FEATURE	VALUE
Isolation Modes	
Secure Streaming	Secure Streaming provides the highest assurance web security technology available
Secure Rendering	Secure Rendering enables a seamless native browsing experience
Advanced RBI	
Smart Isolation	Smart Isolation intelligently and automatically optimizes RBI delivery to balance performance and security by switching between the two isolation modes based on a given destination's risk
Smart Redirection	Smart Redirection automatically determines which links should remain in an RBI session and which should be redirected to Forcepoint SWG for policy enforcement
Privacy	
Data Sovereignty	Data sovereignty controls give customers control over the duration PII is retained, with the ability to wipe PII data for users on request.
File Download Security	
Zero Trust Content Disarm & Reconstruction (CDR)	Zero Trust CDR automatically sanitizes file downloads by stripping active content and rebuilding files safely from scratch using only benign elements and maintains the original file format
Antivirus Scanning	AV scanning engines scan downloaded files for malware signatures to block malicious files
Export to PDF	Convert downloaded files to PDF to neutralize executable code for file types not supported by Forcepoint Zero Trust CDR

(*See* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution-brief-remote-browser-isolation-en_0_0_0_0_0_0_0_0_0_0_0_0_0_0.pdf.)

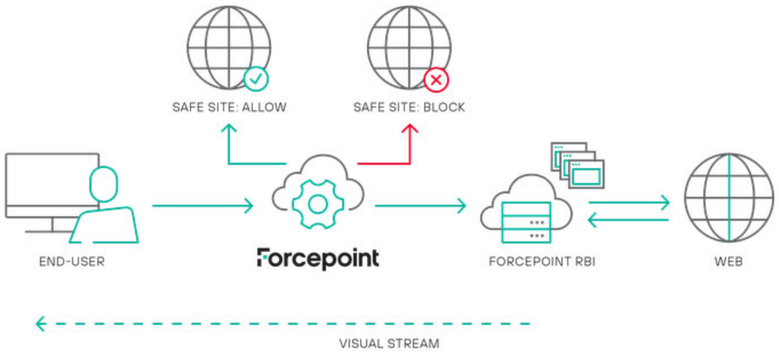


Automatically Balance Security and Performance

Forcepoint RBI makes it easy to provide an end-use experience so seamless you won't even notice a difference to native performance, while also enforcing the highest assurance web security technology whenever there is potential risk. RBI provides a Zero Trust approach to web browsing by neutralizing malware through remote isolation without relying on detection. This not only provides malware protection against ransomware, but zero-day threats as well. Forcepoint RBI also utilizes Zero Trust Content Disarm and Reconstruction (CDR) to provide automatic file sanitization for files downloaded during an RBI session.

(*See* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution-brief-remote-browser-isolation-en_0_0_0_0_0_0_0_0_0_0_0_0_0_0.pdf at page 01.)

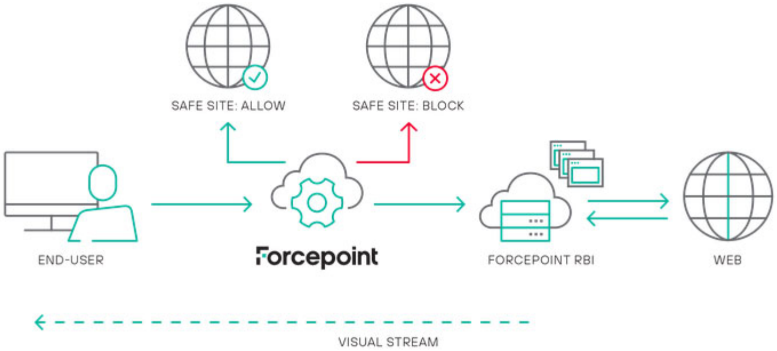
208. The Accused Products perform a method that includes *intercepting, by a protection agent, a request from a web browser*. For example, "[w]ith RBI, web traffic is automatically redirected through an isolated browser in a secure container." (*See* https://www.forcepoint.com/blog/insights/remote-browser-isolation-higher-level-web-security at page 01.)



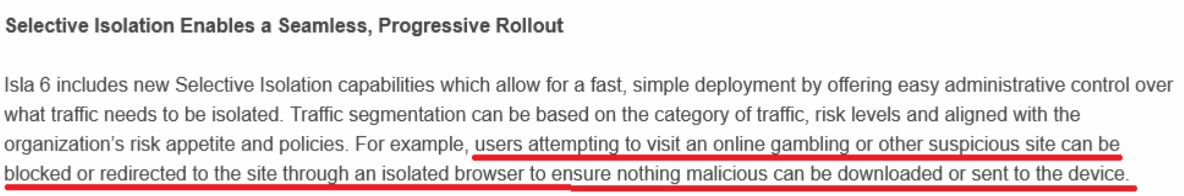
(*See* https://www.forcepoint.com/cyberinc.)

209. "Download interception prevents drive-by downloads that push malware onto endpoints." (*See* https://www.forcepoint.com/sites/default/files/resources/solution_brief/solution-brief-remote-browser-isolation-en_0_0_0_0_0_0_0_0_0_0_0_0_0_0.pdf at page 02.)

210. The Accused Products perform a method that includes *determining, by the protection agent, whether the request is associated with known malicious content* and *when the request is associated with known malicious content, blocking, by the protection agent, the request*. As one example, the Accused Products utilize risk-based isolation (*e.g.*, using Threat Intelligence) to determine if websites should be trusted, isolated, blocked, etc. As another example, the Accused Products are "commonly used when dealing with websites that aren't known to be either 'good' (and can typically be safely allowed) or 'bad' (and are usually blocked), allowing such uncategorized sites to be used without fear." RBI can "detect[] a potential security threat" such as a "website built by hackers with malicious intent" and "block[] access" to protect "your organization and you from malware infections and other harm." On information and belief, each request is analyzed to determine "good" (allow) and "bad: (block). Indeed, Forcepoint "analyzes millions of websites every hour, putting them into more than 90 categories in over 50 languages and inspecting them for malicious content." If "you've been denied access to a website because of Forcepoint, your organization is using our technology to apply its Internet use policy."



