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

Webroot, Inc. and Open Text, Inc., ***Plaintiffs,*** **v.** **Trend Micro, Inc.** ***Defendant.***	**Civil Action No.** **6:22-cv-00239-ADA** **JURY TRIAL DEMANDED**
Trend Micro, Inc. ***Counterclaim-Plaintiff,*** **v.** **Webroot, Inc., Open Text, Inc., and Open Text Corp.,** ***Counterclaim-Defendants.***	

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Webroot, Inc. ("Webroot") and Open Text, Inc. ("OpenText") (collectively "Plaintiffs") allege against Trend Micro Inc. ("Trend Micro" 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.

IPR2023-00657
Open Text Inc. EX-2017

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 as an update to a "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 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 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. For example, 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 methods of "on execution" malware analysis; new architectures that efficiently and effectively distribute workloads across the network; new forensic techniques that enable fast, efficient, and accurate analysis of malware attacks; and new advanced memory scanning techniques.

10. Plaintiffs' patented technology makes security software, platforms, and appliances 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 (*e.g.*, not requiring downloading and using full signature databases and time-consuming virus scans).

11. Plaintiff Webroot has implemented this 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 and other innovations, including U.S. Patent No. 8,418,250 (the "'250 Patent"), U.S. Patent No. 8,726,389 (the "'389 Patent"), U.S. Patent No. 9,578,045 (the "'045 Patent"), U.S. Patent No. 10,257,224 (the "'224 Patent"), U.S. Patent No. 10,284,591 (the "'591 Patent"); U.S. Patent No. 10,599,844 (the "'844 Patent"); U.S. Patent No. 11,409,869 (the "'869 Patent"); U.S. Patent No. 8,856,505 (the "'505 Patent"); U.S. Patent No. 8,201,243 (the "'243 Patent"); U.S. Patent No. 8,719,932 (the "'932 Patent"); and U.S. Patent No. 8,181,244 (the "'244 Patent") (Exhibits 1-11.).

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 Trend Micro, Inc. is a direct competitor of Webroot and provides security software and systems that, without authorization, implement Plaintiffs' patented technologies. Trend Micro's infringing security software includes, but is not limited to, Apex One, Apex Central, Smart Protection Network, Deep Discovery XDR—Detection and response, Deep Discovery Endpoint Sensor, DeepSecurity, and Cloud One-Workload Security, (collectively, "Trend Micro Security Suite" or "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 '250, '389, '045, '224, '591,'844, '869, '505 '243, '932, and '244 Patents (collectively the "Asserted Patents"). As a result of Trend Micro's unlawful competition in this judicial 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. Plaintiff brings claims under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*, for 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 one or more of 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 this District including employees in engineering, customer support, legal and compliance teams, IT, and corporate development. OpenText also has a data center located in this District. OpenText is in the computer systems design and services industry. OpenText sells and services software in the United States.

23. Defendant Trend Micro, Inc. is a Texas corporation with its corporate headquarters and principal place of business at 225 E John Carpenter Fwy Ste 1500, Irving, Texas, 75062. Trend

Micro maintains an additional Texas office at 11305 Alterra Pkwy, Austin, Texas 78758. Trend Micro is registered with the Secretary of State to conduct business in Texas.

JURISDICTION & VENUE

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 Trend Micro because it 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 Trend Micro has, either directly and through its extensive network of partnerships including those with local IT service providers, purposefully 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.*, WBR_TMC000006, *Find a Trend Micro Partner*, https://www.trendmicro.com/en_us/partners/find-a-partner.html.)

27. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because, upon information and belief, Defendant Trend Micro regularly conducts business within this District and has continuous and systematic contacts with this District, such as by maintaining a regular and established place of business in this District. Trend Micro has also committed acts of infringement in this District. Moreover, on November 16, 2020, Trend Micro admitted this district is a proper forum for venue. *See Invicta Networks, Inc. v. Trend Micro Inc.*, Case No. 6:20-cv-00766-ADA, Dkt. 9 at 2. (Nov. 16, 2020).

28. On information and belief, Trend Micro 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. Trend Micro's operations in this District include client outreach and sales for each of the Accused Products. As detailed above, Trend Micro has customer-facing project managers in this District. Trend Micro also provides technical support to partners and customers located in this District, including from its office in the District.

30. In addition, Trend Micro Security Suite's End User License Agreements all reference Trend Micro Inc. as the rights-holder under the contract. (*See* WBR_TMC020098, Trend Micro End User License Agreement § 30, www.trendmicro.com/en_us/about/legal.html?modal=en-english-mulitcountry-consumer-eula.pdf.) Thus, Trend Micro has entered into license agreements with end-users covering the Accused Products in Texas and in this District.

31. On information and belief, Trend Micro uses and/or tests the Accused Products in this District, including at its offices in this District. For example, Trend Micro advertises itself as a customer of its own products. (*See* WBR_TMC000003, "Trend Micro Uses Deep Security Smart Check to Automate Secure DevOps" https://www.contentree.com/caseStudy/trend-micro-uses-deep-security-smart-check-to-automate-secure-devops_273515.) Additionally, on information and belief, Trend Micro maintains servers in this District that operate Trend Micro's products that practice the Asserted Patents. (*See, e.g.*, WBR_TMC007093, https://officesnapshots.com/2017/09/11/trend-micro-offices-austin.) Trend Micro's use, operation and testing of the Accused Products are acts of infringement occurring in this District.

32. Trend Micro further sells, offers for sale, advertises, makes, installs, maintains, and/or otherwise provides endpoint security software and security services, including the Accused

Products, the use of which infringes the Asserted Patents in this District. Trend Micro performs these infringing acts directly in this District.

33. Trend Micro also performs these infringing acts through other entities such as re-sellers, managed service providers and cybersecurity experts located in this District, including for example, through its "partners." (*See* WBR_TMC000006, *Find a Trend Micro Partner*, https://www.trendmicro.com/ en_us/partners/find-a-partner.html.)

34. 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 of equivalents, including the provision of, use, operation, sales, offering for sale, installation, maintenance and advertising of the Trend Micro Security Suite. Trend Micro also infringes (directly or indirectly) the Asserted Patents by using, offering for sale, selling, installing, maintaining, operating, providing instructions, and/or advertising Trend Micro's Security Suite including the Accused Products within this District, either literally or under the doctrine of equivalents.

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

36. Defendant Trend Micro encourages and induces third parties including partners and customers to use the Accused Products in any infringing way at least by making Trend Micro's security services available for download or purchase, widely advertising those services, providing applications that allow partners and users to access those 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.*, Trend Micro, *Contact Support - North America*, https://success.trendmicro.com/contact-support-north-

america.)

37. Defendant Trend Micro also contributes to the infringement of its customers and end users of the Accused Products by offering to sell or selling 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, 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.

38. 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

39. 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.

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

Advanced Malware Detection Patents
U.S. Patent Nos. 8,418,250 and 8,726,389

41. The ’250 and ’389 Patents are part of the same patent family and generally disclose and claim systems and processes related to real-time and advanced classification techniques for as-yet unknown malware. These patents are collectively known as the “Advanced Malware Detection” Patents. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’250 and ’389 Patents. Webroot has granted Plaintiff OpenText an exclusive license to the ’250 and ’389 Patents.

42. The ’250 Patent is entitled “Methods and Apparatus for Dealing with Malware,” was filed on June 30, 2006, and duly and legally issued by the United States Patent and Trademark Office (“USPTO”) on April 9, 2013. The ’250 Patent claims priority to Foreign Application No. 0513375.6 (GB), filed on June 30, 2005. A true and correct copy of the ’250 Patent is attached as Exhibit 1.

43. The ’389 Patent is also entitled “Methods and Apparatus for Dealing with Malware,” was filed on July 8, 2012, and was duly and legally issued by the USPTO on May 13, 2014. The ’389 Patent claims priority to the same Foreign Application as the ’250 Patent. A true and correct copy of the ’389 Patent is attached as Exhibit 2.

44. Malware detection systems in use at the time the Advanced Malware Detection Patents were 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.

45. 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 2, '389 Patent, 2:9-17.)

46. 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.

47. 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. (*Id.*) 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 2, '389 Patent, 2:9-23, 2:63-67.)

48. By contrast, the methods and systems disclosed and claimed in the '250 and '389 Patents 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.

49. 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 2, '389 Patent, 3:14-24; Exhibit 1, '250 Patent, 3:7-18.) 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, '250 Patent, 3:11-18.)

50. The approaches in the Advanced Malware Detection Patents 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. 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. (WBRT001252 at 1663-1664, '250 Patent Prosecution History, 2010-09-07 Amendment at 16-17.)

51. Each of the claimed inventions of the Advanced Malware Detection Patents 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 Advanced Malware Detection Patents improve 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, ’250 Patent, 2:5-3:18.)

52. In particular, the ‘250 Patent describes and claims methods and systems that include receiving *behavioral data about or associated with a computer object* from remote computers on which the object or similar objects are stored; comparing in a base computer the data about the computer object received from the remote computers; and, classifying the computer object as malware on the basis of said comparison if the data indicates the computer object is malware. In effect, this process builds a central picture of objects and their interrelationships and activities across the entire community and allows automation of the process of identifying malware by aggregating and comparing the activity of objects running across the community (*i.e.*, on multiple remote computers).

53. The ’250 Patent further provides that a mask is automatically generated for an object that defines “acceptable behavior” for the object. The operation of the computer object is then monitored and if the actual monitored behavior extends beyond that permitted by the mask, the object is disallowed from running and reclassified as malware.

54. The claimed methods and systems of the ’250 Patent constitute technical improvements over the traditional anti-malware systems and provide numerous advantages to computer systems and the process of detecting malware. In addition to the advantages set forth above, the methods and systems claimed in the ’250 Patent provide additional advantages in dealing with objects that do not initially exhibit suspicious behavior, but later start to exhibit malevolent behavior. Traditional malware systems could only mark a computer object as good or bad (*i.e.*, a binary decision), and did so by examining the signature of the object itself against a

database of "known bad" signatures. This approach does not permit the system to automatically deal with the case where an object does not initially exhibit suspicious behavior but starts to exhibit malevolent behavior in the future.

55. By contrast, the '250 Patent improves these systems by generating an appropriate behavior mask for the object and then continuing to monitor the behavior of the object. If the object operates out of bounds of the permitted behavior, then an appropriate action is taken, such as disallowing the computer object from running and reclassifying the object as malware. Thus, the systems and methods described and claimed further the operation and security of the network by stopping an object from running and changing the classification of an object in real-time when unacceptable behavior is identified. (*See* Exhibit 1, '250 Patent, 3:47-50; 4:19-30.)

56. Furthermore, the methods and systems claimed in the '250 Patent, including generating a "mask" of acceptable behavior, allowing an object to run, continuing to monitor the object, and disallowing/reclassifying the object if the behavior extends beyond that permitted by the mask, are not routine or conventional. For example, while a "safe," mask-permitted version of notepad.exe "would not be expected to perform a wide variety of events, such as transmitting data to another computer or running other programs or running other programs" a "modified" and potentially "malevolent" version of notepad.exe could perform those unexpected events. (*See* Exhibit 1, '250 Patent, 11:27-41.) Unlike traditional malware systems that would have already made a binary determination that the notepad.exe object is safe, the methods and systems of the '250 Patent re-classify that version of notepad.exe as malware when its behavior becomes unexpected and "extends beyond that permitted by the mask." (*Id.* at 4:19-30.)

57. The applicants provided another example illustrating the unconventional nature and technical advantages and improvements, offered by the claimed systems and methods during

prosecution:

> As an example, suppose a new version of Internet Explorer appeared. This could be a legitimate update to Internet Explorer released by Microsoft or alternatively it could be a file infected with a virus. In the prior art, the new object would have an unknown signature, so an in-house analyst would laboriously analyse the new object and determine whether or not it was safe. Whilst this analysis is carried out, the object would either be blocked, which would cause huge inconvenience to users of the new object, or allowed to run, in which case there is a risk of the object performing malevolent acts. In contrast, the present invention would collect data at the base computer from remote computers running the new version of Internet Explorer. Using the information collected, the system could determine that the new object purports to be a new version of Internet Explorer. However, it may not be apparent at this point whether or not the new object is capable of malevolent behaviour. In this scenario the present invention generates an appropriate behavioural mask for the object, e.g. by using a profile of behaviour of previous versions of Internet Explorer that are known not to be malware, or by using a profile for the behaviour appropriate for a web browser. The remote computers are allowed to let the new version run whilst monitoring its behaviour against the mask. The instant the new object exhibits some new, malevolent behaviour, this can be stopped at the remote computer, as well as being flagged to the base computer and used at the base computer to change the classification of the object. Thus, the present invention allows an instant response to an object changing its behaviour to exhibit malevolent behaviour in the future. (*See* WBRT001252 at 1665-1666, ’250 Patent Prosecution History, 2010-09-07 Amendment at 18, 19.)

58. Similarly, 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 2, ’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.

59. Through continuous aggregate analysis of events involving computer objects as they occur across network endpoints, 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.)

60. 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; Exhibit 1, '250 Patent, 3:7-18.)

61. The Advanced Malware Detection Patents provide 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.). These patents all provide 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).

62. The systems and methods claimed in the Advanced Malware Detection Patents 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 claimed inventions in these patents 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.

Forensic Visibility Patents
U.S. Patent No. 9,578,045 and U.S. Patent No. 10,257,224

63. The ’045 and ’224 Patents are part of the same patent family and are each generally directed to providing forensic visibility into computing devices in a communication network by analyzing network events and creating audit trails. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’045 and ’224 Patents. Webroot has granted OpenText an exclusive license to the ’045 and ’224 Patents.

64. The ’045 Patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on May 5, 2014, and was duly and legally issued by the USPTO on February 21, 2017. The ’045 Patent claims priority to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’045 Patent is attached as Exhibit 3.

65. The ’224 Patent is also entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on February 20, 2017 and was duly and legally issued by the USPTO on April 9, 2019. The ’224 Patent claims priority to the ’045 Patent and also to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’224 Patent is attached as Exhibit 4.

66. The ’045 and ’224 Patents describe and claim inventive and patentable subject matter that significantly improves on traditional network forensic tools used to discover or identify security issues on computer networks. Network forensics generally relates to intercepting and

analyzing network events to discover the source of security attacks. (*See* Exhibit 3, ’045 Patent, 1:22-24; Exhibit 4, ’224 Patent, 1:24-26.)

67. The ’045 and ’224 Patents improved on these prior art network forensic tools by providing a technical solution to a technical problem experienced by computer networks and computer network operation. Unlike traditional network forensic tools, these patents create forensic visibility into the computing devices on the communication network to identify malware or other security issues in operation of those devices. (*See* Exhibit 3, ’045 Patent, 2:36-38; Exhibit 4, ’224 Patent, 2:38-40.)

68. In particular, the Forensic Visibility Patents improve network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event in comparison to other events, and generating/transmitting an “event line” that includes information for the event. (*See* Exhibit 3, ’045 Patent, cl. 1; Exhibit 4, ’224 Patent, cl. 1.) The described and claimed systems and methods intercept network events, create audit trails, or contextual states, for each individual event by correlating the event to objects such as their originating processes, devices, and/or users, and establishing a global perspective of the objects. The claimed systems and methods of the Forensic Visibility Patents address an identified weakness in conventional systems and processes; namely the ability to monitor, capture and/or analyze what is occurring at computing devices on a computer network, thereby providing an improved way to address the technical problem of discovering security attacks or security problems within a computer network.

69. In addition to analyzing the behavior of an object to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (*See* Exhibit 3, ’045 Patent, 2:39-45 (“The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in

U.S. application Ser. No. 13/372,375 filed Feb. 13, 2012, 'Methods and Apparatus for Dealing with Malware.'").) In particular, in many cases a potentially malicious object is identified by the system as a result of other events that provide information as to whether the code is malicious. For example, if an object or event under investigation originated from an object or event that is known to be malicious or have malicious behaviors or characteristics, the presence of the known, malicious object provides a further indication that the potentially malicious object or event is malicious as well.

70. The patents further explain that in addition to context information, the systems and techniques can also use information from the network to obtain a global perspective of the network operation. The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or similar objects) that have been identified previously as malicious. Indeed, in the context of modern computers and network systems that generate tens of millions of events every minute, the use of a global perspective and contextual information to correlate an event or object under investigation with prior, related events and objects—including the originating object—significantly improves the ability of the system to identify potential threats.

71. The patents further disclose technical improvements to forensic systems by "assembling" or "generating" an "event line" based on the contextual information—including the correlation to the originating object—and global perspective. (*See, e.g.*, Exhibit 3, '045 Patent, 9:50-58.) The generation of the event line makes it easier for end users to "identify events, and/or instances of malware, that require more immediate attention"—thereby improving the accuracy and efficiency of identifying additional malicious code, as well as enabling administrators to more readily analyze malware, assess vulnerabilities, and correct damage done by the originating objects

(and other objects in the event chain). (*See* Exhibit 3, ’045 Patent, 9:45-49.) The generation and use of an event line itself was, at the time, an unconventional way in which event information, contextual state information, and global perspectives are generated, communicated, and/or potentially displayed to, and interacted with by, an administrator or end user.

72. Thus, the ’224 and ’045 Patents describe and claim systems and methods that provide technical advantages and improvements over traditional network security and forensic systems, including more efficient and accurate identification of malware (*e.g.*, the contextual and global perspective information reduced false negative and positives for malware detection). The described systems and methods also improved the identification of other malware (and corresponding events) that might otherwise go undetected in prior systems, thereby improving system performance and reducing the number of resources required.

73. Indeed, the described systems and methods enable end-to-end forensic visibility into event occurrences across a networked environment and from the bottom of the stack to the top, thereby improving upon conventional network forensic products. (*See* Exhibit 3, ’045 Patent, 2:31-38, 3:49-55; Exhibit 4, ’224 Patent, 2:33-40, 3:52-59; *see also* Exhibit 3, ’045 Patent, 4:36-41; Exhibit 4, ’224 Patent, 4:39-44.)

74. Applicant further explained during prosecution how the generation of contextual state information and obtaining a global perspective—including for objects and events other than those that were detected, such as the originating object—are unconventional steps in the areas of malware detection and network forensics. For example, Applicant explained how the described systems and methods improve the system performance of computing devices:

> In this case, the claimed invention provides for determining correlations between events and objects and creating an audit trail for each individual event. For example, a context analyzer may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. After the analysis is complete, a sensor

> agent may use the correlated data to generate a global perspective for each event such that an administrator is able to forensically track back any event which occurs to what triggered it. Thus, the global perspective represents a drastic transformation of raw event data into a comprehensive, system-wide forensic audit trail. (WBRT005145 at 5274-5275, '045 Patent Prosecution History, 2016-03-16 Amendment at 11-12.)
>
> In this case, examples of the claimed systems and methods provide low level system filters which intercept system events "in a manner such that the operation of the system filter does not impact system performance." Specification, para. [0008]. For example, on an average system, because tens of millions of events take place every minute, the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. Examples of the present systems and methods address this shortcoming by providing a system filter that substantially improves the system performance of the computing devices in the system. (*See* WBRT005145 at 5275, '045 Patent Prosecution History, 2016-03-16 Amendment at 12.)

75. During prosecution, Applicant further explained how the claims are directed to solving a technical problem and a specific improvement in computer functionality relating to computer security:

> ***[T]he claims are directed to solving a technical problem***. Typically, network forensic systems use network forensic tools (e.g., network sniffers and packet capture tools) to detect and capture information associated with communication sessions. Although such network forensic tools are operable to passively collect network traffic, the tools reside at a network edge (e.g., outside of a system or hosts). As a result, the network forensic tools have no ability to obtain useful information within a host or to establish any sort of context from within a host that is generating and/or receiving network events. To address this, aspects of the present disclosure enable methods for providing forensic visibility into systems and networks. For example, a local aggregator/interpreter, context analyzer and sensor agent may provide visibility into occurrences across an environment to ensure that a user (e.g., an administrator) is aware of any system change and data communications in and out of the computing devices residing on the network. During this process, identified events may be correlated to objects, thus creating an audit trial [sic] for each individual event. (*See* WBRT005145 at 5272-5273, '045 Patent Prosecution History, 2016-03-16 Amendment at 9-10 (emphasis added).)
>
> Here, ***the claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing end-to-end***

> ***visibility of events within a system and/or network***. (*See* WBRT006334 at 6791-6792, '224 Patent Prosecution History, 2018-08-29 Amendment at 10-11 (citing '224 Patent specification) (emphasis added).)
>
> The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem. For example: "It is, therefore, one aspect of the present disclosure to provide a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event. For example, a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network." (*See* WBRT006334 at 6793-6794, '224 Patent Prosecution History, 2018-08-29 Amendment at 11-12 (citing '224 Patent specification).)

76. In response to these arguments, the Examiner withdrew a rejection based on 35 U.S.C. § 101 and allowed the claims of the Forensic Visibility Patents to issue. As recognized by the USPTO Examiner, the claimed inventions of the '045 and '224 Patents provide a technical solution to the technical problem of forensic visibility regarding events in a computer network.

US. Patent No. 10,284,591

77. U.S. Patent No. 10,284,591 is entitled "Detecting and Preventing Execution of Software Exploits," was filed on January 27, 2015 and was duly and legally issued by the USPTO on May 7, 2019. The '591 Patent claims priority to provisional application 61/931,772 filed January 27, 2014. A true and correct copy of the '591 Patent is attached as Exhibit 5. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '591 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the '591 Patent.

78. The '591 Patent describes and claims an "anti-exploit" technique to prevent undesirable software and/or other computer exploits from executing. (*See* Exhibit 5, '591 Patent, 1:13-28, 1:32-33.) Computer "exploits" include code, software, data, or commands that take advantage of a bug, glitch, or vulnerability in a computer system. To accomplish this goal, the novel anti-exploit techniques described and claimed in the '591 Patent monitor memory space of

a process for execution of functions and performs "stack walk processing" upon invocation of a function in the monitored memory space. (*Id.* at 1:33-39.) During that stack walk processing, a memory check may be performed to detect suspicious behavior. (*Id.*) If the memory check detects certain types of suspicious behavior, an alert may be triggered that prevents the execution of a payload for the invoked function. (*Id.* at 1:39-48.)

79. The '591 Patent describes and claims unconventional "stack walk processing" techniques for detecting and preventing unwanted software exploits during which memory checks are performed before an address of an originating caller function is reached. The anti-exploit techniques can include performing "memory checks performed during the stack walk processing once an address is reached for an originating caller function." (*See id.* at 8:6-7.) In one embodiment, "memory checks from the lowest level user function of the hooked function down through the address of the originating caller function" may be performed to detect and identify suspicious behavior. (*Id.* at 6:7-11.)

80. The "stack walking" and "memory checks" described and claimed in the '591 Patent are fundamentally rooted in computer technology—in fact, they are processes only performed within a computer context. The techniques described and claimed in the '591 Patent addresses a problem that specifically arises in the realm of computer technology (namely, computer exploit identification) by, *inter alia*, performing memory checks and detection specified behavior during stack walking.

81. The '591 Patent further describes and claims unconventional techniques that address identified weaknesses in conventional exploit prevention technologies. For example, unlike exploit prevention technologies that try to prevent an exploit from ever starting its own shellcode to execute a malicious payload, the '591 Patent describes and claims techniques that

prevent shellcode from executing a malicious payload even if the shellcode has been started. (*See id.* at 6:24-30; *see also id.* at 7:56-62.) Thus, these unconventional techniques address an identified weakness in conventional exploit prevention systems and provide technical advantages including enhanced security protection, improved detection of potential security exploits, reduction in error rate identifying and marking suspicious behavior (*e.g.*, false positives), and improved usability and interaction for users who are not required to continuously monitor for security exploits. (*Id.* at 2:44-51.) As such, the ’591 Patent describes and claims specific computer-related technological steps to accomplish an improvement in computer security and functionality and is directed to a specific technological solution to a problem unique to computers.

U.S. Patent Nos. 10,599,844 and 11,409,869

82. 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 6. 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.

83. The ’869 Patent, entitled “Automatic Threat Detection of Executable Files Based on Static Data Analysis,” is a continuation of the ’844 Patent and claims priority to the application of the ’844 Patent. The ’869 Patent was filed on February 14, 2020 and was duly and legally issued by the USPTO on August 9, 2022. A true and correct copy of the ’869 Patent is attached as Exhibit 7. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’869 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’869 Patent.

84. The ’844 and ’869 Patents address and improve 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. Some 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 6, ’844 Patent, 1:7-13.)

85. 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 6, ’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.)

86. Another approach for protecting against potential threats from unknown executable files involved wavelet decomposition to determine software entropy. (*See* WBRT007115 at 7491, ’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

WBRT007492.) This process required significant computing resources—typically taking hours to complete—and was not sufficiently accurate in identifying malware.

87. The ’844 and ’869 Patents significantly improve upon and address shortcomings associated with these prior approaches. The Patents describe and claim 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 without decrypting or executing the 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 6, ’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 and ’869 Patents improve 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 6, ’844 Patent, 2:46-56.)

88. The ’844 and ’869 Patents describe and claim 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 6, ’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.)

89. Second, the '844 and '869 Patents describe and claim 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 6, '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 6, '844 Patent, 9:2-18.)

90. The '844 and '869 Patents are 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 and '869 Patents improved upon the accuracy and efficiency of malware detection. (*See* Exhibit 6, '844 Patent, 2:15-45.)

91. 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 and '869 Patents address a problem necessarily involving computers and improve upon the operation of computer networks.

In particular, the ’844 and ’869 Patents achieve 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 6, ’844 Patent, 2:15-57.)

U.S. Patent No. 8,856,505

98. U.S. Patent No. 8,856,505 (the “’505 Patent”), entitled “Malware Management Through Kernel Detection During a Boot Sequence,” was filed on April 30, 2012 and was duly and legally issued by the USPTO on October 7, 2014. The ’505 Patent claims priority to, and is a continuation of, U.S. Patent No. 8,190,868 filed August 7, 2006. A true and correct copy of the ’505 Patent is attached as Exhibit 8. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’505 Patent. The ’505 Patent describes and claims techniques to prevent rootkits, spyware, and/or other undesirable software from executing. (*See* Exhibit 8, ’505 Patent, 2:17-29, 4:3-5.). In general, periodic scanning of a computing system often fails to identify pestware, much less stop pestware from executing. (*Id*. at 1:61-67.) The intervening time between periodic scans permits pestware to cloak and execute, leaving the infected computing system

exposed, and ultimately vulnerable to the collection and reporting of information held thereon to the malicious third-party. (*Id*.) And pestware that loads relatively early in the boot sequence may be generally undetectable (*e.g.*, cloaked) when scanned later in the boot sequence or otherwise. (*Id*.)

99. The pestware management techniques of the ’505 Patent mitigate these, and other challenges associated with pestware detection and mitigation, including pestware that executes early in the boot sequence and/or that may be undetectable or cloaked once a computing system runs native applications. (*Id*. at 2:17-29, 3:39-46.) The ’505 Patent describes and claims techniques that can monitor and identify pestware events early in the boot sequence of a computing system. (*Id*. at 3:19-31.) As additional drivers and applications are loaded in the course of the boot sequence, techniques that are described and claimed can monitor the loadings and other events and facilitate management of the pestware. (*Id*. at 4:19-31, 4:53-62). Thus, the pestware management techniques may operate to stop pestware before it cloaks and executes, including stopping pestware which may otherwise be undetectable by conventional, periodic, post-boot-sequence scans.

100. The ’505 Patent describes and claims an unconventional “kernel-level monitor” to facilitate the management of pestware early in the boot sequence of a computing system. (*Id*. at 3:1-14.) The kernel-level monitor “begins early in the boot and operating system loading process,” (*Id*. at 3:25-27), and “is responsible for detecting pestware or pestware activity on a protected computer or system,” (*Id*. at 3:19-21). Attempts by pestware to modify the operating system are monitored and intercepted by the kernel-level monitor, for example, by using “driver hooks and monitoring mechanisms,” which may be placed into the operating system kernel during an early portion of the boot sequence. (*Id*. at 3:32-39, 4: 53-62.) Accordingly, the kernel-level monitor can be configured to identify changes at the kernel-level (*e.g.*, such as those changes which may be

attempted by a rootkit or other malicious component), prior to the time when those changes may become generally undetectable. (*Id*. at 4:53-62, 5:1-12.)

101. The ’505 Patent further describes and claims unconventional techniques that permit scanning of the “registry” during the boot sequence “before most services are loaded and executed.” (*Id*. at 6: 4:10.) Performing this type scanning early in the boot process provides new and unexpected benefits, including providing additional information that may be utilized in the identification of malicious programs. For example, scanning the protected parts of the computer such as the registry early in the boot process enables later “examin[ation] and utiliz[ation]” of that information to, for example, “generate new behavior rules for the kernel-level monitor.” (*Id*. at 6:4-10.)

102. The ’505 Patent describes and claims unconventional techniques that address technical weaknesses in conventional mitigation techniques for pestware. (*Id*. at 1:46-66, 2:1-29.) The ’505 Patent describes and claims techniques that permit pestware management at the kernel level, early in the boot sequence before the malicious code can cause damage or conceal itself. (*Id*. at 2:17-29, 4:63-67, 5:1-12.) Thus, these novel and unconventional techniques provide technical advantages such as enhanced security protection, improved detection of pestware, and adaptability to evolving pestware threats. (*Id*. at 1:46-66, 2:1-29.) As such, the ’505 Patent describes and claims specific computer-related technological steps to accomplish an improvement in computer security and functionality and is directed to a specific technological solution to a problem unique to computers.

Kernel-Level API Monitoring Patents
U.S. Patent Nos. 8,201,243 and 8,719,932

103. The ’243 and ’932, Patents are part of the same patent family. Plaintiff Webroot

owns by assignment the entire right, title, and interest in and to the ’243 and ’932 Patents.

104. The ’243 Patent, entitled “Backwards Researching Activity Indicative of Pestware,” was filed on April 20, 2006 and was duly and legally issued by the USPTO on June 12, 2012. A true and correct copy of the ’243 Patent is attached as Exhibit 9.

105. The ’932 Patent, also entitled “Backwards Researching Activity Indicative of Pestware,” was filed on June 6, 2012 and was duly and legally issued by USPTO on May 6, 2014. The ’932 Patent claims priority to the ’243 Patent. A true and correct copy of the ’932 Patent is attached as Exhibit 10.

106. At the time the ’243 and ’932 Patents were filed, conventional pestware-detection-and-removal solutions struggled to stay ahead of evolving pestware because they relied on “definitions of known pestware to search for and remove files on a protected system.” (Exhibit 9, ’243 Patent, 1:63-65.) “Th[os]e definitions were often slow and cumbersome to create,” and “it was often difficult to locate the pestware in order to create the definitions,” in the first place. (*Id.* at 1:65-67.) Furthermore, relying on definitions made it difficult to distinguish wanted pestware from unwanted pestware. (*Id.* at 1:60-62.)

107. To overcome these and other shortcomings, the ’243 and ’932 Patents describe and claim novel “systems and methods for discovering the source of activity that is indicative of pestware.” (*Id*. at 2:17-19.) For example, the ’243 and ’932 Patents describe and claim the use of a kernel-mode driver to monitor the behavior of processes running on a computer, for example monitoring API calls, to detect pestware. (*Id.* at 4:24-29.) The inventors found that this approach provided technical advantages, such as the ability to “intercept” “when a process (e.g., the pestware process) attempt[ed] to spawn … another pestware process or alter a registry entry, … before it [wa]s carried out by an operating system of the protected computer.” (*Id.* at 5:46-50.)

108. Moreover, the ’243 and ’932 Patents describe and claim techniques that enable the identification of suspected pestware as well as externally networked sources that, for example, may be the source of the pestware on the system. This approach provides benefits, such as identifying the source of malicious malware, which can be used to identify new malware (*e.g.*, based on a known source of malware) as well as to block potential malware based on a known malicious source.

U.S. Patent No. 8,181,244

109. The ’244 Patent, entitled “Backwards Researching Activity Indicative of Pestware,” was filed on April 20, 2006 and was duly and legally issued by USPTO on May 15, 2012. A true and correct copy of the ’244 Patent is attached as Exhibit 11. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’244 Patent.

110. At the time the ’244 Patent was filed, prior-art pestware-detection-and-removal solutions struggled to stay ahead of evolving pestware. Prior-art pestware-detection-and-removal solutions relied on “definitions of known pestware to search for and remove files on a protected system.” (Exhibit 11, ’244 Patent, 1:63-65.) “Th[os]e definitions were often slow and cumbersome to create,” and “it was often difficult to locate the pestware in order to create the definitions,” in the first place. (*Id.* at 1:65-67.) Furthermore, relying on definitions made it difficult to distinguish wanted pestware from unwanted pestware. (*Id.* at 1:60-62.)

111. To overcome these shortcomings, the ’244 Patent introduced novel “systems and methods for discovering the source of activity that is indicative of pestware.” (*Id.* at 2:17-19.) The ’244 Patent employed a kernel-mode driver to monitor the behavior of processes running on a computer, for example monitoring API calls, to detect pestware. (*Id.* at 4:24-29.) Once the ’244 Patent detected “pestware activity,” the ’244 Patent issued a timestamp and assembled a log of

events that occurred at or around that time. (*Id.* at 6:2-9.) Then, using the log of events, the ’244 Patent was able to “trac[e] … the pestware activity to an origin of the pestware … associated with the activity.” (*Id.* at 8:23-26.) Additionally, by using a kernel-mode driver, the ’244 Patent was able to “intercept” “when a process (*e.g.*, the pestware process) attempt[ed] to spawn … another pestware process or alter a registry entry, … before it [wa]s carried out by an operating system of the protected computer.” (*Id.* at 5:46-50.)

112. The ’244 Patent describes and claims technological solutions to a technological problem. For example, embodiments enable the identification of suspected pestware as well as externally networked sources that, for example, may be the source of the pestware on the system. This approach provides benefits, such as identifying the source of malicious malware, which can be used to identify new malware (*e.g.*, based on a known source of malware) as well as to block potential malware based on a known malicious source.

ACCUSED PRODUCTS

113. Defendant’s Accused Products operate to provide various aspects of malware and network threat detection, prevention, and remediation.

114. For example, Trend Micro offers several threat-detection product suites including, for example, Apex One, Apex Central, Cloud One Network Security, Deep Discovery, Deep Security, Vision One, Network One, Endpoint Protection with Detection and Response, as well as Trend Micro’s EDR/XDR and Cloud Products.

115. Trend Micro’s Apex One generally provides endpoint security. For example, Apex One monitors endpoints and network traffic while using a combination of techniques (such as reputation-based, behavior-based, anti-exploit, and machine learning-based analyses) to detect and block malicious files. Similarly, Trend Micro’s Endpoint Protection with Detection and Response

products include Trend Micro's EDR/XDR products provide endpoint security and endpoint detection and response.

116. Trend Micro's Apex Central generally provides "centralized visibility and investigation." Apex Central monitors endpoints and provides a centralized view to manage, monitor, and report across multiple layers of security.

117. Trend Micro's Deep Discovery provides "Advanced Threat Protection." Similar to Apex One, Deep Discovery monitors networks and uses various techniques (such as reputation-based, behavior-based, anti-exploit, and machine learning-based analyses) to detect and block malicious files.

118. Trend Micro's Cloud One Workload Security ("Cloud One") is Trend Micro's security suite for cloud-based operations. Similar to Deep Discovery and Apex One, Trend Micro's Cloud One uses various techniques (such as reputation-based, behavior-based, anti-exploit, and machine learning-based analyses) to detect and address security threats to workloads running in cloud or hybrid cloud environments, including securing cloud container environments.

119. On information and belief, each of Trend Micro's security suites relies on Trend Micro's Smart Protection Network for global threat intelligence. Smart Protection Network is Trend Micro's cloud-based approach for gathering global threat intelligence data and building models for recognizing threats. Smart Protection Network collects global threat data, and analyzes the collected data using big data and machine learning to provide threat intelligence back to its customers' endpoints.

120. On information and belief, each of Trend Micro's security suites is equipped with a collection of Trend Micro modules, including Trend Micro's XDR and Trend Micro's Vision One. Vison One is on of Trend Micro's XDR offering. Among other things, Vision One enables

network and security administrators to gain forensic insights into the events behind a network attack.

121. On information and belief, each of Trend Micro's security suites is equipped with Trend Micro's machine learning modules, including Trend Micro's Predictive Machine Learning Engine or Trend Micro's TrendX Hybrid Machine Learning Model. Trend Micro's machine learning modules enable Trend Micro's security suites to make decisions about whether communications and/or computer objects are potentially malicious or otherwise harmful.

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE '250 PATENT)

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

123. Trend Micro has infringed and continues to infringe one or more claims of the '250 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 such as Trend Micro's Apex One, Vision One, and Smart Protection Network, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '250 Patent as demonstrated below.

