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

TAASERA LICENSING LLC,	§ § §	Case No. 2:21-cv-00441-JRG-RSP
Plaintiff,	§ §	**JURY TRIAL DEMANDED**
v.	§ § §	
TREND MICRO INCORPORATED,	§ §	
Defendant.	§ § §	

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Taasera Licensing LLC ("Taasera Licensing" or "Plaintiff") for its Amended

Complaint against Defendant Trend Micro Incorporated ("Trend Micro") alleges as follows:

THE PARTIES

1.   Taasera Licensing is a limited liability company, organized and existing under the

laws of the State of Texas, with its principal place of business located at 100 West Houston Street,

Marshall, Texas 75670.

2.   Upon information and belief, Trend Micro is a Japanese corporation whose stock

is publicly traded on the Tokyo Stock Exchange, with a principal place of business located at

Shinjuku Maynds Tower, 2-1-1 Yoyogi, Shibuya-ku, Tokyo, Japan 151-0053. Upon information

and belief, Trend Micro does business in Texas and in the Eastern District of Texas, directly or

through intermediaries, such as its subsidiaries.

JURISDICTION

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

4.   This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States. Upon information and belief, Trend Micro conducts business at its U.S. Headquarters located at 225 E. John Carpenter Freeway, Suite 1500, Irving, Texas 75062.

5.   Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) and (c) because the Defendant is a foreign corporation subject to personal jurisdiction in this Judicial District. The Defendant, through its own acts, makes, uses, sells, and/or offers to sell infringing products within this Judicial District, regularly does and solicits business in this Judicial District, and has the requisite minimum contacts with the Judicial District such that this venue is a fair and reasonable one. Upon information and belief, Trend Micro directly or indirectly participated in the stream of commerce that results in products, including the accused products, being made, used, offered for sale, and/or sold in the State of Texas and/or imported into the United States to the State of Texas.

6.   Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business

2

in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

7.   On January 11, 2005, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 6,842,796 (the "'796 Patent") entitled "Information Extraction from Documents with Regular Expression Matching." A true and correct copy of the '796 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=6842796.

8.   On March 2, 2010, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,673,137 (the "'137 Patent") entitled "System and Method for the Managed Security Control of Processes on a Computer System." A true and correct copy of the '137 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=7673137.

9.   On December 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,327,441 (the "'441 Patent") entitled "System and Method for Application Attestation." A true and correct copy of the '441 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8327441.

10.   On September 30, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,850,517 (the "'517 Patent") entitled "Runtime Risk Detection Based on User, Application, and System Action Sequence Correlation." A true and correct copy of the '517 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8850517.

11.   On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the "'038 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true

and correct copy of the '038 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8955038.

12.   On March 24, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,990,948 (the "'948 Patent") entitled "Systems and Methods for Orchestrating Runtime Operational Integrity." A true and correct copy of the '948 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=8990948.

13.   On July 28, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,092,616 (the "'616 Patent") entitled "Systems and Methods for Threat Identification and Remediation." A true and correct copy of the '616 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=9092616.

14.   On March 28, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,608,997 (the "'997 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '997 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=9608997.

15.   On March 20, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,923,918 (the "'918 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '918 Patent is available at http://pdfpiw.uspto.gov/.piw?PageNum=0&docid=9923918.

16.   Taasera Licensing is the sole and exclusive owner of all right, title, and interest in the '796 Patent, the '137 Patent, the '441 Patent, the '517 Patent, the '038 Patent, the '948 Patent, the '616 Patent, the '997 Patent, and the '918 Patent (collectively, the "Patents-in-Suit"), and holds

the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including

the filing of this patent infringement lawsuit. Taasera Licensing also has the right to recover all

damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive

relief as appropriate under the law.

FACTUAL ALLEGATIONS

17.   The Patents-in-Suit generally cover systems and methods for network security

systems.

18.   Five of the Patents-in-Suit were invented by International Business Machines

("IBM"). IBM pioneered the field of network security. Every year, IBM spends billions of dollars

on research and development to invent, market, and sell new technology, and IBM obtains patents

on many of the novel inventions that come out of that work, including the Patents-in-Suit. The six

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

decade.

19.   Four of the Patents-in-Suit were developed by TaaSera, Inc. TaaSera, Inc. was a

leader in preemptive breach detection systems, and comprised of security architects and subject

matter experts with decades of experience in firewalls, intrusion detection, security event

management, malware analysis, and endpoint security. The TaaSera, Inc. patents identify patterns

of malicious coordinated network and endpoint behaviors.

20.   The '796 Patent generally relates to technology that extracts information from

documents with regular expression matching. The technology described in the '796 Patent was

developed by Geoffrey G. Zweig and Mukund Padmanabhan of IBM.

21.   The '137 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '137 Patent was developed by Thomas James Satterlee and William Frank Hackenberger of IBM.

22.   The '441 Patent generally relates to technology for application attestation. The technology described in the '441 Patent was developed by Srinivas Kumar and Gurudatt Shashikumar of TaaSera, Inc.

23.   The '517 Patent generally relates to runtime risk detection based on user, application, and/or system actions. The technology described in the '517 Patent was developed by Srinivas Kumar of TaaSera, Inc.

24.   The '038 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '038 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

25.   The '948 Patent generally relates to technology that provides runtime operational integrity profiles identifying a threat level of subjects or applications. The technology described in the '948 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

26.   The '616 Patent generally relates to technology that provides integrity profiles identifying a threat level of a system. The technology described in the '616 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

27.   The '997 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '997 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

28.   The '918 Patent generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the '918 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

29.   Defendant has infringed and continues to infringe one or more of the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or import products that implement the network security inventions claimed in the Patents-in Suit. For example, the Accused Products include at least Trend Micro OfficeScan, Cloud App Security, ScanMail for Microsoft Exchange, ScanMail for Lotus Domino, InterScan Messaging Security, InterScan Web Security, IM Security for Microsoft Lync, Portal Protect for Microsoft SharePoint, Smart Protection for Endpoints & Complete, Deep Discovery Inspector, Apex Central, Vision One, and Apex One.

30.   TaaSera, Inc. manufactured commercial and academic versions of its NetTrust Security Appliance. NetTrust combined breach detection with security analytics to identify hidden threatening network behaviors. The analytics engine analyzed behavioral profiles, threat patterns, and contextual evidence to rank systems by their risk of breach.

31.   Upon information and belief, Taasera Licensing and its predecessors have complied with the requirements of 35 U.S.C. § 287(a).

<div align="center">

COUNT I
(Infringement of the '796 Patent)

</div>

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

33.   Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '796 Patent.

34.   Defendant has and continues to directly infringe the '796 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making,

using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '796 Patent including, but not limited to, claim 1.[1] Such products incorporate the integrated Data Loss Prevention (iDLP) feature and include at least the Trend Micro OfficeScan, Cloud App Security, ScanMail for Microsoft Exchange, ScanMail for Lotus Domino, InterScan Messaging Security, InterScan Web Security, IM Security for Microsoft Lync, Portal Protect for Microsoft SharePoint, Smart Protection for Endpoints & Complete, and Apex One, Vision One (the "'796 Accused Products") which practice a method of automatically processing an input sequence of data symbols, the method comprising the steps of: identifying at least one regularly identifiable expression in the input sequence of data symbols, wherein the at least one regularly identifiable expression represents a pattern that is matchable in accordance with a programming language that supports such a regularly identifiable expression; identifying at least a portion of information associated with the at least one regularly identifiable expression; and extracting the portion of information.

35.   Every '796 Accused Product practices automatically processing an input sequence of data symbols. For example, the Trend Micro Worry-Free Business Security -- Messaging Security incorporates iDLP rules.

---

[1] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website   at https://www.trendmicro.com/product_trials/service/index/us/165?_ga=2.224034523.1797687026.1660610776-1305895883.1660610776&_gac=1.124065528.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWua fJO6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

Trend Micro™

INTEGRATED DATA LOSS PREVENTION

Protect Your Data

Now more than ever, your data is on the move—whether it's on a laptop, flash drive, or moving across physical, virtual, and cloud infrastructures. At any point along the way, your financial data, customer information, intellectual property, or trade secrets could be lost or stolen. Securing this data is further complicated by several growing risk factors:

- Rapidly evolving compliance regulations and mandates
- Continued growth of workforce mobility
- Employees using their own mobile devices and consumer apps for work
- Rising frequency of advanced persistent threats (APTs) and data breach incidents

To avoid the embarrassment, reputation damage, regulatory fines, and revenue loss, today's enterprises must be able to identify, track, and secure all confidential data from multiple points within the organization and in the cloud, without impacting employee productivity and performance. In the past, many organizations tried traditional data loss prevention (DLP) solutions but found they were too intrusive, too complex to manage, and too costly to acquire, deploy, and maintain.