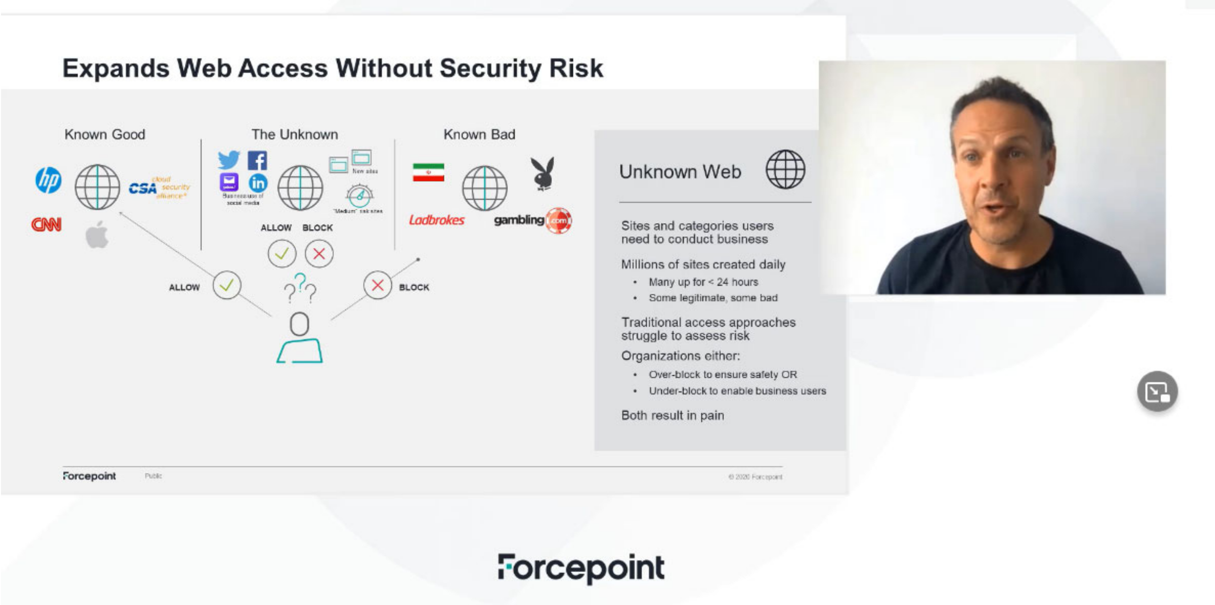
(*See* https://www.forcepoint.com/cyberinc.)



Selective Isolation Enables a Seamless, Progressive Rollout

Isla 6 includes new Selective Isolation capabilities which allow for a fast, simple deployment by offering easy administrative control over what traffic needs to be isolated. Traffic segmentation can be based on the category of traffic, risk levels and aligned with the organization's risk appetite and policies. For example, users attempting to visit an online gambling or other suspicious site can be blocked or redirected to the site through an isolated browser to ensure nothing malicious can be downloaded or sent to the device.

(*See* https://www.businesswire.com/news/home/20210218005375/en/Cyberinc-Introduces-Isla-Isolation-Platform-6-With-Smart-Isolation-Setting-a-New-Standard-in-Security-and-a-Seamless-User-Experience.)



Expands Web Access Without Security Risk

Unknown Web

Sites and categories users need to conduct business

Millions of sites created daily
- Many up for < 24 hours
- Some legitimate, some bad

Traditional access approaches struggle to assess risk

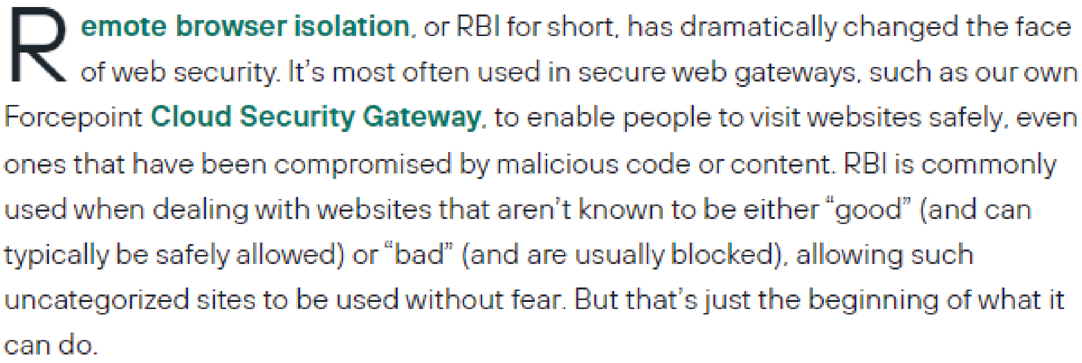
Organizations either:
- Over-block to ensure safety OR
- Under-block to enable business users