124. For example, claim 1 of the '250 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from each of plural remote computers on which the computer object or similar objects are stored, the data including information about behavior of the objects running on one or more remote computers;
>
> determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware;

classifying the computer object as malware when the data indicates that the computer object is malware;

when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware;

automatically generating a mask for the computer object that defines acceptable behavior for the computer object, wherein the mask is generated in accordance with normal behavior of the object determined from said received data;

running said object on at least one of the remote computers;

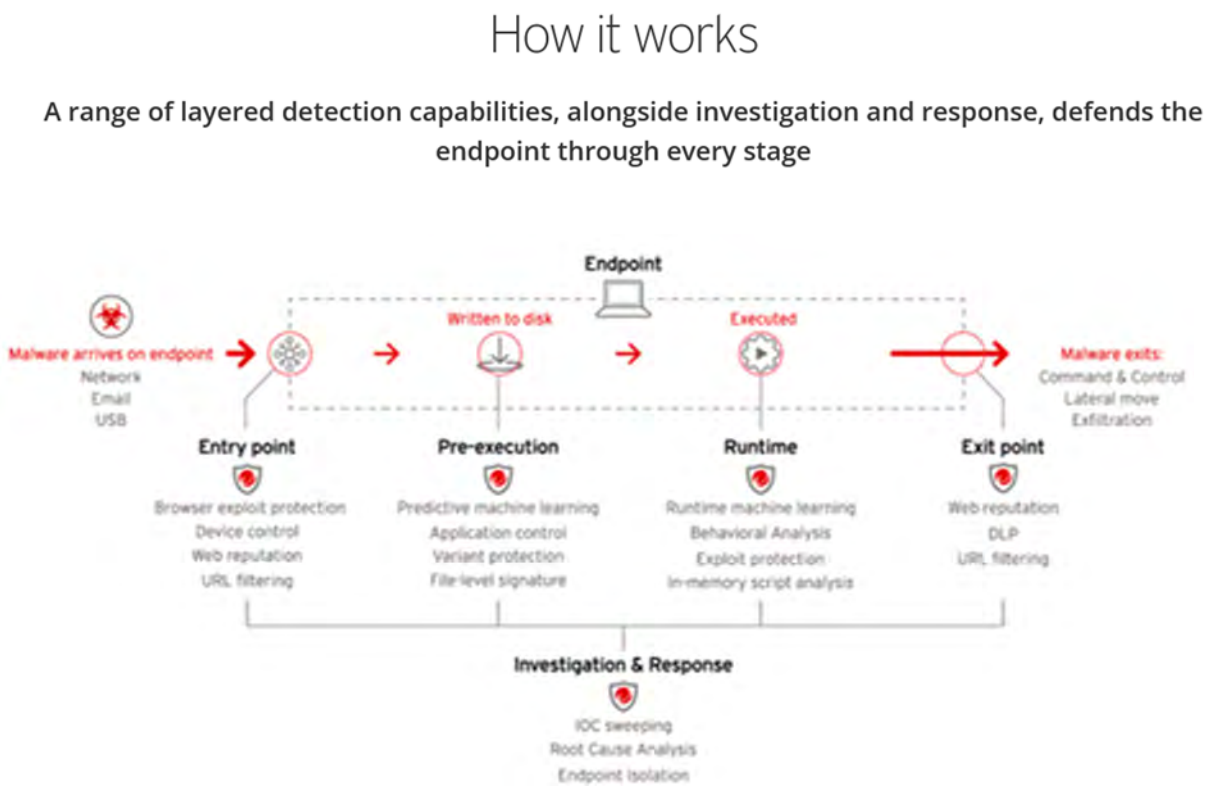
automatically monitoring operations of the object on the at least one of the remote computers;

allowing the computer object to continue to run when behavior of the computer object is permitted by the mask;

disallowing the computer object to run when the actual monitored behavior of the computer object extends beyond that permitted by the mask; and,

reclassifying the computer object as malware when the actual monitored behavior extends beyond that permitted by the mask.

125. To the extent the preamble is limiting, the Accused Products perform *a method of classifying a computer object as malware, the method comprising*. For example, the Accused Products, including Trend Micro's Apex One, "protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks." (*See* WBR_TMC007314, https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf (hereinafter "*Apex One Administrator's Guide*").) Apex One classifies objects as malware at least in part by conducting "Behavior Monitoring," which "protects endpoints through Malware Behavior Blocking and Event Monitoring." (*See id.* at 9-2.) Additionally, Apex One monitors objects to determine whether they display behaviors associated with malware. (*See id.* at 9-2.) Apex One also shares information with the Smart Protection Cloud which generates intelligence, including lists of known good and known bad objects. (*See id.* at 14-61.) Additionally, as the image below illustrates, Apex One provides many investigation tools to classify an object as malware at different stages including entry, pre-execution, runtime, and exit.



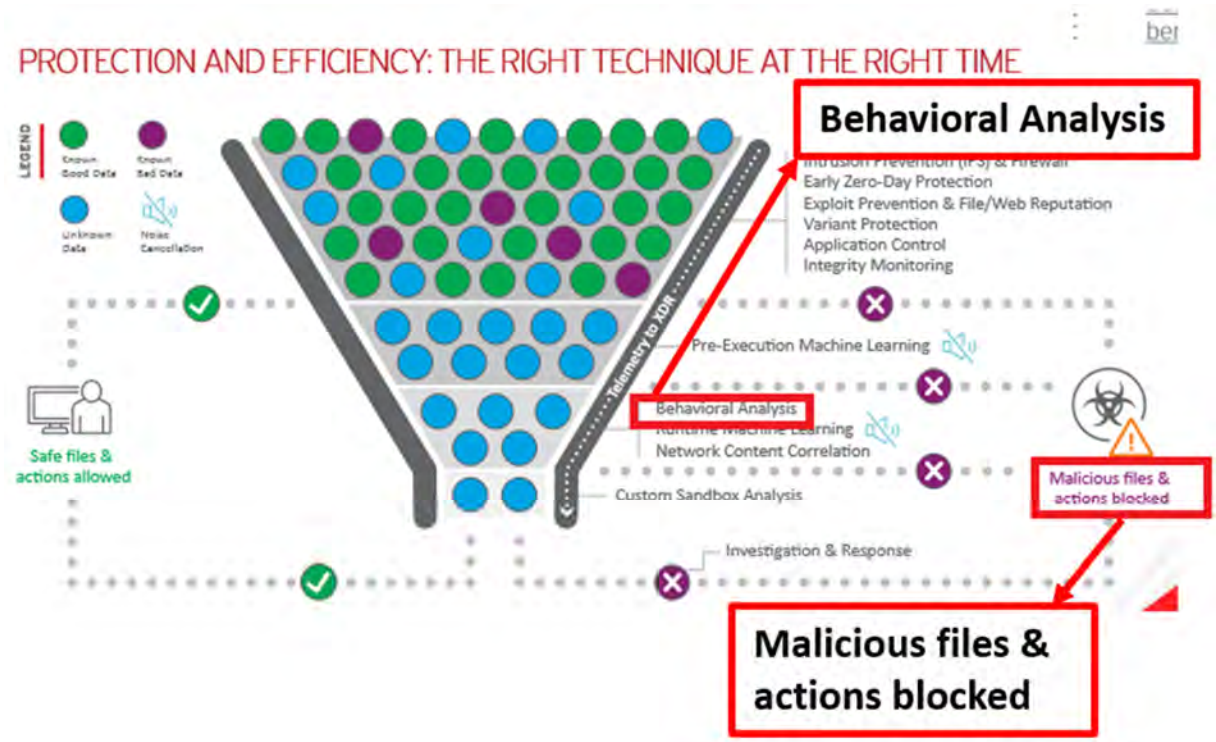
(*See* WBR_TMC001652, *Trend Micro Vision One* https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html.)

126. The Accused Products perform a method that includes *at a base computer, receiving data about a computer object from each of plural remote computers on which the computer object or similar objects are stored, the data including information about behavior of the objects running on one or more remote computers.* For example, Trend Micro's Apex One "consists of a client program that resides at the endpoint and server program that manages all clients." (*See* WBR_TMC007314, *Apex One Administrator's Guide* at 1-2.) Each endpoint provides information about computer objects and processes to a network server, including behavior monitoring logs. For example, "Security Agents log unauthorized program access instances and send the logs to the server." (*Id.* at 9-22.) The logs contain: "Date/Time unauthorized process was detected, Violation, which is the event monitoring rule violated by the process, Action performed

when violation was detected, event, which is the type of object accessed by the program, operation, which is the action performed by the unauthorized program, [and] target, which is the process that was accessed." (*Id.* at 9-23.)

127. The Accused Products perform a method that includes *determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware; classifying the computer object as malware when the data indicates that the computer object is malware* [*and*] *when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware*. As explained above, Apex One protects "enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks" by, *inter alia*, classifying objects as malware at least in part by conducting "Behavior Monitoring," which "protects endpoints through Malware Behavior Blocking and Event Monitoring" using the information received from each endpoint. (*See id.* at 9-2.)

128. As an example, the figure below, taken from Trend Micro's datasheet on Apex One, illustrates how the threat analysis initially assesses whether an object is malicious and, if identified, will classify and block those objects. The process includes "behavior analysis." Moreover, the Apex One also identifies "known" good and bad objects, which were classified based on prior analysis, including behavior analysis.



Threat Detection Capabilities

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- In-memory analysis for identification of fileless malware
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- Data loss prevention (DLP)
- Device and application control
- Ransomware rollback
- Sandbox and breach detection integration
- Extended detection and response (XDR)

(*See* WBR_TMC002543, *Datasheet: Trend Micro Apex One*, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3a-icon-datasheet-e4288a.)

129. The Accused Products perform the step of *automatically generating a mask for the computer object that defines acceptable behavior for the computer object, wherein the mask is generated in accordance with normal behavior of the object determined from said received data*. For example, Trend Micro's Apex One monitors systems to determine the behaviors of programs, and uses a list of events to recognize when a program is acting outside of the norm, or in a malicious way. The table below lists system events that indicate the program operating outside of normal behavior.

TABLE 9-1. Monitored System Events

EVENTS	DESCRIPTION
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the web browser is redirected to infected, non-existent, or fake websites.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at 9-6.)

EVENTS	DESCRIPTION
Suspicious Behavior	Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspicious behavior should be used with caution.
New Internet Explorer Plugin	Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.
Internet Explorer Setting Modification	Malware programs may change Internet Explorer settings, including the home page, trusted websites, proxy server settings, and menu extensions.
Security Policy Modification	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.
Program Library Injection	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.
Shell Modification	Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.
New Service	Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.
System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.
Firewall Policy Modification	The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.

(*See id.* at 9-7.)

130. In addition, the tables below show different actions associated with different behaviors, including defining acceptable behavior (*e.g.*, "allows programs associated with an event to run") as well as suspicious behaviors (*e.g.*, "blocks programs associated with an event from running").

TABLE 9-2. Actions on Monitored System Events

ACTION	DESCRIPTION
Assess	The Security Agent always allows programs associated with an event to run and logs the event for assessment. This is the default action for all monitored system events. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Allow	The Security Agent always allows programs associated with an event to run.

(*See id.* at 9-8.)

ACTION	DESCRIPTION
Ask when necessary	The Security Agent prompts users to allow or deny programs associated with an event from running and adds the programs to the exception list If the user does not respond within a certain time period, the Security Agent automatically allows the program to run. The default time period is 30 seconds. To modify the time period, see *Configuring Global Behavior Monitoring Settings on page 9-18*. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Deny	The Security Agent always blocks programs associated with an event from running and logs the event. After blocking a program with notifications enabled, the Security Agent displays a notification on the endpoint. For details about notifications, see *Behavior Monitoring Notifications for Security Agent Users on page 9-21*.

(*See id.* at 9-9.)

131. The Accused Products perform the function *running said object on at least one of the remote computers* [*and*] *automatically monitoring operations of the object on the at least one of the remote computers*. As explained above, the Accused Products initially analyze and classify objects or processes as malicious or not. An object that is not malicious is permitted to run.

However, as explained above, the Accused Products continue to monitor the behavior of the object running on the endpoints for behavior that is outside normal behavior. For example, Apex One includes Behavior Monitoring, which "constantly monitors endpoints for unusual modifications to the operating system or on installed software." (*See id.* at 9-2.) Apex One additionally includes event monitoring, which "monitors system areas for certain events, allowing administrators to regulate programs that trigger such events. (*See id.* at 9-6.)

132. The Accused Products further identify non-malware binaries, proactively marking them as good files.

(*See* WBR_TMC006612, https://www.trendmicro.com/en_us/business/capabilities/machine-learning.html.)

133. The Accused Products perform the functions *allowing the computer object to continue to run when behavior of the computer object is permitted by the mask* [*and*] *disallowing the computer object to run when the actual monitored behavior of the computer object extends*

beyond that permitted by the mask. As explained above, Apex One includes Behavior Monitoring, which "constantly monitors endpoints for unusual modifications to the operating system or on installed software. (*See* WBR_TMC007314, *Apex One Administrator's Guide* at 9-2.) Apex One additionally includes event monitoring, which "monitors system areas for certain events, allowing administrators to regulate programs that trigger such events." (*See id.* at 9-6.) Malware Behavior Blocking "observes system events over a period of time…. [,] detects known malicious behavior and blocks the associated program." (*See id.* at 9-6.) In other words, Apex One's Malware Behavior Blocking blocks programs when they display malicious behaviors, permitting the other programs to continue running when the behavior is normal.

134. As another example and as explained above, Apex One provides various actions on monitored systems. Certain objects are allowed to run so long as they run within the bounds of acceptable behaviors. For example, the figure below shows different actions associated with different behaviors. Certain actions "allow[] programs associated with an event to run," while other actions disallow the object to run when the behavior extends beyond the acceptable behaviors (*i.e.*, "blocks programs associated with an event from running").

TABLE 9-2. Actions on Monitored System Events

ACTION	DESCRIPTION
Assess	The Security Agent always allows programs associated with an event to run and logs the event for assessment. This is the default action for all monitored system events. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Allow	The Security Agent always allows programs associated with an event to run.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at 9-8.)

ACTION	DESCRIPTION
Ask when necessary	The Security Agent prompts users to allow or deny programs associated with an event from running and adds the programs to the exception list If the user does not respond within a certain time period, the Security Agent automatically allows the program to run. The default time period is 30 seconds. To modify the time period, see *Configuring Global Behavior Monitoring Settings on page 9-18*. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Deny	The Security Agent always blocks programs associated with an event from running and logs the event. After blocking a program with notifications enabled, the Security Agent displays a notification on the endpoint. For details about notifications, see *Behavior Monitoring Notifications for Security Agent Users on page 9-21*.

(*See id.* at 9-9.)

135. The Accused Products perform the function of *reclassifying the computer object as malware when the actual monitored behavior extends beyond that permitted by the mask*. As discussed above, the Accused Products continually monitor objects and processes running on endpoint computers for suspicious behavior (*i.e.*, behavior outside of normal behavior), at which point the object or process is reclassified as malware. For example, "[b]y continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides 'better together' security." (*See* WBR_TMC007314, *Apex One Administrator's Guide* at 4-5.)

Accordingly, on information and belief, when an object is determined to be malicious based on its behaviors, information concerning that object is provided to the Smart Protection Network to be classified as malware.

136. Each claim in the ’250 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’250 Patent.

137. Trend Micro became aware of the ’250 Patent at least when the original Complaint was filed in March 2022. Plaintiffs have also marked their products with the ’250 Patent, including on its web site, since at least July 2020.

138. Defendant directly infringes at least claim 1 of the ’250 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 this software and system to protect its 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.

139. Defendant’s partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’250 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

140. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’250 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,

Defendant encourages and induces customers with specific intent to use Trend Micro's security software in a manner that infringes claim 1 of the '250 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

141. Defendant 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.

142. Defendant further encourages and induces its customers to infringe claim 1 of the '250 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 its Trend Micro security software, and services in the United States. (*See*, *e.g.*, WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/user protection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal= s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator's Guide.)

143. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

144. 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 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 '250 Patent.

145. 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 '250 Patent.

146. 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 the Accused Products into the United States, 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.

147. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the behavioral analysis and related functionality described above, is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’250 patent, that functionality could not be performed.

148. Additionally, the accused functionality, including the behavioral analysis and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without a central computer or the “Smart Protection Network” that compiles and correlates behavioral data from processes that run on the endpoints protected by the Accused Products, the Accused Products could not assess which behaviors on any given endpoint constitute a threat. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’250 Patent, that functionality could not be performed.

149. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and

systems. For example, the Accused Products and accused functionalities (including the behavioral analysis functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as to generating a "mask for the computer object that defines acceptable behavior for the computer object") as recited in the claims of the '250 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

150. Defendant's infringing actions have continued after the original Complaint was filed. Defendant had knowledge of the '250 patent and of the specific conduct that constitutes infringement of the '250 patent at least based on the original Complaint, yet has continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

151. 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 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 '250 Patent.

152. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant's infringement of the '250 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.

153. 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 '250 Patent.

154. Defendant's infringement of the '250 Patent is knowing and willful. Defendant had actual knowledge of the '250 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the '250 Patent from at least the date Plaintiffs marked their products with the '250 Patent and/or provided notice of the '250 Patent on their website.

155. 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 '250 Patent constitutes willful infringement.

156. Plaintiffs' allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs' Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court's Standing Order Governing Patent Proceedings served July 12, 2022.

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

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

158. Trend Micro 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 features such as Trend Micro's Cloud One Deep Security ("Cloud One Deep Security"), Deep Security,

Apex One, and Apex Central, 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.

159. For example, claim 1 of the ’389 Patent recites:

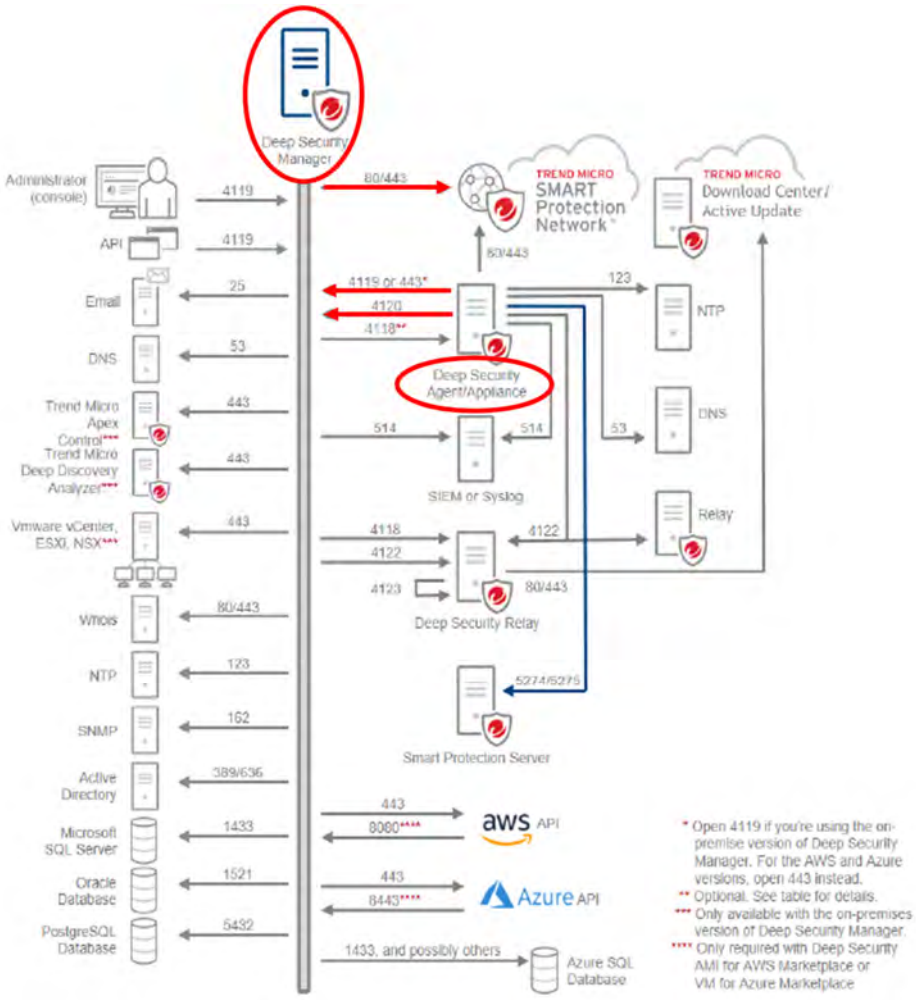
> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated 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.

160. To the extent the preamble is limiting, the Accused Products perform *a method of classifying a computer object as malware*. For example, Trend Micro’s Deep Security “provides agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware.” (*See* WBR_TMC012314, *Deep Security 12.0*

Guide for On-Premise Installations, https://help.deepsecurity.trendmicro.com/12_0/on-premise/Deep_Security_12.0_On-Premise_Administration_Guide.pdf (hereinafter "*12.0 Installation Guide*").) "To identify threats, [Deep Security's] anti-malware module checks files on the local hard drive against a comprehensive threat database…. [,] [and] checks files for certain characteristics, such as compression and known exploit code." (*See id.* at PDF p. 770.)

161. The Accused Products perform a method that includes, *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 and 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*. As explained below, the Accused Products receive information from multiple endpoint computers across the network about each computer object, including information about events and behaviors of the object.

162. As an example, the illustration below shows a system in which "Deep Security Manager" receives data from "Deep Security Agents or Appliances" running on multiple endpoints in the network.



(*See* WBR_TMC012314, *12.0 Installation Guide* at PDF p. 208.) As illustrated in this example, the Deep Security Manager receives data through the 4119 (or 443) and 4120 ports, and the Deep Security Agent/Agent and the Deep Security Manager send data to Trend Micro's Smart Protection network through 80/443 ports. (*Id.*) Additionally, Trend Micro's Deep Security system allows the Deep Security Manager to "send events to an external Syslog or Security Information and Event Management (SIEM) server … for centralized monitoring, custom reporting, or to free local disk space on Deep Security Manager." (*See id.* at PDF p. 1215.)

163. As explained above, the data sent from the agents running on the remote computers includes event and behavior information, which includes events initiated or involving the computer

object when the computer object is created, configured or runs on the first remote computer, including 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. For example, as shown in the figure below, Trend Micro's Deep Security includes decoders that "parse [] raw log entry in fields" for each event—*i.e.*, the information received from the remote computers—and includes, for example the "full_log" of the "entire event," "program_name," "action," and any other data extracted from the event. (*See id.* at PDF p. 995.)

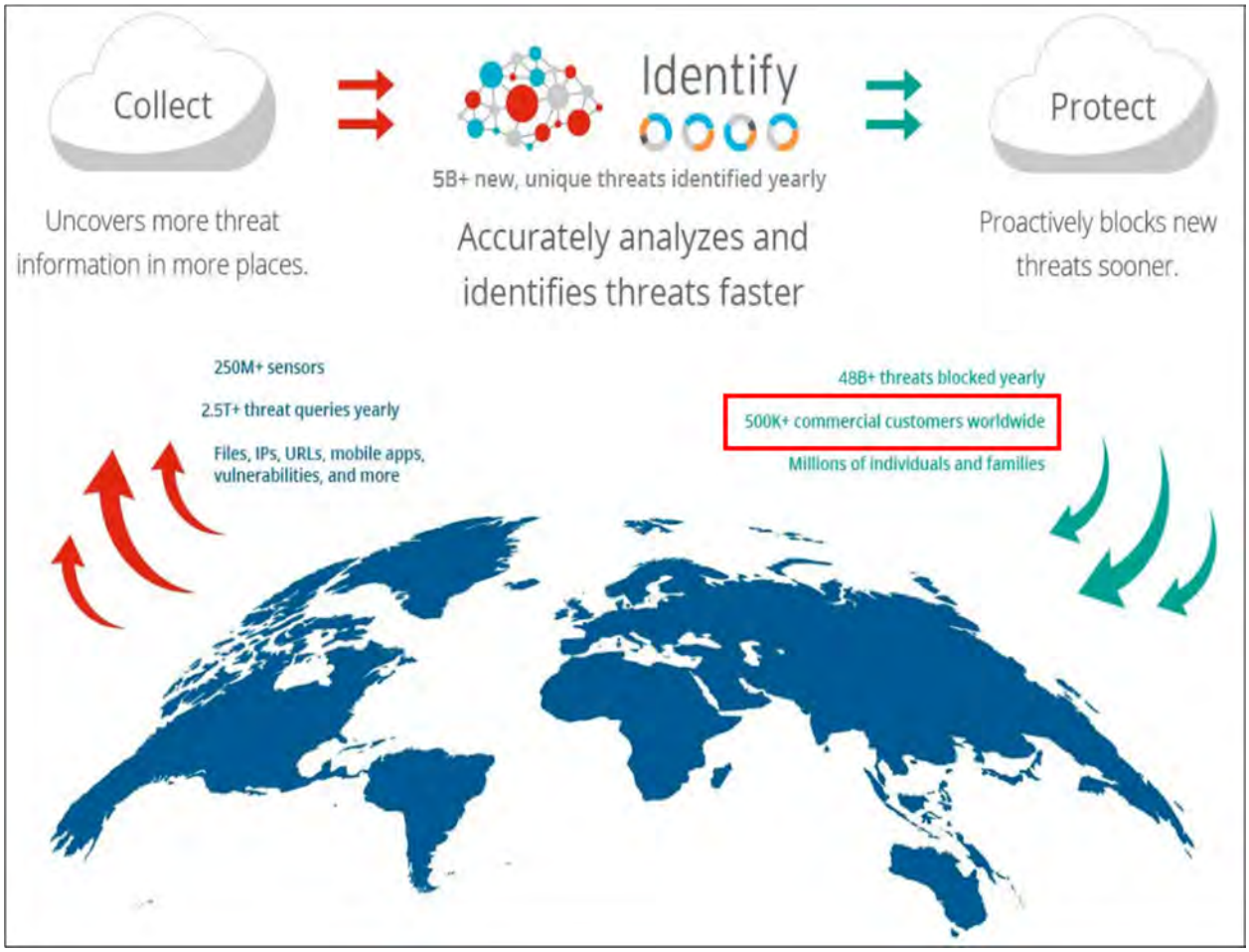
Decoders

A Log Inspection rule consists of a list of files to monitor for changes and a set of conditions to be met for the rule to trigger. When the Log Inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log**: the message section of the event
- **full_log**: the entire event
- **location**: where the log came from
- **hostname**: hostname of the event source
- **program_name**: program name from the syslog header of the event
- **srcip**: the source IP address within the event
- **dstip**: the destination IP address within the event
- **srcport**: the source port number within the event
- **dstport**: the destination port number within the event
- **protocol**: the protocol within the event
- **action**: the action taken within the event
- **srcuser**: the originating user within the event
- **dstuser**: the destination user within the event
- **id**: any ID decoded as the ID from the event
- **status**: the decoded status within the event
- **command**: the command being called within the event
- **url**: the URL within the event
- **data**: any additional data extracted from the event
- **systemname**: the system name within the event

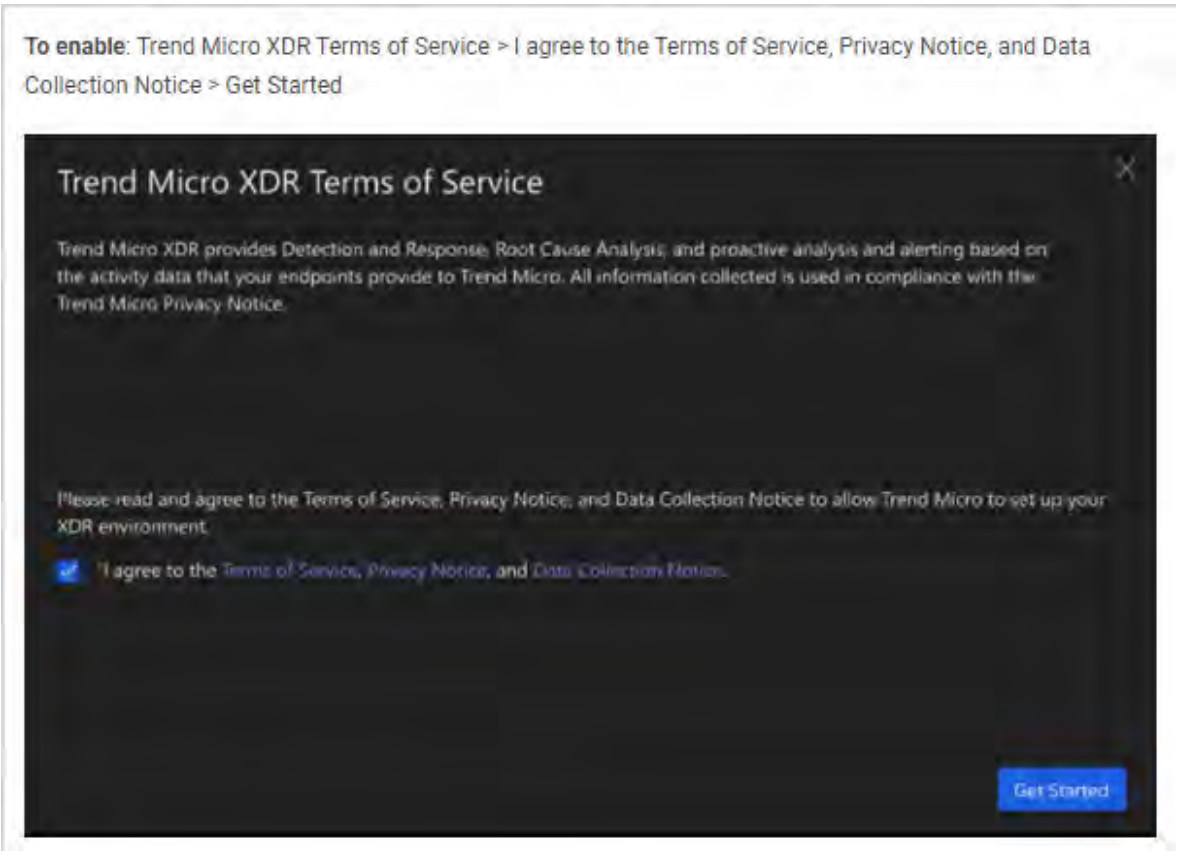
Rules examine this decoded data looking for information that matches the conditions defined in the rule.

164. As another example, Trend Micro's Smart Protection Network collects data from remote computers. As illustrated in the figure below, the Smart Protection Network collects and analyzes data from sensors across the globe and a plurality of customer computers ("500K+ commercial customers worldwide"). (*See* Trend Micro, *Smart Protection Network – Global Threat Intelligence*, https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html.)



(*See* Trend Micro, *Smart Protection Network – Global Threat Intelligence*, https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html.) The data collected depends on Trend Micro's specific endpoint product. The following lists are taken from Trend Micro's terms of service for various products, in which Trend Micro notifies users of

the specific data that is collected to assist Trend Micro in compiling data to analyze global security threat events.



(*See* WBR_TMC004168, https://success.trendmicro.com/solution/000262137 ("*Data Collection Notice*").)

ENDPOINT INVENTORY - ENABLE TREND MICRO VISION ONE CAPABILITIES	
DATA COLLECTED	• Command line • File name • File owner • File signer • Host name • IP address • Process owner • Registry data • User name • URL • Windows event log

(*See id.*)

DATA SOURCE: 3RD PARTY LOGS (SPLUNK ENTERPRISE)	
DATA COLLECTED	Data transmitted relates to URL access events. • Event time • Source IP address • Host name: from where the event is initiated • Website: the URL • Count: aggregated times of the access • User name: user who initiates the event

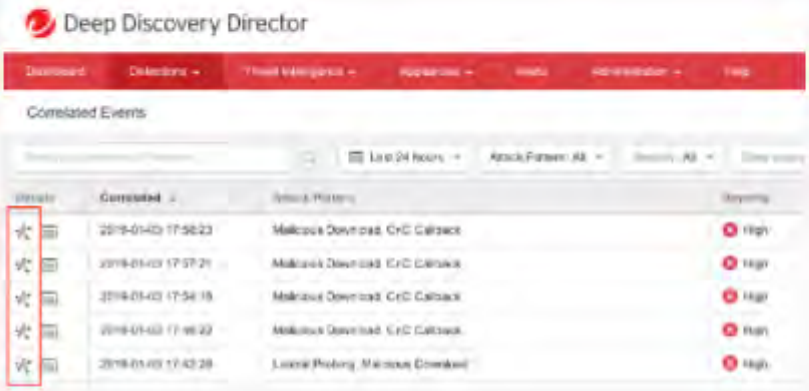
(*See id.*)

Endpoint Sensor

Endpoint Sensor is a powerful monitoring and investigation tool used to identify the presence, location, and entry point of threats. Through the use of detailed system event recording and historical analysis, you can perform Historical Investigations to discover hidden threats throughout your network and locate all affected endpoints.

ENDPOINT SENSOR	
DATA COLLECTED	• Command line • File name • File owner • File signer • Host name • IP address • Process owner • Registry data • User name • URL • Windows event log
CONSOLE LOCATION	Apex Central console Policies > Policy Management > Apex One Security Agent > Endpoint Sensor Settings
CONSOLE SETTINGS	Enable Endpoint Sensor **Endpoint Sensor Settings** Enable Endpoint Sensor Enable Attack Discovery to detect known attack indicators on endpoints

(*See* WBR_TMC004210, https://success.trendmicro.com/solution/1120644 (hereinafter "*Apex One Data Collection Notice*").)

DATA COLLECTED	IP address
CONSOLE LOCATION	Detections > Correlated Events
CONSOLE SETTINGS	Correlated Events 

DATA COLLECTED	• IP address • URL • domain name • file SHA-1
CONSOLE LOCATION	Threat Intelligence > Product Intelligence > Synchronized Suspicious Objects
CONSOLE SETTINGS	Synchronized Suspicious Objects

(*See* WBR_TMC004248, https://success.trendmicro.com/solution/000268655#xdr.)

165. The Accused Products perform a method that includes *storing, at the base computer, said data received from the first and second remote computers*. For example, as illustrated in the figure below, Trend Micro's Deep Security Manager is connected to several databases: Microsoft SQL server, Oracle Database, PostgreSQL Database, and possibly others including Azure SQL Database. (*See* WBR_TMC012314, *12.0 Installation Guide* at PDF p. 209.) Additionally, security events are stored on the Deep Security Manager's database. Trend Micro's Deep Security Administration Guide explains that events can be forwarded to the Syslog or SIEM server "to free local disk space on Deep Security Manager." (*See id.* at PDF p. 1215.) In another example, "Smart protection includes services that provide anti-malware signatures, web reputations, and threat databases that are stored in-the-cloud." (*See* WBR_TMC007314, *Apex One Administrator's Guide* at 4-3.)

166. 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*. The Accused Products, for example, correlate the data received from end points across the network into databases that are capable of being queried. In one example, Trend Micro's Deep Security system includes a log inspection feature that "provide[s] a framework to parse, analyze, rank and correlate events across a wide variety of systems." (*See* WBR_TMC012314, *12.0 Installation Guide* at PDF p. 988.) "The log inspection feature … enables real-time analysis of third party log files…. delivered in the form of rules included in a security update." (*See id.* at PDF p. 989.) In this way, log files received from Deep Security administrators and other computers across the network are correlated to information data received from objects received from other computers.

167. As an additional example, Trend Micro's Deep Discovery can be configured to include Trend Micro's Vision One. (*See* WBR_TMC004262, Trend Micro, Deep Security 20 Administration Guide, (https://help.deepsecurity.trendmicro.com/20_0/on-premise/Deep_Security_20_Administration_Guide.pdf) at PDF pp. 1685-86.) Vision One offers a single platform "to correlate and analyze data … [and] visualize the entire chain of events across security layers or drill down into an execution profile or network traffic analysis." (*See* WBR_TMC007101, Trend Micro, Vision One Solution Brochure at 2, https://www.trenddefense.com/datasheets/xdr-datasheet.pdf.) Vision One "automatically correlat[es] threat data from multiple sources, [which] speeds up and removes manual steps involved in investigations and enables security analysts to quickly find the story of an attack." (*Id.* at 3.)

168. Trend Micro's accused products perform a method that includes c*omparing, 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.* For example, when connected to Trend Micro Apex Central, Trend Micro's "Deep Security Manager will be able to retrieve the suspected object list from Trend Micro Apex Central, share it with protected computers, and compare local objects against the Apex Central Suspicious Object List." (*See* WBR_TMC012314, *12.0 Installation Guide* at PDF p. 802.) Additionally, Trend Micro advertises that the Smart Protection Network learns from past actions "patterns of newly identified threats are maintained (sometimes for years) in the growing dataset of the Smart Protection Network," which allows for retrospective analysis. (*See* Trend Micro, *Smart Protection Network*, Whitepaper.) The Accused Products therefore identify relationships between the correlated data and other objects or entities, such as any new or unknown objects or entities.

169. 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, for example, when connected to Trend Micro Apex Central, Trend Micro's "Deep Security Manager will be able to retrieve the suspected object list from Trend Micro Apex Central, share it with protected computers, and compare local objects against the Apex Central Suspicious Object List." (*See* WBR_TMC012314, *12.0 Installation Guide* at PDF p. 802.) "To identify threats, [Deep Security's] anti-malware module checks files on the local hard drive against a comprehensive threat database…. [,] [and] checks files for certain characteristics, such as compression and known exploit code." (*Id.* at PDF p. 766.)

170. 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.

171. Trend Micro became aware of the '389 Patent at least when the original Complaint was filed in March 2022. Plaintiffs have also marked their products with the '389 Patent, including on its web site, since at least July 2020.

172. Defendant directly infringes at least claim 1 of the '389 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 this software and system to protect its 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.

173. Defendant's partners, customers, and end users of its 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 using the Accused Products and corresponding systems and services, as described above.