Reduce the Cost and Complexity of DLP

Trend Micro™ Integrated DLP minimizes the complexity and cost of data security by integrating DLP functionality directly into your existing Trend Micro solutions and management consoles. With a lightweight plug-in, you can quickly and easily gain visibility and control of your sensitive data and prevent data loss via USB, email, Software as a Service (SaaS) applications, web, mobile devices, and cloud storage. The DLP plug-in requires no extra hardware or software, and it leverages built-in regional and industry-specific templates to simplify deployment and comply with regional guidelines and regulations. Integrated DLP allows you to deploy data security for a fraction of the cost and time of traditional enterprise DLP solutions.

Advantages of Integrated DLP

Protect your data—today
Deploy DLP immediately and gain visibility and control of your data right away

Lower DLP costs
Save on deployment and maintenance costs compared to traditional DLP

Protect privacy
Identify, monitor, and prevent data loss— on or off network

Comply with regulations
Implement controls for protection, visibility, and enforcement

Educate users
Notify employees of risky behavior or enforce user controls if necessary

Integrated DLP on Endpoints

Strengthens Data Protection and Control

- Empowers IT to restrict the use of USB drives, USB attached mobile devices, CD/DVD writers, cloud storage, and other removable media with granular device control and DLP policies
- Enables cloud storage with DLP enforcement of file encryption as well as SaaS application usage with DLP for Microsoft® Office 365®
- Detects and reacts to improper data use based on keywords, regular expressions, and file attributes
- Educates employees on corporate data usage policies through alerts, blocking or soft-blocking, and reporting

Supports Compliance

- Simplifies regulatory compliance with out-of-the-box compliance templates
- Speeds audits and enforcement with forensic data capture and real-time reporting
- Provides regional specific templates and data protection options, helping customers comply with data protection guidelines such as General Data Protection Regulation (GDPR)

Streamlines Administration, Lowers Costs

- Simplifies deployment and maintenance with a lightweight DLP plug-in
- Improves visibility and control with a fully-integrated, centrally-managed solution
- Reduces resource demand and performance impact with a single agent for endpoint security, device control, and content DLP

Integrated DLP on Network Gateways and in the Cloud

Strengthens Data Protection and Control

- Inspects your network 24x7 with real-time monitoring
- Tracks and documents sensitive data flowing through network egress points, mobile devices, or via SaaS applications
- Identifies risky business processes and improves corporate data usage policies
- Detects and reacts to improper data use based on keywords, regular expressions, and file attributes

Supports Compliance

- Aids in compliance of regulations such as GDPR, with out-of-the-box compliance templates
- Speeds audits and enforcement with forensic data capture and real-time reporting

Streamlines Administration, Lowers Costs

- Simplifies deployment with a DLP plug-in, requiring no additional hardware or software
- Improves visibility and control with a fully-integrated, centrally-managed solution
- Automates response to policy violations with options to log, bypass, block, encrypt, alert, modify, quarantine, or delete data

2

---

[2] https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/endpoint/intedgraded-data-loss/DS_IntegratedDLP.pdf

36.   Every '796 Accused Product practices identifying at least one regularly identifiable expression in the input sequence of data symbols, wherein the at least one regularly identifiable expression represents a pattern that is matchable in accordance with a programming language that supports such a regularly identifiable expression. For example, Trend Micro Worry-Free Business Security -- Messaging Security enforces iDLP rules created using regular expressions.

Adding a Rule Using Your Own Regular Expression

You can use your own regular expressions with Data Loss Prevention rules. You are not limited to auto-generated expressions.

⚠ Regular expressions are a powerful string-matching tool. Ensure that you are comfortable with regular expression syntax before using these expressions. Poorly written regular expressions can dramatically impact performance. Trend Micro recommends starting with simple regular expressions. When creating new rules, use the "archive" action and observe how Data Loss Prevention manages messages using the rule. When you are confident that the rule has no unexpected consequences, you can change the action.

To add a rule using your own regular expression:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention > Add** to open the Add Rule screen.
2. In the **Select target** section select one or more of the following email fields for the rule to evaluate:
   - Header (**From, To, Cc**)
   - **Subject**
   - **Body**
   - **Attachment**
3. In the **Add details** section, select **Regular expression (user-defined)**. A "Rule Name" and "Regular Expression" field display.
4. In the provided field type a **Rule Name**. This field is required.
5. In the **Regular Expression** field type a regular expression, beginning with a "REG."prefix, up to 255 characters long including the prefix.

   ⚠ Be very careful when pasting into this field. If any extraneous characters, such as an OS-specific line feed or an HTML tag, is included in the content of your clipboard, the expression pasted will be inaccurate. For this reason, Trend Micro recommends typing the expression by hand.

6. To verify that the regular expression matches the intended pattern, select **Provide another example to verify the rule (Optional)**. A test field appears below this option.
7. Type another example of the pattern that you just entered (40 characters or less). For example, if this expression is to match a series of account numbers of the pattern "CC-????? 20??" type another example that matches, such as "cc-65432 2012"and then click **Test**. The tool validates the new sample against the existing regular expression and places a green check mark (✅) icon next to the field if the new sample matches. If the regular expression does not match the new sample, a red X icon (❌) appears next to the field.
8. Click **Next**. The Data Loss Prevention > Add Rule screen with "Select an action" and "Notification" sections appears.
9. Finalize the rule by configuring the action, notification, and advanced options sections as explained in steps 4 through 7.

3

---

37.   Every '796 Accused Product practices identifying at least a portion of information associated with the at least one regularly identifiable expression. For example, Trend Micro Worry-Free Business Security -- Messaging Security extracts information to use in the notification of a match to an iDLP rule.

---

[3] https://docs.trendmicro.com/all/smb/wfbs-a/v7.0/en-us/wfbs-a_7.0_olh/WFBS/Managing_the_Messaging_Security_Agent/DLPAddingEditingRules.htm

Configuring Data Loss Prevention Notifications

The following explains the steps required to configure data loss prevention notifications:

Procedure

1. On the left menu, click **Data Loss Prevention → Policies**. The **Data Loss Prevention** screen appears.
2. Click **Add**, to add a new policy, or click an existing policy from the **Policy** column. The **Data Loss Prevention: Edit Policy** screen appears.
3. Click the **Notification** tab.
4. Under **People to notify**, select **Notify administrator** to enable data loss prevention notifications.
5. Under **People to notify**, click **Show details** and configure the following:
   - **To**—the global email address(es) appear in this field. You can enter additional email addresses, separated by a semicolon (;) to create unique notifications.
   - **Subject**—type a subject that will appear in the subject line of the email (for example: Data Loss Prevention Notification).
   - **Message**—you can create a unique message using variables like: [Server Name], [Data Loss Prevention Rules], [Date], [Time], [File Name/Web Content Title], [File/Web Content Location], [Action], and [Violator].

   > **Note**
   > The available variables appear in the left window, and the message body in the right window.

6. Under **Settings**, choose the delivery options for this notification according to the following:
   - **Send consolidated notifications every [xx] [hours or days]**—select this option to send a notification according to the number of hours or days you type in the variable field.
   - **Send consolidate notifications every [xx] occurrences**—select this option to send a notification after a certain number of occurrences as you stipulate in the variable field.
   - **Send individual notifications**—select this option to send a notification each time an event occurs.
7. Under **Advanced Notification** (SNMP), select **SNMP** to enable this option.
8. Click **Show details** to expand the options, and configure according to the following:
   - **IP Address**
   - **Community**
   - **Message**
9. Select **Write to Windows event log** to write each notification to the Windows event log.
10. Click **Save**.

4

38.   Defendant has and continues to indirectly infringe one or more claims of the '796 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '796 Accused Products (*e.g.*, products incorporating the iDLP feature).

39.   Defendant has and continues to indirectly infringe one or more claims of the '796 Patent including, but not limited to, claim 1, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to

---

[4] *Id.*

11

sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with the knowledge that these products, or the use thereof, infringe the '796 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '796 Patent by providing these products to customers and end-users for use in an infringing manner.

40.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '796 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[5] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the integrated Data Loss Prevention feature.[6]

41.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '796 Patent in an amount to be proved at trial.