Both result in pain

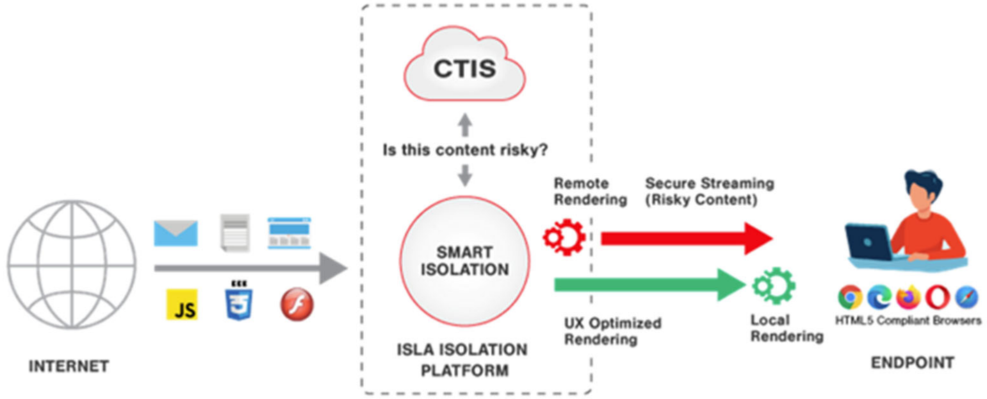
Forcepoint Public © 2020 Forcepoint

Forcepoint

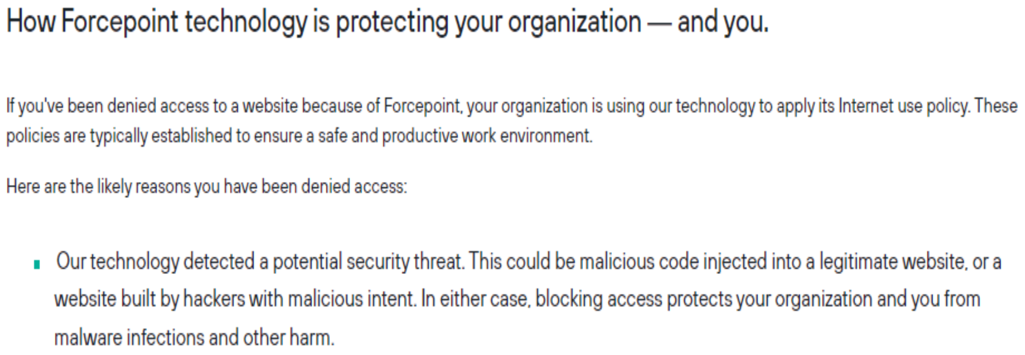
(*See* https://www.forcepoint.com/form/thank-you-your-interest-webcast?form_id=1427&resource=36739&category=webcasts.)



Remote browser isolation, or RBI for short, has dramatically changed the face of web security. It's most often used in secure web gateways, such as our own Forcepoint **Cloud Security Gateway**, to enable people to visit websites safely, even ones that have been compromised by malicious code or content. RBI is commonly used when dealing with websites that aren't known to be either "good" (and can typically be safely allowed) or "bad" (and are usually blocked), allowing such uncategorized sites to be used without fear. But that's just the beginning of what it can do.



(*See* https://www.forcepoint.com/blog/insights/forcepoint-acquires-cyberinc-rbi at page 02.)



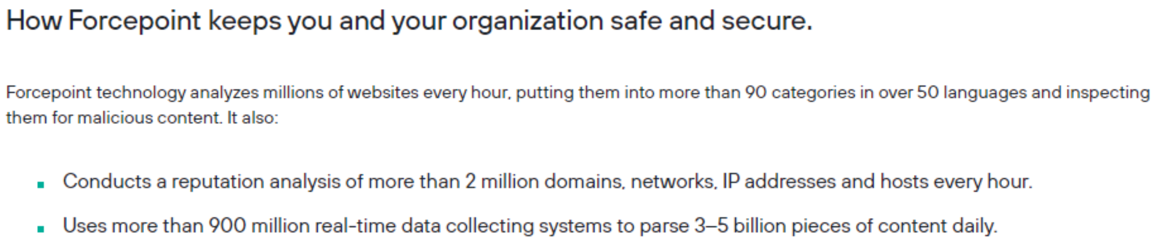
How Forcepoint technology is protecting your organization — and you.

If you've been denied access to a website because of Forcepoint, your organization is using our technology to apply its Internet use policy. These policies are typically established to ensure a safe and productive work environment.

Here are the likely reasons you have been denied access:

- Our technology detected a potential security threat. This could be malicious code injected into a legitimate website, or a website built by hackers with malicious intent. In either case, blocking access protects your organization and you from malware infections and other harm.

(*See* https://www.forcepoint.com/company/blocked-by-forcepoint at page 01.)



How Forcepoint keeps you and your organization safe and secure.

Forcepoint technology analyzes millions of websites every hour, putting them into more than 90 categories in over 50 languages and inspecting them for malicious content. It also:

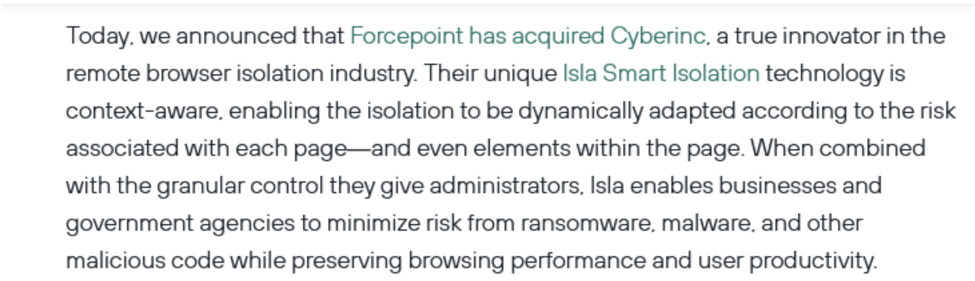
- Conducts a reputation analysis of more than 2 million domains, networks, IP addresses and hosts every hour.
- Uses more than 900 million real-time data collecting systems to parse 3–5 billion pieces of content daily.

(*See* https://www.forcepoint.com/company/blocked-by-forcepoint at page 01.)

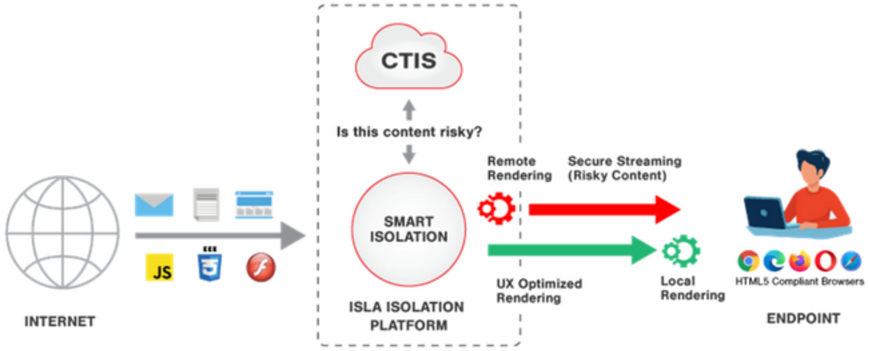
211. The Accused Products perform a method that includes *when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers* and *receiving, at the protection agent on a remote computer, web content from the one or more web servers, wherein web content comprises data for assembling a web page, and wherein the web content is received in response to the request*. As one example "Smart Isolation fetches…all pages remotely." (https://staging.cyberinc.com/wp-content/uploads/2021/03/isla-

smart-isolation-datasheet-1.pdf.) As explained above, "[w]ith RBI, web traffic is automatically redirected through an isolated browser in a secure container. There, potentially risky web content can be rendered with the results sent to the user as a safe stream of pixels, providing a familiar, native browser experience." (*See* https://www.forcepoint.com/blog/insights/remote-browser-isolation-higher-level-web-security at page 01.)