174. Defendant has 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’389 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

175. Defendant 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.

176. Defendant 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, including its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC007101, https://www.trenddefense.com/datasheets/xdrdatasheet.pdf; WBR_TMC018637, https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html;

WBR_TMC000006, https://www.trendmicro.com/en_us/partners/find-apartner.html; WBR_TMC006003, https://www.trendmicro.com/en_us/business/products/hybrid-cloud/deep-security.html; WBR_TMC004262, https://help.deepsecurity.trendmicro.com/20_0/on-premise/Deep_Security _20_Administration_Guide.pdf; *see also* WBR_TMC012314, *12.0 Installation Guide*.)

177. For example, on information and belief, Defendant 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. (*Id*.) 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. (*Id.*)

178. 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 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 '389 Patent.

179. 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 ’389 Patent.

180. 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 the Accused Products into the United States, 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.

181. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the behavioral analysis and related functionality described above, is an integral part of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’389 Patent, that functionality could not be performed.

182. Additionally, the accused functionality, including the behavioral analysis and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without a central computer or the Smart Protection Network that compiles and correlates behavioral data from processes that run on the endpoints protected by the Accused Products, the Accused Products could not assess which behaviors on any given endpoint constitute a threat. These processes are continually running when the system is in use and, on information and belief,

cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’389 Patent, that functionality could not be performed.

183. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the behavioral analysis functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying relationships between correlated data about objects received from remote computers) as recited in the claims of the ’389 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

184. Defendant’s infringing actions have continued after the original Complaint was filed. Defendant had knowledge of the ’389 Patent and of the specific conduct that constitutes infringement of the ’389 Patent at least based on the original Complaint, yet has continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

185. 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 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 ’389 Patent.

186. Plaintiffs have suffered and continue 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.

187. 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.

188. Defendant’s infringement of the ’389 Patent is knowing and willful. Defendant had actual knowledge of the ’389 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the ’389 Patent from at least the date Plaintiffs marked their products with the ’389 Patent and/or provided notice of the ’389 Patent on their website.

189. 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.

190. Plaintiffs’ allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE ’045 Patent)

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

192. Trend Micro has infringed and continues to infringe one or more claims of the ’045 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States, and will continue to do so unless enjoined by this Court. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’045 Patent as demonstrated below.

193. For example, claim 1 of the ’045 Patent recites:

> 1. A method comprising:
>
> gathering one or more events defining an action of a first object acting on a target;
>
> generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;
>
> obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to at least one event across a network;
>
> assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and
>
> transmitting the assembled event line.

194. To the extent the preamble is construed to be limiting, the Accused Products

including Trend Micro's XDR, Detection and Response products and services ("XDR"), Apex One (*e.g.* with XDR), and Vision One perform a method as further explained below. For example, "XDR" performs a method for endpoint protection, wherein threat cases/attacks are analyzed in detail.

Correlated detection	Integrated investigation and response
Powerful security analytics correlate data across the customer environment and Trend Micro's global threat intelligence to deliver fewer, higher-confidence alerts, leading to better, earlier detection.	One place for investigation simplifies the steps to achieving an attack-centric view of an entire chain of events across security layers with the ability to take response actions from a single place.

(*See* WBR_TMC015739, https://www.trendmicro.com/en_in/business/products/detection-response/xdr.html).

Trend Micro™ XDR collects and correlates deep activity data across multiple vectors - email, endpoints, servers, cloud workloads, and networks - enabling a level of detection and investigation that is difficult or impossible to achieve with SIEM or individual point solutions.

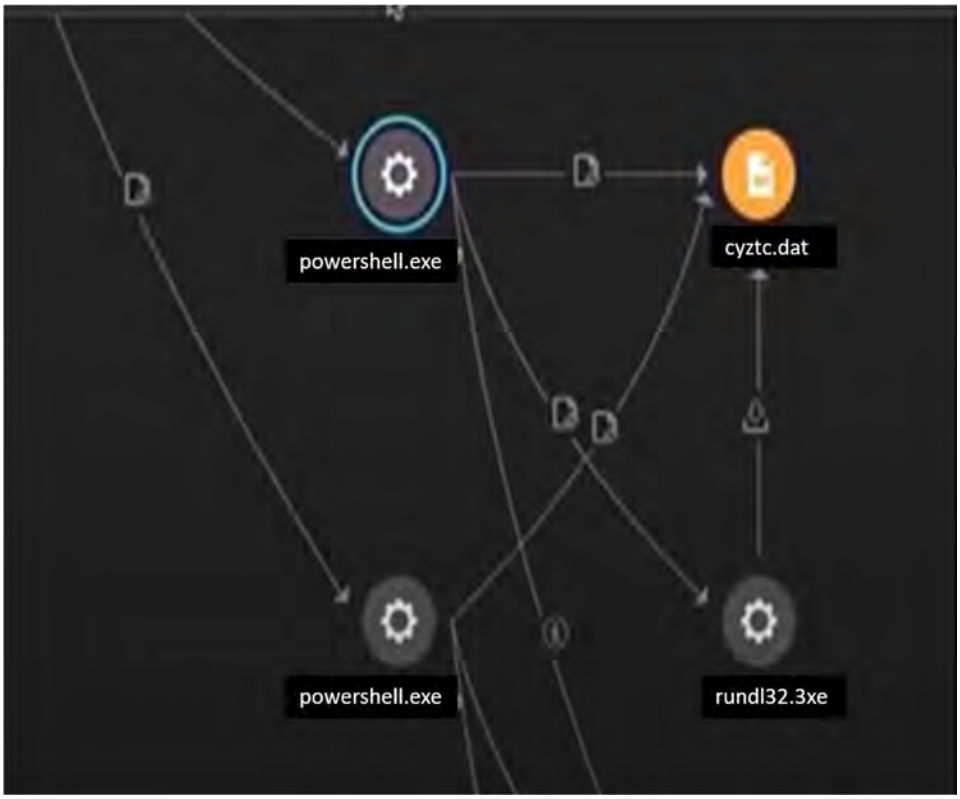
With a combined context, events that seem benign on their own suddenly become meaningful indicators of compromise, and you can quickly contain the impact, minimising the severity and scope.

XDR provides a SIEM connector to forward alerts. By correlating events from Trend Micro products, fewer, higher-confidence alerts are sent, reducing the triage effort required by security analysts. Upon clicking on a SIEM alert, an analyst can access the XDR investigation workbench to get further visibility, conduct deeper analysis, and take necessary action.

(*See* WBR_TMC015739, https://www.trendmicro.com/en_in/business/products/detection-response/xdr.html).

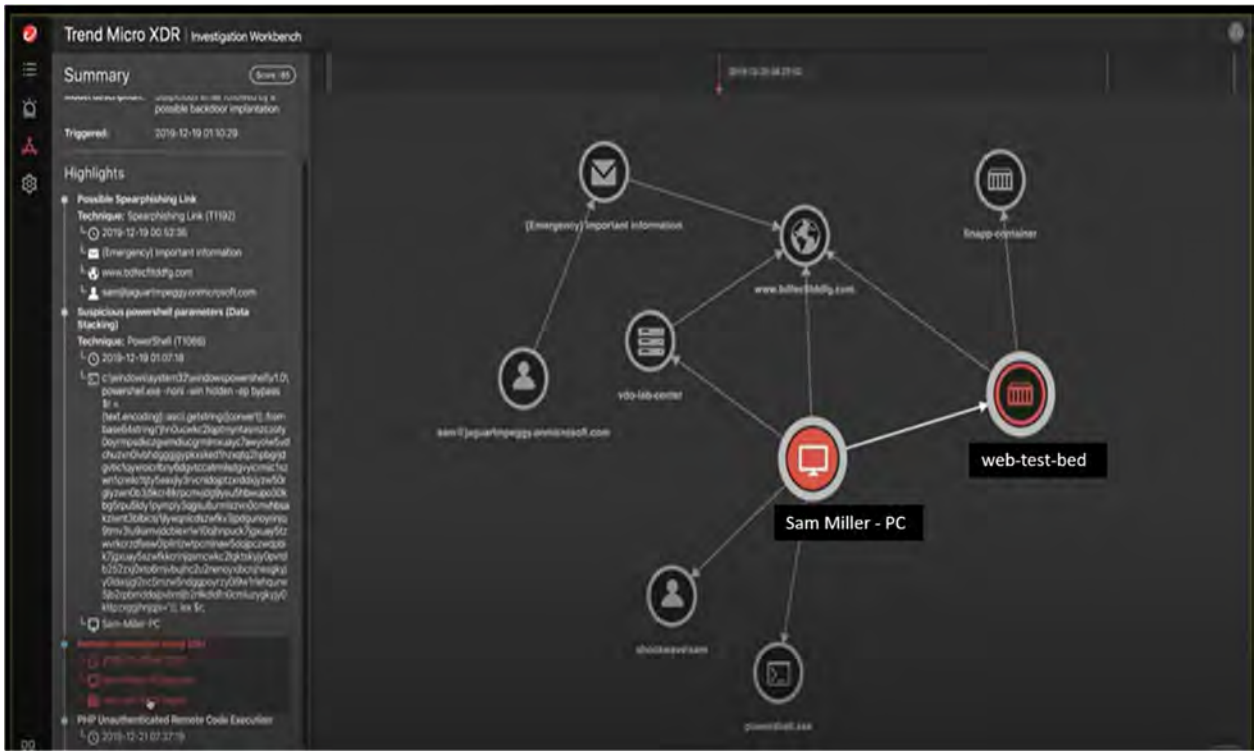
195. The Accused Products perform a method that includes *gathering one or more events defining an action of a first object acting on a target*. For example, in the example shown below, the "Summary" tab for Trend Micro's XDR contains Threat Case/Attack information. It highlights what XDR has detected: What object was detected, its target, and what actions it triggered on the target. Additionally, the Analysis chain displays information about where the object originated and what action the originating object performed on the object (or an intermediate object). The "Incident Trigger" (such as "powershelle.exe" in the example below) and the originating node/object (*e.g.*, "[Emergency] Important Information" in the example shown below) are linked by a chain of events known as the "Analysis Chain." In the example below, the host system Sam-Miller-PC received an e-mail that contained a malicious URL, which triggered/launched the Internet Explorer program (explorer.exe) in the system. A backdoor was possibly implanted after the user (Sam Miller) received the e-mail message. This chain of events (launching of the www.bdfecfitddfg.com URL) caused the Windows PowerShell (powershell.exe) to run a suspicious command and caused the execution of cyzfc.dat However, this activity (execution of a suspicious file) was detected and prevented by XDR.

(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

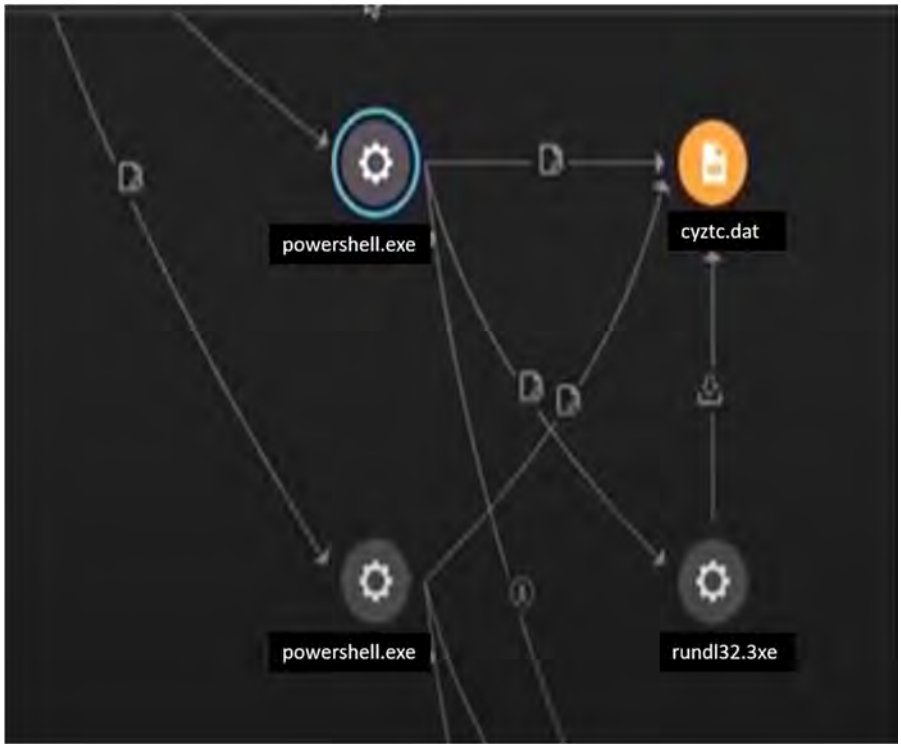


(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

196. The Accused Products perform a method that includes *generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object*. For example, and as explained above, the "Analysis Chain" in Trend Micro's XDR product contains the majority of the Threat Case/Attack information. It displays a graph of what XDR has detected; the "attack kill chain." The "Incident Trigger" (such as powershell.exe in the example below) and the originating node/object (*e.g.*, "[Emergency] Important Information" in the example shown below) are linked by a chain of events known as the "attack kill chain." In the example below, powershell.exe executed an executable file named rundl32.3xe, which launched the cyzlc.dat and triggered it to run a suspicious command and, hence, execute a potentially malicious file powershell.exe, which was detected and blocked by XDR. The details of the process/attack kill chain, *i.e.*, the critical paths, processes, files, domains, etc. involved include the "*contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object*." Additionally, as shown below, XDR displays a summary highlighting specific details of any event selected from the chain, details including time of the event, the victim host system/endpoint, the command line code, and the technique of the attack.

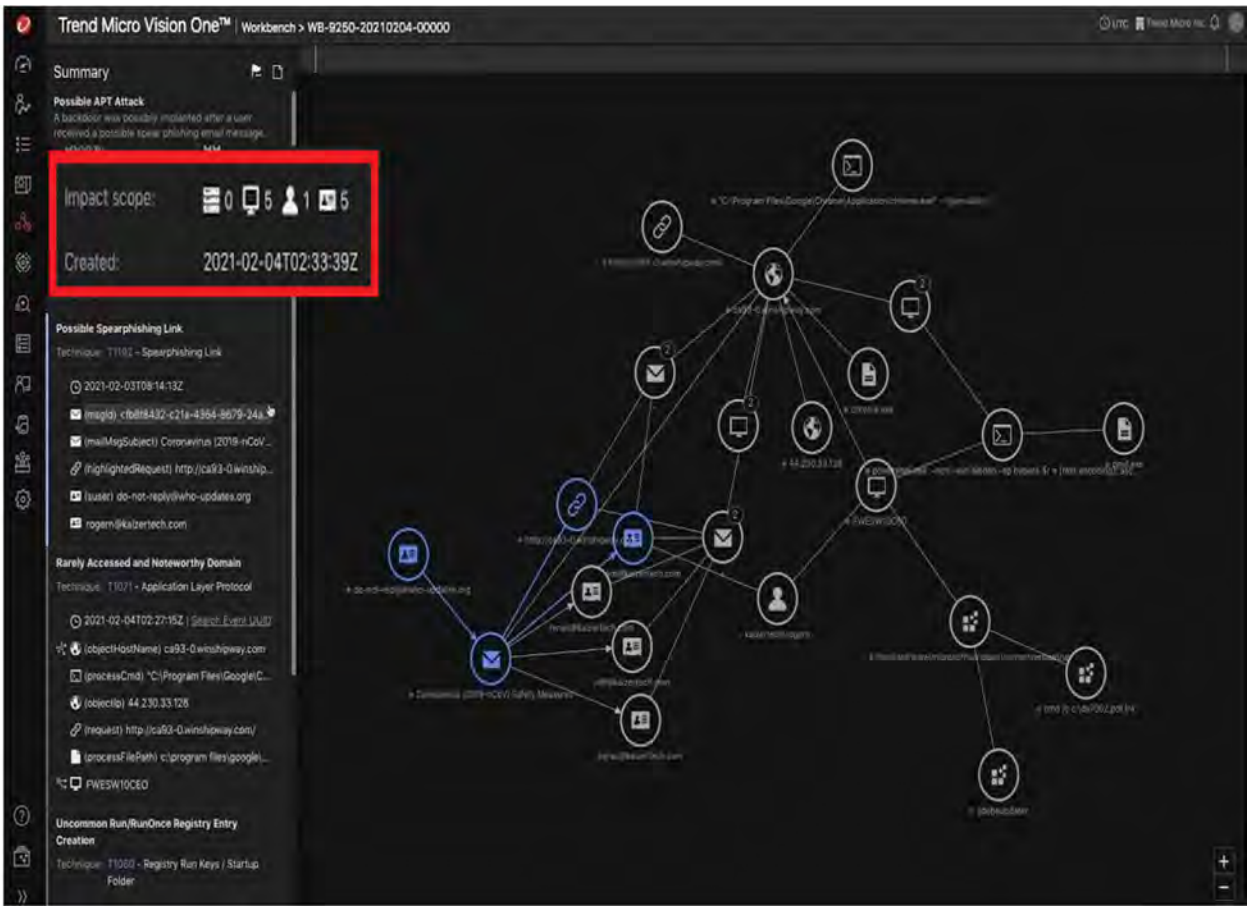


(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)



(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

197. The Accused Products perform a method that includes *obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network*. As shown below, the Accused Products obtain a "Global Perspective" for each event. For example, Trend Micro's XDR Product provides information such as the age (*e.g.*, "created 2021-02-04T02:33:39Z") and popularity (*e.g.*, "impact scope").



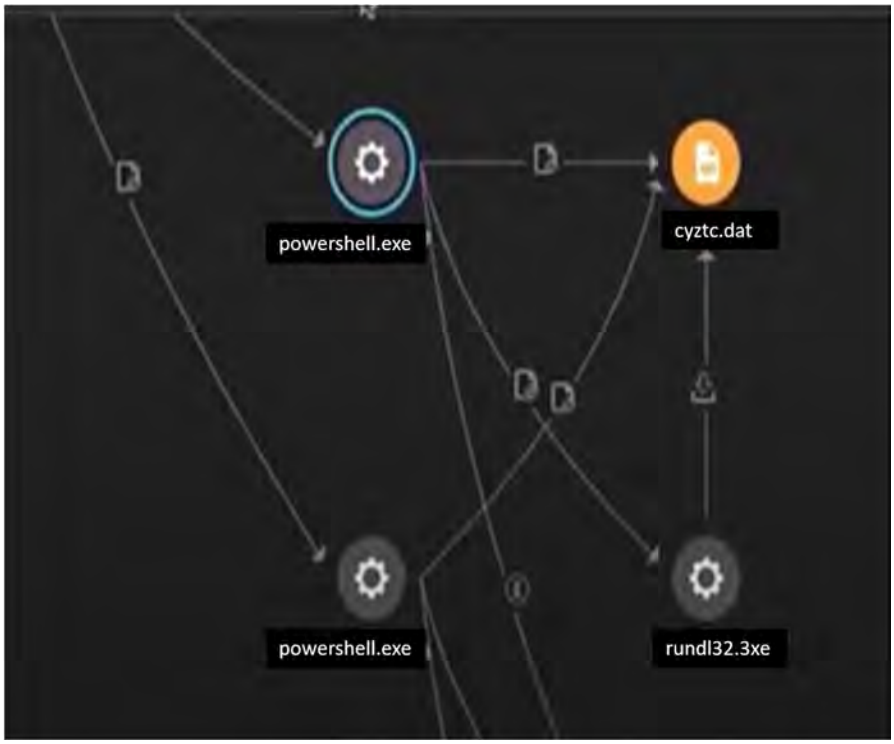
(*See* WBR_TMC000001, https://www.youtube.com/watch?v=odGDYzQbe80.)

198. The Accused Products perform a method that includes *assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target*, and the originating object. As explained above, the "Analysis Chain" generated by Trend Micro's XDR product contains the majority of the Threat Case/Attack information. It displays a graph of what XDR has detected; the "attack kill chain." The "Incident Trigger" (such as powershell.exe in the example below) and the originating node/object (*e.g.*, "[Emergency] Important Information" in the example shown below) are linked by a chain of events known as the "attack kill chain."

199. In the example below, powershell.exe executed an executable file named rundll32.exe, which launched the cyzlc.dat and triggered it to run a suspicious command and hence execute a potentially malicious file powershell.exe, which was detected and blocked by XDR.

200. Additionally, as shown below, XDR displays a summary highlighting specific details of any event selected from the chain, details including time of the event, the victim host system/endpoint, the command line code, and the technique of the attack.

(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)



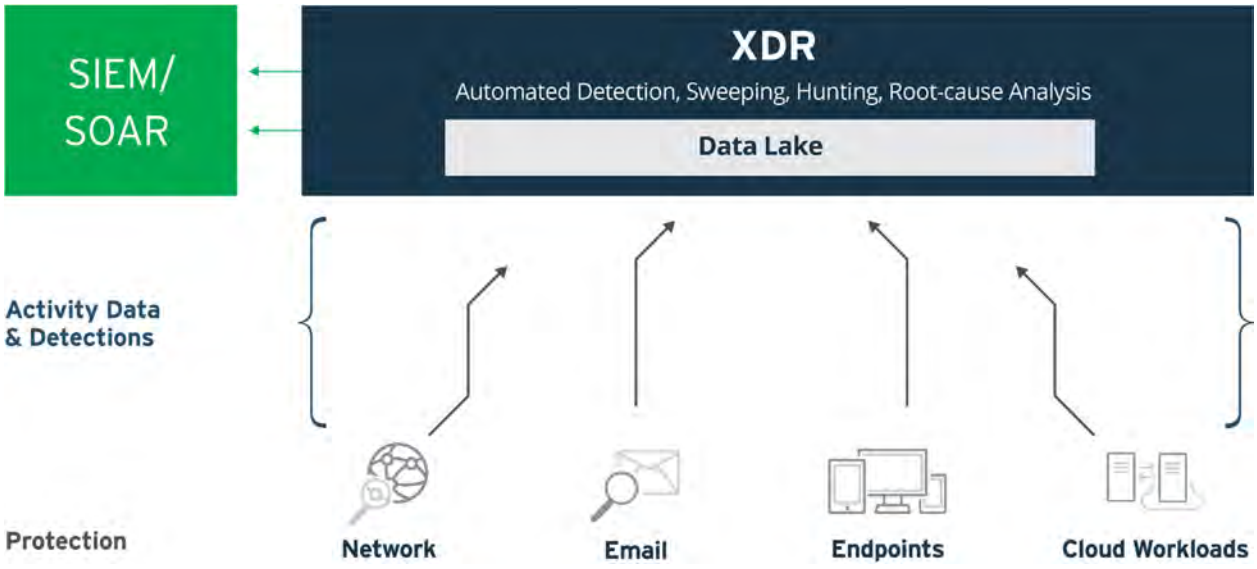
(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

201. The Accused Products perform a method that includes *transmitting the assembled event line*. For example, Trend Micro's XDR displays the generated event line (*e.g.*, it is transmitted to the display of the endpoint) when a particular threat case/alert from the list of alerts is selected. As explained above, the "Analysis Chain" contains the majority of the Threat Case/Attack information. The "attack kill chain" can be generated, stored or displayed (*e.g.*, on a user or administrator's client-side web browser).

202. On information and belief, the information on the series of events or attack chain is also transmitted to an XDR server or database for subsequent analysis and/or use.

> Trend Micro™ XDR collects and correlates deep activity data across multiple vectors - email, endpoints, servers, cloud workloads, and networks - enabling a level of detection and investigation that is difficult or impossible to achieve with SIEM or individual point solutions.
>
> With a combined context, events that seem benign on their own suddenly become meaningful indicators of compromise, and you can quickly contain the impact, minimising the severity and scope.
>
> XDR provides a SIEM connector to forward alerts. By correlating events from Trend Micro products, fewer, higher-confidence alerts are sent, reducing the triage effort required by security analysts. Upon clicking on a SIEM alert, an analyst can access the XDR investigation workbench to get further visibility, conduct deeper analysis, and take necessary action.

(*See* WBR_TMC015739, https://www.trendmicro.com/en_in/business/products/detection-response/xdr.html.)



(*See* WBR_TMC006032, https://www.trendmicro.com/en_in/what-is/xdr.html.)

203. Each claim in the ’045 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’045 Patent.

204. Trend Micro has been aware of the ’045 Patent since at least the filing of the original Complaint in March 2022. Further, Plaintiffs have marked their products with the ’045 Patent, including on its web site, since at least July 2020.

205. Defendant directly infringes at least claim 1 of the ’045 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 this software and system to protect its 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.

206. Defendant’s partners, customers, and end users of its Accused Products and

corresponding systems and services directly infringe at least claim 1 of the ’045 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

207. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’045 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’045 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

208. Defendant 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.

209. Defendant further encourages and induces its customers to infringe claim 1 of the ’045 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC007101, https://www.trenddefense.com/datasheets/xdr-datasheet.pdf; https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html;

https://www.trendmicro.com/en_us/partners/find-apartner.html; WBR_TMC006003, https://www.trendmicro.com/en_us/business/products/hybrid-cloud/deep-security.html; WBR_TMC004262, https://help.deepsecurity.trendmicro.com/20_0/on-premise/Deep_Security_20_Administration_Guide.pdf; WBR_TMC001652, *Trend Micro Vision One*, https://www.trendmicro.com/en_us/business/products/detection-response.html; WBR_TMC018673, Trend Micro, *Solution Brief: Trend Micro Vision One*, www.trendmicro.com/en_us/business/products/detection-response.html?modal=s1c-btn-solution-brief-847e3d; WBR_TMC000001, Trend Micro Vision One – XDR Workbench Demo: https://www.youtube.com/watch?v=odGDYzQbe80; WBR_TMC018705, *Trend Micro XDR Overview* at 5:35, YouTube (Oct. 19, 2020), https://www.youtube.com/watch?v=PUUj7fQPxiE; WBR_TMC016690, https://success.trendmicro.com/dcx/s/solution/000286401?language=en_US&sfdcIFrameOrigin=null.)

210. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

211. 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 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 '045 Patent.

212. 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 '045 Patent.

213. 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 the Accused Products into the United States, 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.

214. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including collecting and correlating "deep activity" and the functionality behind generating the "Analysis Chain," "attack kill chain," and "incident trigger," are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '045 Patent, that functionality could not be

performed.

215. Additionally, the accused functionality, including the collecting and correlating and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without a central computer or the Smart Protection Network that compiles and correlates event data from processes that run on the endpoints protected by the Accused Products, the Accused Products could not generate a contextual state, obtain a global perspective, and/or assemble an event line. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’045 Patent, that functionality could not be performed.

216. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the correlating functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as generating the “analysis chain” and the “kill chain”) as recited in the claims of the ’045 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

217. Defendant’s infringing actions have continued after the original Complaint was filed. Defendant had knowledge of the ’045 Patent and of the specific conduct that constitutes

infringement of the ’045 Patent at least based on the original Complaint, yet has continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

218. 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 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 ’045 Patent.

219. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’045 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.

220. 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 ’045 Patent.

221. Defendant’s infringement of the ’045 Patent is knowing and willful. Defendant had actual knowledge of the ’045 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the ’045 Patent from at least the date Plaintiffs marked their products with the ’045 Patent and/or provided notice of the ’045 Patent on their website.

222. 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 '045 Patent with knowledge of the '045 Patent constitutes willful infringement.

223. Plaintiffs' allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs' Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court's Standing Order Governing Patent Proceedings served July 12, 2022.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE '224 Patent)

224. Plaintiffs reallege and incorporates by reference the allegations of the preceding paragraphs of this Complaint.

225. Trend Micro has infringed and continues to infringe one or more claims of the '224 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States, and will continue to do so unless enjoined by this Court. The Accused Products, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '224 Patent as demonstrated below.

226. For example, claim 1 of the '224 Patent recites:

> 1. A method comprising:
>
> gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;
>
> generating contextual state information for the event by correlating the event to an originating object of the first object;
>
> obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global

perspective relates to one or more other events related to the event across a network;

generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmitting the generated event line.

227. To the extent the preamble is construed to be limiting, the Accused Products, including Trend Micro's Deep Discovery XDR, Detection and Response products and services ("XDR"), Apex One (*e.g.* with XDR), and Vision One perform a method as further explained below. For example, "XDR" performs a method for endpoint protection, wherein threat cases/attacks are analyzed in detail.

Correlated detection

Powerful security analytics correlate data across the customer environment and Trend Micro's global threat intelligence to deliver fewer, higher-confidence alerts, leading to better, earlier detection.

Integrated investigation and response

One place for investigation simplifies the steps to achieving an attack-centric view of an entire chain of events across security layers with the ability to take response actions from a single place.

(*See* WBR_TMC015739, https://www.trendmicro.com/en_in/business/products/detection-response/xdr.html.)

(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

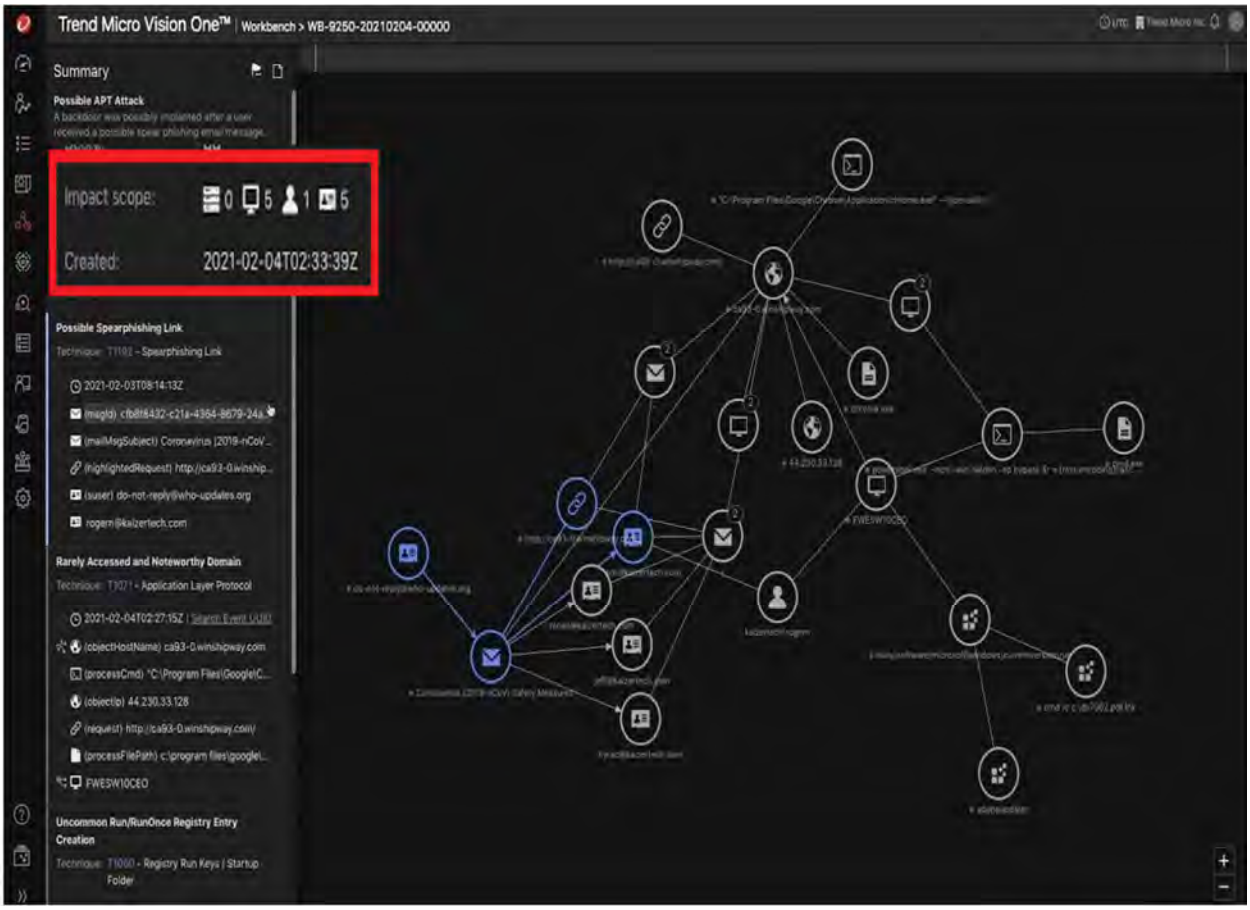
228. The Accused Products, including Trend Micro's XDR, perform a method that includes *gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device*. In particular, in the example shown below, the "Summary" tab contains Threat Case/Attack information. It highlights what XDR has detected: What object was detected, its target, and what actions it triggered on the target. Additionally, the Analysis chain displays information about where the object originated and what action it performed on the object. The "Incident Trigger" (such as "powershelle.exe" in the example below) and the originating node/object (*e.g.*, "[Emergency] Important Information" in the example shown below) are linked by a chain of events known as the "Analysis Chain." In the example below, the host system Sam-Miller-PC received an e-mail that contained a malicious URL, which triggered/launched the Internet Explorer program (explorer.exe) in the system. A backdoor was possibly implanted after the user (Sam Miller) received the e-mail message. This chain of events (launching of the

www.bdfecfitddfg.com URL) caused the Windows PowerShell (powershell.exe) to run a suspicious command and cause the execution of cyzfc.dat (*i.e.*, action of the first object). However, this activity (execution of a suspicious file) was detected and prevented by XDR. (*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

229. The Accused Products, including Trend Micro's XDR, perform a method that includes *generating contextual state information for the event by correlating the event to an originating object of the first object*. For example, and as explained above, the "Summary" tab contains the Threat Case/Attack information such as what object was detected, its target, and what actions it triggered on the target. Additionally, the Analysis chain displays information about where the object originated and what action it performed on the object. The "Incident Trigger" (such as "powershelle.exe" in the example below) and the originating node/object (*e.g.*, "[Emergency] Important Information" in the example shown below) are linked by a chain of events known as the "Analysis Chain." It highlights what XDR has detected. In the example below, the host system Sam-Miller-PC received an e-mail that contained a malicious URL, which triggered/launched the Internet Explorer program (explorer.exe) in the system. A backdoor was possibly implanted after the user (Sam Miller) received the e-mail message. This chain of events (launching of the www.bdfecfitddfg.com URL) caused the Windows PowerShell (powershell.exe) to run a suspicious command and cause the execution of cyzfc.dat (*i.e.*, action of the first object). However, this activity (execution of a suspicious file) was detected and prevented by XDR. The details of the process/attack kill chain, *i.e.*, the critical paths, processes, files, domains, etc. involved, include the "*contextual state information for the event by correlating the event to an originating object of the first object*."

(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

230. The Accused Products, including Trend Micro's XDR, perform a method that includes *obtaining a global perspective for the event based on the contextual state information wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network.* For example, XDR generates and displays details such as time of the event, the victim host system, the command line code, technique of the attack, etc., and provides information about each of the objects and events in the analysis chain described above (such as when an object or event is selected). As another example, as shown below, Trend Micro's XDR Product provides information such as the age (*e.g.*, "created 2021-02-04T02:33:39Z") and popularity (*e.g.*, "impact scope") of each of the objects.



(*See* WBR_TMC000001, https://www.youtube.com/watch?v=odGDYzQbe80.)

231. The Accused Products, including Trend Micro's XDR, perform a method that includes *generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object*. As explained above, the "Summary" tab provided by the Trend Micro XDR contains the Threat Case/Attack information. What object was detected, its target, and what actions it triggered on the target. Additionally, the Analysis chain displays information about where the object originated and what action it performed on the object. The "Incident Trigger" (such as "powershelle.exe" in the example below) and the originating node/object (*e.g.*, "[Emergency] Important Information" in the example shown below) are linked by a chain of events known as the

"Analysis Chain," which highlights what XDR has detected. In the example below, the host system Sam-Miller-PC received an e-mail that contained a malicious URL, which triggered/launched the Internet Explorer program (explorer.exe) in the system. A backdoor was possibly implanted after the user (Sam Miller) received the e-mail message. This chain of events (launching of the www.bdfecfitddfg.com URL) caused the Windows PowerShell (powershell.exe) to run a suspicious command and cause the execution of cyzfc.dat (*i.e.*, action of the first object). However, this activity (execution of a suspicious file) was detected and prevented by XDR.

(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

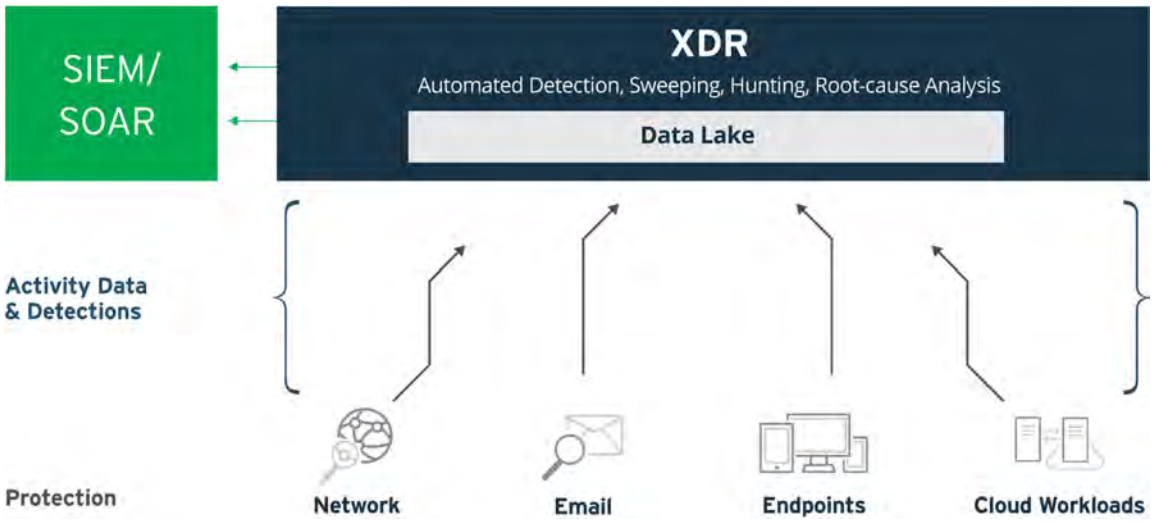
232. The Accused Products, including Trend Micro's XDR, perform a method that includes *transmitting the generated event line*. For example, Trend Micro's XDR displays the generated event line (*e.g.*, is transmitted to the display of the endpoint) when a particular threat case/alert from the list of alerts is selected. As explained above, the "Analysis Chain" contains the majority of the Threat Case/Attack information. The "attack kill chain" can be generated, stored

or displayed (*e.g.*, on a user or administrator's client-side web browser).