42.   Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '796 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

<div align="center">

COUNT II
(Infringement of the '137 Patent)

</div>

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

---

[5] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[6] https://docs.trendmicro.com/all/smb/wfbs-a/v7.0/en-us/wfbs-a_7.0_olh/WFBS/Managing_the_Messaging_Security_Agent/DLPAddingEditingRules.htm

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

45.   Defendant has and continues to directly infringe the '137 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '137 Patent including, but not limited to, claim 1.[7] Such products incorporate the Application Control feature and include at least Trend Micro Apex One and Trend Micro Vision One (the "'137 Accused Products") which practice a method for implementing security for a computing device comprising the steps of: interrupting the loading of a new program for operation with the computing device; validating the new program; if the new program is validated, permitting the new program to continue loading and to execute in connection with the computing device; if the new program is not validated, monitoring the new program while it loads and executes in connection with the computing device, wherein the step of monitoring the new program while it executes is performed at the operating system kernel of the computing device.

46.   Every '137 Accused Product practices interrupting the loading of a new program for operation with the computing device. For example, the Trend Micro Apex One performs application control.

---

[7] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJ O6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

How does application control work?
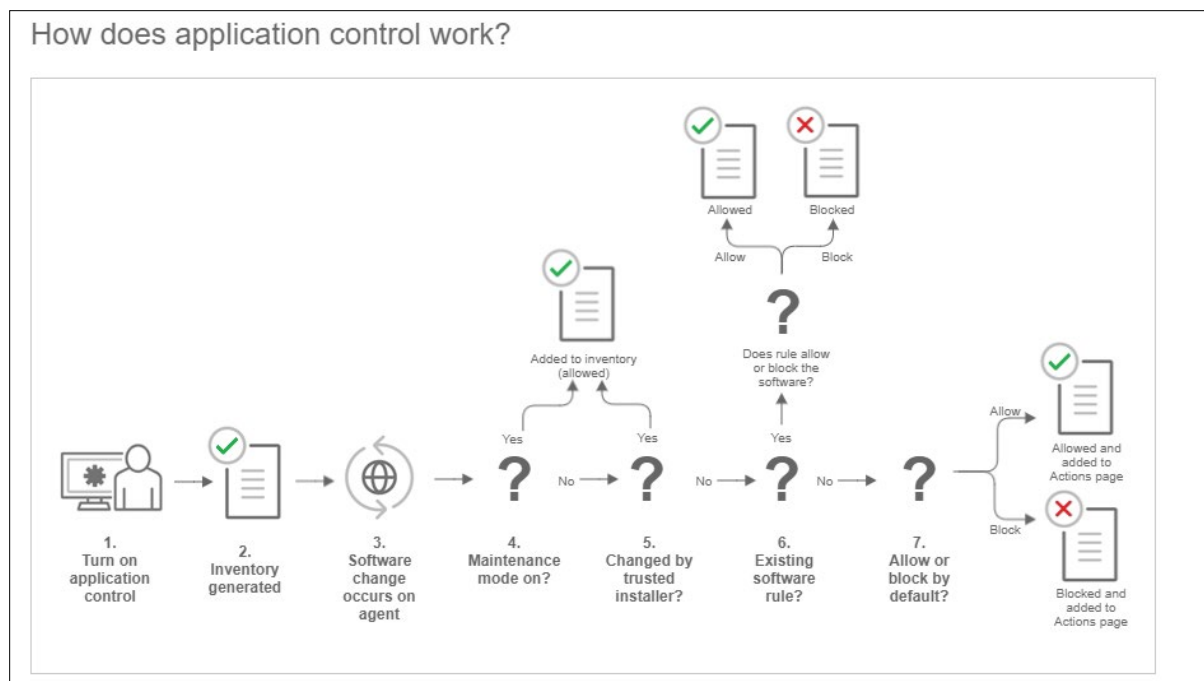
47.   Every '137 Accused Product practices permitting the new program to continue loading and executing in connection with the computing device if the new program is validated. For example, Trend Micro Apex One (Deep Security Agent) permits new programs to run if the new program was initiated by a trusted installer.

48.   Every '137 Accused Product practices monitoring the new program while it loads and executing in connection with the computer device. For example, if the new program passes Trend Micro Apex One (Deep Security Agent) Application Control, it will continue to be monitored by Application Control, for example, to determine if it launches a new process and it will be monitored by the endpoint run-time solutions, such as Behavior Analysis.

---

[8] https://help.deepsecurity.trendmicro.com/azure/application-control.html
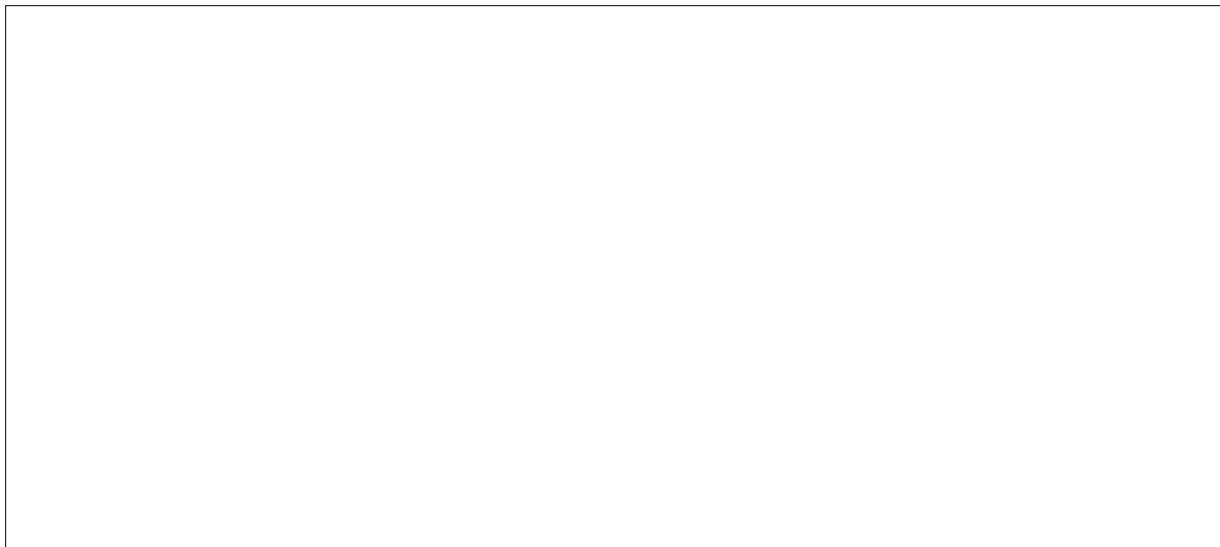
49.   Defendant has and continues to indirectly infringe one or more claims of the '137 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as '137 Accused Products (*e.g.*, products incorporating the Application Control feature).

50.   Defendant has and continues to indirectly infringe one or more claims of the '137 Patent including, but not limited to, claim 1, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '137 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '137 Patent by providing these products to end-users for use in an infringing manner.

---

[9] https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html

51.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '137 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[10] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Application Control and Predictive Machine Learning features.[11]

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

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

COUNT III
(Infringement of the '441 Patent)

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

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

56.   Defendant has and continues to directly infringe the '441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each

---

[10] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[11]   https://help.deepsecurity.trendmicro.com/azure/application-control.html;   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

and every limitation of one or more claims of the '441 Patent including, but not limited to, claim 1.[12] Such products incorporate the Predictive Machine Learning feature and include at least the Trend Micro Vision One and Trend Micro Apex One (the "'441 Accused Products") which practice a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.

57.   Every '441 Accused Product practices a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server. For example, Trend Micro Apex One incorporates predictive machine learning to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks.

---

[12] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJO6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

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.
Process	After detecting an unknown or low-prevalence process, the Security Agent monitors the process using the Contextual Intelligence Engine, and sends the behavioral report to the Predictive Machine Learning engine. Through 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.
	Process detection also monitors script execution. If the Contextual Intelligence Engine detects the execution of a suspicious script, Predictive Machine Learning takes the configured action.
	Predictive Machine Learning performs script blocking on the following types of scripts: - cscript - jar - powershell - vbs - wscript
	Depending on how you configure Predictive Machine Learning, the Security Agent can "Terminate" the affected process or script and attempt to clean the file that executed the process or script.

13

58.   Every '441 Accused Product practices receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application, and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components. For example, Trend Micro Apex One

---

[13] 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

receives process attributes, context information, and processes behavior information for detected threats.

59.   Every '441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result. For example, Trend Micro Apex One logs information related to each detected threat, including the result of the detected threat.