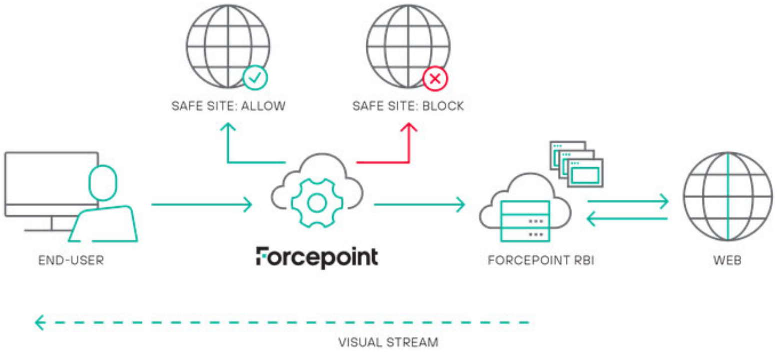
212. In addition, Forcepoint's RBI "adapts the browsing experience with dynamic risk assessment, powered by Cyberinc Threat Intelligence Service, to remotely fetch and execute web pages and safely render them according to risk levels." RBI "adapts web rendering according to the risk levels of the page or web element with two complementary approaches to rendering" including "Secure Streaming model" that "renders elements remotely and securely streams harmless pixels to the endpoint to offer the strongest possible security" and "UX Optimized model" that "intelligently renders harmful pages and web elements remotely while rendering the less harmful pages and elements locally to balance native user experience and security." (*See* https://www.businesswire.com/news/home/20210218005375/en/Cyberinc-Introduces-Isla-Isolation-Platform-6-With-Smart-Isolation-Setting-a-New-Standard-in-Security-and-a-Seamless-User-Experience.)



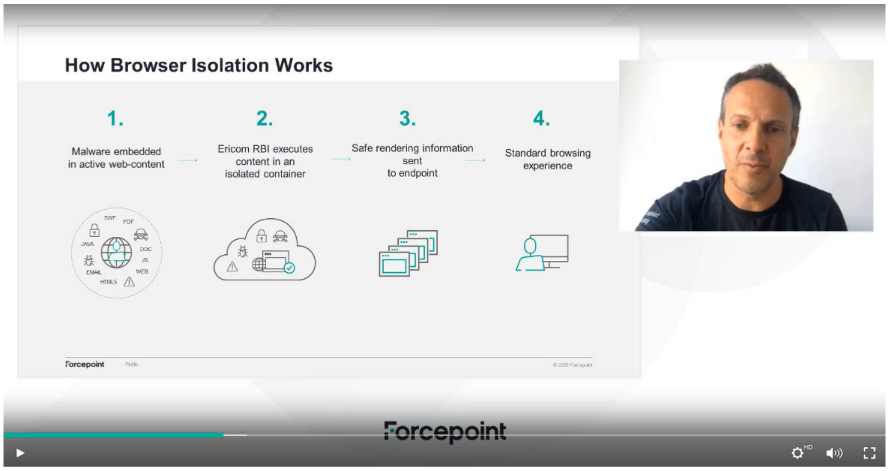
Today, we announced that Forcepoint has acquired Cyberinc, a true innovator in the remote browser isolation industry. Their unique Isla Smart Isolation technology is context-aware, enabling the isolation to be dynamically adapted according to the risk associated with each page—and even elements within the page. When combined with the granular control they give administrators, Isla enables businesses and government agencies to minimize risk from ransomware, malware, and other malicious code while preserving browsing performance and user productivity.



(*See* https://www.forcepoint.com/blog/insights/forcepoint-acquires-cyberinc-rbi.)



(*See* https://www.forcepoint.com/cyberinc.)



How Browser Isolation Works

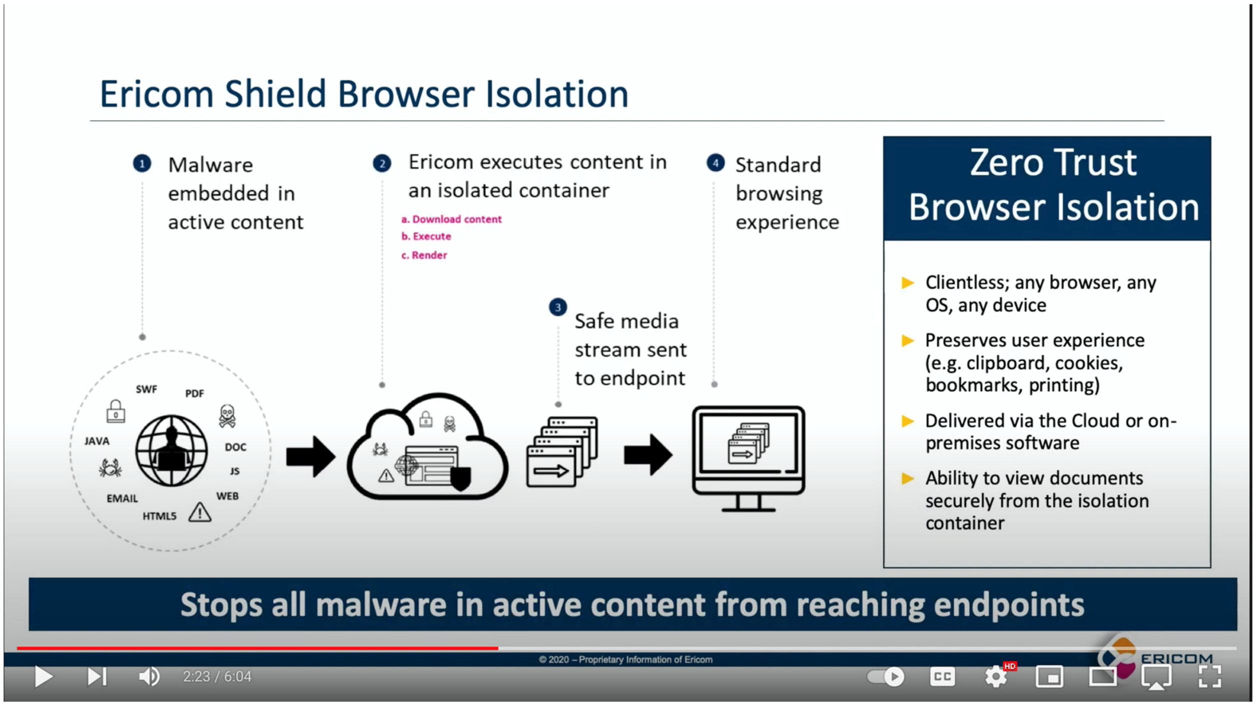
1. Malware embedded in active web-content