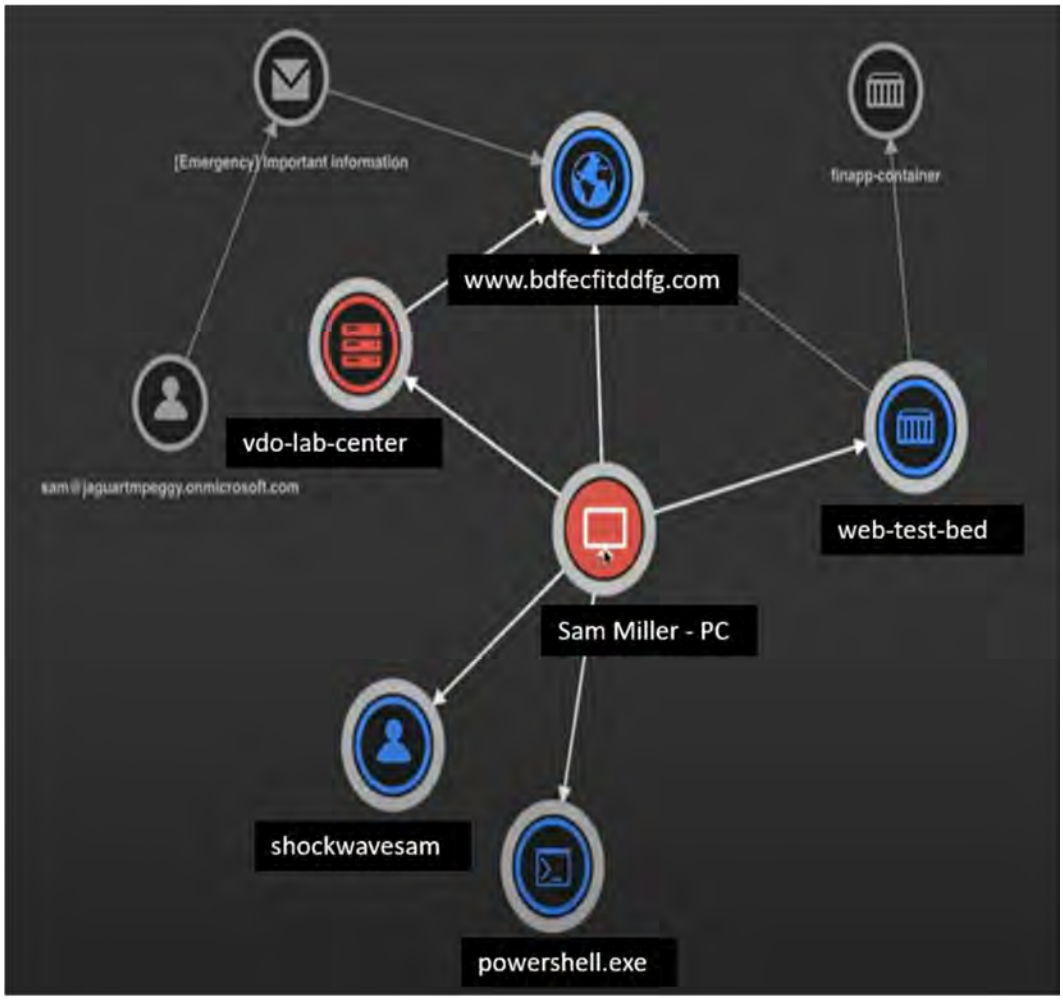
233. On information and belief, the information on the series of events or attack chain is also transmitted to an XDR server or database for subsequent analysis and/or use.

> Trend Micro™ XDR collects and correlates deep activity data across multiple vectors - email, endpoints, servers, cloud workloads, and networks - enabling a level of detection and investigation that is difficult or impossible to achieve with SIEM or individual point solutions.
>
> With a combined context, events that seem benign on their own suddenly become meaningful indicators of compromise, and you can quickly contain the impact, minimising the severity and scope.
>
> XDR provides a SIEM connector to forward alerts. By correlating events from Trend Micro products, fewer, higher-confidence alerts are sent, reducing the triage effort required by security analysts. Upon clicking on a SIEM alert, an analyst can access the XDR investigation workbench to get further visibility, conduct deeper analysis, and take necessary action.

(*See* WBR_TMC015739, https://www.trendmicro.com/en_in/business/products/detection-response/xdr.html.)



(*See* WBR_TMC006032, https://www.trendmicro.com/en_in/what-is/xdr.html.)



(*See* WBR_TMC000002, https://www.youtube.com/watch?v=WcaKLbpkCuU.)

234. Each claim in the ’224 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’224 Patent.

235. Trend Micro has been aware of the ’224 Patent since at least the filing of the original Complaint filed in March 2022. Further, Plaintiffs have marked their products with the ’224 Patent, including on its web site, since at least July 2020.

236. Defendant directly infringes at least claim 1 of the ’224 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 this software and system to protect its 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.

237. Defendant’s partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’224 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

238. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’224 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’224 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the

customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

239. Defendant 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.

240. Defendant further encourages and induces its customers to infringe claim 1 of the ’224 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC007101, https://www.trenddefense.com/datasheets/xdr-datasheet.pdf; https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html; https://www.trendmicro.com/en_us/partners/find-apartner.html; WBR_TMC006003, https://www.trendmicro.com/en_us/business/products/hybrid-cloud/deep-security.html; WBR_TMC004262, https://help.deepsecurity.trendmicro.com/20_0/on-premise/Deep_Security_20_Administration_Guide.pdf; WBR_TMC001652, *Trend Micro Vision One*, https://www.trendmicro.com/en_us/business/products/detection-response.html; WBR_TMC018673, *Solution Brief: Trend Micro Vision One*, www.trendmicro.com/en_us/business/products/detection-response.html?modal=s1c-btn-solution-brief-847e3d; WBR_TMC000001, Trend Micro Vision One – XDR Workbench Demo: https://www.youtube.com/watch?v=odGDYzQbe80; WBR_TMC018705, *Trend Micro XDR*

Overview at 5:35, YouTube (Oct. 19, 2020), https://www.youtube.com/watch?v=PUUj7fQPxiE; WBR_TMC016690, https://success.trendmicro.com/dcx/s/solution/000286401?language=en_US&sfdcIFrameOrigin=null.)

241. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

242. 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 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 '224 Patent.

243. 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 '224 Patent.

244. 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 the Accused Products into the United States, 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.

245. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including collecting and correlating "deep activity" and the functionality behind generating the "Analysis Chain," "attack kill chain," and "incident trigger," are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '224 Patent, that functionality could not be performed.

246. Additionally, the accused functionality, including the collecting and correlating and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without a central computer or the Smart Protection Network that compiles and correlates event data from processes that run on the endpoints protected by the Accused Products, the Accused Products could not generate a contextual state, obtain a global perspective, and/or assemble an event line. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no

longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’224 Patent, that functionality could not be performed.

247. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the correlating functionality) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as generating the “analysis chain” and the “kill chain”) as recited in the claims of the ’224 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

248. Defendant’s infringing actions have continued after the original Complaint was filed. Defendant had knowledge of the ’224 Patent and of the specific conduct that constitutes infringement of the ’224 Patent at least based on the original Complaint, yet has continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

249. 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 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 ’224 Patent.

250. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’224 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.

251. 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 ’224 Patent.

252. Defendant’s infringement of the ’224 Patent is knowing and willful. Defendant had actual knowledge of the ’224 Patent at least by the time Plaintiffs filed this lawsuit and had constructive knowledge of the ’224 Patent from at least the date Plaintiffs marked their products with the ’224 Patent and/or provided notice of the ’224 Patent on their website.

253. 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 ’224 Patent with knowledge of the ’224 Patent constitutes willful infringement.

254. Plaintiffs’ allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

FIFTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’591 Patent)

255. Plaintiffs reallege and incorporate the preceding paragraphs of this complaint.

256. Defendant has infringed and continues to infringe one or more claims of the ’591 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features such as Trend Micro’s Apex One and Deep Security, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’591 Patent as demonstrated below.

257. For example, claim 1 of the ’591 Patent recites:

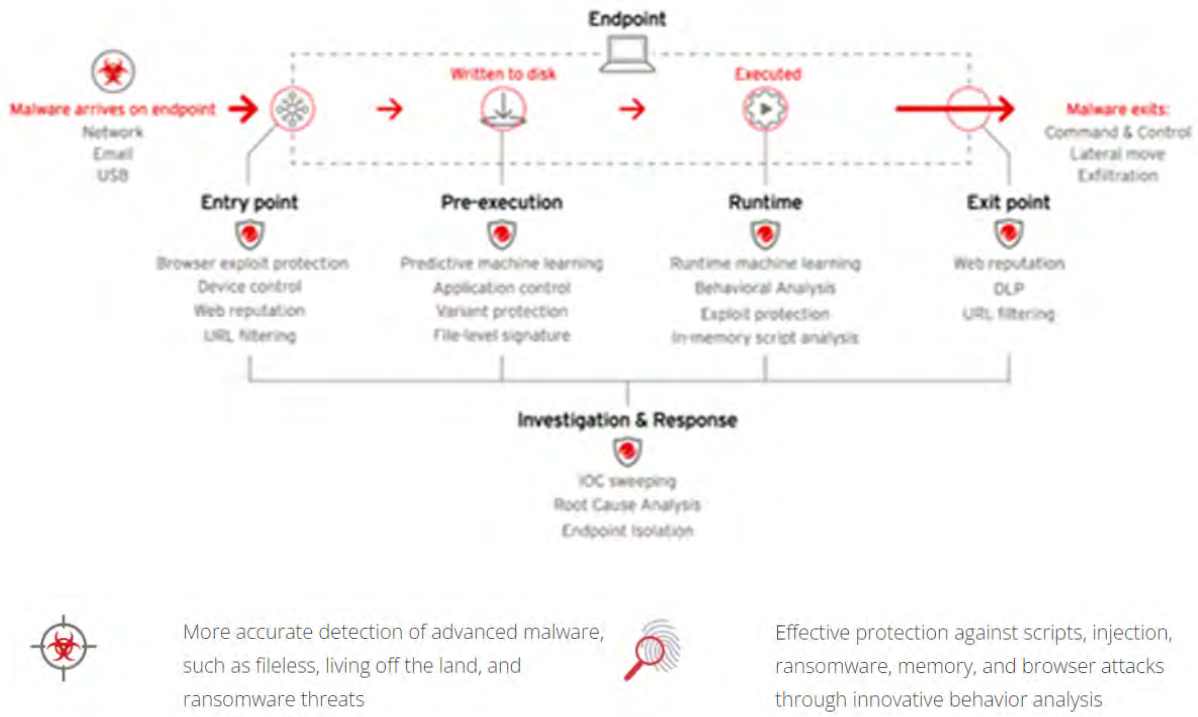
> 1. A computer-implemented method comprising:
>
> monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;
>
> invoking one of the plurality of functions as a result of receiving a call from an application programming instance;
>
> executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and
>
> performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:
>
> code execution is attempted from non-executable memory,
>
> a base pointer is identified as being invalid,
>
> an invalid stack return address is identified,
>
> attempted execution of a return-oriented programming technique is detected,
>
> the base pointer is detected as being outside a current thread stack, and

a return address is detected as being inside a virtual memory area,

wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

258. The Accused Products perform each of the method steps of claim 1 of the ’591 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 include “[a] range of layered detection capabilities” including “[e]xploit protection” and “detection of advanced malware such as fileless, living off the land” and “[e]ffective protection against scripts, injection, ransomware, memory, and browser attacks though innovative behavior analysis.” The Accused products are implemented in the network’s endpoint computers. (*See* WBR_TMC006039, https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_iug.pdf (hereinafter “*Apex One Installation Guide*”).)

A range of layered detection capabilities, alongside investigation and response, defends the endpoint through every stage



More accurate detection of advanced malware, such as fileless, living off the land, and ransomware threats

Effective protection against scripts, injection, ransomware, memory, and browser attacks through innovative behavior analysis

(*See* WBR_TMC001652, https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html.)

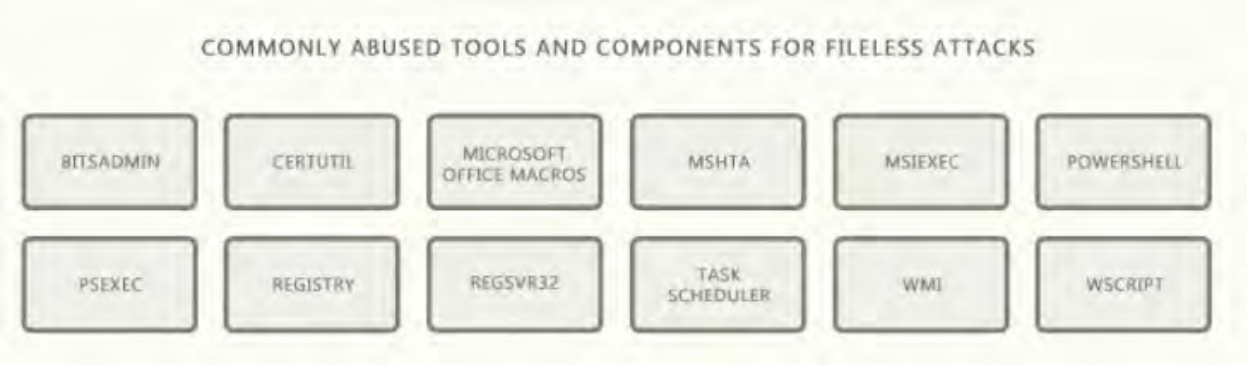
259. On information and belief, the Accused Products perform a method that includes *monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space*. For example, the Accused Products perform "In-memory Runtime Analysis" and "Behavior Monitoring scan[ning] the system memory for suspicious process." (*See* WBR_TMC007156, https://docplayer.net/173024260-Endpoint-security-webinar-24-29-oktober-2019.html at 19.) The Accused Products include the "APEX ONE ENDPOINT SENSOR … that monitors events and

quickly examines what processes or events are triggering malicious activity" including "malicious scripts, injection, ransomware, and memory and browser attacks related to fileless threats." (*See* WBR_TMC006205, *Fileless Threats 101*, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems.) In addition, Apex One Endpoint Sensors are installed on endpoint computers. (*See* WBR_TMC006039, *Apex One Installation Guide*, https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_iug.pdf at 2-20.) Thus, on information and belief, the Apex One Endpoint Sensors installed on endpoint computers monitor a memory space of the endpoint computer by loading a component for evaluating the at least one monitored function as claimed.

260. On information and belief, the Accused Products perform a method that includes *invoking one of the plurality of functions as a result of receiving a call from an application programming instance*. For example, Trend Micro's Apex One "employs a variety of threat detection capabilities … [to] protect[] against … fileless threats" such as "abuse[s] [of] task automation and configuration management framework PowerShell." (*See* WBR_TMC006205, *Fileless Threats 101*, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems.)

261. In another example, Trend Micro explains that "[m]any fileless threats abuse PowerShell, in particular, as it is a built-in feature on many Windows operating systems." (*See* WBR_TMC007168, *Risks Under the Radar Understanding Fileless Threats*, https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats.) Trend Micro explains that "[t]he Microsoft framework is [] capable of accessing application programming interfaces (APIs) that execute crucial system and application functions." (*Id.*) Trend Micro then suggests that the best way to "detect the misuse

of PowerShell [is] through behavioral detection, *i.e.*, discerning a PowerShell session executed via an encoded command in command line." (*Id.*) Trend Micro advertises that "[b]y tracking non-file-based indicators and through technologies like endpoint detection and response, [they] blocked more than 1.4 million fileless events in [a] year." (*See* WBR_TMC006205, *Fileless Threats 101*, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems.) In the figure below, for example, Trend Micro identifies "commonly abused tools and components for fileless attacks" that, on information and belief, the Accused Products monitor.



(*See* WBR_TMC006205, *Fileless Threats 101*, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems.)

262. In another example, Trend Micro Apex One "monitors events" (*e.g.*, a function call from an application instance) "and quickly examines what processes or events are triggering malicious activity." (*See* WBR_TMC006205, *Fileless Threats 101*, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems.)

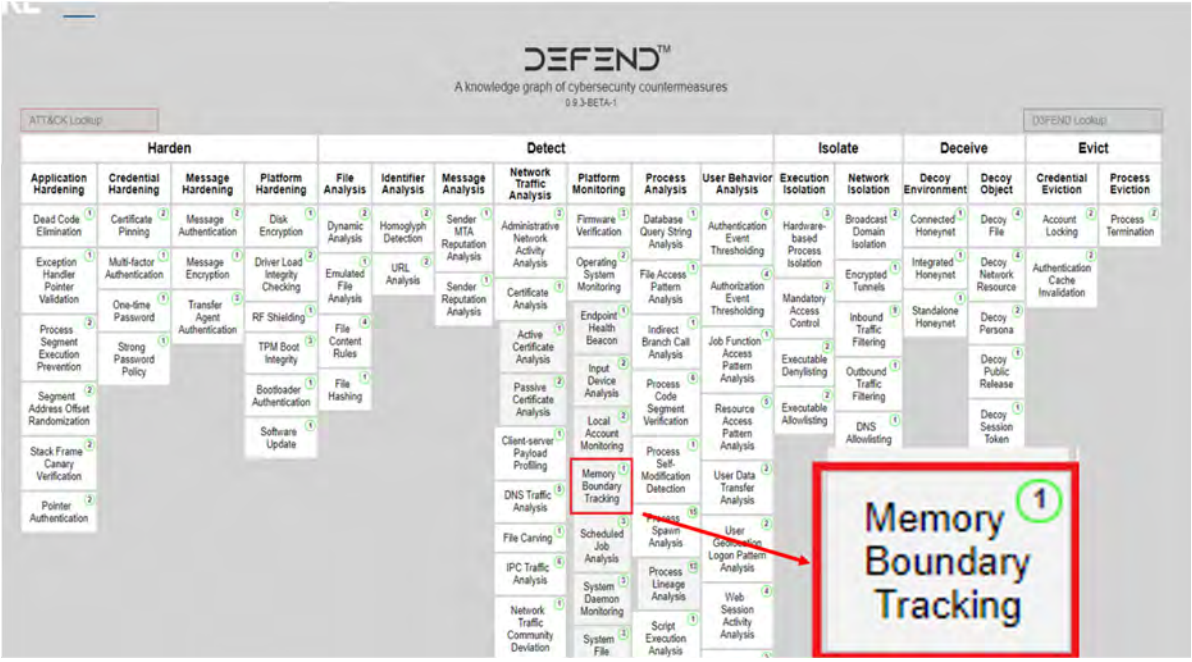
263. On information and belief, the Accused Products perform a method that includes *executing stack walk processing upon the invocation of one of the plurality of functions in the*

monitored memory space [*and*] *performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior*. For example, to protect against fileless attacks, Trend Micro's "Security Agent policies provide increased real-time protection against the latest fileless attack methods through enhanced memory scanning for suspicious process behaviors [and] can terminate suspicious processes before any damage can be done." (*See* WBR_TMC007314, Apex One Administrator's Guide 1-2.) In another example, the Accused Products' enhanced memory scanning protects against fileless attacks including in-memory exploits and misuse of tools such as BITSAdmin, CertUtil, and msiexec and "scripts that run directly on the command line for fileless payload delivery and malicious command execution." (*See* WBR_TMC006205, *Fileless Threats 101*, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems.) Thus, on information and belief, Trend Micro's enhanced memory scanning traces a memory stack for fileless attack prevention.

264. As an additional example, in response to an illegal file access event, Trend Micro's Cloud One Security performs a stack trace leading back to execution. Trend Micro's Cloud One offers "visibility into how the vulnerability in your code would have been exploited, including a stack trace down to the line of code." (*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf.) On information and belief, performing the stack trace requires a stack walking process to trace back the code executions in memory.

265. In another example, the Accused Products "provide[] general information about threats detected by Attack Discovery" including "Tactics" and "Techniques" mapped to the

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework. (*See* WBR_TMC007314, *Apex One Administrator's Guide*, https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf at B-11.) The MITRE ATT&CK framework includes companion project D3FEND for defensive cybersecurity techniques, which includes "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." On information and belief, the Accused Products incorporate the MITRE D3FEND defensive cybersecurity techniques including "Memory Boundary Tracking."



Memory Boundary Tracking

ID: D3-MBT (Memory Boundary Tracking)

Definition

Analyzing a call stack for return addresses which point to unexpected memory locations.

How it works

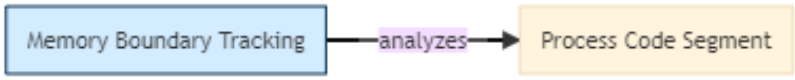
This technique monitors for indicators of whether a return address is outside memory previously allocated for an object (i.e. function, module, process, or thread). If so, code that the return address points to is treated as malicious code.

Considerations

Kernel malware can manipulate memory contents, for example modifying pointers to hide processes, and thereby impact the accuracy of memory allocation information used to perform the analysis.

Digital Artifact Relationships:

This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.



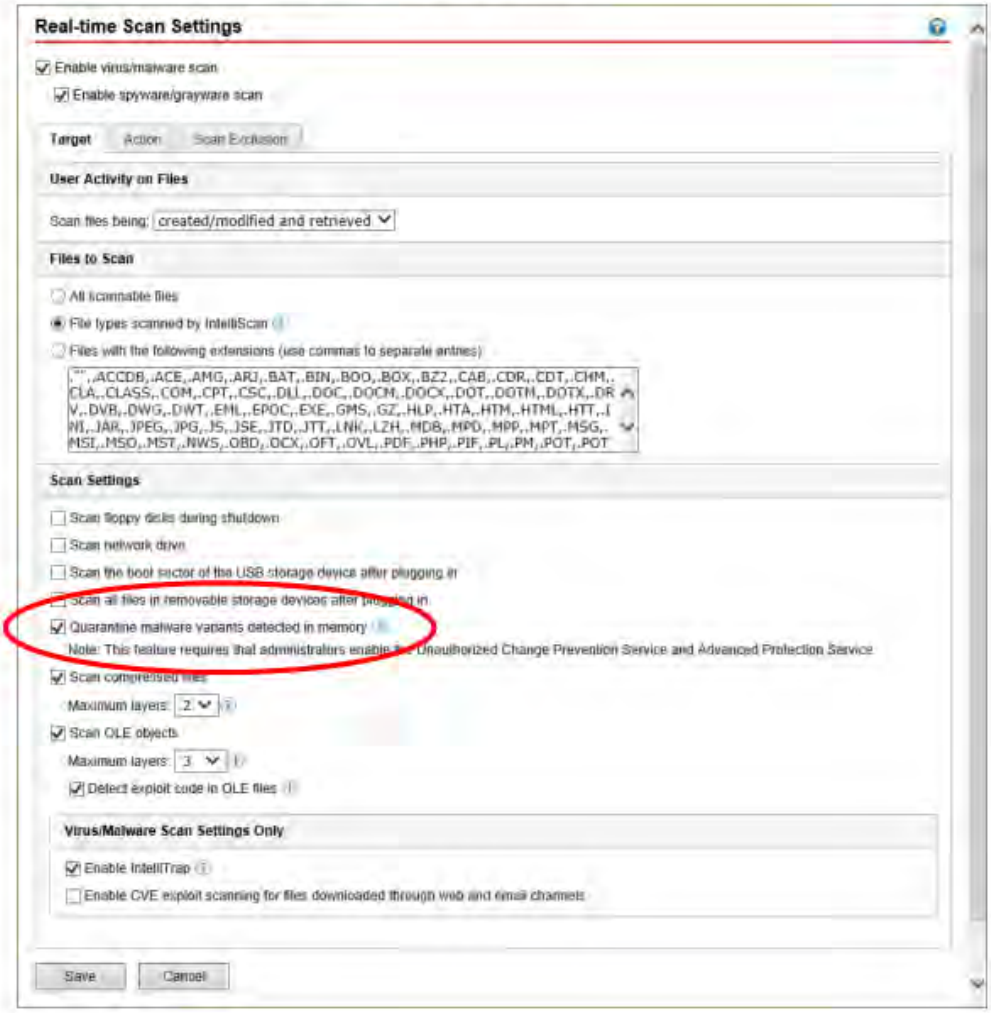
(*See* WBR_TMC007250, https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking; *see also* WBR_TMC020110, https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html; WBR_TMC020494, https://d3fend.mitre.org/resources/D3FEND.pdf.)

266. The Accused Products perform a method that includes *wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area.* For example, the Accused Products monitor memory for "actions that are not typically performed by a given process. Using a number of mechanisms, including Data Execution Prevention (DEP)" and "Structured Exception Handling Overwrite Protection (SEHOP)…Deep Security can determine whether a process has been compromised and then terminate the process to prevent further infection." (*See* WBR_TMC018641, https://help.deepsecurity.trendmicro.com/20_0/on-premise/anti-malware-behavior-monitoring.html.) These detected actions or process would include, for example, "inject[ing] code into user processes through DLL injection, which calls an

API with escalated privilege." (*Id.*) When one of these of these suspicious behaviors are identified, the Accused products trigger an alert by blocking and/or quarantining the detected malware. (*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html.)

267. The Accused Products perform a method that includes *wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating*. For example, the Accused Products include "Security Agents [that] can terminate suspicious processes before any damage can be done" and "[t]erminate programs that exhibit abnormal behavior associated with exploit attacks." Additionally, the Accused products can "quarantine malware variants detected in memory." (*See* WBR_TMC006039, *Apex One Installation Guide*, https://docs.trendmicro.com/all/ent/apex-one/2019/en-us/apexOne_2019_iug.pdf at 7-28.) As shown below, Apex One can be configured to invoke certain functions for quarantining malware variants that are detected in memory during the Dynamic Memory Scan. On information and belief, this feature prevents unauthorized changes or prevents execution of the invoked function.

Dynamic Memory Scan is configured in the **Real-Time Scan Settings** by enabling **Quarantine malware variants detected in memory**. In addition, the **Unauthorized Change Prevention Service** and **Advanced Protection Service** must be enabled.



(*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 212.)

268. Each claim in the ’591 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’591 Patent.

269. Trend Micro became aware of the ’591 Patent at least when the original Complaint was filed in March 2022. Plaintiffs have also marked their products with the ’591 Patent, including

on its web site, since at least July 2020.

270. Defendant directly infringes at least claim 1 of the ’591 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 this software and system to protect its 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.

271. Defendant’s partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’591 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

272. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’591 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’591 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

273. Defendant 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.

274. Defendant further encourages and induces its customers to infringe claim 1 of the ’591 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator’s Guide; WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf.)

275. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

276. 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 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 '591 Patent.

277. 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 '591 Patent.

278. 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 the Accused Products into the United States, 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.

279. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including fileless attack protection and enhanced memory scanning, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could,

the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’591 Patent, that functionality could not be performed.

280. Additionally, the accused functionality, including the collecting and correlating and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products’ enhanced memory scanning functionality, the Accused Products could not detect and protect against fileless attacks. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’591 Patent, that functionality could not be performed.

281. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the memory scanning functionality) constitute a material part of the inventions claimed because such scanning is integral to the processes identified above (such as executing a stack walk for suspicious behavior) as recited in the claims of the ’591 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

282. Defendant's infringing actions have continued after the original Complaint was filed. Defendant had knowledge of the '591 Patent and of the specific conduct that constitutes infringement of the '591 Patent at least based on the original Complaint, yet has continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

283. 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 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 '591 Patent.

284. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant's infringement of the '591 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.

285. 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 '591 Patent.

286. Defendant's infringement of the '591 Patent is knowing and willful. Defendant had actual knowledge of the '591 Patent at least by the time Plaintiffs filed this lawsuit and had

constructive knowledge of the ’591 Patent from at least the date Plaintiffs marked their products with the ’591 Patent and/or provided notice of the ’591 Patent on their website.

287. 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 ’591 Patent with knowledge of the ’591 Patent constitutes willful infringement.

288. Plaintiffs allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs’ Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court’s Standing Order Governing Patent Proceedings served July 12, 2022.

SIXTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’844 PATENT)

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

290. Trend Micro 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, for example Apex One, include features such as Trend Micro’s Predictive Machine Learning Engine or Trend Micro’s TrendX Hybrid Machine Learning Model that, when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’844 Patent as demonstrated below.

291. For example, 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.

292. The Accused Products perform each of the method steps 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.

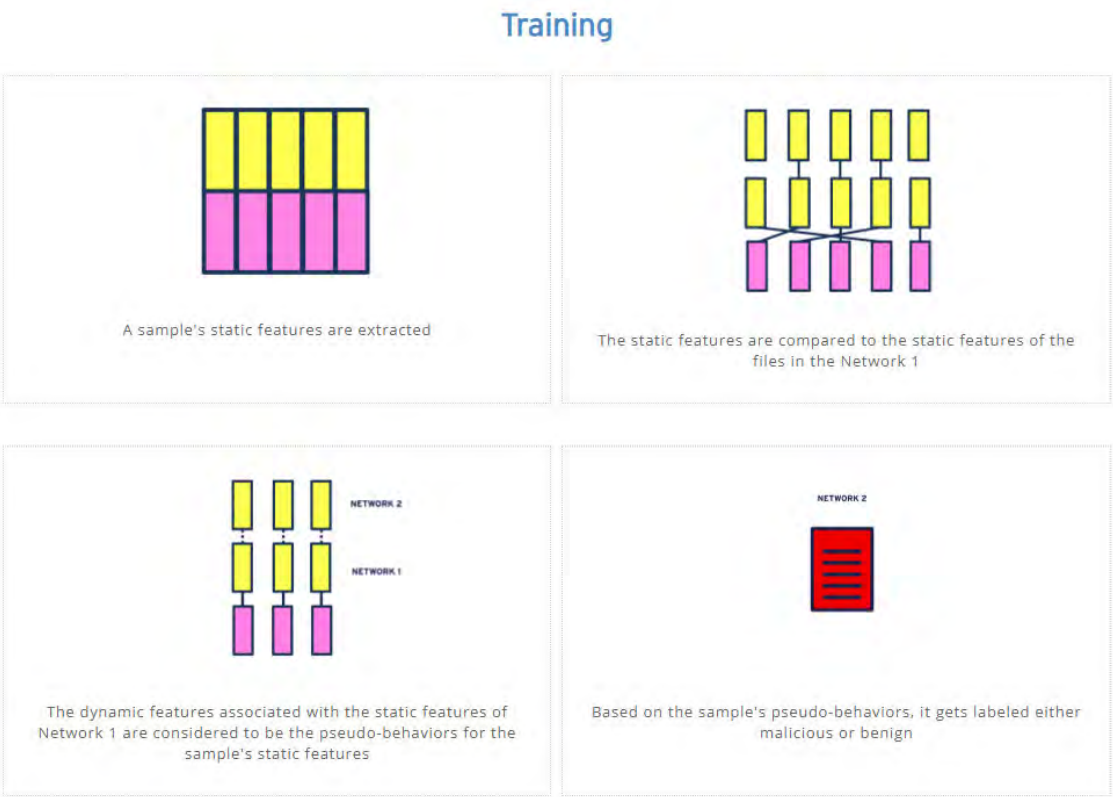
293. The Accused Products perform a method that includes "*extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file*." For example, Apex One uses "machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features." (*See* WBR_TMC006596, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx.) According to the "File" detection type, "[a]fter detecting an unknown or low-prevalence file, the Security Agent scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network." (*See* WBR_TMC006596, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx.) On information and belief, Apex One's Predictive Machine Learning extracts file

features without regard to whether or not the file was encrypted or packed. For example, in a report on Machine Learning, Trend Micro explains the static method to malware detection "allows for the quick analysis of a file without needing it to be executed within a system." (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.) Instead, a machine learning model can decipher whether a file is malicious or not based on its static information or attributes" such as its "header information, printable strings, and its file type and size, serve as the bases of a file's basic signature." (*Id.*)

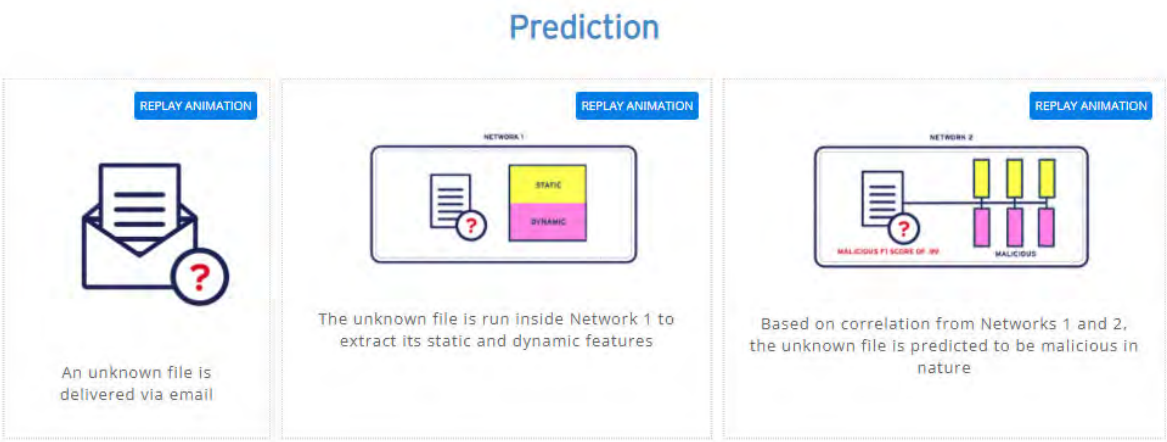
294. The Accused Products, including Trend Micro's Apex One, perform a method that includes "*extracting a plurality of static data points … wherein the plurality of static data points represent predefined character strings in the executable file*." As discussed above, Apex One uses an Advanced Threat Scan Engine (ATSE) to extract file features. The file features include "header information, printable strings, and its file type and size." (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

295. The Accused Products, including Trend Micro's Apex One, 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.*" For example, as shown below, Trend Micro's machine learning model creates a training model using static data features. For example, "[i]n the pre-training phase, large volumes of known samples gathered from the Trend Micro™ Smart Protection Network™ infrastructure are used"

including extracting "[s]tatic features." (*Id.*) These samples would include malware, known benign files, such as known good files, and known unwanted files such as grayware. (*See, e.g.*, WBR_TMC002543, *Datasheet: Trend Micro Apex One*, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3a-con-datasheet-e4288a; *see also* WBR_TMC007254, https://success.trendmicro.com/solution/1121211-excluding-spyware-grayware-detections.) "The extracted features are then mapped out to determine which static features are related to the dynamic or behavioral features." (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.) The pairs of features collected are then used to train a machine learning model." In the training phase, "[s]tatic features and the corresponding predicted behaviors from Network 1 are used to predict if the file is malicious or otherwise and is, afterwards, labeled. The result of this stage is called Network 2." (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)



(*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.) Furthermore, as shown below, Trend Micro uses the trained data set to predict if an unknown file is malicious or benign. On information and belief, these predictions are based on a feature vector generated by the plurality of static data points.



(*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

296. For example, the collection of extracted features is assembled into a feature vector before comparison with the machine learning model. Trend Micro identifies a patent application ("U.S. Patent App. 15/659,403") for its machine learning model. (*See* WBR_TMC020512, U.S. Pub. 2019/0034632 A1 (the "'632 Publication"); *see also* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.) The '632 Publication describes the "second network" as "an artificial neural network for a deep learning model" that "is trained" using the static features and predicted-behavior features as input data, and a malicious label data as output, where the malicious label is "already known data that indicates whether each of the known sample is malicious or benign." (*See* '632 Publication at [0046].)

297. The '632 Publication further describes the detection stage during which files are determined as malware or not. (*See* '632 Publication at [0048].) The '632 Publication explains

"[t]he unknown sample 402 is scanned or processed 104 to extract static features 106…. [, which] are then used by the first network 115 to generate associated predicted-behavior features 302 for the unknown sample 402." (*See* '632 Publication at [0049].) Once "[t]he extended static feature set [] includes both the static features 106 and the predicted-behavior features 302 [it] is then used as input data by the second network 305 to generate a real-time prediction 404 in the form of a malicious score." (*Id*.) In other words, the extracted features are arranged into a feature vector to generate predicted behavior features, which is then used for the prediction phase.

298. The Accused Products, including Trend Micro's Apex One, 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 … wherein the collection of data comprises at least a portion of the plurality of static data points*." As explained above for the prior limitation, once Trend Micro's machine learning models have been trained, they are used to predict whether an unknown file is malicious. Trend Micro advertises that when an unknown file is received its static and dynamic features are extracted. The extracted features are then compared against the machine learning model to predict whether the file is malicious or benign. (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features; *see also* '632 Publication at [0048]-[0050].)