Viewing Predictive Machine Learning Logs

1. Go to one of the following:
   ○ **Logs > Agents > Security Risks**
   ○ **Agents > Agent Management**
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Go to the Predictive Machine Learning Log Criteria screen:
   ○ From the Security Risk Logs screen, click **View Logs > Predictive Machine Learning Logs**.
   ○ From the Agent Management screen, click **Logs > Predictive Machine Learning Logs**.
4. Specify the log criteria and then click **Display Logs**.
5. View logs. Logs contain the following information:

Item	Description
Date/Time	The time the detection occurred
Endpoint	The endpoint on which the detection occurred
IP Address	The IP address and port number of the source endpoint
Security Threat	The name of the security threat determined by the Predictive Machine Learning engine
Result	The result of the action taken
Infected File/Object	The name of the file object or the program that executed the process
Type	The type of object that triggered the detection ("File" or "Process")
File Path	The path of the file object or the path of the program that executed the process
Infection Channel	The channel the threat originated from
Details	A link that displays the detailed analysis for the specific detection For more information, see Predictive Machine Learning Log Details.

[14]

---

[14] https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/unknown-threat-logs/viewing-predictive-m.aspx

60.   Defendant has and continues to indirectly infringe one or more claims of the '441 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as '441 Accused Products (*e.g.*, products incorporating the predictive machine learning feature).

61.   Defendant has and continues to indirectly infringe one or more claims of the '441 Patent including, but not limited to, claim 1, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '441 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '441 Patent by providing these products to end-users for use in an infringing manner.

62.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '441 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[15] Defendant provides product manuals and

---

[15] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/

documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Predictive Machine Learning feature.[16]

63.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '441 Patent in an amount to be proved at trial. Upon information and belief, Taasera and prior assignees of the '441 Patent, prior assignees' affiliates, and prior assignees' sublicensees to the '441 Patent, complied with the marking statute 35 U.S.C. § 287. Accordingly, Taasera is entitled to pre-suit damages.

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

COUNT IV
(Infringement of the '038 Patent)

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

66.   Neither Taasera Licensing nor TaaSera, Inc. have licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '038 Patent.

67.   Defendant has and continues to directly infringe the '038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '038 Patent including, but not limited to, claim 23.[17] Such products incorporate the Vulnerability Protection feature and include at least the Trend

---

[16]   https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-one-2019-server-online-help/protecting-trend_cli/protecting-against-u_001/unknown-threat-logs/viewing-predictive-m.aspx

[17] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website   at   https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-

Micro Apex One and Trend Micro Vision One (the "'038 Accused Products") which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

68.   Every '038 Accused Product practices a method for controlling the operation of an endpoint. For example, the Trend Micro Apex One performs Vulnerability Protection on endpoints.

1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJ
O6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

VULNERABILITY PROTECTION

Backed by world-class vulnerability research, Apex One security's virtual patching delivers the most-timely vulnerability protection in the industry across a variety of endpoints.

Stop zero-day threats immediately on your endpoints—on and off the network.

Trend Micro Vulnerability Protection, along with Trend Micro's portfolio of endpoint capabilities extend protection to critical platforms, including legacy operating systems.

Defends Against Advanced Threats

- Blocks known and unknown vulnerability exploits before patches are deployed.
- Protects end-of-support and legacy operating systems, for which patches may never be provided.
- Dynamically adjusts security configuration based on the location of an endpoint.
- Protects endpoints with minimal impact on network throughput, performance, or user productivity.
- Shields endpoints against unwanted network traffic with multiple protection layers.
- Protects systems that hold sensitive data, critical to regulatory and corporate policy compliance.

Removes Bad Data from Business-Critical Traffic

- Applies control filters to alert/block specific traffic such as instant messaging and media streaming.
- Uses deep packet inspection to identify content that may harm the application layer.
- Filters forbidden network traffic and ensures allowed traffic through stateful inspection.

Provides Earlier Protection

- Provides protection before patches are deployed and often before patches are available.
- Shields operating system and common applications from known and unknown attacks.
- Detects malicious traffic that hides by using supported protocols over non-standard ports.
- Blocks traffic likely to damage at-risk components using vulnerability-facing network inspection.
- Prevents networking backdoors from penetrating into the corporate network.
- Blocks all known exploits with intrusion prevention signatures.
- Defends custom and legacy applications using custom filters that block user-defined parameters.

Software

Protection Points

- Endpoints

Threat Protection

- Vulnerability exploits
- Denial of service attacks
- Illegitimate network traffic
- Web threats

Features and Benefits

- Eliminates risk exposure due to missing patches
- Extends the life of legacy and end-of-support (EOS) operating systems
- Reduces down-time for recovery with incremental protection against zero-day attacks
- Allows patching on your own terms and timelines
- Lowers potential legal exposure by improving data security compliance
- Enhances firewall protection for remote and mobile enterprise endpoints

18

69.   Every '038 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies and maintaining the plurality of policies in a data store on the computing system. For example, Trend Micro Apex One allows configuration of a plurality of policies (*e.g.*, Intrusion Prevention rules) at a system remote from the endpoint through a provided user interface which are stored in a data store.

---

[18] https://www.trenddefense.com/datasheets/sb-apex-one.pdf
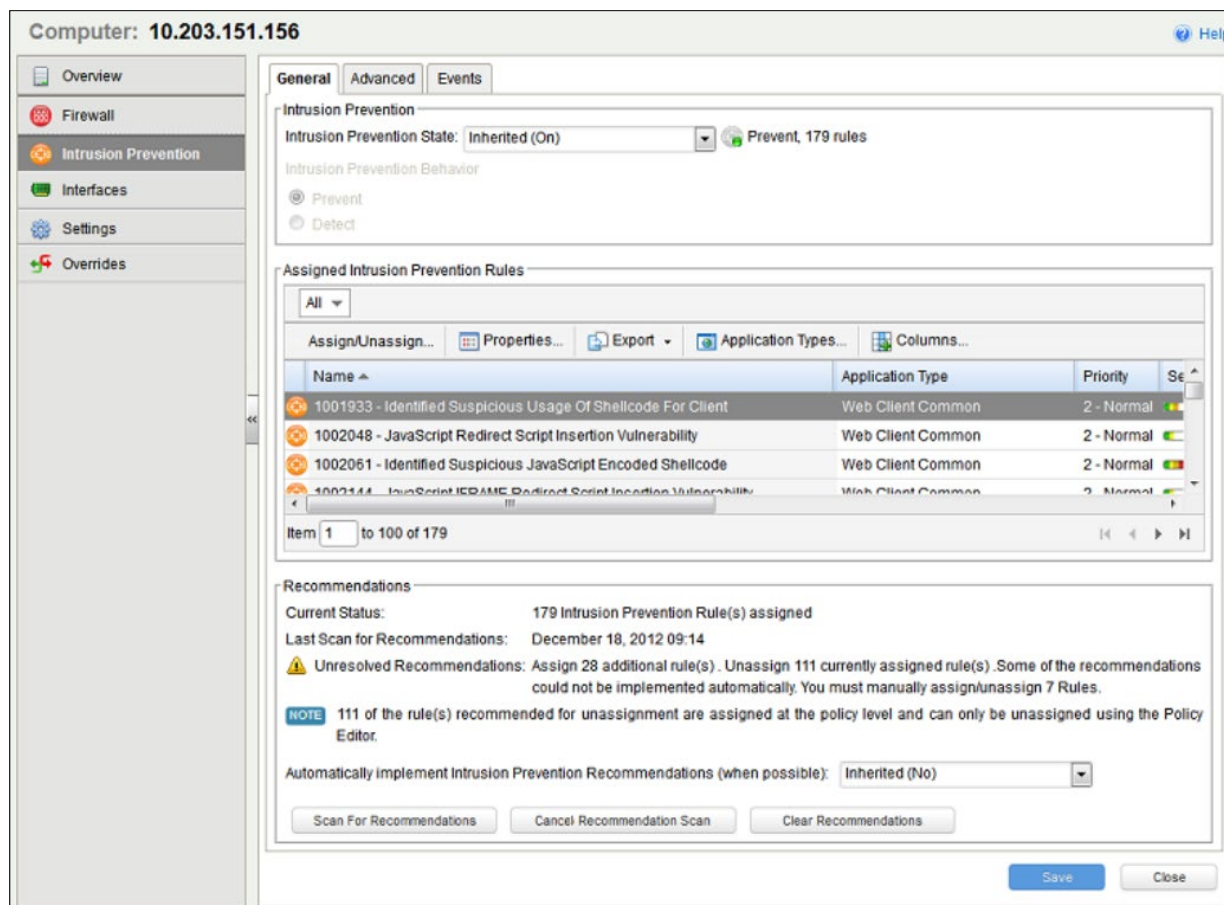
19

70.   Every '038 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Trend Micro Apex One (Vulnerability Protection) identifies, from the plurality of polices (*e.g.*, Intrusion Prevention rules), vulnerability attack indicators on the endpoint to monitor.