2. Ericom RBI executes content in an isolated container

3. Safe rendering information sent to endpoint

4. Standard browsing experience

(*See* https://www.forcepoint.com/form/thank-you-your-interest-webcast?form_id=1427&resource=36739&category=webcasts.)



Ericom Shield Browser Isolation

1 Malware embedded in active content

2 Ericom executes content in an isolated container

a. Download content
b. Execute
c. Render

3 Safe media stream sent to endpoint

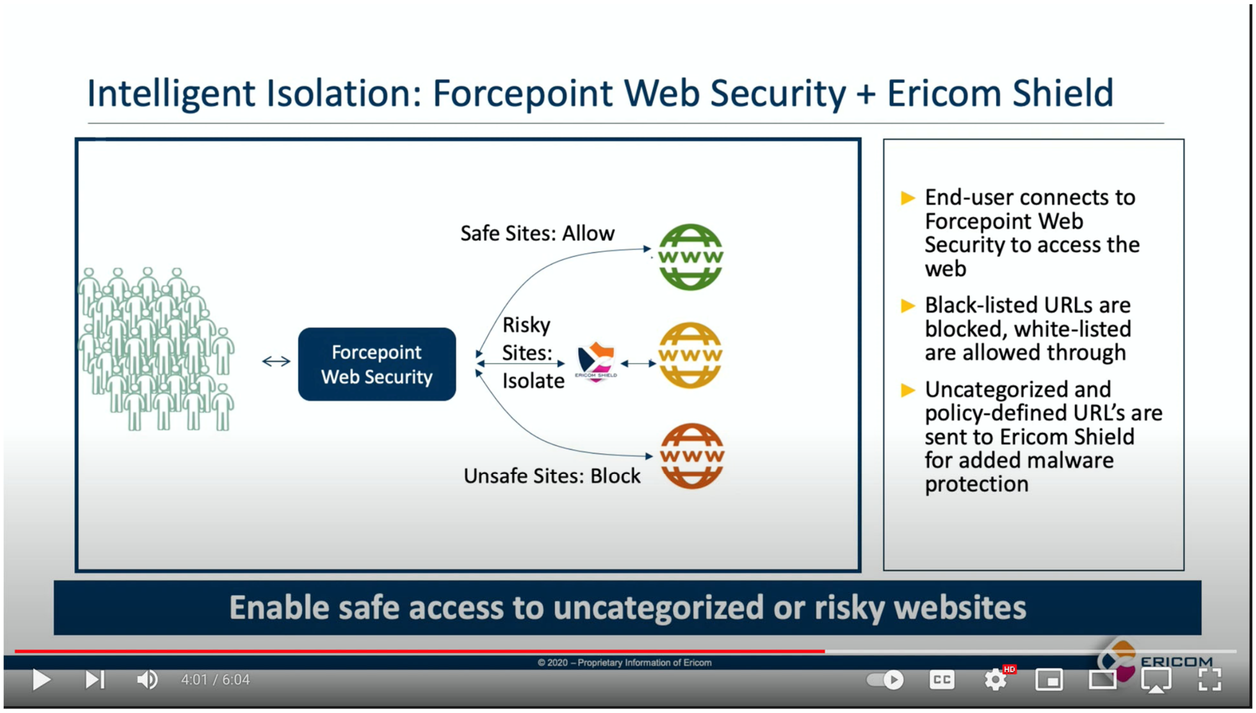
4 Standard browsing experience

Zero Trust Browser Isolation

- Clientless; any browser, any OS, any device
- Preserves user experience (e.g. clipboard, cookies, bookmarks, printing)
- Delivered via the Cloud or on-premises software
- Ability to view documents securely from the isolation container

Stops all malware in active content from reaching endpoints

© 2020 – Proprietary Information of Ericom



Intelligent Isolation: Forcepoint Web Security + Ericom Shield

Forcepoint Web Security

Safe Sites: Allow

Risky Sites: Isolate

Unsafe Sites: Block

- End-user connects to Forcepoint Web Security to access the web
- Black-listed URLs are blocked, white-listed are allowed through
- Uncategorized and policy-defined URL's are sent to Ericom Shield for added malware protection

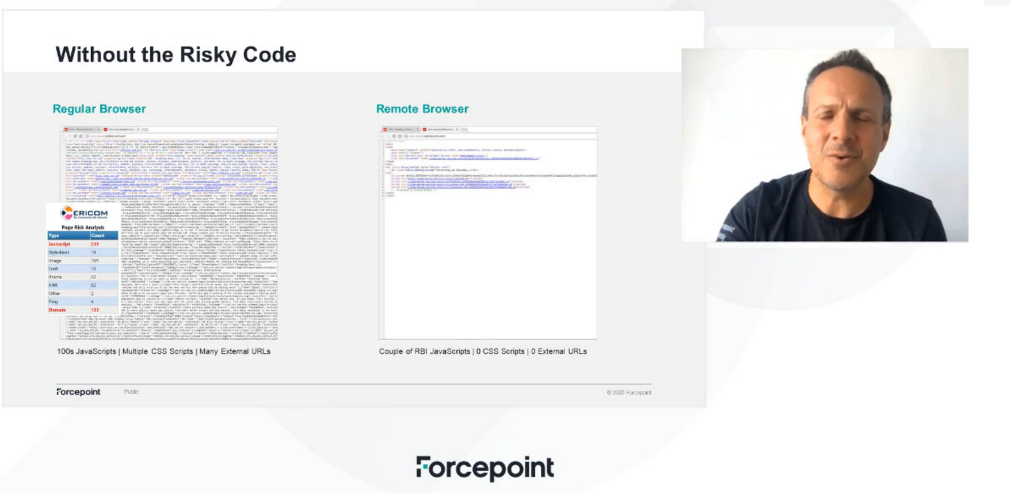
Enable safe access to uncategorized or risky websites

© 2020 – Proprietary Information of Ericom

(*See* https://www.youtube.com/watch?v=1R0J2LPT1R8.)