299. The Accused Products, including Trend Micro's Apex One, 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 … 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 discussed above, Trend Micro's Apex One, as well as other Trend Micro products, rely on machine learning to identify malware threats. Trend Micro advertises that its machine learning uses "noise cancellation for minimizing false positives." (*See* WBR_TMC006612, https://www.trendmicro.com/en_us/business/capabilities/machine-learning.html.) On information and belief, that includes selectively turning on or off one or more features of the feature vector 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.

300. In addition, Trend Micro advertises that its machine learning engine takes into consideration that "what is malicious can be environment-dependent." (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.) Trend Micro explains that adware, for example "can be considered malicious in certain environments, but not in some." Thus, on information and belief, depending on the environment being monitored, certain features are selectively turned on and off to prevent detecting malware in an environment where it would not be considered malware.

301. The Accused Products, including Trend Micro's Apex One, perform a method that includes "*evaluating the feature vector using support vector processing to determine whether the executable file is harmful*." As discussed above, Apex One, as well as other Trend Micro products, rely on machine learning models that once trained, can predict whether an unknown file is malicious. Trend Micro's machine learning model uses support vector processing to determine whether a file is harmful. Trend Micro's '632 Publication describes the detection stage during which files are determined as malware or not. (*See* '632 Publication at [0048].) The '632 Publication explains "[t]he unknown sample 402 is scanned or processed 104 to extract static

features 106…. [, which] are then used by the first network 115 to generate associated predicted-behavior features 302 for the unknown sample 402." (*See* '632 Publication at [0049].) Once "[t]he extended static feature set [] includes both the static features 106 and the predicted-behavior features 302 [it] is then used as input data by the second network 305 to generate a real-time prediction 404 in the form of a malicious score." (*See* '632 Publication at [0050].) In other words, in order to predict whether a file is malicious, Trend Micro's machine learning model first creates and then evaluates a feature vector to predict whether the file is malware or harmful.

302. 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.

303. Trend Micro has been aware of the '844 Patent since at least March 31, 2020 when an examiner rejected Trend Micro's patent application 15/659,403 over the '844 Patent's prior publication, Publication No. 2016/0225435 to Schmidtler. Trend Micro further became aware of the '844 Patent when the original Complaint was filed in March 2022. Plaintiffs have also marked their products with the '844 Patent, including on its web site, since at least July 2020.

304. 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 this software and system to protect its 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.

305. Defendant's partners, customers, and end users of its 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.

306. 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 willful blindness to the possibility that its acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software 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 engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

307. Defendant 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.

308. Defendant further encourages and induces its customers to infringe claim 1 of the ’844 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC006598 at 6605, https://www.trendmicro.com/vinfo/mx/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-

behavioral-features; WBR_TMC006220, Apex One Student Guide; WBR_TMC018694, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-patch-3-online-help/protecting-trend_cli/using-company_name-s/osce-osce_sm_prot_so.aspx#GUID-523B5AFA-4B86-4A42-AAB3-3ED450693792; WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator's Guide.)

309. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

310. 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 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 ’844 Patent.

311. 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.

312. 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 the Accused Products into the United States, 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.

313. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the machine learning static analysis and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’844 patent, that functionality could not be performed.

314. Additionally, the accused functionality, including the machine learning static analysis related functionality described above, itself has no substantial non-infringing uses because

the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products' machine learning functionality, the Accused could not deploy their machine learning model to determine whether or not an object is malicious or benign based on the object's static features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '844 patent, that functionality could not be performed.

315. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the machine learning static analysis) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above as recited in the claims of the '844 patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

316. Defendant's infringing actions have continued after the original Complaint was filed. Defendant had knowledge of the '844 patent and of the specific conduct that constitutes infringement of the '844 patent at least based on the original Complaint, yet has continued to engage in the infringing activity, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

317. 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 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.

318. 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.

319. 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.

320. Defendant’s infringement of the ’844 Patent is knowing and willful. 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.

321. 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 ’844 Patent with knowledge of the ’844 Patent constitutes willful infringement.

322. Plaintiffs' allegations of infringement, indirect infringement, and willful infringement with respect to this patent are further set forth in Plaintiffs' Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to the Court's Standing Order Governing Patent Proceedings served July 12, 2022.

SEVENTH CAUSE OF ACTION
(INFRINGEMENT OF THE '869 PATENT)

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

324. Trend Micro has infringed and continues to infringe one or more claims of the '869 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 Apex One, include features such as Trend Micro's Predictive Machine Learning Engine or Trend Micro's TrendX Hybrid Machine Learning Model that, when used for their ordinary and customary purposes, practice each element of at least claim 46 of the '869 Patent as demonstrated below.

325. For example, claim 46 the '869 Patent recites:

> A system comprising:
>
> at least one memory;
>
> at least one processor configured to perform operation of:
>
> identifying static data points that may be indicative of either a harmful or benign executable file; and
>
> associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files; and
>
> at least one processor configured to perform operation of:

identifying an executable file to be evaluated;

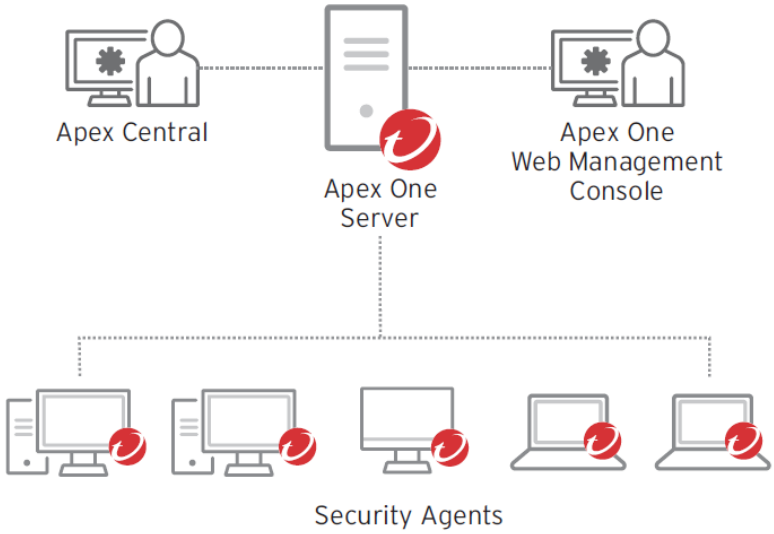
extracting a plurality of static data points from the executable file;

generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and

evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files.

326. To the extent the preamble is limiting, the Accused Products comprise or are used as part of *a system* as further explained below. For example, the Accused Products operate as part of a network of malware protection components, including, among other things, endpoint protection agents and Trend Micro's network of servers and related computers providing the cloud of global information (including Trend Micro's Smart Protection Network). For example, as discussed in the paragraphs that follow, Trend Micro's endpoint agents extract features from files and provide them to Trend Micro's Smart Protection Network for analysis using Trend Micro's machine learning models.

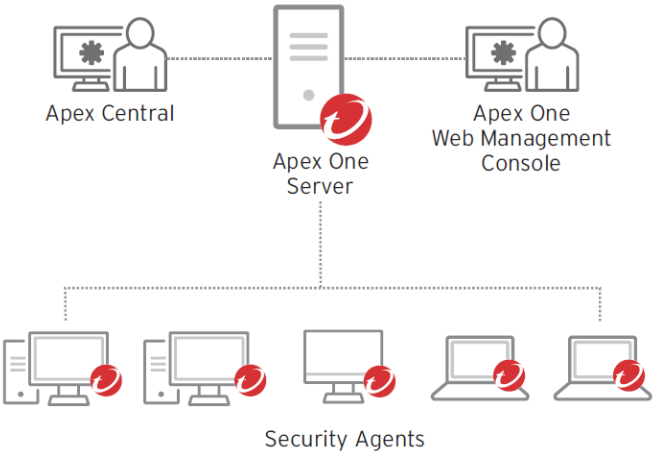
Apex One protects endpoint computers from malware, network viruses, Web-based threats, spyware, and mixed threat attacks (both known and unknown). It uses a client/server architecture that consists of a Security Agent program that resides on the endpoint and a Server program that manages all Agents. The Agent guards the endpoint and reports on its security status to the Server. Apex One offers threat detection, response, and investigation within a single agent on both Windows and Mac computers.



(*See* WBR_TMC006220, *Apex One Student Guide* at 6235.)

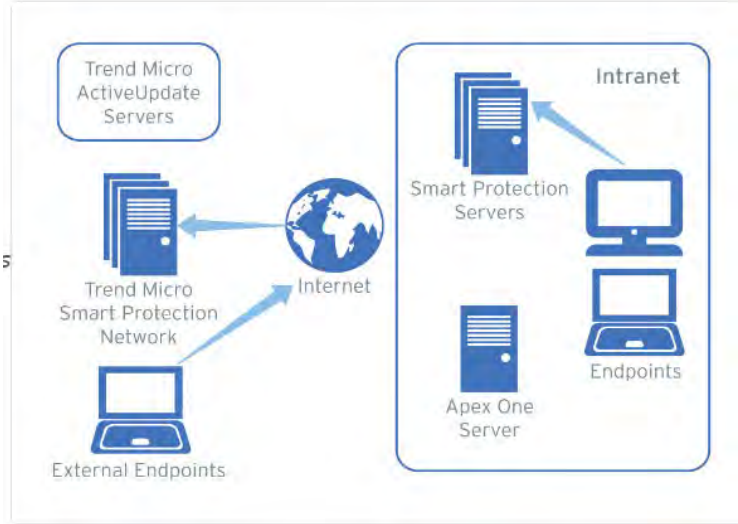
327. The system comprising the Accused Products include *at least one memory*. For example, Trend Micro's Smart Protection Network receives information from endpoint devices across the globe and uses it to train Trend Micro's machine learning model. Both the end point devices and the computers/servers that comprise the Smart Protection Network include one or more memory to store instructions for execution by processors to perform the analyses described herein, the received information (*e.g.*, concerning objects and processes), and/or the machine learning models (as well as the instructions for creating the models, training the models, executing the models, as well as the data associated with those processes).

Apex One protects endpoint computers from malware, network viruses, Web-based threats, spyware, and mixed threat attacks (both known and unknown). It uses a client/server architecture that consists of a Security Agent program that resides on the endpoint and a Server program that manages all Agents. The Agent guards the endpoint and reports on its security status to the Server. Apex One offers threat detection, response, and investigation within a single agent on both Windows and Mac computers.



(*See* WBR_TMC006220, *Apex One Student Guide* at 6235.)

328. The system comprising the Accused Products further comprises *at least one processor*. For example, the end point devices and the computers/servers that comprise the Smart Protection Network include one or more processors that execute instructions to perform the analyses described herein. Indeed, as shown above, the end point devices execute the "security agents" using one or more processors, and Trend Micro's Smart Protection Network comprises one or more computers or servers that each include one or more processors for performing the operations associated with the Smart Protection Network's functionality. For example, the image below illustrates Trend Micro's Smart Protection Network as running on one or more servers.



(*See* WBR_TMC020523, *Usage of Smart Protection Patterns*, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-patch-3-online-help/protecting-trend_cli/using-company_name-s/smart-protection-pat/usage-of-smart-prote.aspx.)

329. One or more processors in systems comprising the Accused Products are configured to perform operation of *identifying static data points that may be indicative of either a harmful or benign executable file* and *associating the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files*. For example, the Accused Products use "machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features."

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

(*See* WBR_TMC006596, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-

l.aspx.)

330. The Accused Products use "Predictive Machine Learning" that "uses algorithms to examine large volumes of information or training data to discovery unique patterns." "Predictive Machine Learning can evaluate unknown threats found in suspicious process of files" "by using good and bad sample files to extract the file features that will be used to train the Machine Learning Model"—a model that "takes advantage of Trend Micro's Smart Protection Network and Threat Research," which facilitates "educat[ing] the model with the file features that will enable the technology to have high detection rate." After an Accused Product "detects an unknown file or process, it extracts the file/process features to the model and uses the technology to predict if the file is good or bad."

Predictive Machine Learning

Apex One incorporates Predictive Machine Learning technology to provide better protection for threats such as ransomware or advanced persistent threats.

Predictive Machine Learning operates on the concept that a computer can learn information without human mediation. It uses algorithms to examine large volumes of information or training data to discover unique patterns. This system analyzes these patterns, groups them accordingly, and makes predictions. Through repetition, it learns by inference without a need to be deliberately programmed each and every time.

Predictive Machine Learning can evaluate unknown threats found in suspicious process of files originating from USB, web, or email channels. It does this by using good and bad sample files to extract the file features that will be used to train the Machine Learning Model. This model takes advantage of Trend Micro's Smart Protection Network and Threat Research, to educate the model with the file features that will enable the technology to have high detection rate.

Once Apex One detects an unknown file or process, it extracts the file/process features to the model and uses the technology to predict if the file is good or bad.

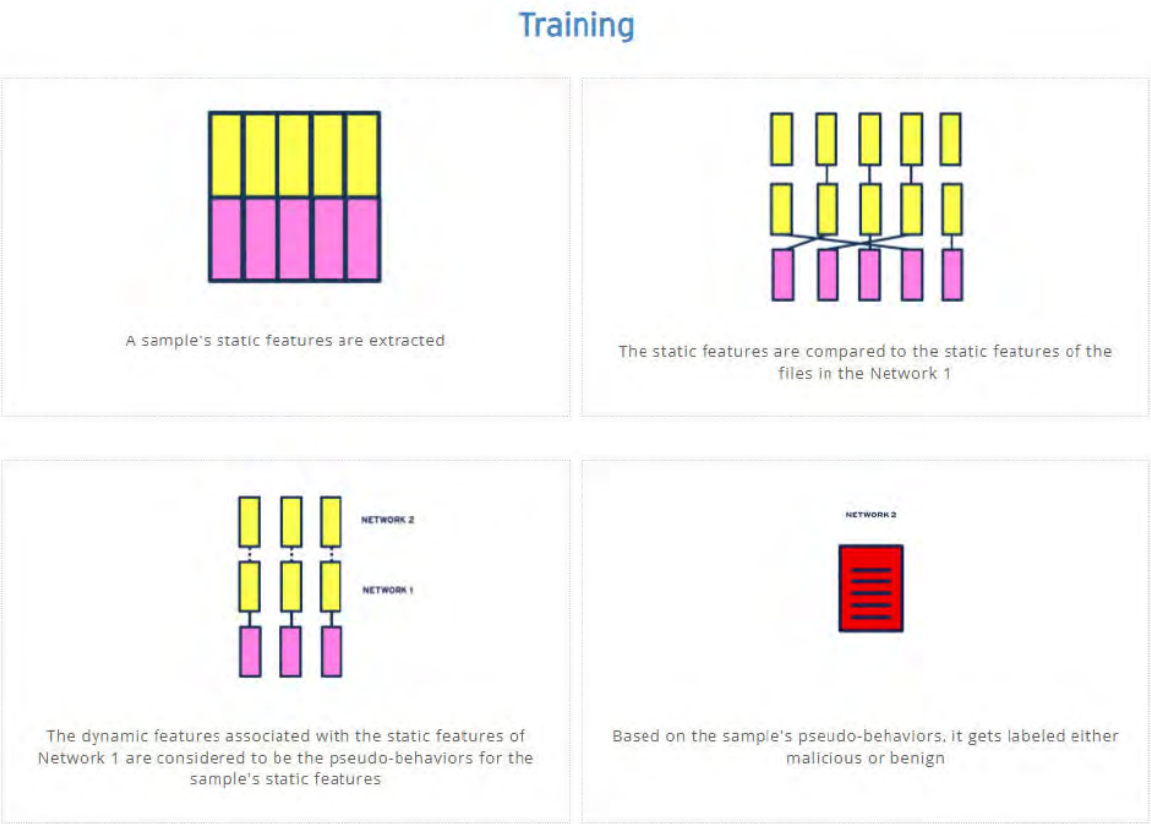
(*See* WBR_TMC006220, *Apex One Student Guide* at 6439.)

331. As an example, the Smart Protection Network is responsible for gathering "large volumes of known samples" and training machine learning models on those samples. (*See* WBR_TMC006598, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-

correlating-static-and-behavioral-features.) Training begins in the pre-training phase. "Static features are extracted, and the samples are also run in a sandbox to extract their dynamic features." (*Id.*) "The extracted features are then mapped out to determine which static features are related to the dynamic or behavioral features." Once mapped, the features "are used to predict if [a] file is malicious or otherwise." (*Id.*) In the training phase, "Network 1, which contains the correlations between static and dynamic features, is used to analyze a sample." (*Id.*) Then, "[s]tatic features and the corresponding predicted behaviors from Network 1 are used to predict if the file is malicious or otherwise and is, afterwards, labeled. The result of this stage is called Network 2." (*Id.*)

> The training phase is the machine learning stage of typical hybrid models. Network 1, which contains the correlations between static and dynamic features, is used to analyze a sample. Samples in training and pre-training don't need to be the same files.
>
> In this stage, the known sample for training no longer needs to be executed in the sandbox to identify its behavior. Static features and the corresponding predicted behaviors from Network 1 are used to predict if the file is malicious or otherwise and is, afterwards, labeled. The result of this stage is called Network 2.

(*See* WBR_TMC006598 at 6606, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)



(*See* WBR_TMC006598 at 6605, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

332. One or more processors in systems comprising the Accused Products are configured to perform operation of *identifying an executable file to be evaluated* and *extracting a plurality of static data points from the executable file.*" For example, as explained above, in the example system comprising endpoint devices that include one or more processors, the endpoint sensors or agents employ Trend Micro's Advanced Threat Scan Engine to determine which executable files need to be evaluated. According to the "File" detection type, "[a]fter detecting an unknown or low-prevalence file, the Security Agent scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on

the Trend Micro Smart Protection Network." "Through the use of malware modeling, [Predictive Machine Learning] compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains."

Detection Type	Description
File	After detecting an unknown or low-prevalence file, the Security Agent scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains.

(*See* WBR_TMC006596, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx.)

333. As another example, the Accused Products use "machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features." Trend Micro's product information explains that the static method to malware detection "allows for the quick analysis of a file without needing it to be executed within a system" and that "a machine learning model can decipher whether a file is malicious or not based on its static information or attributes" such as its "header information, printable strings, and its file type and size," which "serve as the bases of a file's basic signature."

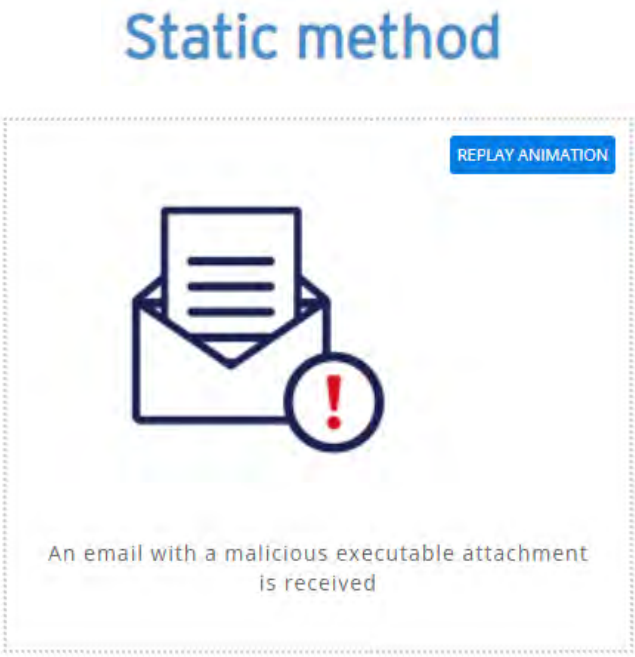
Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

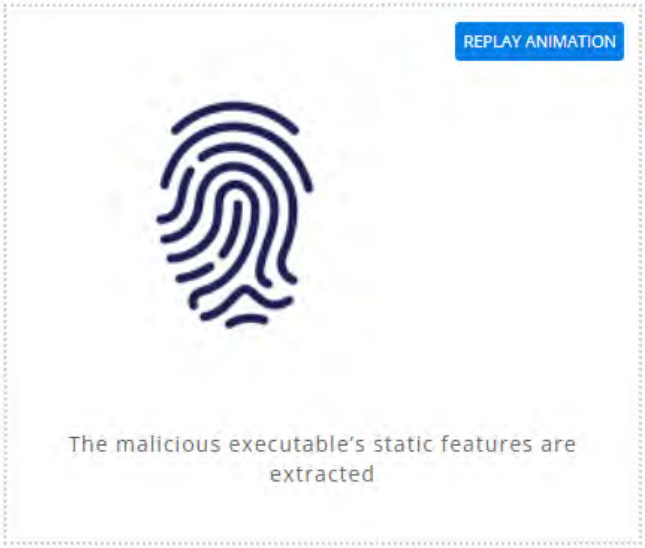
(*See* WBR_TMC006596, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx.)

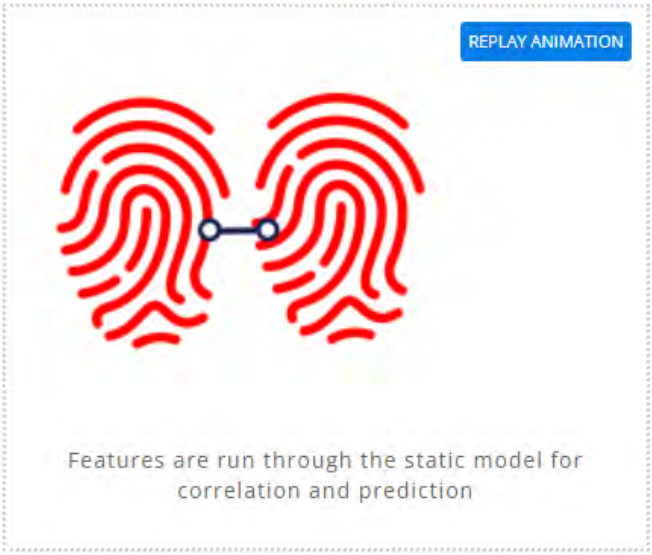
> The basic static approach allows for the quick analysis of a file without needing it to be executed within a system. Instead, a machine learning model can decipher whether a file is malicious or not based on its static information or attributes. A file's technical indicators, such as its hashes, header information, printable strings, and its file type and size, serve as the bases of a file's basic signature.

(*See* WBR_TMC006598 at 6601, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

334. As an example, when "[a]n email with a malicious executable attachment is received," "[t]he malicious executable's static features are extracted," and those "[f]eatures are run through the static model for correlation and prediction."







(*See* WBR_TMC006598 at 6600, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

335. In addition, as explained above, the Accused Products use a hybrid approach called the "TrendX Hybrid Model" that uses both static analysis and dynamic analysis, and involves "[p]re-training, training, and predicting phases." (*See* WBR_TMC006598 at 6608, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-

accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.) Trend Micro's product information explains that the "static approach" is faster than other approaches "[b]ecause a file doesn't have to be executed."

> The static approach does not always work, especially for more sophisticated attacks. What it lacks in comprehensiveness, however, it makes up for in speed. Because a file doesn't have to be executed, information can be extracted faster.

(*See* WBR_TMC006598 at 6601, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

336. One or more processors in systems comprising the Accused Products are configured to perform operation of *generating a feature vector from the plurality of static data points using a classifier trained to classify the static data points based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range*. As explained above, the Accused Products "detect an unknown file or process[] … extracts the file/process features to the model and uses the technology to predict if the file is good or bad." (*See* WBR_TMC006220, *Apex One Student Guide* at 6439.)

Predictive Machine Learning

Apex One incorporates Predictive Machine Learning technology to provide better protection for threats such as ransomware or advanced persistent threats.

Predictive Machine Learning operates on the concept that a computer can learn information without human mediation. It uses algorithms to examine large volumes of information or training data to discover unique patterns. This system analyzes these patterns, groups them accordingly, and makes predictions. Through repetition, it learns by inference without a need to be deliberately programmed each and every time.

Predictive Machine Learning can evaluate unknown threats found in suspicious process of files originating from USB, web, or email channels. It does this by using good and bad sample files to extract the file features that will be used to train the Machine Learning Model. This model takes advantage of Trend Micro's Smart Protection Network and Threat Research, to educate the model with the file features that will enable the technology to have high detection rate.

Once Apex One detects an unknown file or process, it extracts the file/process features to the model and uses the technology to predict if the file is good or bad.

(WBR_TMC006220, *Apex One Student Guide* at 6439.)

As discussed above with respect to Trend Micro's Smart Protection Network, the "Predictive Machine Learning" ("uses algorithms to examine large volumes of information or training data to discover[] unique patterns." (*See* WBR_TMC020525, https://www.trendmicro.com/vinfo/us/security/definition/ machine-learning?) "Predictive Machine Learning can evaluate unknown threats found in suspicious process of files" "by using good and bad sample files to extract the file features that will be used to train the Machine Learning Model." (*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 220.) Indeed, these samples include malware, known benign files, such as known good files, and known unwanted files such as grayware. "Predictive Machine Learning accuracy is largely based on the training from existing verified good and bad files in which the Trend Micro Smart Protection Network is a key component." (*See* WBR_TMC020114,

Apex One Training for Certified Professionals Student Guide, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 221.)

Enhanced application control against malicious software

Prevent unknown and unwanted applications from executing on your corporate endpoints. Trend Micro Apex One™ Application Control allows you to:

- ✓ Block malicious software from running using customizable lockdown, safelisting, and denylisting policies
- ✓ Create dynamic policies by leveraging Trend Micro's application categorization and reputation intelligence to reduce management overhead
- ✓ Correlate data from millions of application events to identify threats and maintain an up-to-date database of validated applications

(*See* WBR_TMC001652, *Trend Micro Vision One* at 1660, https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html.)

Excluding Spyware/Grayware detections

Product/Version includes

Update Date: 2020/01/15 **Article Number:** 000196815

Category: Configure, Remove a Malware / Virus **Rating:** 0

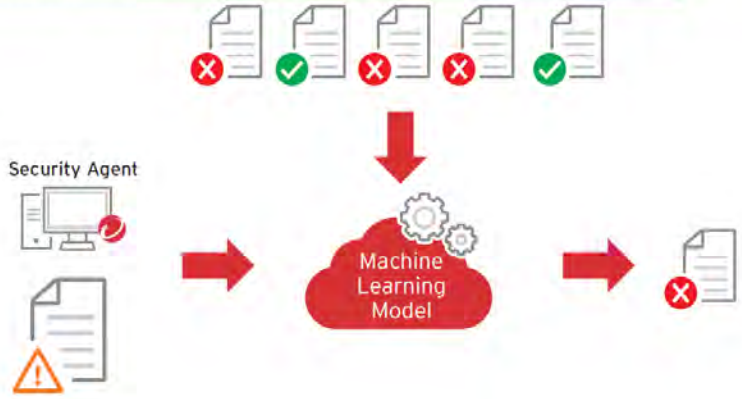
Summary

Grayware refers to applications that have annoying, undesirable, or undisclosed behavior but do not fall into any of the major threat categories such as Virus, Trojan, and Worm. Spyware falls under the Grayware category. It is an application that monitors, gathers personal information, and sends to a third party without the user's knowledge or consent.

There are instances wherein a user's application is detected as Spyware/Grayware. In the event that the application is verified to be malicious, the detection cannot be lifted. Learn how to exclude Spyware/Grayware detections in different Trend Micro products.

(*See* WBR_TMC007254 at 7254, https://success.trendmicro.com/dcx/s/solution/1121211-excluding-spyware-grayware-detections?language=en_US.)

The Predictive Machine Learning design utilizes Portable Executable (PE) file features, such as Opcode, Import table or others like Entropy and Icon to train the Machine Learning Model.



* * * * *

Predictive Machine Learning accuracy is largely based on the training from existing verified good and bad files in which the Trend Micro Smart Protection Network is a key component.

(*See* WBR_TMC006220, *Apex One Student Guide* at 6440.)

337. The machine learning 143nalysis described above and implemented in the Accused

Products also uses "noise cancellation for minimizing false positives."

- **Pre-execution, run-time machine learning techniques, and noise cancellation for minimizing false positives**

(*See* WBR_TMC018720, https://www.trendmicro.com/en_us/business/technologies/machine-learning.html.)

Noise-cancelling techniques – like census and safelisting – throughout every layer of detection to dramatically reduce false positives

(*See* WBR_TMC001652 at 1656, *Trend Micro Vision One*, https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html.)

Leveraging pre-execution and run-time machine learning techniques, along with noise cancellation for minimizing false positives, high-fidelity machine learning delivers multiple layers of detection on new malware and attacks. Layered with other state-of-the art techniques, like behavioral analysis, machine learning provides detection of nearly all new malware without the need for updates.

(*See* WBR_TMC0006612, Machine Learning Threat Prevention Software.)

338. As another example, the Accused Products' machine learning engine takes into consideration that "what is malicious can be environment-dependent." Trend Micro explains that adware, for example "can be considered malicious in certain environments, but not in some."

In the prediction phase, Network 1 and Network 2 are used to predict if an unknown file is malicious or benign. This is especially helpful since the concept of what is malicious can be environment-dependent — adware can be considered malicious in certain environments, but not in some.

(*See* WBR_TMC006598 at 6608, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-

correlating-static-and-behavioral-features.)

339. One or more processors in systems comprising the Accused Products are configured to perform operation of *evaluating the feature vector using a machine learning model to determine whether the executable file fits into one of the categories of files*. For example, the Accused Products use "machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features." After the Accused Products "detect[] an unknown file or process, [they] extract[] the file/process features to the model and uses the technology to predict if the file is good or bad."

Predictive Machine Learning

Apex One incorporates Predictive Machine Learning technology to provide better protection for threats such as ransomware or advanced persistent threats.

Predictive Machine Learning operates on the concept that a computer can learn information without human mediation. It uses algorithms to examine large volumes of information or training data to discover unique patterns. This system analyzes these patterns, groups them accordingly, and makes predictions. Through repetition, it learns by inference without a need to be deliberately programmed each and every time.

Predictive Machine Learning can evaluate unknown threats found in suspicious process of files originating from USB, web, or email channels. It does this by using good and bad sample files to extract the file features that will be used to train the Machine Learning Model. This model takes advantage of Trend Micro's Smart Protection Network and Threat Research, to educate the model with the file features that will enable the technology to have high detection rate.

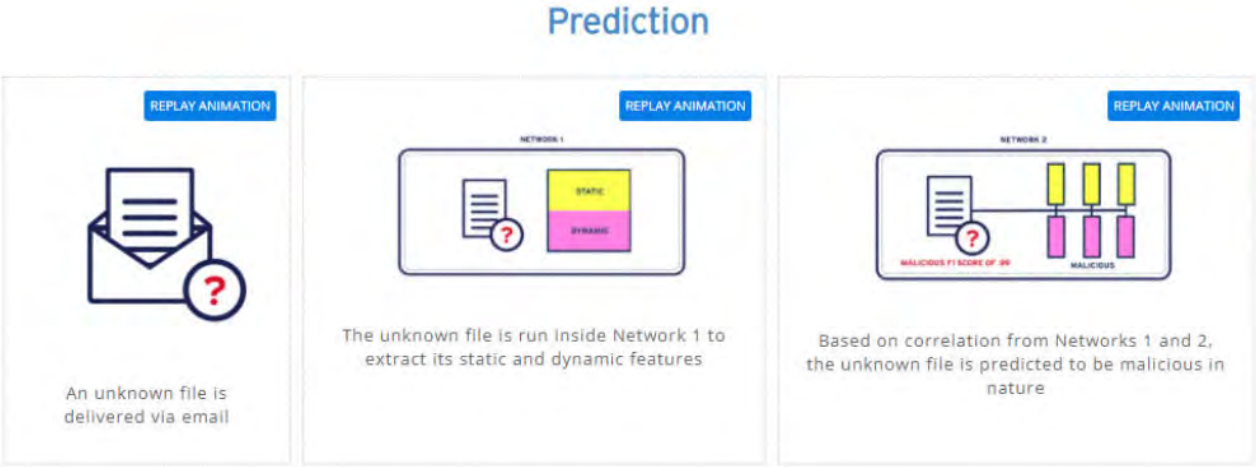
Once Apex One detects an unknown file or process, it extracts the file/process features to the model and uses the technology to predict if the file is good or bad.

(*See* WBR_TMC006220, *Apex One Student Guide* at 6439.)

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

(*See* WBR_TMC006596, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/predictive-machine-l.aspx.)

340. Additionally, Trend Micro's Agents send extracted features to the Smart Protection Network where machine learning models reside. Using "Network 1" and "Network 2" in Trend Micro's "TrendX Hybrid Model," Trend Micro uses the trained data set to predict if an unknown file is malicious or benign.



(*See* WBR_TMC006598 at 6607, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

341. For example, "U.S. Patent App. 15/659,403" (now WBR_TMC020512, U.S. Pub. 2019/0034632 A1 (the "'632 Publication"))—is identified as describing Trend Micro's "TrendX Hybrid Model."

> The TrendX Hybrid Model, a patent-pending innovation (U.S. Patent App. 15/659,403), aims to provide a faster and smarter solution to detecting malware using machine learning technologies. Because it uses both static and dynamic features to analyze unknown files, accuracy is not sacrificed for the sake of efficiency.

(*See* WBR_TMC006598 at 6608, https://www.trendmicro.com/vinfo/br/security/news/security-technology/faster-and-more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features.)

342. The ’632 Publication describes the Accused Products as having a detection stage during which files are determined as malware or not. (*See* ’632 Publication at [0048].) The ’632 Publication explains that “[t]he unknown sample 402 is scanned or processed 104 to extract static features 106…. [, which] are then used by the first network 115 to generate associated predicted-behavior features 302 for the unknown sample 402.” (*See* ’632 Publication at [0049].) Once “[t]he extended static feature set [] includes both the static features 106 and the predicted-behavior features 302 [it] is then used as input data by the second network 305 to generate a real-time prediction 404 in the form of a malicious score.” (*See* ’632 Publication at [0050].)

343. Each claim in the ’869 Patent recites an independent invention. Neither claim 46, described above, nor any other individual claim is representative of all claims in the ‘869 Patent.

344. Trend Micro has been aware of the ’869 Patent since at least the filing of the First Amended Complaint.

345. Defendant directly infringes at least claim 46 of the ’869 Patent, either literally or under the doctrine of equivalents, by practicing the elements described above. For example, on information and belief, Defendant makes and uses the claimed system in an infringing manner as described above by running this software and system to protect its own computer and network operations. On information and belief, Defendant also makes and uses the claimed system 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.

346. Defendant's partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 46 of the '869 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

347. Defendant has actively induced and is actively inducing infringement of at least claim 46 of the '869 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, Defendant encourages and induces customers with specific intent to use Trend Micro's security software in a manner that infringes claim 46 of the '869 Patent at least by offering and providing software that and/or hardware that embodies the system that infringes claim 46 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

348. Defendant encourages, instructs, directs, and/or requires third parties—including its certified partners and/or customers—to practices the claims using the software, services, and systems in infringing ways, as described above.

349. Defendant further encourages and induces its customers to infringe claim 46 of the '869 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 its Trend Micro security software, and services in the United States. See, e.g., (See, e.g., WBR_TMC006598 at 6605, https://www.trendmicro.com/vinfo/mx/security/news/security-technology/faster-and-

more-accurate-malware-detection-through-predictive-machine-learning-correlating-static-and-behavioral-features; WBR_TMC006220, Apex One Student Guide; WBR_TMC018694, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-patch-3-online-help/protecting-trend_cli/using-company_name-s/osce-osce_sm_prot_so.aspx#GUID-523B5AFA-4B86-4A42-AAB3-3ED450693792; WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator's Guide.)

350. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

351. 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 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 ’869 Patent.

352. 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 infringes the claimed system of, and infringes, the ’869 Patent.

353. 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 the Accused Products into the United States, 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.

354. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the machine learning static analysis and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’869 Patent, that functionality could not be performed.

355. Additionally, the accused functionality, including the machine learning static

analysis related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products' machine learning functionality, the Accused could not deploy their machine learning model to determine whether or not an object is malicious or benign based on the object's static features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '869 Patent, that functionality could not be performed.

356. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the machine learning static analysis) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above as recited in the claims of the '869 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

357. 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 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 46 of the ’869 Patent.

358. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’869 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.

359. 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 ’869 Patent.

360. Defendant’s infringement of the ’869 Patent is knowing and willful. Defendant acquired knowledge of the ’869 Patent and of the specific conduct that constitutes infringement of the ’869 Patent at least based on this amended Complaint. Defendant continues to engage in infringing activities after the filing of this amended complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

361. On information and belief, despite Defendant’s knowledge of the Asserted Patents, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant’s continued infringement of the ’869 Patent with knowledge of the ’869 Patent constitutes willful infringement.

EIGHTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’505 PATENT)

362. Plaintiffs reallege and incorporate by reference the allegations of the preceding

paragraphs of this Complaint.

363. Defendant has infringed and continues to infringe one or more claims of the '505 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, The Accused Products, including Trend Micro's Apex One, Network One, Vision One, Endpoint Protection with Detection and Response, Trend Micro's EDR/XDR and Cloud Products, and Trend Micro's Smart Protection Network,, when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '505 Patent, as demonstrated below.