71.   Every '038 Accused Product practices configuring one or more software agents on the endpoint to monitor the plurality of operating conditions. For example, Trend Micro Apex One configures at least the Vulnerability Protection Agent to monitor the plurality of operating conditions (*e.g.*, vulnerability attack indicators on the endpoint).

---

[19] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

72.   Every '038 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents. For example, Apex One/Apex Central receives information regarding whether vulnerability attacks have been detected, gathered by the one or more software agents (*e.g.*, Vulnerability Protection Agent).
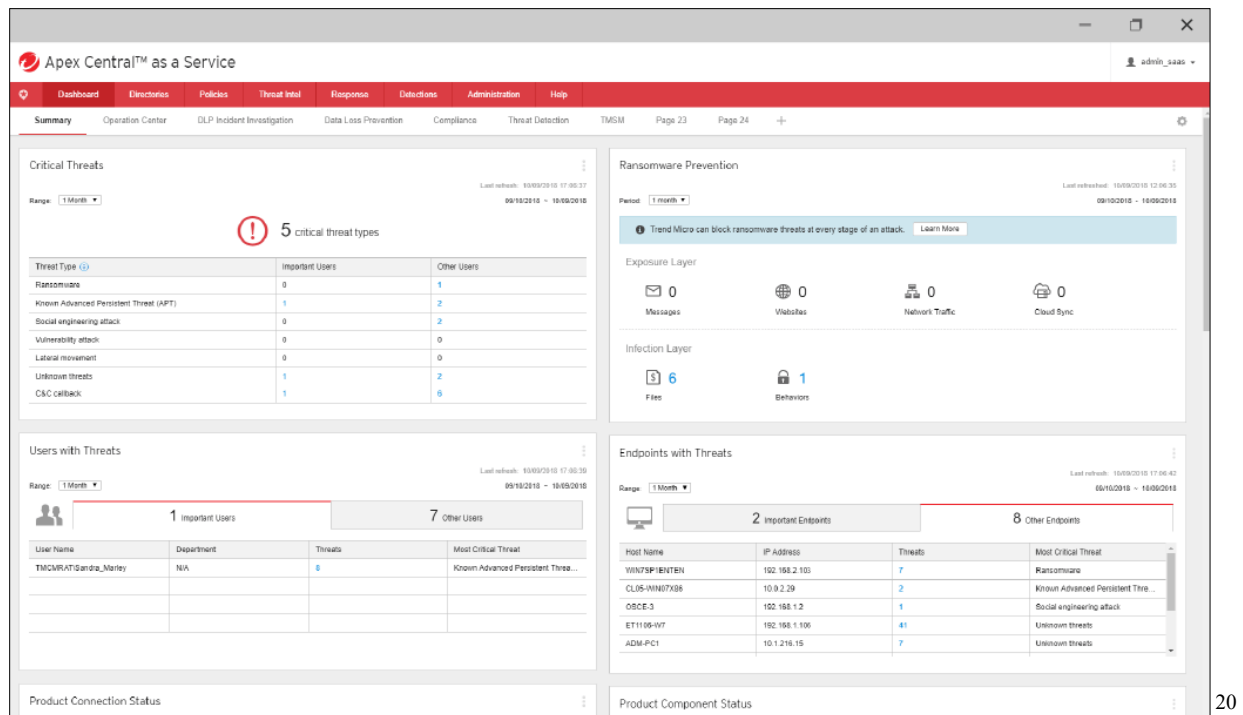
73.   Every '038 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information (*e.g.*, whether vulnerability attacks have been detected) and a plurality of compliance policies in the data store. For example, Trend Micro Apex One determines a compliance state of the endpoint based on the status information and the Intrusion Prevention rules.

---

[20] https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ultimate-protection-against-vulnerabilities.png

74.   Every '038 Accused Product practices initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint. For example, Trend Micro Apex One Intrusion Prevention initiates actions identified in the Intrusion Prevention rules (*e.g.*, controlling network traffic to the endpoint) based on the compliance state which are carried out by the endpoint processor.

Intrusion Prevention

The **Intrusion Prevention** module protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network.

Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.

Intrusion Prevention can be used for the following functions:

- **Virtual patching:** Intrusion Prevention rules can drop traffic designed to leverage unpatched vulnerabilities in certain applications or the operating system itself. This protects the host while awaiting the application of the relevant patches.
- **Protocol hygiene:** this detects and blocks traffic with malicious instructions
- **Application control:** this control can be used to block traffic associated with specific applications like Skype or file-sharing utilities [21]

75.   Defendant has and continues to indirectly infringe one or more claims of the '038 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '038 Accused Products (*e.g.*, products incorporating the Vulnerability Protection feature).

76.   Defendant has and continues to indirectly infringe one or more claims of the '038 Patent including, but not limited to, claim 23, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to

---

[21] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

26

sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '038 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '038 Patent by providing these products to end-users for use in an infringing manner.

77.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '038 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[22] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Vulnerability Protection feature.[23]

78.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '038 Patent in an amount to be proved at trial.

79.   Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '038 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

<div align="center">

COUNT V
(Infringement of the '948 Patent)

</div>

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

---

[22] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[23] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

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

82.   Defendant has and continues to directly infringe the '948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '948 Patent including, but not limited to, claim 1.[24] Such products incorporate the Extended Detection and Response feature and include at least the Trend Micro Apex One with XDR and Trend Micro Vision One with XDR (the "'948 Accused Products") which practice a method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

---

[24] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJ O6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

83. Every '948 Accused Product practices a method of providing real-time operational integrity of an application on a native computing environment. For example, the Trend Micro Apex One with XDR incorporates application integrity monitoring and behavior analysis.

---

84.   Every '948 Accused Product practices monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application. For example, Trend Micro Apex One with XDR monitors for scripts, injection, ransomware, malware, exploits, and browser attacks and follows defined application policies.

---

26 https://www.youtube.com/watch?v=IJARP_4vcHM
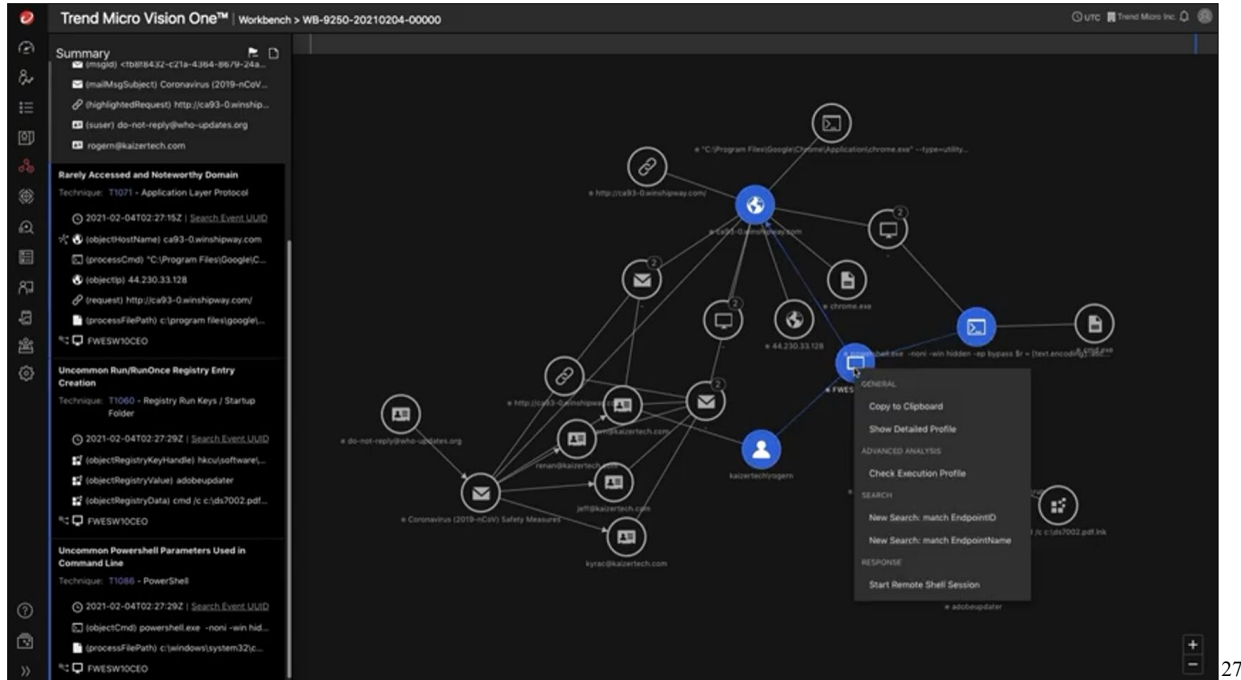
85.   Every '948 Accused Product practices generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor. For example, Trend Micro Apex One security agents generate behavior based events for determining the real time operational integrity of the application executing on the native computer environment.