213. The Accused Products perform a method that includes *when the request is not associated with known malicious content: . . . identifying, by the protection agent, a malware threat within the web content* and *in response to identifying the malware threat, modifying, by the protection agent, the web content, wherein modifying the web content comprises modifying the web content at protocol level to remove the malware threat from the web content.* As explained above, RBI detects "a potential security threat" such as "malicious code injected into a legitimate website." (*See* https://www.forcepoint.com/company/blocked-by-forcepoint at page 01.) The Accused Products also include "Smart Isolation technology," which is "context-aware, enabling the isolation to be dynamically adapted according to the risk associated with each page—and even elements within the page." For example, RBI "adapts web rendering according to the risk levels of the page or web element with two complementary approaches to rendering" including "Secure Streaming model" that "renders elements remotely and securely streams harmless pixels to the

endpoint to offer the strongest possible security" and "UX Optimized model" that "intelligently renders harmful pages and web elements remotely while rendering the less harmful pages and elements locally to balance native user experience and security." (*See* https://www.businesswire.com/news/home/20210218005375/en/Cyberinc-Introduces-Isla-Isolation-Platform-6-With-Smart-Isolation-Setting-a-New-Standard-in-Security-and-a-Seamless-User-Experience.) The Accused Products modify the web content, such as by removing "Javascripts," "CSS scripts," and "URLs."



Without the Risky Code

Page Risk Analysis

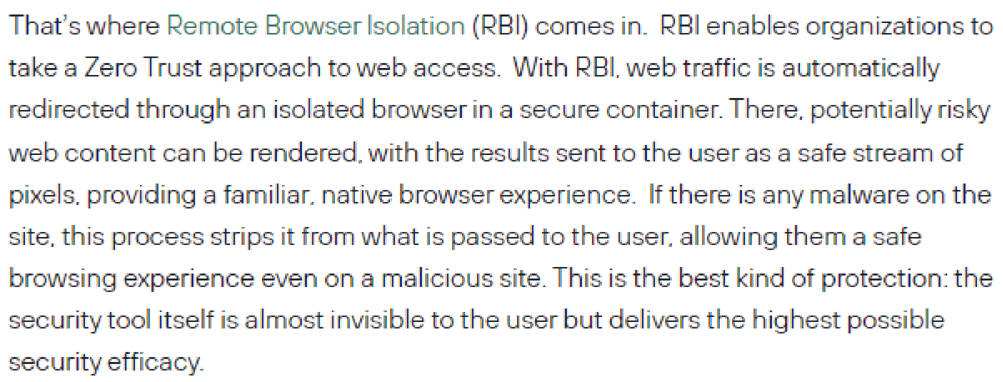
Type	Count
Javascript	239
Stylesheet	19
Image	169
Font	10
Iframe	22
XHR	82
Other	2
Ping	4
Domain	133

100s JavaScripts | Multiple CSS Scripts | Many External URLs

Couple of RBI JavaScripts | 0 CSS Scripts | 0 External URLs

(*See* https://www.forcepoint.com/form/thank-you-your-interest-webcast?form_id=1427&resource=36739&category=webcasts.)

214. Indeed, "[i]f there is any malware on the site, this process strips it from what is passed to the user, allowing them a safe browsing experience even on a malicious site."



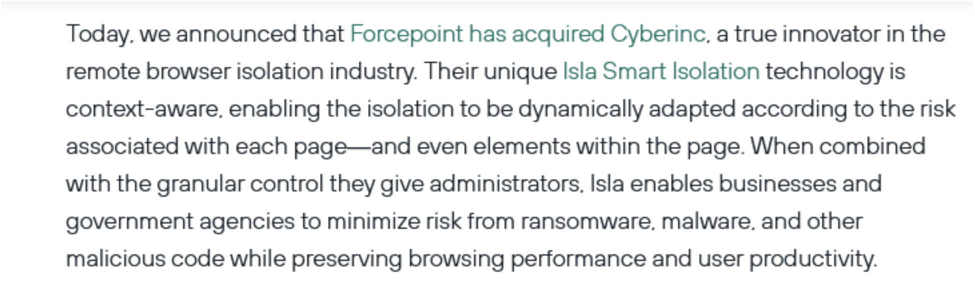
That's where Remote Browser Isolation (RBI) comes in. RBI enables organizations to take a Zero Trust approach to web access. With RBI, web traffic is automatically redirected through an isolated browser in a secure container. There, potentially risky web content can be rendered, with the results sent to the user as a safe stream of pixels, providing a familiar, native browser experience. If there is any malware on the site, this process strips it from what is passed to the user, allowing them a safe browsing experience even on a malicious site. This is the best kind of protection: the security tool itself is almost invisible to the user but delivers the highest possible security efficacy.

(*See* https://www.forcepoint.com/blog/insights/remote-browser-isolation-higher-level-web-security at page 01.)

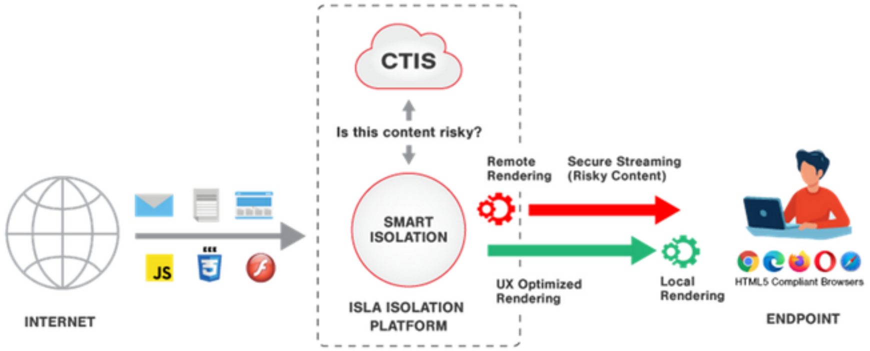
215. The Accused Products perform a method that includes *when the request is not associated with known malicious content: . . . assembling, by the protection agent, a modified version of the web page, wherein the modified web page is assembled using the modified web content, and wherein the modified version of the web page does not comprise the malware threat* and *providing, by the protection agent, the modified version of the web page to the web browser application on the remote computer for rendering and display*. As explained above, "[w]ith RBI, web traffic is automatically redirected through an isolated browser in a secure container. There, potentially risky web content can be rendered with the results sent to the user as a safe stream of pixels, providing a familiar, native browser experience." (*See* https://www.forcepoint.com/blog/insights/remote-browser-isolation-higher-level-web-security at page 01.)