364. For example, claim 1 of the '505 recites:

> 1. A method for managing pestware on a computer comprising:
>
> monitoring events during a boot sequence of the computer;
>
> managing pestware-related events during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded;
>
> managing pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications;
>
> generating, in response to the monitoring, a record of events, the record of events including the pestware-related events;
>
> analyzing the record of events so as to identify the pestware-related event
>
> modifying the set of behavior rules so as to prevent the pestware related events; and
>
> scanning data in a registry of the computer for pestware during the second period in the boot sequence.

365. The Accused Products perform each element of the method of claim 1 of the '505 Patent. To the extent the preamble is construed as limiting, the Accused Products perform *a method*

for managing pestware on a computer, as further exampled below. For example, the Accused Products "offer[] advanced automated threat detection and response against an ever-growing variety of threats, including fileless and ransomware," and "leverage[] a blend of cross-generational threat techniques to provide the broadest protection against all types of threats."

Automated, insightful, all-in-one protection

Automated

Trend Micro Apex One™ protection offers advanced automated threat detection and response against an ever-growing variety of threats, including fileless and ransomware. Our cross-generational blend of modern techniques provides highly tuned endpoint protection that maximizes performance and effectiveness.

Insightful

Get actionable insights, expanded investigative capabilities, and centralized visibility by using an advanced EDR toolset, strong SIEM integration, and an open API set. You have the option to perform correlated, extended threat investigations that go beyond the endpoint and augment your security teams with a managed detection and response service.

All-in-one

In an evolving technological landscape, you need security that goes beyond traditional antivirus. Apex One offers threat detection, response, and investigation within a single agent. Eliminate multiple vendors and consoles and gain deployment flexibility through both SaaS and on-premises deployment options.

Advanced detection techniques

Apex One leverages a blend of cross-generational threat techniques to provide the broadest protection against all types of threats, giving you:

- Pre-execution and runtime machine learning
- More accurate detection of advanced malware, such as fileless, living off the land, and ransomware threats
- Noise-cancelling techniques – like census and safelisting – throughout every layer of detection to dramatically reduce false positives
- Effective protection against scripts, injection, ransomware, memory, and browser attacks through innovative behavior analysis

(*See* WBR_TMC001652, https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html.)

366. The Accused Products perform a method that includes *monitoring events during a boot sequence of the computer*. For example, Apex One includes, among other features, an "Early Boot Cleanup Driver," which "loads before the operating system drivers which enables the detection and blocking of boot-type rootkits."

Damage Cleanup Services Components

COMPONENT	DESCRIPTION
Damage Cleanup Engine 32/64-bit	The Damage Cleanup Engine scans for and removes Trojans and Trojan processes.
Damage Cleanup Template	The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
Early Boot Cleanup Driver 32/64-bit	The Trend Micro Early Boot Cleanup Driver loads before the operating system drivers which enables the detection and blocking of boot-type rootkits. After the Security Agent loads, Trend Micro Early Boot Cleanup Driver calls Damage Cleanup Services to clean the rootkit.

(*See*, WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 199.)

367. When the endpoints "start up," the agent starts "before other third-party" software drivers. The Accused Products then "detect malware during the operating system boot process," including through the "Early Launch Anti-Malware (ELAM) feature as part of the Secure Boot standard to provide boot time protection on end points."

Enable Early Launch Anti-Malware Protection on Endpoints

Apex One supports the Early Launch Anti-Malware (ELAM) feature as part of the Secure Boot standard to provide boot time protection on endpoints. Administrators can enable this feature to start Apex One agents before other third-party software drivers when endpoints start up. This feature enables Apex One agents to detect malware during the operating system boot process.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 327.)

368. The Accused Products perform a method that includes *managing pestware-related events during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded*. For example, the Accused Products include an Early Boot Cleanup Driver, which "loads before the operating system drivers which enables the detection and blocking of boot-type rootkits."

- **Early Boot Cleanup Driver**: The Trend Micro Early Boot Cleanup driver loads before the operating system drivers which enables the detection and blocking of boot-type rootkits. After the Security Agent loads, Trend Micro Early Boot Clean Driver calls Damage Cleanup Services to clean the rootkit.

(*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 201.)

369. The Security Agent loads before the third-party drivers during the boot sequence. The Security Agent scans all third-party software drivers, and after doing so, "reports the driver classification information to the system kernel."

Enable Early Launch Anti-Malware Protection on Endpoints

Apex One supports the Early Launch Anti-Malware (ELAM) feature as part of the Secure Boot standard to provide boot time protection on endpoints. Administrators can enable this feature to start Apex One agents before other third-party software drivers when endpoints start up. This feature enables Apex One agents to detect malware during the operating system boot process.

After scanning all third-party software drivers, the Apex One agent reports the driver classification information to the system kernel. Administrators can define actions based on the driver classifications in Group Policy in Windows and view scan results using Event Viewer on endpoints.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 327.)

370. In addition, the Accused Products integrate with the system kernel, including using a "kernel mode driver [to] monitor[] system events and passes them to the Behavior Monitoring Core Service for policy enforcement." The kernel mode driver passes "system events" to the "Behavior Monitoring Core Service," which "[p]rovides rootkit detection."

Behavior Monitoring Components

COMPONENT	DESCRIPTION
Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.
Behavior Monitoring Core Driver 32/64-bit	This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 200.)

371. The Accused Products perform a method that includes *managing pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications*. As explained above, the Accused Products include kernel level drivers that monitor all periods of the boot sequence. (*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 201; WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 327.) Additionally, the Accused Products include Behavior Monitoring functionality, which constantly operates to detect activity indicative of pestware. For example, "[b]ehavior monitoring constantly monitors endpoints for unusual modifications to the operating system or on

installed software. Behavior Monitoring protects endpoints through Malware Behavior Blocking and Event Monitoring." (WBR_TMC007314, *Apex One Administrator's Guide* at 9-2).

372. The Accused Products perform a method that includes *generating, in response to the monitoring, a record of events, the record of events including the pestware-related events* and *analyzing the record of events so as to identify the pestware-related event*. For example, as explained above, the Accused Products' Early Launch Anti-Malware (ELAM) feature, for example, "detect[s] malware during the operating system boot process." The Accused Products also "log unauthorized program access instances and send the logs to the server." (WBR_TMC007314, *Apex One Administrator's Guide* at 7-89.) Logs include information about the "event monitoring rule violated by the process."

5. View logs. Logs contain the following information:

- Date/Time unauthorized process was detected
- Endpoint where unauthorized process was detected
- Endpoint domain
- Violation, which is the event monitoring rule violated by the process
- Action performed when violation was detected
- Event, which is the type of object accessed by the program
- Risk level of the unauthorized program
- Program, which is the unauthorized program
- Operation, which is the action performed by the unauthorized program

(WBR_TMC007314, *Apex One Administrator's Guide* at 9-23.)

- Target, which is the process that was accessed
- Infection channel from where the threat originated

(*Id.*, *Apex One Administrator's Guide* at 9-24.)

373. As another example, the Accused Products "generate[] logs when [they] detect[] viruses and malware and send[] the logs to the server." (*Id.*, *Apex One Administrator's Guide* at 7-89.) As shown in the table below, those logs include details including an "analysis for the specific detection" as well as "[t]he scan that detected the threat." (*Id.*, *Apex One Administrator's Guide* at 7-90.).

ITEM	DESCRIPTION
Infected File/Object	The location of the file/object on the endpoint
Scan Type	The scan that detected the threat
Result	The result of the action taken **Note** For more information on scan results, see *Virus/ Malware Scan Results on page 7-90*.
IP Address	The IP address and port number of the source endpoint
MAC Address	The MAC address of the infected endpoint
Details	A link that displays the detailed analysis for the specific detection

(*Id.*, *Apex One Administrator's Guide* at 7-90.)

374. Moreover, using Event Monitoring, an Accused Product "detects a monitored system event, [and] it performs the action configured for the event." One such monitored event is the "System File Modification," which is an event associated with "malicious programs [that] modify system files to launch automatically at startup and control system behavior." When monitoring such System File Modification events, the Accused Products may take various actions including, "Assess", "Allow", "Ask when necessary", and "Deny."

When Event Monitoring detects a monitored system event, it performs the action configured for the event.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 394.)

System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 393.)

The following table lists possible actions that administrators can take on monitored system events.

TABLE 9-2. Actions on Monitored System Events

ACTION	DESCRIPTION
Assess	The Security Agent always allows programs associated with an event to run and logs the event for assessment. This is the default action for all monitored system events. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Allow	The Security Agent always allows programs associated with an event to run.

(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 394.)

ACTION	DESCRIPTION
Ask when necessary	The Security Agent prompts users to allow or deny programs associated with an event from running and adds the programs to the exception list If the user does not respond within a certain time period, the Security Agent automatically allows the program to run. The default time period is 30 seconds. To modify the time period, see *Configuring Global Behavior Monitoring Settings on page 9-18*. **Note** This option is not supported for the Program Library Injection (DLL injection) event on 64-bit systems.
Deny	The Security Agent always blocks programs associated with an event from running and logs the event. After blocking a program with notifications enabled, the Security Agent displays a notification on the endpoint. For details about notifications, see *Behavior Monitoring Notifications for Security Agent Users on page 9-20*.

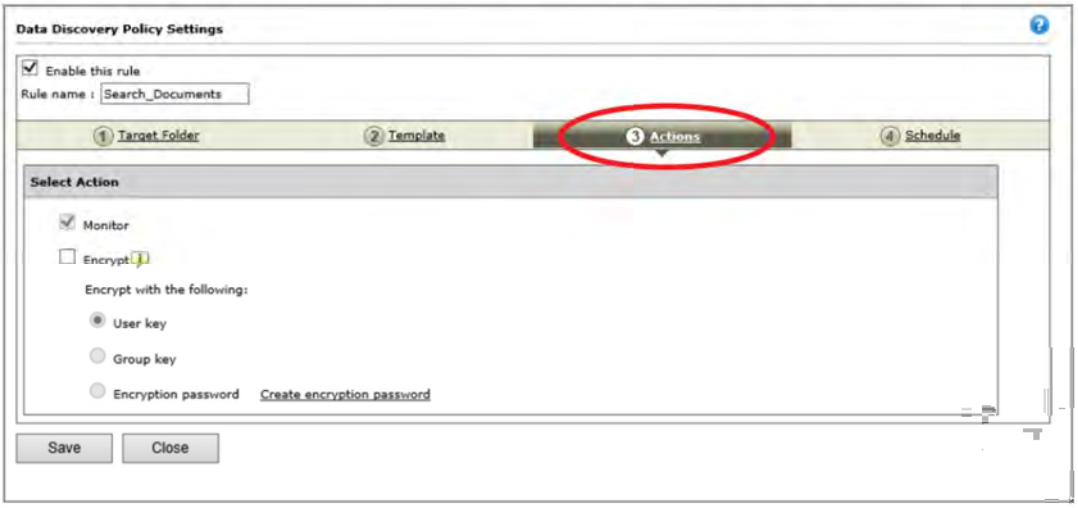
(*See* WBR_TMC007314, *Apex One Administrator's Guide* at PDF p. 395.)

375. When certain policies are triggered, "[d]etections are recorded for analysis."

Actions

Specify one or more of the following: actions to perform when the policy is triggered

- Monitor: Detections are recorded for analysis
- Encrypt: Sensitive files are encrypted using one of the listed methods. Integration with Trend Micro Endpoint Encryption is required to enable this capability.



(*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 290.)

376. Moreover, the "Endpoint Sensor," has the capabilities to perform "[d]etailed root cause analysis (RCA) [that] shows [the] source and spread of attacks."

CUSTOMIZE YOUR ENDPOINT PROTECTION

Apex One is a critical component of Trend Micro™ Smart Protection™ Suites, allowing you to add security and investigation capabilities to fit your organizations unique security needs.

Endpoint Sensor

- Context-aware investigation and response (EDR/XDR), recording, and reporting of system-level activities to rapidly assess attacks across email, endpoint, and server*.
- Server side sweeping for indicators of compromise (IoCs) using multi-level criteria like OpenIOC and YARA.
- Detailed root cause analysis (RCA) shows source and spread of attacks.
- Threat hunting tools leveraging indicators of attack (IoA) and behavioral analysis rules.
- Detects and analyzes advanced threat indicators such as fileless attacks.
- Rapidly respond to threats to limit the scope of impact and protect sensitive data before it is lost.

(*See* WBR_TMC002543, https://www.trenddefense.com/datasheets/ds-apex-one.pdf.)

377. The Accused Products perform a method that includes *modifying the set of behavior rules so as to prevent the pestware related events*. For example, the Accused Products protects against "Zero-Day" attacks using "Behavior Monitoring," which is responsive to newly encountered files. The Accused Products then provide "Connected threat defense," which "integrates with other security products via our global cloud threat intelligence, delivering sandbox rapid response updates to endpoints."

- Connected threat defense: Trend Micro Apex One integrates with other security products via our global cloud threat intelligence, delivering sandbox rapid response updates to endpoints.

(*See* WBR_TMC002543, https://www.trenddefense.com/datasheets/ds-apex-one.pdf.)

378. As another example, on information and belief, the Accused Products' Early Boot and Early Launch detections also rely on rules that are part of, or provided by, Trend Micro's machine learning models, which are constantly evolving to modify the behavior rules. For example, the Accused Products use "Predictive Machine Learning" that use "advanced file feature analysis and heuristic process monitoring." The Accused Products deliver Predictive Machine Learning "through a cloud-based machine learning model and introduces a local model for computers without a network connection."

Predictive Machine Learning

Predictive Machine Learning can protect your network from new, previously unidentified, or unknown threats through advanced file feature analysis and heuristic process monitoring. Apex One delivers this functionality through a cloud-based machine learning model and introduces a local model for computers without a network connection.

(*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 17.)

379. The Accused Products perform a method that includes *scanning data in a registry of the computer for pestware during the second period in the boot sequence*. For example, the Security Agent in the Accused Products performs "scanning for malware."

Scanning for Malware

Security Agents scan endpoint computers for malware through one of the following methods:

- **Real-time Scan:** This method scans files, folders and URLs as soon as they are accessed, triggered by I/O event hooking.
- **Manual Scan:** This method scans files and folders on demand, when initiated by the end user.
- **Scheduled Scan:** This method uses the same scanning methods and has the same detection capabilities as used for on-demand scanning. Scheduled scans are, however, triggered automatically based on a selected frequency (weekly or daily) and a specified time.
- **Scan Now:** This method scans files and folders on demand on one or more target computers when initiated by the Administrator.

380. Moreover, the Security Agent in the Accused Products "records vectors commonly associated with targeted attacks, such as file executions, memory violations, registry changes, and more." And as explained above, the Security Agents in the Accused Products "detect malware during the operating system boot sequence."

On the endpoint, the Apex One Security Agent records vectors commonly associated with targeted attacks, such as file executions, memory violations, registry changes, and more. The Agent creates a database of all the files, activities, and important system resources, and continuously updates this database to record the arrival and execution of suspicious objects. This data is forwarded to Apex One Server on a regular basis.

(*See* WBR_TMC020114, *Apex One Training for Certified Professionals Student Guide*, https://pdfcoffee.com/trend-micro-apex-one-training-for-certified-professionals-student-guidepdf-pdf-free.html at PDF p. 332.)

Enable Early Launch Anti-Malware Protection on Endpoints

Apex One supports the Early Launch Anti-Malware (ELAM) feature as part of the Secure Boot standard to provide boot time protection on endpoints. Administrators can enable this feature to start Apex One agents before other third-party software drivers when endpoints start up. This feature enables Apex One agents to detect malware during the operating system boot process.

(*See* https://docs.trendmicro.com/all/ent/apex-one/patch/en-us/apexOne_p6_ag.pdf at page 327.)

381. Each claim in the ’505 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ’505 Patent.

382. Trend Micro has been aware of the ’505 Patent since at least the filing of this First Amended Complaint.

383. Defendant directly infringes at least claim 1 of the ’505 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 this software and system to protect its 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.

384. Defendant’s partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’505 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

385. Defendant has actively induced and is actively inducing infringement of at least

claim 1 of the ’505 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’505 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

386. Defendant 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.

387. Defendant further encourages and induces its customers to infringe claim 1 of the ’505 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One

Administrator's Guide.)

388. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

389. 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 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 '505 Patent.

390. 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 '505 Patent.

391. 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 the Accused Products into the United States, 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.

392. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the boot sequence malware detection and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’505 Patent, that functionality could not be performed.

393. Additionally, the accused functionality, including the boot sequence malware detection related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products’ boot sequence malware monitoring, the Accused Products could not deploy their Early Launch Anti-Malware feature. These processes are continually running when the system is in use, especially as the system boots up, and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’505 Patent, that functionality could not be performed.

394. In addition, as shown in the detailed analysis above, the products, systems,

modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including the boot sequence malware detection) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as managing pestware-related events during a boot sequence) as recited in the claims of the ’505 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

395. 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 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 ’505 Patent.

396. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’505 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.

397. 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 ’505 Patent.

398. Defendant's infringement of the '505 Patent is knowing and willful. Defendant acquired knowledge of the '505 Patent and of the specific conduct that constitutes infringement of the '505 Patent at least based on this amended Complaint. Defendant continues to engage in infringing activities after the filing of this amended complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

399. On information and belief, despite Defendant's knowledge of the Asserted Patents, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant's continued infringement of the '505 Patent with knowledge of the '505 Patent constitutes willful infringement.

NINTH CAUSE OF ACTION
(INFRINGEMENT OF THE '243 PATENT)

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

401. Trend Micro has infringed and continues to infringe one or more claims of the '243 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, The Accused Products, including Trend Micro's Apex One, Network One, Vision One, Endpoint Protection with Detection and Response, Trend Micro's EDR/XDR and Cloud Products, and Trend Micro's Smart Protection Network, Trend Micro Workforce, Trend Micro Vision One, Trend Micro Service One, and Early Launch Anti-Malware (ELAM), Endpoint Detection and Response, when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '243 Patent as demonstrated below.

402. For example, claim 1 the ’243 Patent recites

> A method for identifying an origin of activity on a computer that is indicative of pestware comprising:
>
> monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;
>
> analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;
>
> identifying, based upon the activity, an object residing on the computer that is a suspected pestware object;
>
> accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from; and
>
> reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity too research whether the particular externally networked source is a Source of pestware.

403. To the extent the preamble is limiting, the Accused Products perform *a method for identifying an origin of activity on a computer that is indicative of pestware* as further explained below. For example, the Accused Products “protect[] enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks.” (WBR_TMC007314, *Apex One Administrator’s Guide* at 1-2.) As part of this protection, the Accused Products include, among other things, a scan engine that “detect[s] different types of viruses and malware … by identify[ing] … [t]ell-tale characteristics of the virus code [and] [t]he precise location within a file where the virus resides.” (*Id.* at 6-3.) The Accused Products also perform specific behavior monitoring, which “constantly monitors endpoints for unusual modifications to the operating system or on installed software.” (WBR_TMC018723, *Apex One whitepaper*, https://powerbox-na-

file.trend.org at 4–6.) The Accused Products further include functionality for performing threat investigations, including returning information about the objects that created suspicious and/or malicious objects. (WBR_TMC018665, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains/es-root-cause-anal_001.aspx.)

404. The Accused Products perform a method that includes *monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log*. For example, the Accused Products use a Kernel-mode driver for monitoring malicious activity. As one example, the Accused Products include a Behavior monitoring core driver 32/64 bit, which is a "kernel mode driver [that] monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement." (WBR_TMC007314, *Apex One Administrator's Guide* at 6-8.)

COMPONENT	DESCRIPTION
Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.
Behavior Monitoring Core Driver 32/64-bit	This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.
Behavior Monitoring Core Service 32/64-bit	This user mode service has the following functions: • Provides rootkit detection • Regulates access to external devices • Protects files, registry keys, and services
Behavior Monitoring Configuration Pattern	The Behavior Monitoring Driver uses this pattern to identify normal system events and exclude them from policy enforcement.
Digital Signature Pattern	This pattern contains a list of valid digital signatures that are used by the Behavior Monitoring Core Service to determine whether a program responsible for a system event is safe.
Policy Enforcement Pattern	The Behavior Monitoring Core Service checks system events against the policies in this pattern.
Memory Scan Trigger Pattern (32/64-bit)	Behavior Monitoring uses the Memory Scan Trigger Pattern to identify possible threats after detecting the following operations: • File write action • Registry write action • New process creation After identifying one of these operations, Behavior Monitoring calls Real-time Scan's Memory Inspection Pattern to check for security risks. For details about the Real-time Scan operations, see *Memory Inspection Pattern on page 6-5*.
Damage Recovery Pattern	The Damage Recovery Pattern contains policies that are used for monitoring suspicious threat behavior.

(WBR_TMC007314, *Apex One Administrator's Guide* at 6-8.)

405. As shown in the table below, the system "provides a list of API functions used by the file/process that may be indicative of the detected threat type."

Threat Indicators	Provides the results of the Predictive Machine Learning analysis • **Threat Probability**: Indicates how closely the file/process matched the malware model • **Probable Threat Type**: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • **Threat Identifiers**: Provides a list a API functions used by the file/process that may be indicative of the detected threat type **Important** API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. • **Similar Known Threats**: Provides a list of known threat types that exhibit similar file/process features to the detection

(WBR_TMC007314, *Apex One Administrator's Guide* at 8-14.) Additionally, the Accused Products "monitor[s] processes and perform[] API hooking to determine if a program is behaving in an unexpected manner." (*Id.* at 9-5.)

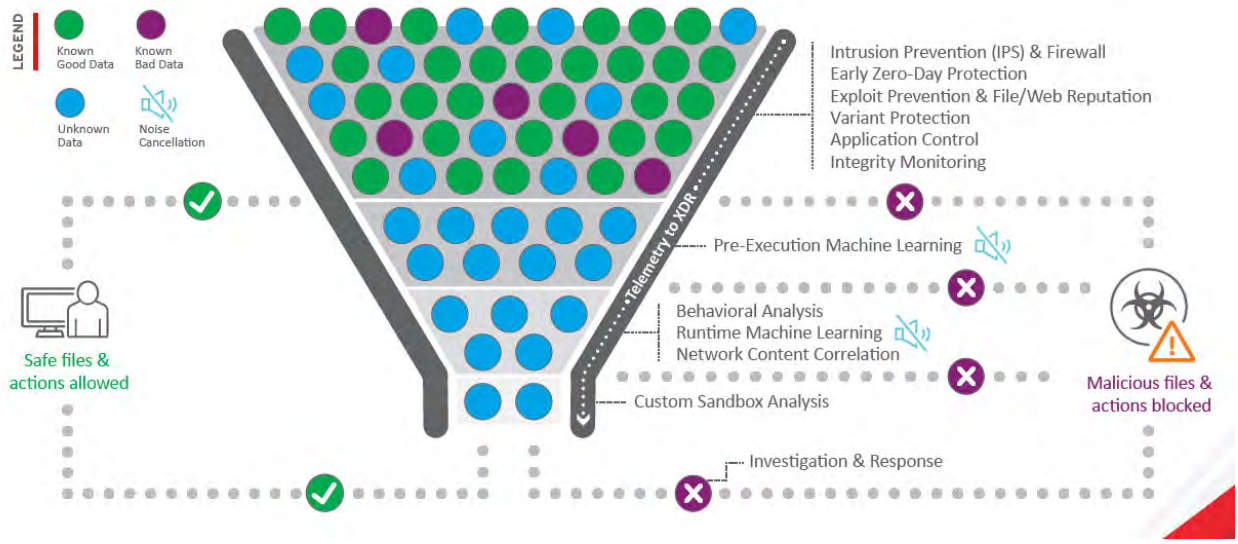
406. As another example, the Accused Products include Deep Security Agents (DSAs) to monitor system endpoints. DSAs install and operate as many as five kernel-level drivers on the endpoint, including at least the following kernel-level drivers: "tbimdsa.sys", "TMEBC.sys", "TmEyes.sys", "TmKmSnsr.sys," and "tmumh.sys." The kernel-level drivers operate, at least in part, by monitoring kernel callbacks and API hooking/redirection.

407. The Accused Products perform a method that includes *analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware*. For example, the Accused Products employ a number of "advanced heuristic" for "detect[ing]

potential threats."

CATEGORY	DESCRIPTION
Unknown Threats	Displays all the features that detect potential threats using advanced heuristics, analysis, or feature modeling • Predictive Machine Learning • Behavior Monitoring • Suspicious Connections • Suspicious File Objects

(WBR_TMC007314, *Apex One Administrator's Guide* at 2-13.) As one example, Trend Micro's machine learning models "compares [a] sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains." (WBR_TMC007314, *Apex One Administrator's Guide* at 8-2.) Likewise, Trend Micro's machine learning models "[t]hrough use of behavioral malware modeling, Predictive Machine Learning compares the process behavior to the model, assigns a probability score, and determines the probable malware type the process is executing." (WBR_TMC007314, *Apex One Administrator's Guide* at 8-3.). Additionally, Behavior Monitoring operates to detect activity indicative of pestware. For example, "[b]ehavior monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through Malware Behavior Blocking and Event Monitoring." (WBR_TMC007314, *Apex One Administrator's Guide* at 9-2.)



(WBR_TMC002543, *Datasheet: Trend Micro Apex One*, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3a-icon-datasheet-e4288a.)

408. As another example, the Accused Products use a "Predictive Machine Learning" module in order to detect emerging and unknown security risks, in part, through "API mapping." The Predictive Learning Machine Learning module operates in part by comparing "the sample [malware] to the malware model, assigns a probability score, and determines the probable malware type that the file contains."

Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

DETECTION TYPE	DESCRIPTION
File	After detecting an unknown or low-prevalence file, the Security Agent scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains. If a functional Internet connection is unavailable, Predictive Machine Learning automatically switches to the local model to provide constant unknown threat protection against portable executable file threats. Depending on how you configure Predictive Machine Learning, the Security Agent can attempt to "Quarantine" the affected file to prevent the threat from continuing to spread across your network.

(*See* WBR_TMC020490, *Predictive Machine Learning*, https://docs.trendmicro.com/en-us/smb/worry-free-business-security-services-67-server-help/policy-management_001/configuring-group-se/predictive-machine-l_002.aspx.)

409. The Accused Products perform a method that includes *identifying, based upon the activity, an object residing on the computer that is a suspected pestware object*. For example, the Accused Products "generate[] logs when [they] detect[] viruses and malware." (WBR_TMC007314, *Apex One Administrator's Guide* at 7-89.) The logs are generated in response to malware detections including scan-based detections and behavior-based detections. (*See*

WBR_TMC007314, *Apex One Administrator's Guide* at 7-89 to 7-90, 9-22 to 9-23.) These logs identify the object: for example, "program, which is the unauthorized program."

> **5.** View logs. Logs contain the following information:
>
> - Date/Time unauthorized process was detected
> - Endpoint where unauthorized process was detected
> - Endpoint domain
> - Violation, which is the event monitoring rule violated by the process
> - Action performed when violation was detected
> - Event, which is the type of object accessed by the program
> - Risk level of the unauthorized program
> - Program, which is the unauthorized program
> - Operation, which is the action performed by the unauthorized program

(WBR_TMC007314, *Apex One Administrator's Guide* at 9-22.)

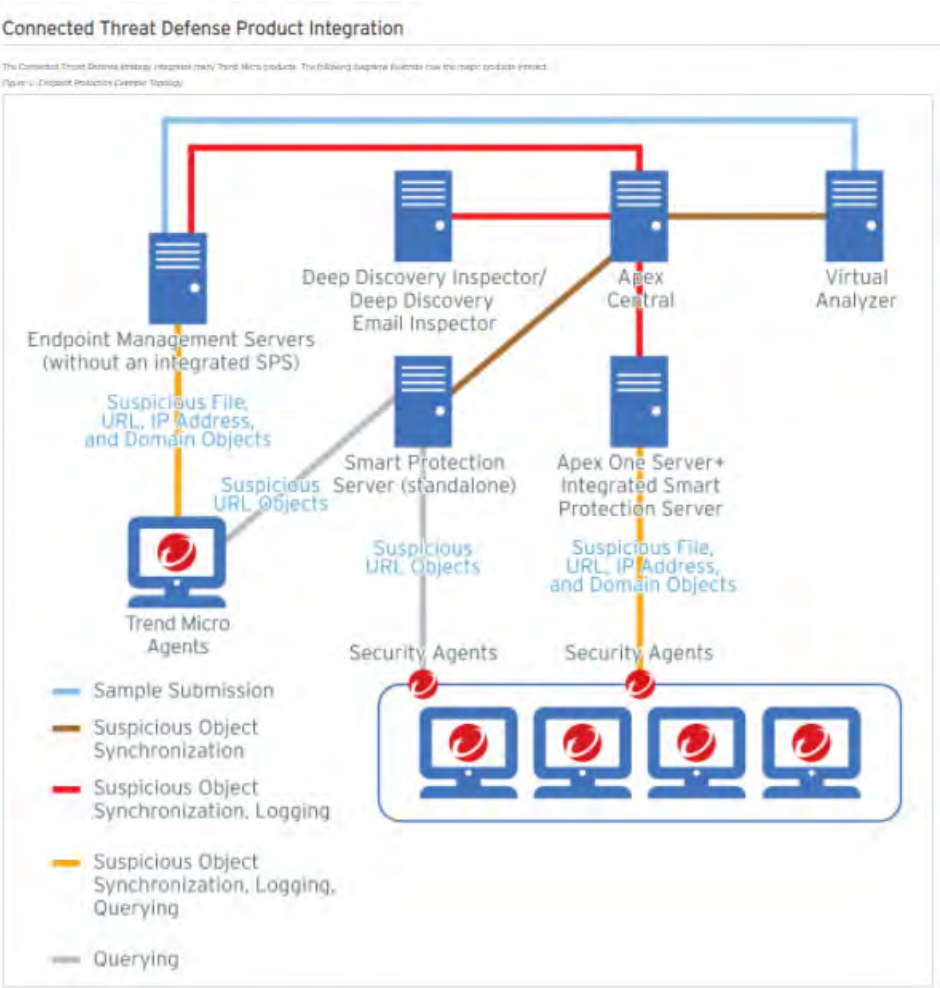
> - Target, which is the process that was accessed
> - Infection channel from where the threat originated

(WBR_TMC007314, *Apex One Administrator's Guide* at 9-23.)

410. As another example, the Accused Products, through Connected Threat Defense, identifies and receives information about identified Suspicious Objects.

FEATURE	BENEFITS
Connected Threat Defense	Configure Apex One to subscribe to the Suspicious Object lists from the Apex Central server. Using the Apex Central console, you can create customized actions for objects detected by the Suspicious Object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment. You can configure Security Agents to submit file objects that may contain previously unidentified threats to a Virtual Analyzer for further analysis. After assessing the objects, Virtual Analyzer adds any objects found to contain unknown threats to the Virtual Analyzer Suspicious Objects lists and distributes the lists to other Security Agents throughout the network.

(WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at 1-4.)



(*See* WBR_TMC016694, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/connected-threat-def_001/connected-threat-def_002.aspx#GUID-27226D06-1A28-4F87-8757-3DF44767BE48.)

411. As another example, the Accused Products use a "Behavior Monitoring" module that "protects endpoints through Malware Behavior Blocking and Event Monitoring." Malware Behavior Blocking and Event Monitoring each operate, in part, by performing "API hooking to determine if a program is behaving in an unexpected manner."

Behavior Monitoring

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**.

(*See* WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 402.)

OPTION	DESCRIPTION
Enable program inspection to detect and block compromised executable files	Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner. Although this procedure increases the overall detection ratio of compromised executable files, it may result in decreased system performance. **Tip** Program inspection provides increased security if you select **Known and potential threats** in the **Threats to block** drop-down.

(*See* WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 405.)

Enable program inspection to detect and block compromised executable files: Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner. Although this procedure increases the overall detection ratio of compromised executable files, it may result in decreased system performance.

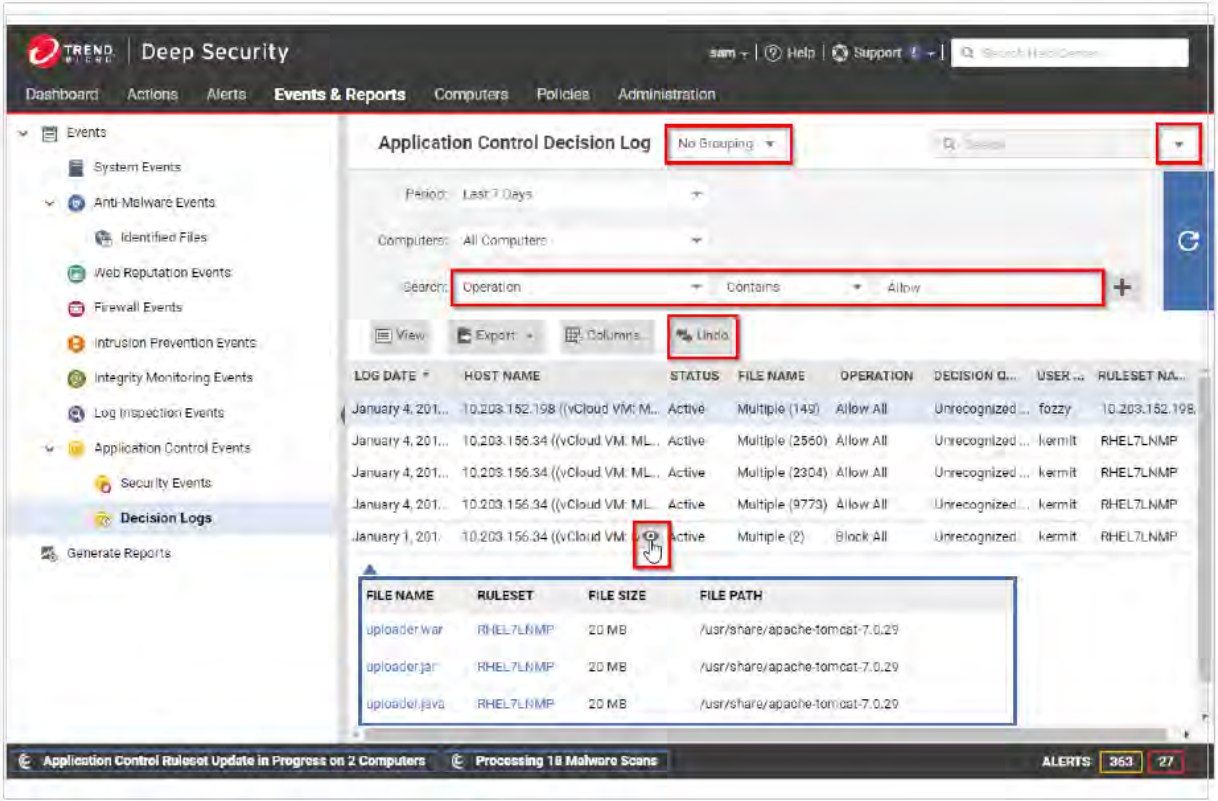
(*See* WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 416.)

412. As another example, the Deep Security Agents continuously monitor applications. For example, "[t]he agent watches for disk write activity on software files, and for attempts to execute software." Suspected malicious activity is identified, including suspected activity associated with the execution of "unrecognized software."