---

[27] *Id.*

86.   Every '948 Accused Product practices correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events. For example, the MITRE ATT&CK framework correlates threat classifications based on the temporal sequence of detected behavioral events.

---

28 *Id*.
29 *Id*.

87.   Every '948 Accused Product practices displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application. For example, Trend Micro Apex One with XDR includes several display options for showing real-time status indications for the operational integrity of the application.
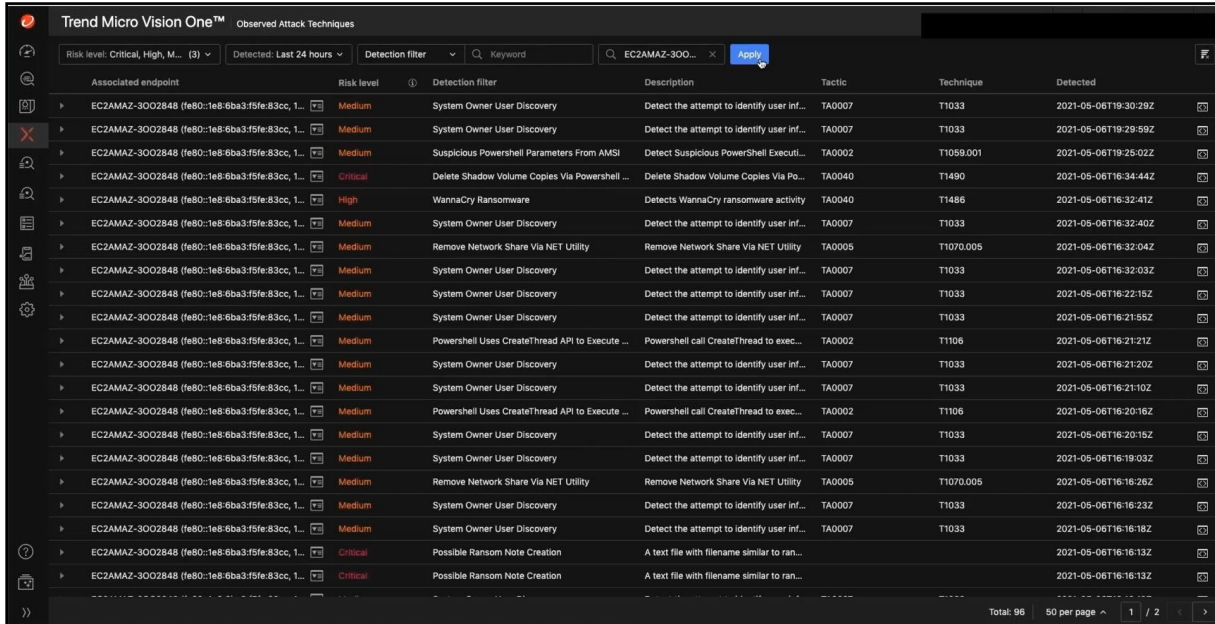

³⁰

33
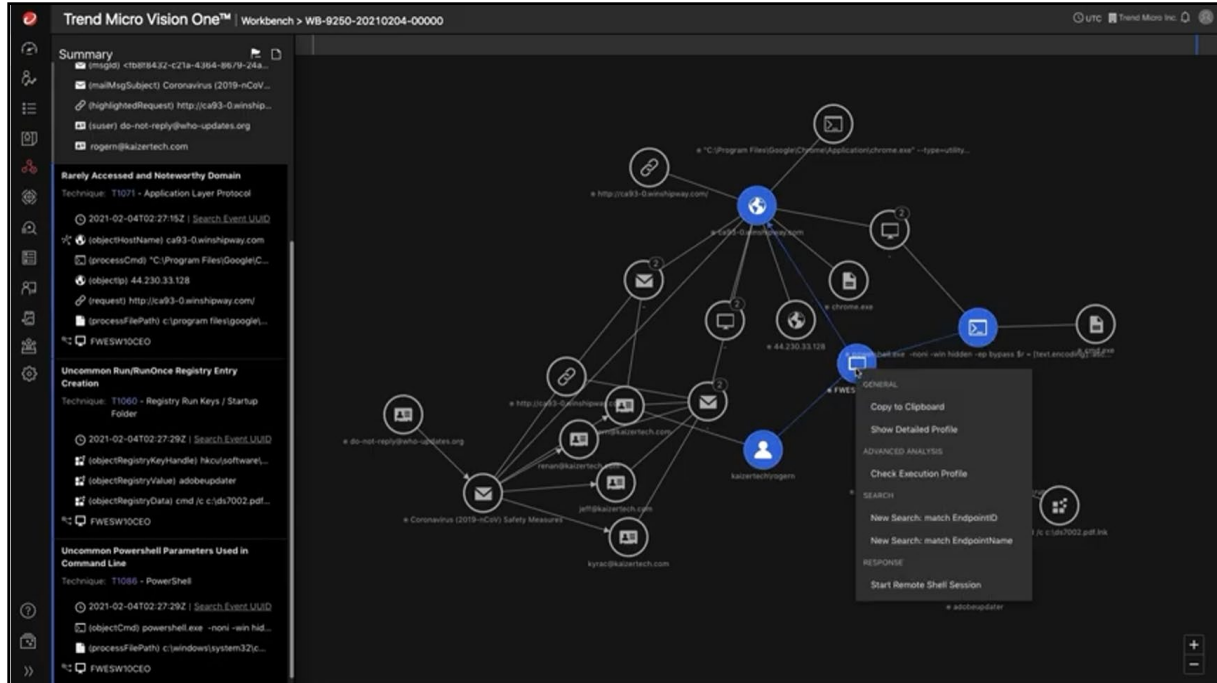
88.   Defendant has and continues to indirectly infringe one or more claims of the '948

Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries,

customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents,

---

[31] *Id.*

[32] *Id.*

by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '948 Accused Products (*e.g.*, products incorporating the Extended Detection and Response feature).

89.   Defendant has and continues to indirectly infringe one or more claims of the '948 Patent including, but not limited to, claim 1, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '948 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '948 Patent by providing these products to end-users for use in an infringing manner.

90.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '948 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[33] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Extended Detection and Response feature.[34]

91.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '948 Patent in an amount to be proved at trial. Upon information and

---

[33] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[34] https://docs.trendmicro.com/en-us/enterprise/trend-micro-vision-one/xdr-part.aspx

belief, Taasera and prior assignees of the '948 Patent, prior assignees' affiliates, and prior assignees' sublicensees to the '948 Patent, complied with the marking statute 35 U.S.C. § 287. Accordingly, Taasera is entitled to pre-suit damages.

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

COUNT VI
(Infringement of the '616 Patent)

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

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

95.   Defendant has and continues to directly infringe the '616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '616 Patent including, but not limited to, claim 1.[35] Such products incorporate the Extended Detection and Response feature and include at least the Trend Micro Apex One and Trend Micro Vision One (the "'616 Accused Products") which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored

---

[35] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJO6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

96.   Every '616 Accused Product practices a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. For example, Trend Micro Apex One with XDR comprises the Apex One Server and security agents to provide operational integrity of a system.

TREND MICRO APEX ONE™

Endpoint security redefined

A blend of advanced threat protection techniques, combined with detection and response, delivered through a single-agent architecture to eliminate security gaps across any user activity and any endpoint.

- **Automated:** Stop attackers sooner with the most effective protection against zero-day threats. It uses a blend of next-gen anti-malware techniques and the industry's most timely virtual patching to quickly stop attackers.
- **Insightful:** Get exceptional visibility and control across your environment. Integrated extended detection and response (XDR) capabilities for cross-layer detection, investigation, and threat hunting.
- **Connected:** Quickly respond to attacks with real-time and local threat intelligence updates and a broad API set for integration with third-party security tools. Flexible deployment options fit perfectly with your environment.

YOU CAN HAVE IT ALL

- **Malware and ransomware protection:** Defends endpoints against malware, ransomware, malicious scripts, and more. With advanced protection capabilities that adapts to protect against unknown and stealthy new threats.
- **Extensive detection and response capabilities:** XDR extends detection and response capabilities with cross-layer detection, threat hunting and investigation across email, endpoints, servers, cloud workloads, and network together in one console
- **The industry's most timely virtual patching:** Vulnerability protection applies virtual patches for protection before a patch is available or deployable.
- **Ransomware rollback:** Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback restores any files encrypted before the detection.
- **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.
- **Flexible deployment:** Trend Micro Apex One™ as a Service saves time, money, and is always up to date with the latest protection. On-premises and hybrid deployments are also fully supported.