216. In addition, Forcepoint's RBI "adapts the browsing experience with dynamic risk assessment, powered by Cyberinc Threat Intelligence Service, to remotely fetch and execute web pages and safely render them according to risk levels." RBI "adapts web rendering according to the risk levels of the page or web element with two complementary approaches to rendering" including "Secure Streaming model" that "renders elements remotely and securely streams

harmless pixels to the endpoint to offer the strongest possible security" and "UX Optimized model" that "intelligently renders harmful pages and web elements remotely while rendering the less harmful pages and elements locally to balance native user experience and security." (*See* https://www.businesswire.com/news/home/20210218005375/en/Cyberinc-Introduces-Isla-Isolation-Platform-6-With-Smart-Isolation-Setting-a-New-Standard-in-Security-and-a-Seamless-User-Experience.)

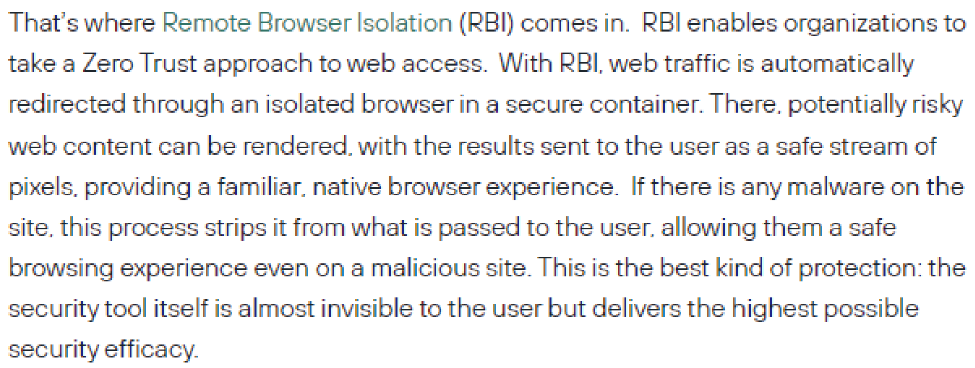


Today, we announced that Forcepoint has acquired Cyberinc, a true innovator in the remote browser isolation industry. Their unique Isla Smart Isolation technology is context-aware, enabling the isolation to be dynamically adapted according to the risk associated with each page—and even elements within the page. When combined with the granular control they give administrators, Isla enables businesses and government agencies to minimize risk from ransomware, malware, and other malicious code while preserving browsing performance and user productivity.



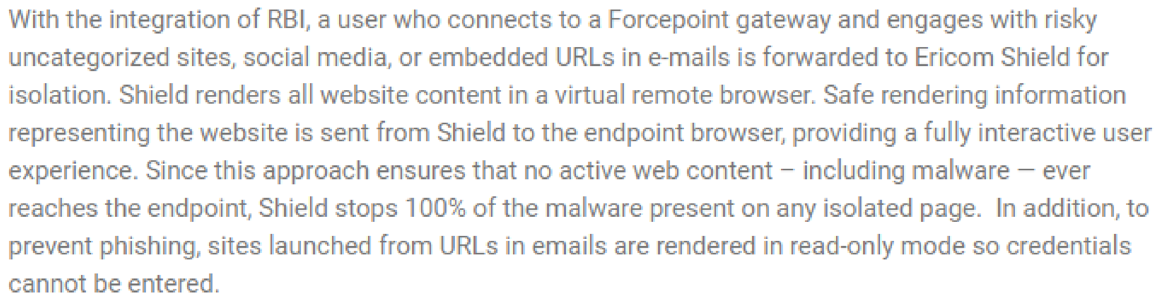
(*See* https://www.forcepoint.com/blog/insights/forcepoint-acquires-cyberinc-rbi.)

217. Moreover, "[i]f there is any malware on the site, this process strips it from what is passed to the user, allowing them a safe browsing experience even on a malicious site." "Safe rendering information representing the website is sent from [the RBI] to the endpoint browser, providing a fully interactive user experience" that "ensures no active web content—including malware—every reaches the endpoint."



That's where Remote Browser Isolation (RBI) comes in. RBI enables organizations to take a Zero Trust approach to web access. With RBI, web traffic is automatically redirected through an isolated browser in a secure container. There, potentially risky web content can be rendered, with the results sent to the user as a safe stream of pixels, providing a familiar, native browser experience. If there is any malware on the site, this process strips it from what is passed to the user, allowing them a safe browsing experience even on a malicious site. This is the best kind of protection: the security tool itself is almost invisible to the user but delivers the highest possible security efficacy.

(*See* https://www.forcepoint.com/blog/insights/remote-browser-isolation-higher-level-web-security at page 01.)



With the integration of RBI, a user who connects to a Forcepoint gateway and engages with risky uncategorized sites, social media, or embedded URLs in e-mails is forwarded to Ericom Shield for isolation. Shield renders all website content in a virtual remote browser. Safe rendering information representing the website is sent from Shield to the endpoint browser, providing a fully interactive user experience. Since this approach ensures that no active web content – including malware — ever reaches the endpoint, Shield stops 100% of the malware present on any isolated page. In addition, to prevent phishing, sites launched from URLs in emails are rendered in read-only mode so credentials cannot be entered.

(*See* https://blog.ericom.com/Browser-Isolation-as-a-Key-Part-of-a-Blueprint-for-SASE-Success/ at page 02.)

218. Each claim in the '928 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '928 Patent.

219. Forcepoint has been aware of the '928 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '928 Patent, including on its web site, since at least July 2020.