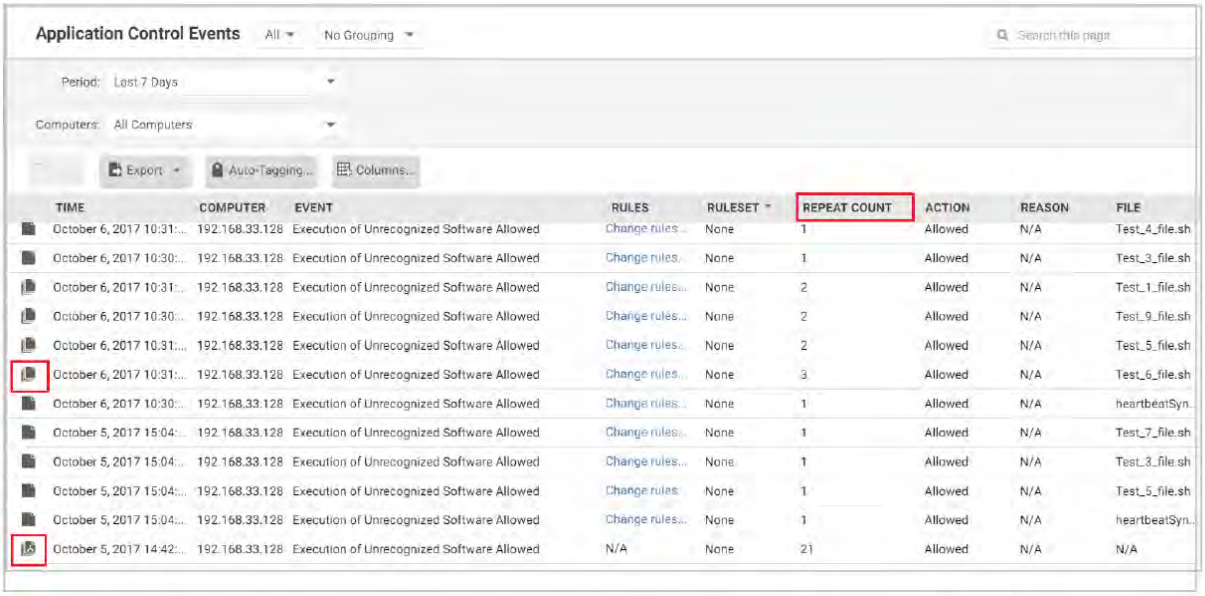
After that, the Deep Security Agent continuously monitors the computer for changes. Application control is integrated with the kernel (on Linux computers) and file system, so it has permissions to monitor the whole computer, including software installed by root or Administrator accounts. The agent watches for disk write activity on software files, and for attempts to execute software. To determine if the software is new or has changed, it compares the file with the hashes of the initially installed software. Change includes differences in:

- File name
- Path or location
- Time stamp
- Permissions
- File contents

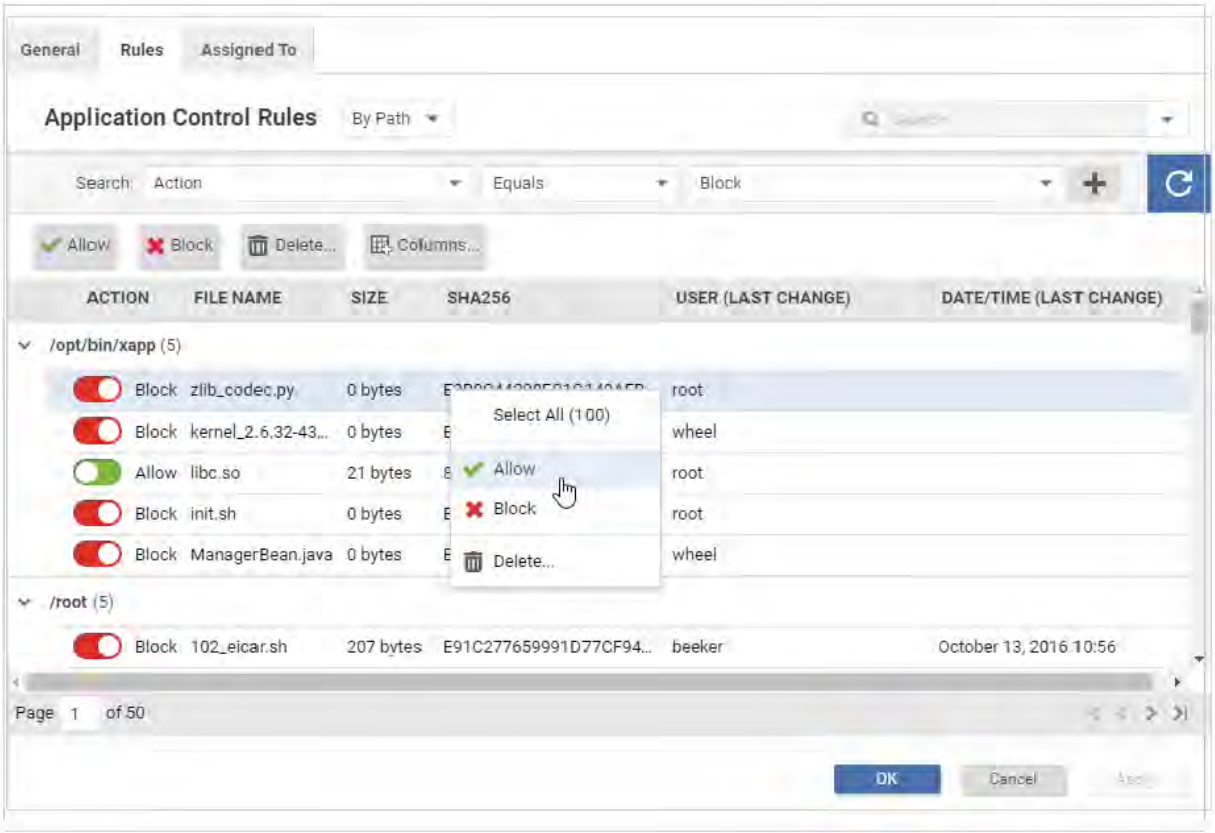
(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 606.)



(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 637.)



(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 618.)



(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 635.)

413. The Accused Products perform a method that includes *accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from*. For example, using Application Security, Trend Micro One "identifies the attacker, type of attack, and blocks it." Application Security provides attack-specific information including "the time, origin, and type,

on every attack that occurs on your apps to a central reporting point." Such attack-specific information includes the "attacker IP", "Base URL", and "URL Path", among other information.

AUTOMATIC PROTECTION

When your app is exposed to a malicious attack, the agent identifies the attacker, type of attack, and blocks it. User data is protected, and you have the insight you need to fix the coding vulnerabilities.

One of the key differentiators with Application Security is the ability to have malware detection where your web application might accept file uploads, such as attachments, pictures/avatars, or PDFs.

Hackers can take advantage of the this by uploading malicious files, such as excel spreadsheets with malicious macros, images with ImageTragick payloads, or PDFs with malicious scripts. You need to be able to quickly and easily block this threat prior to any destination point without forcing developers to write or modify code.

(*See*, WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 2.)

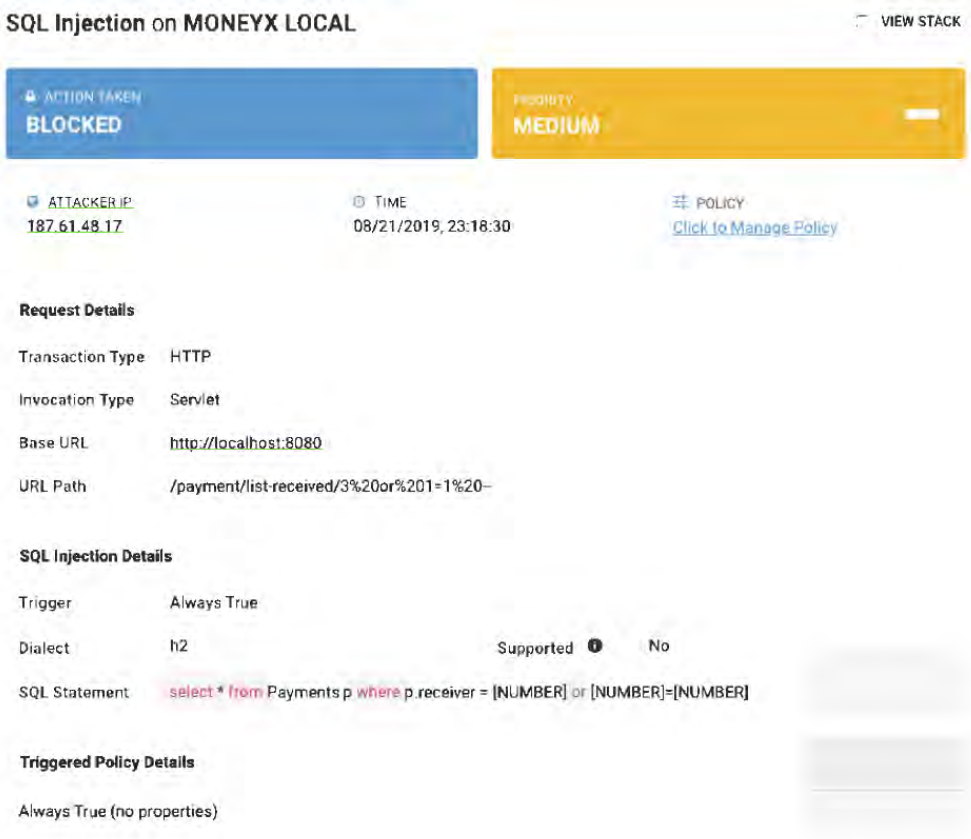
Application Security lets you monitor and review exploitation attempts across an unlimited number of applications. Attack details are propagated across your infrastructure, meaning, if an attack is detected on one application, it is immediately flagged on every app server and for every monitored app in your account.

While the performance experienced by an end user may vary depending on the application type and its overhead, Application Security strives to make sure requests can be handled in under 1 ms.

Application Security delivers information, such as the time, origin, and type, on every attack that occurs on your apps to a central reporting point. Over time, this information builds into a broad profile of the attacks impacting your networks, enabling your web security team to map trends and deploy appropriate resources.

Application Security also gives your developers full visibility into how the vulnerability in your code would have been exploited, including a stack trace down to the line of code (where relevant), reporting of request parameters, and how your app's behavior would have been modified.

(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 3.)



(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 3.)

414. As another example, the Accused Products, through Connected Threat Defense, analyze the Root Cause of a malware event, which includes, among other things, the "First Observed Object," the Network that connects the objects to the internet, etc.

The root cause analysis area shows object types using the following icons:

Icon	Name	Description
	First Observed Object	Marks an object that most likely created the matched object
	Matched Criteria	Marks objects matching the investigation criteria
	Normal Object	Marks objects that have been verified to not pose a threat These are usually common system files.
	Unrated Object	Marks objects that are not system files but do not exhibit suspicious behavior
	Suspicious Object	Marks objects that exhibit behaviors that are similar to known threats
	Malicious Object	Marks objects that match a known threat
	Boot	Objects that launch during system startup
	Browser	Objects that are capable of displaying web pages, usually a web browser
	Email	Objects that can send and receive email messages, usually an email client or server
	File name	Objects that are files on the disk
	Network	Objects related to network connections or the Internet
	Process	Objects that are processes running during the time of execution
	Registry	Objects that are registry keys, entries or data
→	Event	Indicates actions done by the object
---	Association	Indicates relationships between two objects

(WBR_TMC018665, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains/es-root-cause-anal_001.aspx.)

415. As another example, the Accused Products "deliver[] information, such as the time, origin, and type, on every attack that occurs on your apps." Such information may include, in certain instances, an "attacker IP" or "Base URL."

Application Security lets you monitor and review exploitation attempts across an unlimited number of applications. Attack details are propagated across your infrastructure, meaning, if an attack is detected on one application, it is immediately flagged on every app server and for every monitored app in your account.

While the performance experienced by an end user may vary depending on the application type and its overhead, Application Security strives to make sure requests can be handled in under 1 ms.

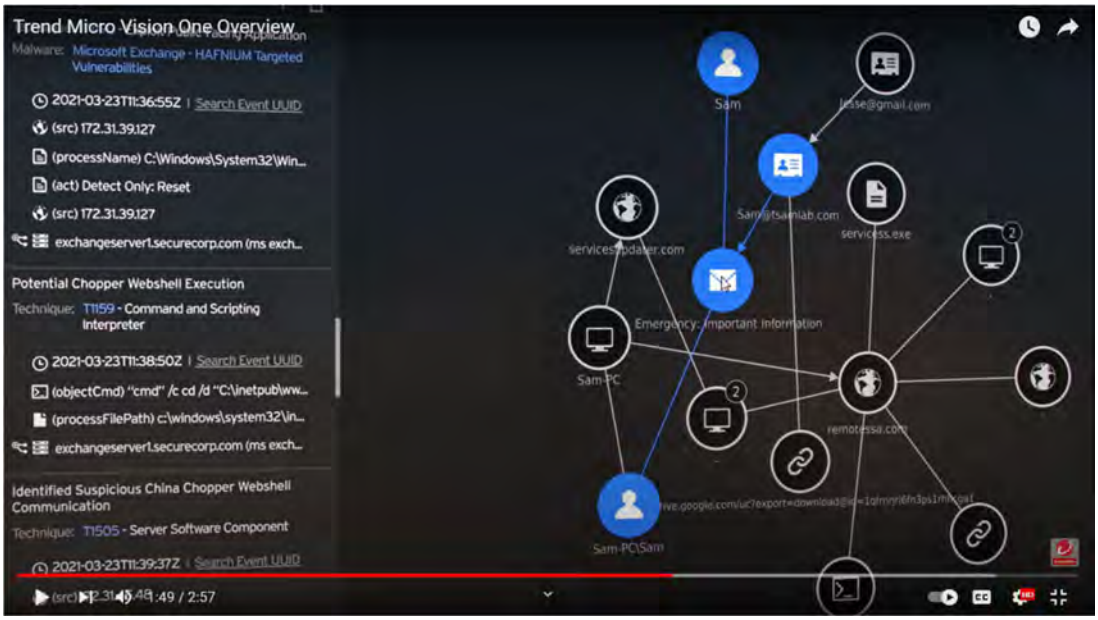
Application Security delivers information, such as the time, origin, and type, on every attack that occurs on your apps to a central reporting point. Over time, this information builds into a broad profile of the attacks impacting your networks, enabling your web security team to map trends and deploy appropriate resources.

Application Security also gives your developers full visibility into how the vulnerability in your code would have been exploited, including a stack trace down to the line of code (where relevant), reporting of request parameters, and how your app's behavior would have been modified.

(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 3.)

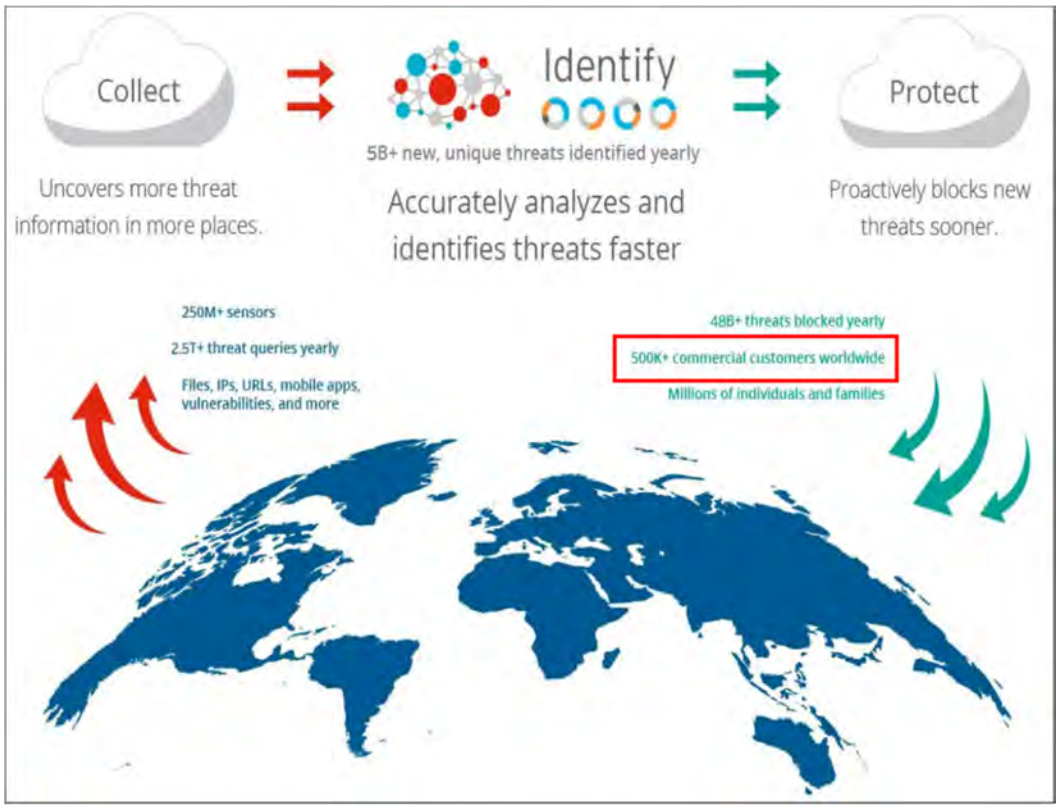
(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 3.)

416. As another example, the Accused Products provide various diagrams, which dynamically illustrate an "attack-centric view" of an attack, including information such as an IP address, a process name, and/or various other information that identifies an origin of an attack.



(*See* WBR_TMC016622, https://www.youtube.com/watch?v=sCMs5MQOCi0 at timestamp, 1:49)

417. The Accused Products perform a method that includes *reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity too research whether the particular externally networked source is a Source of pestware*. For example, the Accused Products share threat data with Trend Micro's Smart Protection Network. The "Smart Protection Network is a global threat intelligence that rapidly and accurately collects and identifies new threats, delivering instant protection for data wherever it resides." (WBR_TMC020109, https://helpcenter.trendmicro.com/en-us/article/tmka-18569.) That information is reported to Trend Micro. For example, "[t]hrough the Trend Micro Zero Day Initiative, … [Trend Micro] understand[s] the latest vulnerabilities and potential exploits and instantly protects [its] customers." (WBR_TMC018637, https://www.trendmicro.com/en_us/about/threat-research.html.)



(*See* Trend Micro, Smart Protection Network – Global Threat Intelligence, https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html.)

418. As another example, the Accused Products include or are integrated with "Trend Micro Service One," which uses information "gleaned from over 500,000 customers and 250 million global sensors" and "constantly monitor[s] and analyze[s] activity data from Trend Micro solution in your environment." Trend Micro Service One enables "security experts [to] detect, hunt, and contain threats," in part, by "correlating data and insights from email, endpoints, servers, cloud workloads, and network sources." Alerts generated by Trend Micro Service One includes "alerts [that] are based on intelligence-driven (threat intelligence reports, threat intelligence feeds, and/or malware analysis) or situational-awareness driven (suspicious events or IoC within the network) methods, processes, and analytics across all your Trend Micro solutions."

Security experts ready, willing, and able, 24/7/365

Scarce and overburdened resources impact both your ability to manage the attack surface lifecycle as well as effectively communicate risk across the organization. With Trend Micro One, limited resources don't have to slow you down. Our world-class experts can help you to be more resilient with premium support that focuses on getting you up and running fast while ensuring your solutions are optimally configured. Managed XDR can help identify and investigate threats, and incident response services are ready to assist during critical attacks.

Leveraging our in-depth knowledge gleaned from over 500,000 customers and 250 million global sensors, our targeted attack detection service scans for early indicators of compromise (IoC), providing proactive, qualified high-risk alerts of potential threats with expert resources to help you take quick action.

(*See* WBR_TMC018719, https://www.trendmicro.com/en_us/business/products/one-platform.html navigate to "Learn More" for access to "Solving the Attack Surface Risk Management Challenge" at p. 4.)

Managed extended detection and response (Managed XDR) service

Trend Micro Service One™ Complete customers enjoy support from the Trend Micro™ Managed XDR service, which is backed by highly qualified cybersecurity experts around the world. They constantly monitor and analyze activity data from Trend Micro solutions in your environment. By correlating data and insights from email, endpoints, servers, cloud workloads, and network sources, our security experts detect, hunt, and contain threats. Your team will be notified of validated detections, allowing you to quickly react and respond and prevent similar attacks from occurring in the future

(*See* WBR_TMC020505, https://www.trendmicro.com/en_us/business/services/service-one.html navigate to "Read Solution Brief" for access to "Trend Micro Service One" at p. 1.)

Detect and respond faster

Our Targeted Attack Detection provides you with a timeline uncovering predictions of the high-risk attack. In addition, you'll receive a detailed action plan to help you react quickly and limit the scope of an attack and minimize business interruptions. View all notifications on our Targeted Attack Detection app, so you can stay on top of any threats discovered in your environment.

Trend Micro Vision One™ customers are eligible for Trend Micro Service One Complete, which provides extended coverage from our global Managed XDR team. Our expert team continually monitors suspicious, malicious and unwanted activity to generate high-fidelity alerts. These alerts are based on intelligence-driven (threat intelligence reports, threat intelligence feeds, and/or malware analysis) or situational-awareness driven (suspicious events or IoC within the network) methods, processes, and analytics across all your Trend Micro solutions.

Within hours of contacting us, our Incident Response experts will have established a customized plan of action with your IT department. Our workforce, tools, and processes will be set up instantly to monitor your network traffic while logs and disk images are already being analyzed for IoC or indicators of attack (IoA). In the background, our incident coordinators will organize the flow of information, making sure all defined stakeholders are being kept in the loop about findings, developments, and key decisions. Concise daily briefings and reports will provide you with all information and insight required to:

419. Each claim in the '243 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '243 Patent .

420. Trend Micro has been aware of the '243 Patent since at least the filing of this Amended Complaint.

421. Defendant directly infringes at least claim 1 of the ’243 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 this software and system to protect its 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.

422. Defendant’s partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’243 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

423. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’243 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’243 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

424. Defendant 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.

425. Defendant further encourages and induces its customers to infringe claim 1 of the ’243 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator’s Guide.)

426. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

427. 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 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 '243 Patent.

428. 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 '243 Patent.

429. 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 the Accused Products into the United States, 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.

430. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and

shown above, or without the system and components identified above that practice the ’243 Patent, that functionality could not be performed.

431. Additionally, the accused functionality, including the functionality for identifying an origin of a malicious activity, API call monitoring, and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products’ API call monitoring, the Accused Products could not deploy their Root Cause Analysis and malware detection features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’243 Patent, that functionality could not be performed.

432. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including monitoring API calls) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying the origin of a malicious activity) as recited in the claims of the ’243 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

433. 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 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 ’243 Patent.

434. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’243 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.

435. 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 ’243 Patent.

436. Defendant’s infringement of the ’243 Patent is knowing and willful. Defendant acquired knowledge of the ’243 Patent and of the specific conduct that constitutes infringement of the ’243 Patent at least based on this amended Complaint. Defendant continues to engage in infringing activities after the filing of this amended complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

437. On information and belief, despite Defendant’s knowledge of the Asserted Patents, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant’s continued infringement of the ’243 Patent with knowledge of the ’243 Patent constitutes willful infringement.

TENTH CAUSE OF ACTION
(INFRINGEMENT OF THE '932 Patent)

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

439. Defendant has infringed and continues to infringe one or more claims of the '932 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including for example Trend Micro One, The Accused Products, including Trend Micro's Apex One, Network One, Vision One, Endpoint Protection with Detection and Response, Trend Micro's EDR/XDR and Cloud Products, and Trend Micro's Smart Protection Network, Trend Micro Workforce, Trend Micro Vision One, Trend Micro Service One, and Early Launch Anti-Malware (ELAM), Endpoint Detection and Response, when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '932 Patent, as demonstrated below.

440. For example, claim 1 of the '932 recites:

> 1. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:
>
> monitoring, using a kernel-mode driver, API call activity on the computer;
>
> storing information related to the API call activity in a log;
>
> analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;
>
> identifying, based upon the API call activity, a suspected pestware object on the computer;
>
> identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and

reporting the identity of the externally networked source to an externally networked pestware research entity, wherein

the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program.

441. The Accused Products perform each element of the method of claim 1 of the '932 Patent. To the extent the preamble is construed as limiting, the Accused Products perform *a method for identifying an origin of activity on a computer that is indicative of pestware*, as further explained below. For example, the Accused Products "protect[] enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks." (WBR_TMC007314, *Apex One Administrator's Guide* at 1-2.) As part of this protection, the Accused Products include, among other things, a scan engine that "detect[s] different types of viruses and malware … by identify[ing] … [t]ell-tale characteristics of the virus code [and] [t]he precise location within a file where the virus resides." (*Id*. at 6-3.) The Accused Products also perform specific behavior monitoring, which "constantly monitors endpoints for unusual modifications to the operating system or on installed software." (WBR_TMC018723, *Apex One whitepaper*, https://powerbox-na-file.trend.org at 4–6.) The Accused Products further include functionality for performing threat investigations, including returning information about the origins and objects that created suspicious and/or malicious objects. (WBR_TMC018665, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains/es-root-cause-anal_001.aspx.)

442. The Accused Products perform a method that includes *monitoring, using a kernel-mode driver, API call activity on the computer* and *storing information related to the API call activity in a log*. For example, the Accused Products use a Kernel-mode driver for monitoring malicious activity.

- **Display a notification message if the endpoint needs to restart to load a kernel mode driver**: After installing a hot fix or an upgrade package that contains a new version of a kernel mode driver, the driver's previous version may still exist on the endpoint. The only way to unload the previous version and load the new one is to restart the endpoint. After restarting the endpoint, the new version automatically installs and no further restart is necessary.

(*See* WBR_TMC018739, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-patch-3-online-help/protecting-trend_cli/keeping-protection-u_001/trend_client_program_008/configuring-trend_cl_001.aspx.)

443. As one example, the Accused Products include a Behavior monitoring core driver 32/64 bit, which is a "kernel mode driver [that] monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement." (WBR_TMC007314, *Apex One Administrator's Guide* at 6-8.)

COMPONENT	DESCRIPTION
Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.
Behavior Monitoring Core Driver 32/64-bit	This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.
Behavior Monitoring Core Service 32/64-bit	This user mode service has the following functions: • Provides rootkit detection • Regulates access to external devices • Protects files, registry keys, and services
Behavior Monitoring Configuration Pattern	The Behavior Monitoring Driver uses this pattern to identify normal system events and exclude them from policy enforcement.
Digital Signature Pattern	This pattern contains a list of valid digital signatures that are used by the Behavior Monitoring Core Service to determine whether a program responsible for a system event is safe.
Policy Enforcement Pattern	The Behavior Monitoring Core Service checks system events against the policies in this pattern.
Memory Scan Trigger Pattern (32/64-bit)	Behavior Monitoring uses the Memory Scan Trigger Pattern to identify possible threats after detecting the following operations: • File write action • Registry write action • New process creation After identifying one of these operations, Behavior Monitoring calls Real-time Scan's Memory Inspection Pattern to check for security risks. For details about the Real-time Scan operations, see *Memory Inspection Pattern on page 6-5*.
Damage Recovery Pattern	The Damage Recovery Pattern contains policies that are used for monitoring suspicious threat behavior.

(*Id.*)

444. As shown in the table below, the system "provides a list of API functions used by the file/process that may be indicative of the detected threat type."

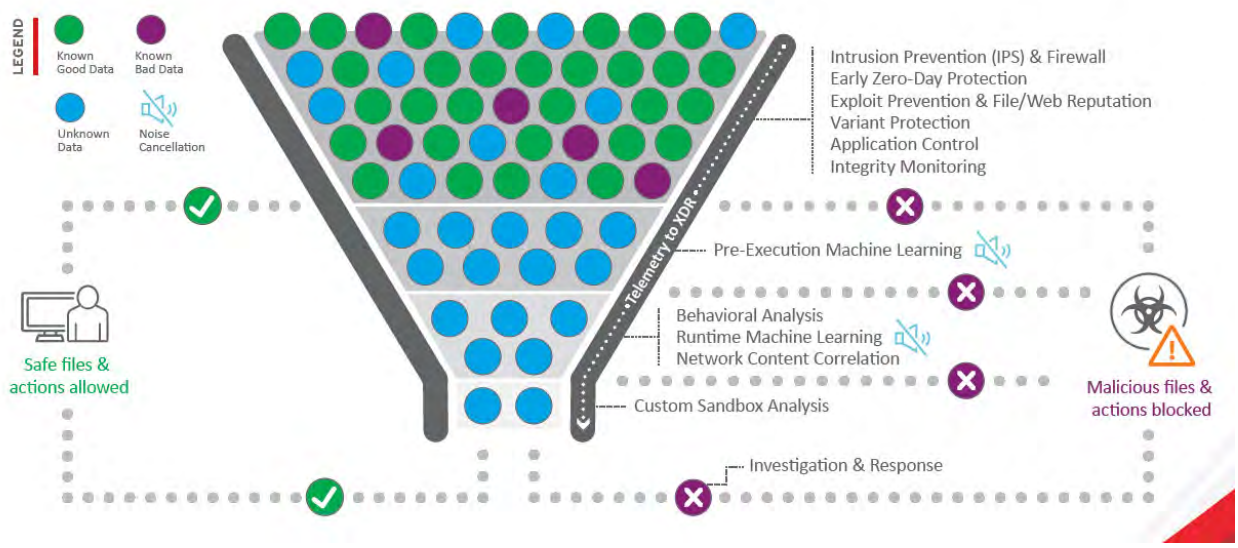
Threat Indicators	Provides the results of the Predictive Machine Learning analysis • **Threat Probability**: Indicates how closely the file/process matched the malware model • **Probable Threat Type**: Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats • **Threat Identifiers**: Provides a list a API functions used by the file/process that may be indicative of the detected threat type **Important** API function identification is only one factor in the determination of the threat type. Predictive Machine Learning uses many other file features and analysis methods to calculate the threat probability and probable threat type. • **Similar Known Threats**: Provides a list of known threat types that exhibit similar file/process features to the detection

(*Id.* at 8-14.) Additionally, the Accused Products "monitor[s] processes and perform[] API hooking to determine if a program is behaving in an unexpected manner." (*Id.* at 9-5.)

445. The Accused Products perform a method that includes *analyzing, heuristically, the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold*. For example, the Accused Products employ a number of "advanced heuristic" for "detect[ing] potential threats."

CATEGORY	DESCRIPTION
Unknown Threats	Displays all the features that detect potential threats using advanced heuristics, analysis, or feature modeling • Predictive Machine Learning • Behavior Monitoring • Suspicious Connections • Suspicious File Objects

(WBR_TMC007314, *Apex One Administrator's Guide* at 2-13). As one example, Trend Micro's machine learning models "compares [a] sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains." (WBR_TMC007314, *Apex One Administrator's Guide* at 8-2.) Likewise, Trend Micro's machine learning models "[t]hrough use of behavioral malware modeling, Predictive Machine Learning compares the process behavior to the model, assigns a probability score, and determines the probable malware type the process is executing." (WBR_TMC007314, *Apex One Administrator's Guide* at 8-3.). Additionally, Behavior Monitoring operates to detect activity indicative of pestware. For example, "[b]ehavior monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through Malware Behavior Blocking and Event Monitoring." (WBR_TMC007314, *Apex One Administrator's Guide* at 9-2).



(WBR_TMC002543, *Datasheet: Trend Micro Apex One*, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3a-icon-datasheet-e4288a.)

446. As another example, the Accused Products use a "Predictive Machine Learning" module in order to detect emerging and unknown security risks, in part, through "API mapping."

The Predictive Learning Machine Learning module operates in part by comparing "the sample [malware] to the malware model, assigns a probability score, and determines the probable malware type that the file contains."

Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

Predictive Machine Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

(WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 386.)

447. The Accused Products perform a method that includes *identifying, based upon the API call activity, a suspected pestware object on the computer*. For example, the Accused Products "generate[] logs when [they] detect[] viruses and malware." (WBR_TMC007314, *Apex One Administrator's Guide* at 7-89.) The logs are generated in response to malware detections including scan-based detections and behavior-based detections. (*See* WBR_TMC007314, *Apex One Administrator's Guide* at 7-89 to 7-90, 9-22 to 9-23.) These logs identify the object: for example, "program, which is the unauthorized program."

5. View logs. Logs contain the following information:
   - Date/Time unauthorized process was detected
   - Endpoint where unauthorized process was detected
   - Endpoint domain
   - Violation, which is the event monitoring rule violated by the process
   - Action performed when violation was detected
   - Event, which is the type of object accessed by the program
   - Risk level of the unauthorized program
   - Program, which is the unauthorized program
   - Operation, which is the action performed by the unauthorized program

(WBR_TMC007314, *Apex One Administrator's Guide* at 9-22.)

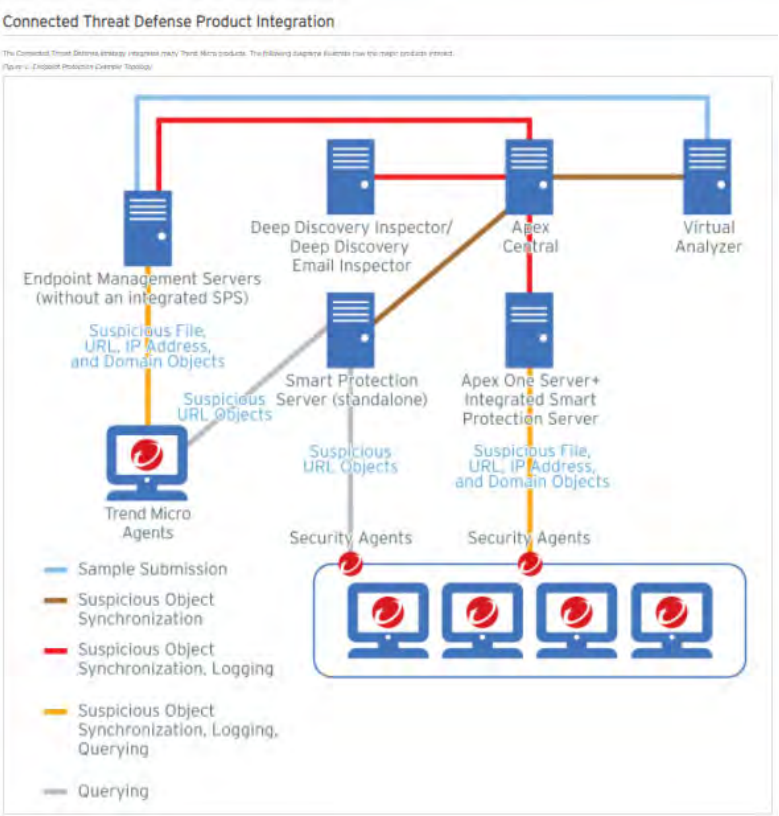
- Target, which is the process that was accessed
- Infection channel from where the threat originated

(WBR_TMC007314, *Apex One Administrator's Guide* at 9-23.)

448. As another example, the Accused Products, through Connected Threat Defense, identify and receive information about identified Suspicious Objects.

FEATURE	BENEFITS
Connected Threat Defense	Configure Apex One to subscribe to the Suspicious Object lists from the Apex Central server. Using the Apex Central console, you can create customized actions for objects detected by the Suspicious Object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment. You can configure Security Agents to submit file objects that may contain previously unidentified threats to a Virtual Analyzer for further analysis. After assessing the objects, Virtual Analyzer adds any objects found to contain unknown threats to the Virtual Analyzer Suspicious Objects lists and distributes the lists to other Security Agents throughout the network.

(WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 26.)



(*See* WBR_TMC016694, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/connected-threat-def_001/connected-threat-def_002.aspx#GUID-27226D06-1A28-4F87-8757-3DF44767BE48.)

449. As another example, the Accused Products use a "Behavior Monitoring" module that "protects endpoints through Malware Behavior Blocking and Event Monitoring." Malware Behavior Blocking and Event Monitoring each operate, in part, by performing "API hooking to determine if a program is behaving in an unexpected manner."

Behavior Monitoring

Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**.

(WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 402.)

OPTION	DESCRIPTION
Enable program inspection to detect and block compromised executable files	Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner. Although this procedure increases the overall detection ratio of compromised executable files, it may result in decreased system performance. **Tip** Program inspection provides increased security if you select **Known and potential threats** in the **Threats to block** drop-down.

(WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 405.)

Enable program inspection to detect and block compromised executable files: Program inspection monitors processes and performs API hooking to determine if a program is behaving in an unexpected manner. Although this procedure increases the overall detection ratio of compromised executable files, it may result in decreased system performance.

(WBR_TMC008165, *Apex One Administrator's Guide for Enterprise and Medium Business* at PDF p. 416.)

450. As another example, Deep Security determines whether files are "suspicious," in part, using a heuristics-based detection approach.

How does Threat Intelligence work?

1. When all the components are configured properly, the Deep Security Agent uses heuristic detection to analyze files on the protected computer and determines whether they are suspicious.
2. Optionally, you can manually or automatically send suspicious files from Deep Security to Trend Micro Vision One or Deep Discovery Analyzer, which executes and observes the suspicious file in a sandbox (a secure, isolated virtual environment).
3. Deep Security Manager gets the sandbox analysis results from Trend Micro Vision One or Deep Discovery Analyzer.

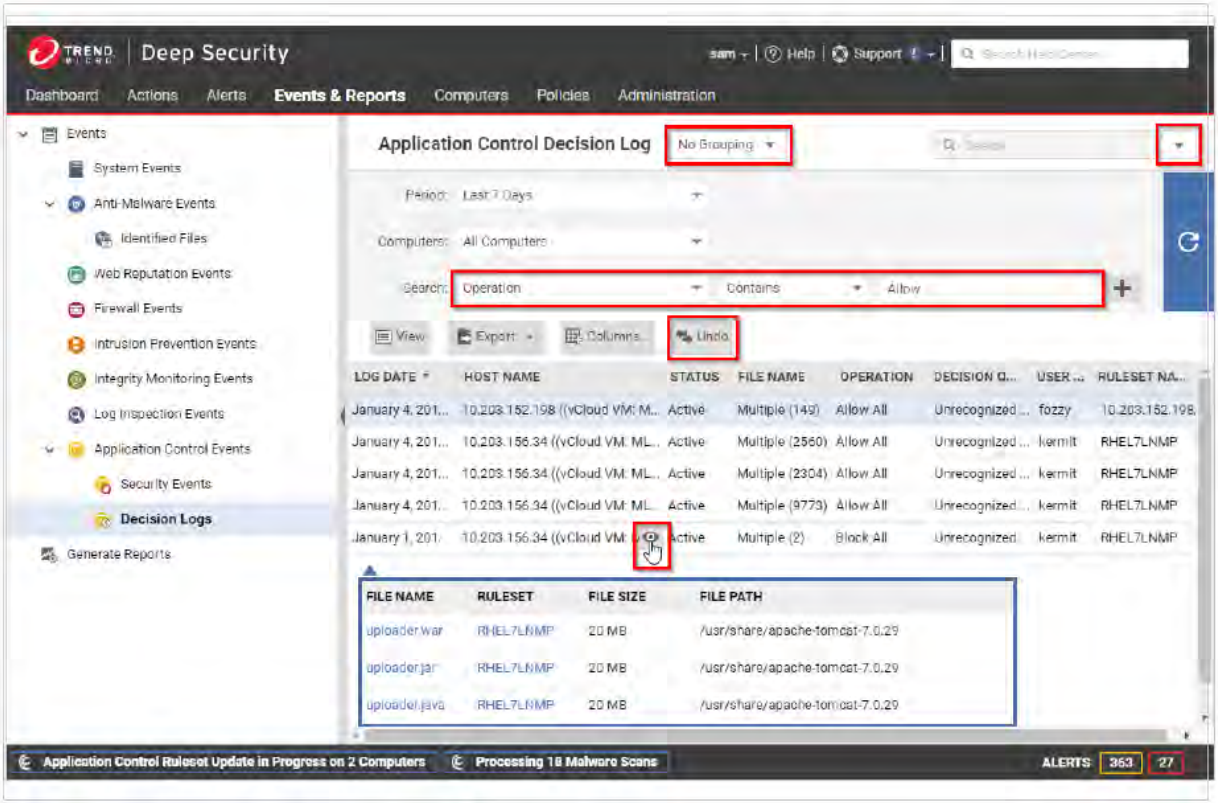
(*See* WBR_TMC018641, https://help.deepsecurity.trendmicro.com/20_0/on-premise/anti-malware-threat-intelligence.html.)