Protection Points
- Physical endpoints
- Microsoft® Windows® PCs and servers
- Mac computers
- Point of sale (POS) and ATM endpoints

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 how we stack up

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html

## PROTECTION AND EFFICIENCY: THE RIGHT TECHNIQUE AT THE RIGHT TIME
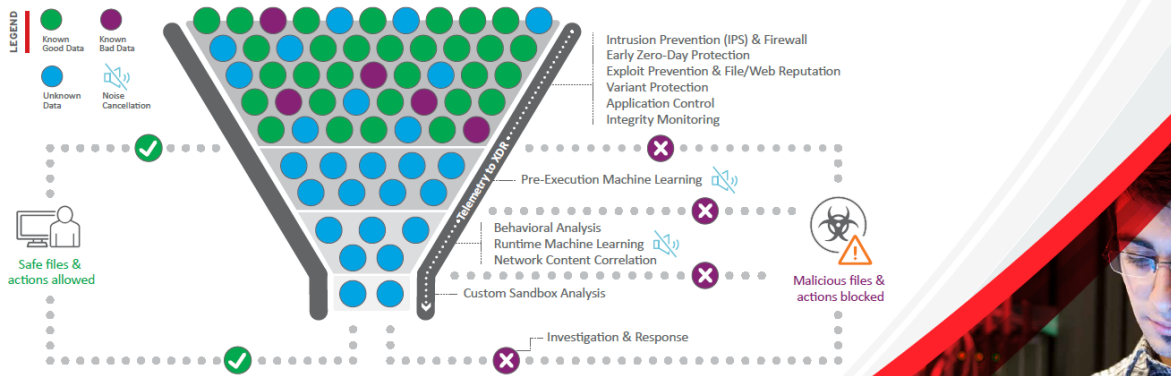
97.   Every '616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored

---

[36] https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ds-apex-one.pdf

device and applications executing on the monitored device at runtime. For example, the security

agents send events, context, and status information.

98.   Every '616 Accused Product practices receiving, at the trust orchestration server,

the dynamic context including the endpoint events of the monitored device and the applications

executing on the monitored device at runtime. For example, Trend Micro Apex One receives

dynamic context including endpoint events and the applications executing on the monitored device

in runtime.
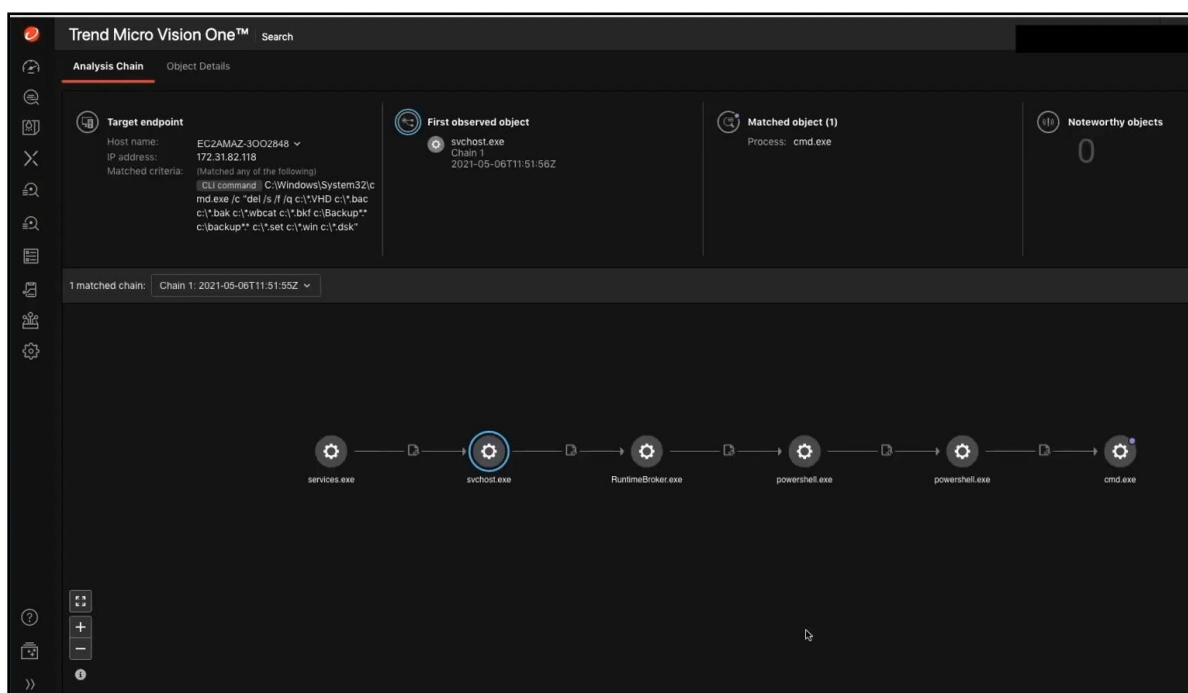
99.   Every '616 Accused Product practices analyzing, by the trust orchestration server,

the received endpoint events. For example, Trend Micro Apex One with XDR receives endpoint

events (*i.e.*, data related to potential security threats).

---

100.   Every '616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, Trend Micro Apex One with XDR receives MITRE ATT&CK data and other third-party network endpoint assessments.

---
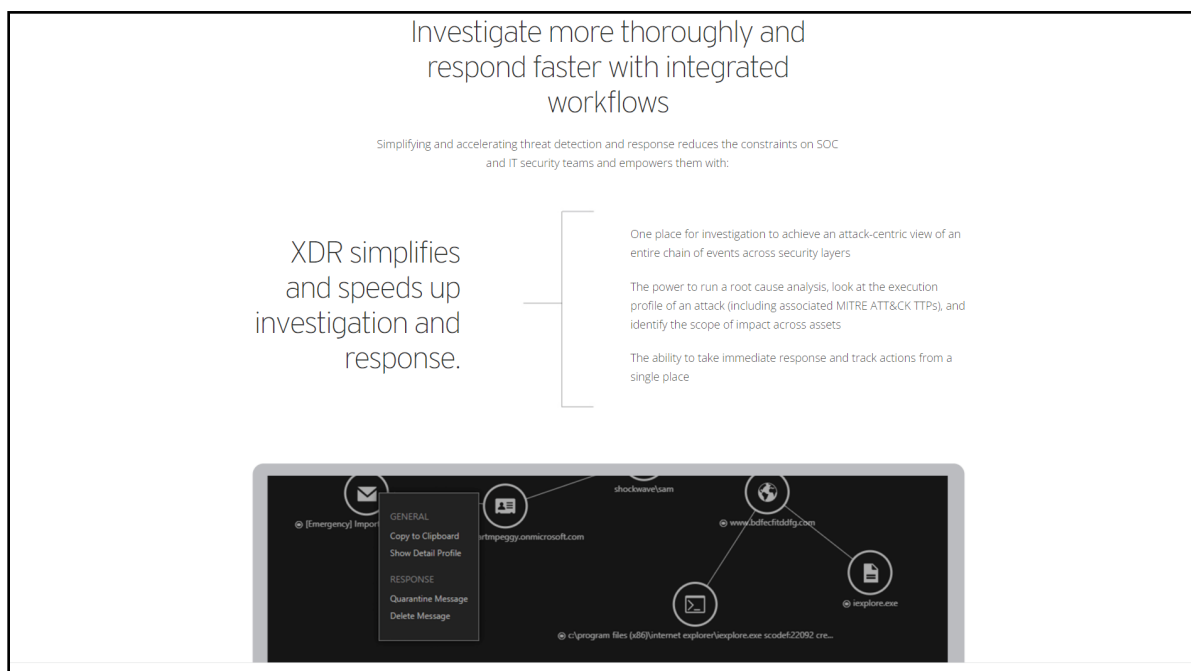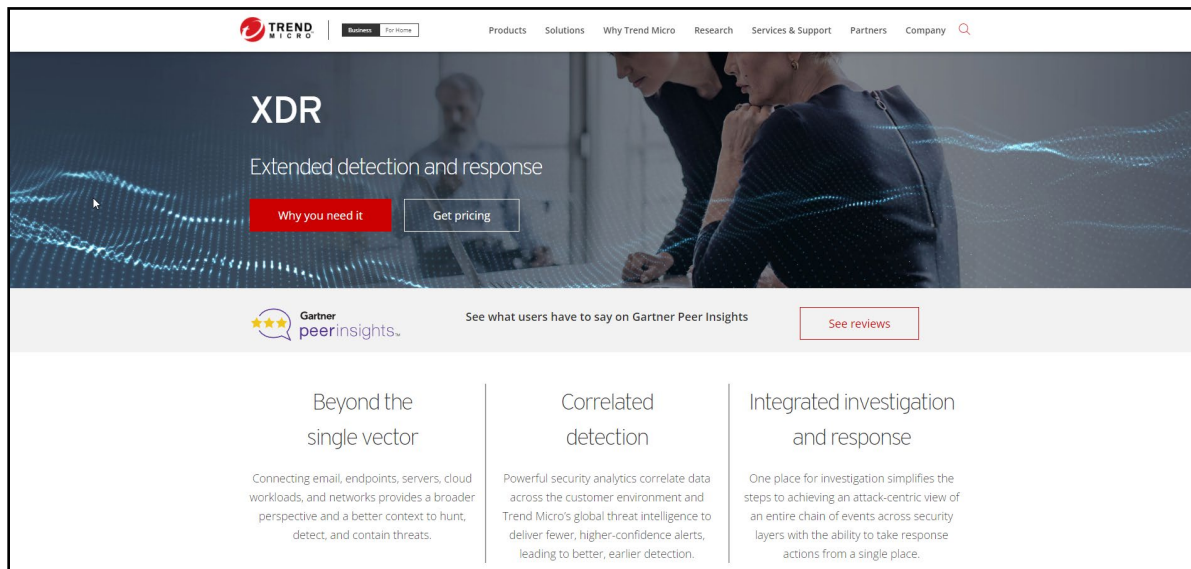
[38] https://www.trendmicro.com/en_us/business/products/detection-response/xdr.html
[39] *Id.*