220. Forcepoint directly infringes at least claim 1 of the '928 Patent, literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, the Forcepoint performs a method in an infringing manner as described above by

running the Accused Products to protect its own computer and network operations. On information and belief, the Forcepoint performs a method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Forcepoint performs the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

221. Forcepoint's partners, customers, and end users of the Accused Products and corresponding systems and services directly infringe at least claim 1 of the '928 Patent, literally or under the doctrine of equivalents, at least by performing the claimed methods when using the Accused Products and corresponding systems and services, as described above.

222. Forcepoint actively induced and is actively inducing infringement of at least claim 1 of the '928 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, Forcepoint encourages and induces customers to use Forcepoint's security software in a manner that infringes claim 1 of the '928 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 activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of its Accused Products, including Remote Browser Isolation software, SaaS model, and services in the United States. (*See, e.g.*, Forcepoint, *Configure Remote Browser Isolation*, https://www.websense.com/content/support/library/web/hosted/admin_guide/rbi_support.aspx.)

223. Forcepoint encourages, instructs, directs, and/or requires third parties—including its partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

224. Forcepoint further encourages and induces its customers to infringe claim 1 of the

’928 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, including Gateway Protection software, SaaS model, and services in the United States. (*See, e.g.*, Forcepoint, *Configure Remote Browser Isolation*, https://www.websense.com/content/support/library/web/hosted/admin_guide/rbi_support.aspx.)

225. For example, on information and belief, Forcepoint 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. (*See* Forcepoint, *Configure Remote Browser Isolation*, https://www.websense.com/content/support/library/web/hosted/admin_guide/rbi_support.aspx.) On further information and belief, Forcepoint also provides customer service or technical support to purchasers of the Accused Products and corresponding system and services, which directs and encourages customers to perform certain actions as a condition to use the Accused Products in an infringing manner. (*Id.*)

226. Forcepoint and/or its partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Forcepoint and/or a Forcepoint partner, which obligates each customer to perform certain actions as a condition to use of the Accused Products. Further, in order to receive the benefit of Forcepoint’s and/or its partners continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the ’928 Patent.

Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Forcepoint 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 '844 Patent.

227. Forcepoint also contributes to the infringement of its partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the claimed methods, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the '928 Patent.

228. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to Forcepoint. For example, on information and belief, Forcepoint directs and/or controls the activities or actions of its partners in connection with the Accused Products by contractual agreement or otherwise requiring partners to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. Forcepoint further directs and/or controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the method steps of at least claim 1 of the '928 Patent.

229. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant's infringement of the '928 Patent. Defendant is therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for

Defendant’s infringement, but no less than a reasonable royalty.

230. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendant, its agents, employees, representatives, and all others acting in concert with Defendant from infringing the ’928 Patent. On information and belief, Plaintiffs have lost potential customers, business opportunities, and goodwill in the community. Plaintiffs will continue to suffer these harms absent an injunction.

231. Defendant’s infringement of the ’928 Patent is knowing and willful. On information and belief, Defendant had actual knowledge of the ’928 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the ’928 Patent from at least the date Plaintiffs marked its products with the ’928 Patent and/or provided notice of the ’928 Patent on its website.

232. On information and belief, despite Defendant’s knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant’s continued infringement of the ’928 Patent with knowledge of the ’928 Patent constitutes willful infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request 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 Plaintiffs to compensate them for Defendant’s past infringement of the Asserted Patents, through the date of trial in this action;

c) That this Court award pre- and post-judgment interest on such damages to Plaintiffs;

d) That this Court order an accounting of damages incurred by Plaintiffs 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 Plaintiffs their costs and attorneys' fees incurred in this action;

f) That this Court award increased damages under 35 U.S.C. § 284;

g) That this Court preliminarily and permanently enjoin Defendant from infringing any of the Asserted Patents;

h) That this Court order Defendant to:

(i) recall and collect from all persons and entities that have purchased any and all products found to infringe any of the Asserted Patents that were made, offered for sale, sold, or otherwise distributed in the United States by Defendant or anyone acting on their behalf;

(ii) destroy or deliver all such infringing products to Plaintiffs;

(iii) revoke all licenses to all such infringing products;

(iv) disable all web pages offering or advertising all such infringing products;

(v) destroy all other marketing materials relating to all such infringing products;

(vi) disable all applications providing access to all such infringing software; and

(vii) destroy all infringing software that exists on hosted systems,

i) That this Court, if it declines to enjoin Defendant from infringing any of the Asserted Patents, award damages for future infringement in lieu of an injunction; and

j) That this Court award such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully requests a trial by jury on all issues triable thereby.

DATED: March 31, 2022

By:*/s/ Jeffrey D. Mills*
Jeffrey D. Mills
Texas Bar No. 24034203
KING & SPALDING LLP
500 West Second St.
Suite 1800
Austin, Texas 78701
Telephone: (512) 457-2027
Facsimile: (512) 457-2100
jmills@kslaw.com

Christopher C. Campbell (D.C. Bar No. 444262)
Patrick M. Lafferty *(pro hac vice to be filed)*
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
Telephone: (202) 626-5578
Facsimile: (202) 626-3737
ccampbell@kslaw.com
plafferty@kslaw.com

Britton F. Davis *(pro hac vice to be filed)*
Brian Eutermoser (*pro hac vice to be filed)*
KING & SPALDING LLP
1401 Lawrence Street
Suite 1900.
Denver, CO 80202
Telephone: (720) 535-2300
Facsimile: (720) 535-2400
bfdavis@kslaw.com
beutermoser@kslaw.com

Steve Sprinkle
Texas Bar No. 00794962
SPRINKLE IP LAW GROUP, P.C.
1301 W. 25th Street, Suite 408
Austin, Texas 78705
Telephone: (512) 637-9220
ssprinkle@sprinklelaw.com

Mark D. Seigmund
STECKLER WAYNE CHERRY & LOVE, PLLC
8416 Old McGregor Road
Waco, Texas 76712
Telephone: (254) 651-3690
Facsimile: (254) 651-3689
mark@swclaw.com

Attorneys for Plaintiffs Open Text, Inc. and Webroot, Inc.