451. As another example, the Deep Security Agents continuously monitor applications. For example, "[t]he agent watches for disk write activity on software files, and for attempts to execute software." Suspected malicious activity is identified, including suspected activity associated with the execution of "unrecognized software."

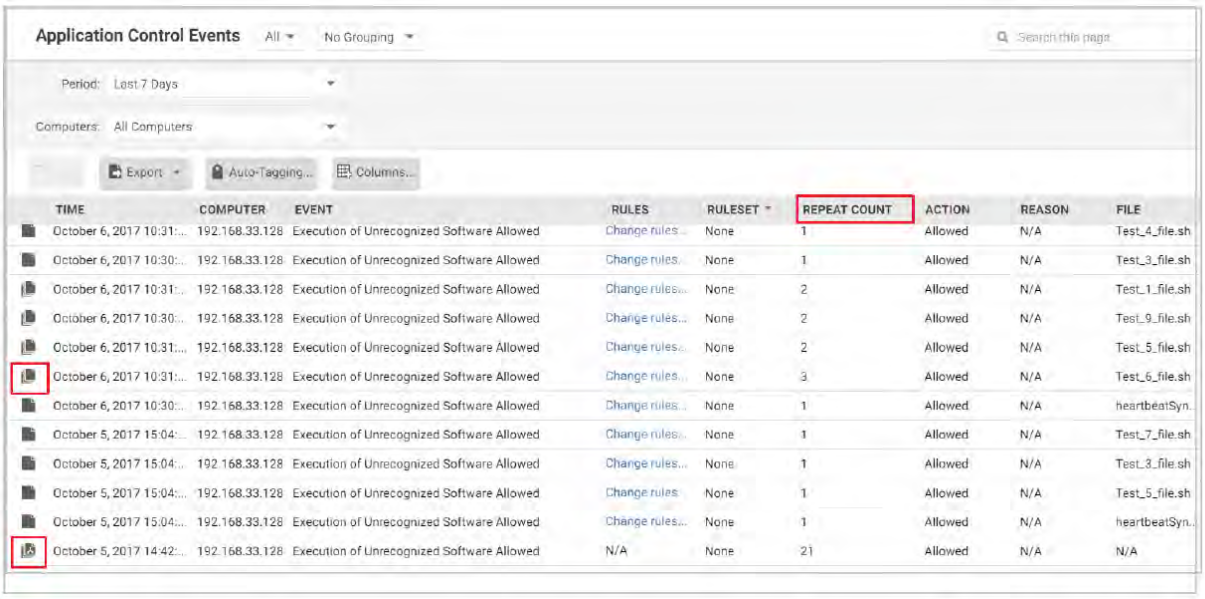
After that, the Deep Security Agent continuously monitors the computer for changes. Application control is integrated with the kernel (on Linux computers) and file system, so it has permissions to monitor the whole computer, including software installed by root or Administrator accounts. The agent watches for disk write activity on software files, and for attempts to execute software. To determine if the software is new or has changed, it compares the file with the hashes of the initially installed software. Change includes differences in:

- File name
- Path or location
- Time stamp
- Permissions
- File contents

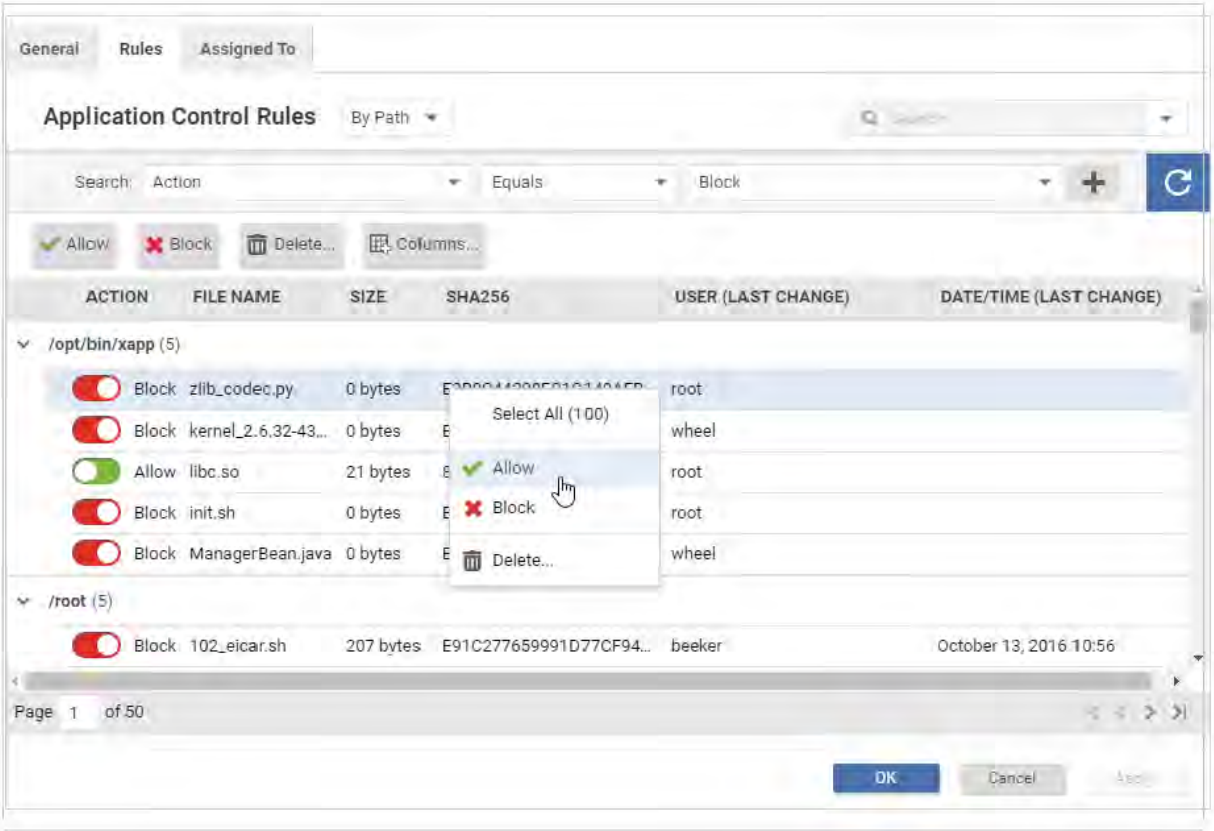
(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 606.)



(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 637.)



(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 618.)



(*See* WBR_TMC018740, *Deep Security 10.3*, https://help.deepsecurity.trendmicro.com/10_3/on-premise/Deep_Security_10.3_On-Premise_Administration_Guide at PDF p. 635.)

452. The Accused Products perform a method that includes *identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object.* For example, using Application Security, Trend Micro One "identifies the attacker, type of attack, and blocks it." Application Security provides attack-specific information including "the time, origin, and type, on every attack that occurs on your apps to a central reporting point." Such attack-specific information includes the "attacker IP", "Base URL", and "URL Path", among other information.

AUTOMATIC PROTECTION

When your app is exposed to a malicious attack, the agent identifies the attacker, type of attack, and blocks it. User data is protected, and you have the insight you need to fix the coding vulnerabilities.

One of the key differentiators with Application Security is the ability to have malware detection where your web application might accept file uploads, such as attachments, pictures/avatars, or PDFs.

Hackers can take advantage of the this by uploading malicious files, such as excel spreadsheets with malicious macros, images with ImageTragick payloads, or PDFs with malicious scripts. You need to be able to quickly and easily block this threat prior to any destination point without forcing developers to write or modify code.

(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 2.)

Application Security lets you monitor and review exploitation attempts across an unlimited number of applications. Attack details are propagated across your infrastructure, meaning, if an attack is detected on one application, it is immediately flagged on every app server and for every monitored app in your account.

While the performance experienced by an end user may vary depending on the application type and its overhead, Application Security strives to make sure requests can be handled in under 1 ms.

Application Security delivers information, such as the time, origin, and type, on every attack that occurs on your apps to a central reporting point. Over time, this information builds into a broad profile of the attacks impacting your networks, enabling your web security team to map trends and deploy appropriate resources.

Application Security also gives your developers full visibility into how the vulnerability in your code would have been exploited, including a stack trace down to the line of code (where relevant), reporting of request parameters, and how your app's behavior would have been modified.

(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 3.)

SQL Injection on MONEYX LOCAL VIEW STACK

ACTION TAKEN **BLOCKED**

PRIORITY **MEDIUM**

ATTACKER IP 187.61.48.17

TIME 08/21/2019, 23:18:30

POLICY Click to Manage Policy

Request Details

Transaction Type	HTTP
Invocation Type	Servlet
Base URL	http://localhost:8080
URL Path	/payment/list-received/3%20or%201=1%20–

SQL Injection Details

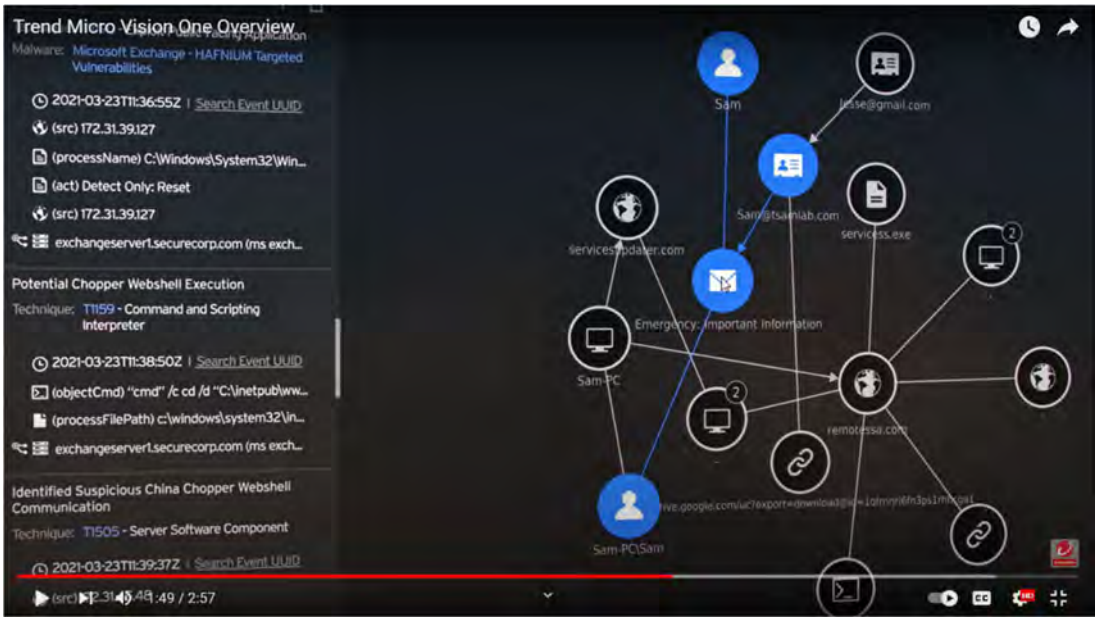
Trigger	Always True		
Dialect	h2	Supported	No
SQL Statement	select * from Payments p where p.receiver = [NUMBER] or [NUMBER]=[NUMBER]		

Triggered Policy Details

Always True (no properties)

(*See* WBR_TMC016686, *Cloud One Application Security*, https://resources.trendmicro.com/rs/945-CXD-062/images/DS02_Cloud_One_Application_Security_191108US_Web.pdf at p. 3.)

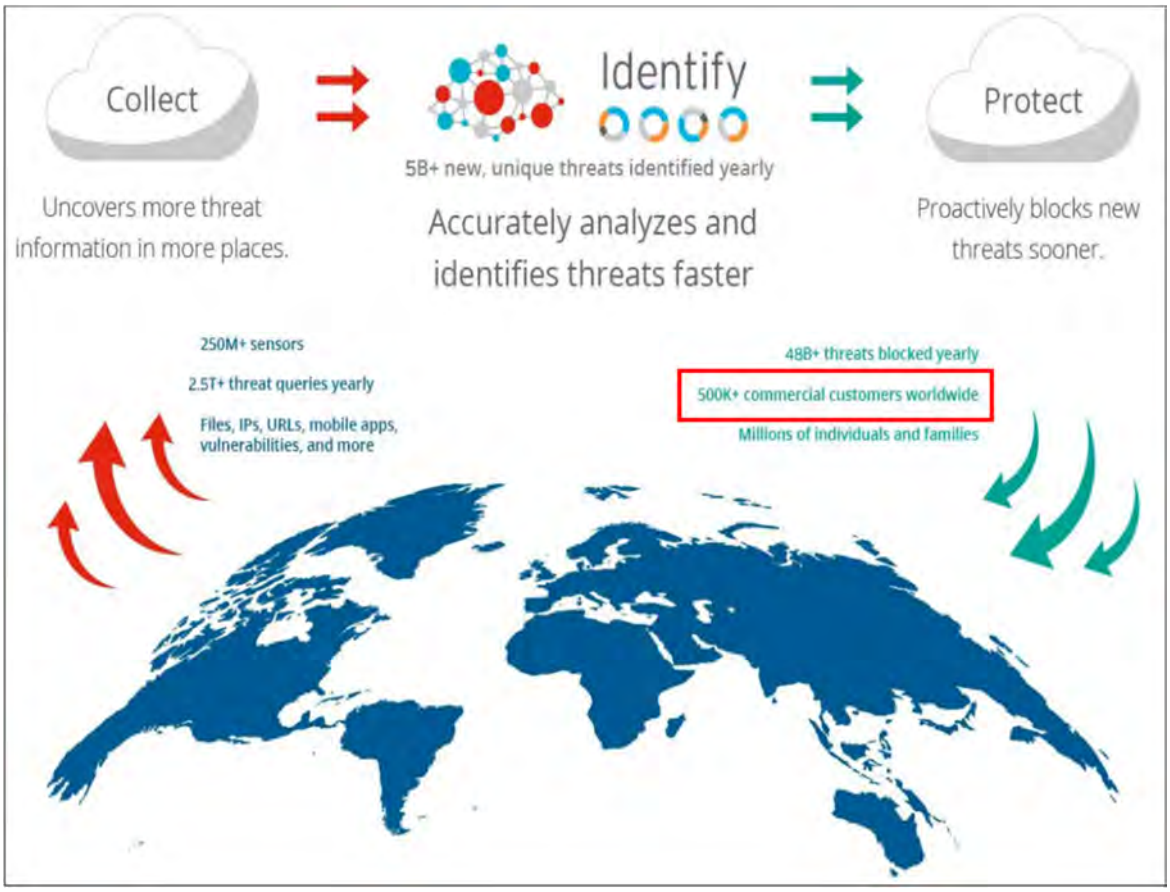
453. As another example, the Accused Products provide various diagrams, which dynamically illustrate an "attack-centric view" of an attack, including information such as an IP address, a process name, and/or various other information that identifies an origin of an attack.



(*See* WBR_TMC016622, https://www.youtube.com/watch?v=sCMs5MQOCi0 at timestamp 1:49)

454. The Accused Products perform a method that includes *reporting the identity of the externally networked source to an externally networked pestware research entity, wherein the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program*. As explained for the prior limitation, the Accused Products identify and provide information on "the attacker [and] type of attack" including "the time, origin, and type, on every attack that occurs on your apps to a central reporting point." Such attack-specific information includes the "attacker IP," "Base URL," and "URL Path," as well as "email origin of an attack."

455. In addition, for example, the Accused Products share this data with Trend Micro's Smart Protection Network. The "Smart Protection Network is a global threat intelligence that rapidly and accurately collects and identifies new threats, delivering instant protection for data wherever it resides." (*See* WBR_TMC020109, https://helpcenter.trendmicro.com/en-us/article/tmka-18569.) The information is reported to Trend Micro research. For example, "[t]hrough the Trend Micro Zero Day Initiative, … [Trend Micro] understand[s] the latest vulnerabilities and potential exploits and instantly protects [its] customers." (WBR_TMC020538, https://www.trendmicro.com/en_us/about/threat-research.html.)



(*See* Trend Micro, Smart Protection Network – Global Threat Intelligence, https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html.)

456. As another example, the Accused Products include or are integrated with "Trend Micro Service One," which uses information "gleaned from over 500,000 customers and 250 million global sensors" and "constantly monitor[s] and analyze[s] activity data from Trend Micro solution in your environment." Trend Micro Service One enables "security experts [to] detect, hunt, and contain threats," in part, by "correlating data and insights from email, endpoints, servers, cloud workloads, and network sources." Alerts generated by Trend Micro Service One includes "alerts [that] are based on intelligence-driven (threat intelligence reports, threat intelligence feeds, and/or malware analysis) or situational-awareness driven (suspicious events or IoC within the network) methods, processes, and analytics across all your Trend Micro solutions."

Security experts ready, willing, and able, 24/7/365

Scarce and overburdened resources impact both your ability to manage the attack surface lifecycle as well as effectively communicate risk across the organization. With Trend Micro One, limited resources don't have to slow you down. Our world-class experts can help you to be more resilient with premium support that focuses on getting you up and running fast while ensuring your solutions are optimally configured. Managed XDR can help identify and investigate threats, and incident response services are ready to assist during critical attacks.

Leveraging our in-depth knowledge gleaned from over 500,000 customers and 250 million global sensors, our targeted attack detection service scans for early indicators of compromise (IoC), providing proactive, qualified high-risk alerts of potential threats with expert resources to help you take quick action.

(*See* WBR_TMC018719, https://www.trendmicro.com/en_us/business/products/one-platform.html navigate to "Learn More" for access to "Solving the Attack Surface Risk Management Challenge" at p. 4.)

✔ Managed extended detection and response (Managed XDR) service

Trend Micro Service One™ Complete customers enjoy support from the Trend Micro™ Managed XDR service, which is backed by highly qualified cybersecurity experts around the world. They constantly monitor and analyze activity data from Trend Micro solutions in your environment. By correlating data and insights from email, endpoints, servers, cloud workloads, and network sources, our security experts detect, hunt, and contain threats. Your team will be notified of validated detections, allowing you to quickly react and respond and prevent similar attacks from occurring in the future

(*See* WBR_TMC020505, https://www.trendmicro.com/en_us/business/services/service-one.html *navigate to* "Read Solution Brief" for access to "Trend Micro Service One" at p. 1.)

Detect and respond faster

Our Targeted Attack Detection provides you with a timeline uncovering predictions of the high-risk attack. In addition, you'll receive a detailed action plan to help you react quickly and limit the scope of an attack and minimize business interruptions. View all notifications on our Targeted Attack Detection app, so you can stay on top of any threats discovered in your environment.

Trend Micro Vision One™ customers are eligible for Trend Micro Service One Complete, which provides extended coverage from our global Managed XDR team. Our expert team continually monitors suspicious, malicious and unwanted activity to generate high-fidelity alerts. These alerts are based on intelligence-driven (threat intelligence reports, threat intelligence feeds, and/or malware analysis) or situational-awareness driven (suspicious events or IoC within the network) methods, processes, and analytics across all your Trend Micro solutions.

Within hours of contacting us, our Incident Response experts will have established a customized plan of action with your IT department. Our workforce, tools, and processes will be set up instantly to monitor your network traffic while logs and disk images are already being analyzed for IoC or indicators of attack (IoA). In the background, our incident coordinators will organize the flow of information, making sure all defined stakeholders are being kept in the loop about findings, developments, and key decisions. Concise daily briefings and reports will provide you with all information and insight required to:

457. Each claim in the '932 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '932 Patent.

458. Trend Micro has been aware of the '932 Patent since at least the filing of this amended Complaint.

459. Defendant directly infringes at least claim 1 of the '932 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 this software and system to protect its 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.

460. Defendant's partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the '932 Patent, literally or

under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

461. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’932 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’932 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

462. Defendant 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.

463. Defendant further encourages and induces its customers to infringe claim 1 of the ’932 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 its Trend Micro security software, and services in the United States. (*See*, *e.g.*, WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One,

www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator's Guide.)

464. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

465. 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 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 '932 Patent.

466. 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 '932 Patent.

467. 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 the Accused Products into the United States, 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.

468. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the ’932 Patent, that functionality could not be performed.

469. Additionally, the accused functionality, including the functionality for identifying an origin of a malicious activity, API call monitoring, and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products’ API call monitoring, the Accused Products could not deploy their Root Cause Analysis and malware detection features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing

each of the steps as described and shown above, or without the system and components identified above that practice the ’932 Patent, that functionality could not be performed.

470. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including monitoring API calls) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying the origin of a malicious activity) as recited in the claims of the ’932 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

471. 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 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 ’932 Patent.

472. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’932 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.

473. 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 ’932 Patent.

474. Defendant’s infringement of the ’932 Patent is knowing and willful. Defendant acquired knowledge of the ’932 Patent and of the specific conduct that constitutes infringement of the ’932 Patent at least based on this amended Complaint. Defendant continues to engage in infringing activities after the filing of this amended complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

475. On information and belief, despite Defendant’s knowledge of the Asserted Patents, Defendant made the deliberate decision to sell products and services that they knew infringe these patents. Defendant’s continued infringement of the ’932 Patent with knowledge of the ’932 Patent constitutes willful infringement.

ELEVENTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’244 PATENT)

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

477. Trend Micro has infringed and continues to infringe one or more claims of the ’244 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 The Accused Products, including Trend Micro’s Apex One, Network One, Vision One, Endpoint Protection with Detection and Response, Trend Micro’s EDR/XDR and Cloud Products, and Trend Micro’s Smart Protection Network, when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’244 Patent as demonstrated below.

478. For example, claim 1 the ’244 Patent recites:

> A method for identifying an origin of suspected pestware activity on a computer, the method comprising:
>
> monitoring, with a kernel-mode driver, activity on the computer;
>
> generating an activity log on a file storage device of the computer from the kernel-mode driver;
>
> receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval;
>
> issuing a timestamp after receiving the time of interest;
>
> identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp; and
>
> accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware;
>
> wherein the recorded history of externally networked sources is stored on the file storage device.

479. To the extent the preamble is limiting, the Accused Products perform *a method for identifying an origin of suspected pestware activity on a computer*. As explained below in detail, the Accused Products “protect[] enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks.” (WBR_TMC007314, *Apex One Administrator’s Guide* at 1-2.) As part of this protection, the Accused Products include, among other things, a scan engine that “detect[s] different types of viruses and malware … by identify[ing] … [t]ell-tale characteristics of the virus code [and] [t]he precise location within a file where the virus resides.” (*Id.* at 6-3.) The Accused Products also perform specific behavior monitoring, which “constantly monitors endpoints for unusual modifications to the operating system or on installed software.”

(WBR_TMC018723, *Apex One whitepaper*, https://powerbox-na-file.trend.org at 4–6.) The Accused Products further include functionality for performing threat investigations, including returning information about the objects that created suspicious and/or malicious objects. (WBR_TMC018665, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains/es-root-cause-anal_001.aspx.)

480. The Accused Products perform a method that includes "*monitoring, with a kernel-mode driver, activity on the computer*" and "*generating an activity log on a file storage device of the computer from the kernel-mode driver*." The Accused Products use a kernel-mode driver for monitoring malicious activity. As one example, the Accused Products include a behavior monitoring core driver 32/64 bit, which is a "kernel mode driver [that] monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement." (WBR_TMC007314, *Apex One Administrator's Guide* at 6-8.)

COMPONENT	DESCRIPTION
Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.
Behavior Monitoring Core Driver 32/64-bit	This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.
Behavior Monitoring Core Service 32/64-bit	This user mode service has the following functions: • Provides rootkit detection • Regulates access to external devices • Protects files, registry keys, and services
Behavior Monitoring Configuration Pattern	The Behavior Monitoring Driver uses this pattern to identify normal system events and exclude them from policy enforcement.
Digital Signature Pattern	This pattern contains a list of valid digital signatures that are used by the Behavior Monitoring Core Service to determine whether a program responsible for a system event is safe.
Policy Enforcement Pattern	The Behavior Monitoring Core Service checks system events against the policies in this pattern.
Memory Scan Trigger Pattern (32/64-bit)	Behavior Monitoring uses the Memory Scan Trigger Pattern to identify possible threats after detecting the following operations: • File write action • Registry write action • New process creation After identifying one of these operations, Behavior Monitoring calls Real-time Scan's Memory Inspection Pattern to check for security risks. For details about the Real-time Scan operations, see *Memory Inspection Pattern on page 6-5*.
Damage Recovery Pattern	The Damage Recovery Pattern contains policies that are used for monitoring suspicious threat behavior.

(*Id.*) "Behavior monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through Malware Behavior Blocking and Event Monitoring." (WBR_TMC007314, *Apex One Administrator's Guide* at 9-2.) On information and belief, the monitored behavior and events are stored in a file storage device on the endpoint computer.

481. The Accused Products perform a method that includes "*receiving, from a user via an interface of the computer, a time of interest relating to a suspicion of pestware on the computer,*

wherein the time of interest includes a time interval." For example, the Accused Products, including Connected Threat Defense, provides a "web-based management console" that includes a Threat Investigation tool "to perform investigations" and "locate suspicious objects in the network." (*See* WBR_TMC016659, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains.aspx; WBR_TMC018684, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-threat-investig.aspx.) The user can initiate a preliminary investigation or a detailed investigation, depending on the desired scope of investigation. (*See* WBR_TMC018684, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-threat-investig.aspx.) Regardless of the investigation type, the user can set a custom investigation criteria by "specify[ing] or load[ing] up to 10 user-defined criteria, or load[ing] a C&C callback event" that includes a "period" corresponding to a specified time. https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-preliminary-inv.aspx. At least when the user specifies a C&C callback event, the user is inputting a time of interest relevant to the user's suspicion of pestware.

6. (Optional) To load C&C callback events, click **Select Criteria**.

a. Click **Yes**.

Note:
Applying existing criteria overwrites any criteria currently specified.

b. Go to the **C&C Callback Events** tab.

c. Select a criteria.
Click **Period** to filter the C&C callback events by the specified time.

d. Click **Load C&C Callback Events**.

Note:
The **Log Query** screen provides additional details about C&C callback events in case you need to review them before selection. To go to the **Log Query** screen, navigate to **Detections** > **Logs** > **Log Query**, and then filter by **Network Events** > **C&C Callback**.

(*See* WBR_TMC018677, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-preliminary-inv/es-starting-an-ass/es-supported-forma.aspx.)

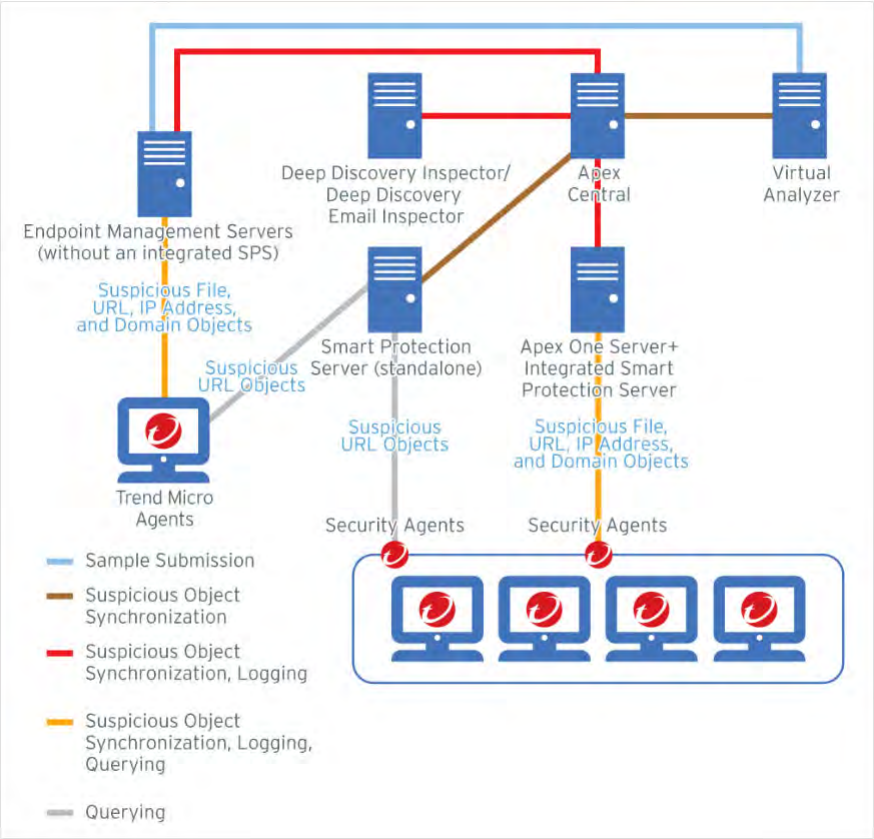
482. The Accused products perform the function: *issuing a timestamp after receiving the time of interest* [and] *identifying, based upon the time of interest, indicia of pestware, wherein the identifying is initiated by the issuing the timestamp*. For example, after the user specifies search criteria, such as by using a time stamp, "[t]he assessment goes through the server metadata and updates the result pane as soon [as] it finds a match." (*See* WBR_TMC018656, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-preliminary-inv.aspx.) Additionally, as shown in the table below, when an object is created, modified, or accessed, the Accused Products generate Indicators of Compromise that are available as searchable criteria.

Category	Item	Required Condition
FILEITEM	FULLPATH	IS, CONTAINS, STARTS-WITH, ENDS-WITH
	FILEPATH	IS
	FILENAME	IS, CONTAINS, STARTS-WITH, ENDS-WITH
	MD5SUM	IS
	SHA1SUM	IS
	SHA256SUM	IS
	SIZEINBYTES	IS
	CREATED	IS, GREATER-THAN, LESS-THAN
	MODIFIED	GREATER-THAN, LESS-THAN
	ACCESSED	GREATER-THAN, LESS-THAN

(*See* WBR_TMC018692, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-detailed-inv-in/supported-ioc-indica.aspx; *see also* WBR_TMC018656, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-preliminary-inv.aspx (explaining that OpenIOC rules can be used to "define investigation criteria").)

483. The Accused Products perform the function: *accessing, using a hardware processor of the computer, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify, based at least in part upon the identified*

indicia of pestware, a reference to an identity of an externally networked source that is suspected of originating pestware; wherein the recorded history of externally networked sources is stored on the file storage device. For example, the Accused Products, through Connected Threat Defense, connect endpoint devices to a central server for the ability "to locate suspicious objects in the network." (*See* WBR_TMC018684, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-threat-investig.aspx.) Once connected, servers, such as the server running Apex Central (as illustrated in the figure below), collect and store, in a database, behavior information from the endpoints and, then, analyze the stored information to detect objects that may be pestware. (*See id.* (explaining that Threat Investigation is used "to locate suspicious objects in the network"); *see also* WBR_TMC020509, *Understanding the Apex Central Database*, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/tools-and-additional/administering-the-da/understanding-the-co.aspx.)



(*See* WBR_TMC016694, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/connected-threat-def_001/connected-threat-def_002.aspx#GUID-27226D06-1A28-4F87-8757-3DF44767BE48.) At Apex Central, users can initiate threat investigations, where the user sets investigation criteria, and Apex Central conducts a "Root Cause Analysis" of the endpoint to return investigation results. (*See* WBR_TMC018656, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-preliminary-inv.aspx; *Starting a Root Cause Analysis from an Assessment*, WBR_TMC020492, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-preliminary-inv/es-starting-root-c.aspx; *Detailed Investigations*, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-detailed-inv-in.aspx.) The

investigation returns, for example, an analysis chain, which identifies, among other things, the first observed object as well as the objects related to the network connection. The first observed object would indicate the identity of the externally networked source that originated the pestware.

The root cause analysis area shows object types using the following icons:

Icon	Name	Description
	First Observed Object	Marks an object that most likely created the matched object
	Matched Criteria	Marks objects matching the investigation criteria
	Normal Object	Marks objects that have been verified to not pose a threat These are usually common system files.
	Unrated Object	Marks objects that are not system files but do not exhibit suspicious behavior
	Suspicious Object	Marks objects that exhibit behaviors that are similar to known threats
	Malicious Object	Marks objects that match a known threat
	Boot	Objects that launch during system startup
	Browser	Objects that are capable of displaying web pages, usually a web browser
	Email	Objects that can send and receive email messages, usually an email client or server
	File name	Objects that are files on the disk
	Network	Objects related to network connections or the Internet
	Process	Objects that are processes running during the time of execution
	Registry	Objects that are registry keys, entries or data
	Event	Indicates actions done by the object
	Association	Indicates relationships between two objects

(WBR_TMC018665, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains/es-root-cause-anal_001.aspx; WBR_TMC016659, https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/threat-defense/es-chapter-introdu/es-investigation-r/es-analysis-chains.aspx.)

484. Each claim in the ’244 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the ‘244 Patent.

485. Trend Micro has been aware of the ’244 Patent since at least the filing of this Amended Complaint.

486. Defendant directly infringes at least claim 1 of the ’244 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 this software and system to protect its 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.

487. Defendant’s partners, customers, and end users of its Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’244 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

488. Defendant has actively induced and is actively inducing infringement of at least claim 1 of the ’244 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, Defendant encourages and induces customers with specific intent to use Trend Micro’s security software in a manner that infringes claim 1 of the ’244 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including the activities described below.

489. Defendant 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.

490. Defendant further encourages and induces its customers to infringe claim 1 of the ’244 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 its Trend Micro security software, and services in the United States. (*See, e.g.*, WBR_TMC016674, Endpoint Security with Apex One, https://www.trendmicro.com/en_us/business/products/userprotection/sps/endpoint.html; WBR_TMC002543, Datasheet: Trend Micro Apex One, www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html?modal=s3aicon-datasheet-e4288a; WBR_TMC000006, Find a Trend Micro Partner, https://www.trendmicro.com/en_us/partners/find-a-partner.html; WBR_TMC007314, Apex One Administrator’s Guide.)

491. For example, on information and belief, Defendant 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. (*Id.*) 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. (*Id.*)

492. 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 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 '244 Patent.

493. 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 '244 Patent.

494. 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 the Accused Products into the United States, 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.

495. Indeed, as shown above, the Accused Products have no substantial non-infringing uses because the accused functionality, including the functionality for identifying an origin of a malicious activity and related functionality, are integral parts of the Accused Products and must be performed for the Accused Products to perform their intended purpose. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer suitably function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and

shown above, or without the system and components identified above that practice the '244 patent, that functionality could not be performed.

496. Additionally, the accused functionality, including the functionality for monitoring computer activity using a kernel-mode driver and generating an activity log, and related functionality described above, itself has no substantial non-infringing uses because the components, modules and methods identified above are a necessary part of that functionality. For example, without the Accused Products' kernel-mode driver, the Accused Products could not deploy their Root Cause Analysis and malware detection features. These processes are continually running when the system is in use and, on information and belief, cannot be removed or disabled (or, if they could, the system would no longer function for its intended purpose). Moreover, for the same reasons, without performing each of the steps as described and shown above, or without the system and components identified above that practice the '244 Patent, that functionality could not be performed.

497. In addition, as shown in the detailed analysis above, the products, systems, modules, and methods provided by Defendant constitute a material part of the invention—indeed, they provide all the components, modules, and features that perform the claimed methods and systems. For example, the Accused Products and accused functionalities (including monitoring computer activity using a kernel-mode driver and generating an activity log) constitute a material part of the inventions claimed because such analysis is integral to the processes identified above (such as identifying the origin of a malicious activity) as recited in the claims of the '244 Patent. None of these products are staple goods—they are sophisticated and customized cyber security and malware detection products, methods, and systems.

498. 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 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 ’244 Patent.

499. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendant’s infringement of the ’932 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.

500. 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 ’932 Patent.

501. Defendant’s infringement of the ’932 Patent is knowing and willful. Defendant acquired knowledge of the ’244 Patent and of the specific conduct that constitutes infringement of the ’244 Patent at least based on this amended Complaint. Defendant continues to engage in infringing activities after the filing of this amended complaint, including by selling, making, configuring, and installing the Accused Products and performing the accused functionality, and by engaging in activities that constitute inducing infringement and contributory infringement as described above.

502. On information and belief, despite Defendant’s knowledge of the Asserted Patents, Defendant made the deliberate decision to sell products and services that they knew infringe these

patents. Defendant's continued infringement of the '244 Patent with knowledge of the '244 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 its 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: September 7, 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

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

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

Christopher C. Campbell (DC Bar No. 444262)
Patrick M. Lafferty *(pro hac vice)*
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)*
Brian Eutermoser (*pro hac vice)*
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

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

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing instrument was served or delivered electronically via the U.S. District Court ECF filing system to all counsel of record on this 7th day of September, 2022.

/s/ Jeffrey D. Mills
Jeffrey D. Mills