YOU CAN HAVE IT ALL

- **Advanced malware and ransomware protection:** Defends endpoints—on or off the corporate network—against malware, trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like cryptomalware and fileless malware.

- **Detection and response capabilities:** Advanced detection and response capabilities are included with Apex One. An optional investigation tool; Trend Micro Endpoint Sensor, and our MDR service are available as add-ons.

- **The industry's most timely virtual patching**: Trend Micro Apex One™ Vulnerability Protection™ virtually patches known and unknown vulnerabilities, giving you instant protection before a patch is available or deployable.

- **Connected threat defense**: Apex One integrates with other security products locally—on your network and also via Trend Micro's global cloud threat intelligence—to deliver network sandbox rapid response updates to endpoints when a new threat is detected. This enables faster time-to-protection and reduces the spread of malware.

- **Centralized visibility and control**: When deployed with Trend Micro Apex Central™, multiple capabilities can be managed through a single console to provide central visibility and control across all functions.

- **Mobile security integration**: Integrate Trend Micro™ Mobile Security™ and Apex One by using Apex Central to centralize security management and policy deployment across all endpoints. Mobile Security includes mobile device threat protection, mobile app management, mobile device management (MDM), and data protection.

- **Available on-premises or as a service**: Apex One can be deployed on-site in your network or is available as a service, with full product parity between the two deployment options.

KEY BUSINESS ISSUES

* Too many malware and ransomware threats getting through, advanced threats evade pre-execution detection

* Need one solution to protect against all known and unknown threats on PC, endpoints, and Macs

* Difficulty correlating and prioritizing all alerts coming through

* Users require more automation and insights when dealing with potential threats

* Endpoint security solutions that don't talk to each other, lengthens time to protection and increase the management burden

* Risks of users working remotely, and sharing information in new ways via the cloud, etc.

* Patching endpoints quickly and thoroughly is difficult, leading to vulnerabilities

Threat Detection Capabilities

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- File reputation
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- DLP
- Device control
- Good file check
- Sandbox and breach detection integration
- Detection and response
- Endpoint encryption (requires separate agent)
- Vulnerability protection

See how we stack up

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html [40]

---

[40] https://www.trenddefense.com/datasheets/sb-apex-one.pdf

101.   Every '616 Accused Product practices generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments. For example, Trend Micro Apex One with XDR generates vulnerability data and assessed severity scores based at least in part on analyzing the third-party network endpoint assessments (*e.g.*, MITRE ATT&CK tactics and techniques).

---

[41] https://www.youtube.com/watch?v=IJARP_4vcHM

YOU CAN HAVE IT ALL

- **Advanced malware and ransomware protection:** Defends endpoints—on or off the corporate network—against malware, trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like cryptomalware and fileless malware.

- **Detection and response capabilities:** Advanced detection and response capabilities are included with Apex One. An optional investigation tool; Trend Micro Endpoint Sensor, and our MDR service are available as add-ons.

- **The industry's most timely virtual patching:** Trend Micro Apex One™ Vulnerability Protection™ virtually patches known and unknown vulnerabilities, giving you instant protection before a patch is available or deployable.

- **Connected threat defense:** Apex One integrates with other security products locally—on your network and also via Trend Micro's global cloud threat intelligence—to deliver network sandbox rapid response updates to endpoints when a new threat is detected. This enables faster time-to-protection and reduces the spread of malware.

- **Centralized visibility and control:** When deployed with Trend Micro Apex Central™, multiple capabilities can be managed through a single console to provide central visibility and control across all functions.

- **Mobile security integration:** Integrate Trend Micro™ Mobile Security™ and Apex One by using Apex Central to centralize security management and policy deployment across all endpoints. Mobile Security includes mobile device threat protection, mobile app management, mobile device management (MDM), and data protection.

- **Available on-premises or as a service:** Apex One can be deployed on-site in your network or is available as a service, with full product parity between the two deployment options.

KEY BUSINESS ISSUES

* Too many malware and ransomware threats getting through, advanced threats evade pre-execution detection

* Need one solution to protect against all known and unknown threats on PC, endpoints, and Macs

* Difficulty correlating and prioritizing all alerts coming through

* Users require more automation and insights when dealing with potential threats

* Endpoint security solutions that don't talk to each other, lengthens time to protection and increase the management burden

* Risks of users working remotely, and sharing information in new ways via the cloud, etc.

* Patching endpoints quickly and thoroughly is difficult, leading to vulnerabilities

Threat Detection Capabilities

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- File reputation
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- DLP
- Device control
- Good file check
- Sandbox and breach detection integration
- Detection and response
- Endpoint encryption (requires separate agent)
- Vulnerability protection

See how we stack up

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html [43]

102.   Every '616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, Trend Micro Apex One with XDR correlates the received endpoint events and the generated temporal events (*e.g.*, vulnerability data and assessed severity scores).

103.   Every '616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, Trend Micro Apex One with XDR generates an integrity profile for the system in displaying detected MITRE ATT&CK tactics and techniques.

---

[43] https://www.trenddefense.com/datasheets/sb-apex-one.pdf

44

45

104.   Defendant has and continues to indirectly infringe one or more claims of the '616

Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries,

---

[44] https://www.youtube.com/watch?v=odGDYzQbe80&t=1s
[45] *Id*.

customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '616 Accused Products (*e.g.*, products incorporating the Extended Detection and Response feature).

105.   Defendant has and continues to indirectly infringe one or more claims of the '616 Patent including, but not limited to, claim 1, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '616 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '616 Patent by providing these products to end-users for use in an infringing manner.

106.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end- users, infringe the '616 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[46] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Extended Detection and Response feature.[47]

---

[46] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[47] https://docs.trendmicro.com/en-us/enterprise/trend-micro-vision-one/xdr-part.aspx

107.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '616 Patent in an amount to be proved at trial. Upon information and belief, Taasera and prior assignees of the '616 Patent, prior assignees' affiliates, and prior assignees' sublicensees to the '616 Patent, complied with the marking statute 35 U.S.C. § 287. Accordingly, Taasera is entitled to pre-suit damages.

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

<div align="center">

COUNT VII
(Infringement of the '997 Patent)

</div>

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

110.   Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '997 Patent.

111.   Defendant has and continues to directly infringe the '997 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '997 Patent including, but not limited to, claim 21.[48] Such products incorporate the Vulnerability Protection feature and include at least the Trend Micro Apex One and Trend Micro Vision One (the "'997 Accused Products") which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of

---

[48] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJO6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

policies; maintaining the plurality of policies in a data store on the computing system; identifying,

from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;

configuring one or more software services provided by an operating system on the endpoint to

monitor the plurality of operating conditions; receiving, across a network, at the computing system,

status information about the plurality of operating conditions on the endpoint gathered by the one

or more software services; determining, by the computing system, a compliance state of the

endpoint based on the status information and a plurality of compliance policies in the data store;

and initiating, remotely by the computing system, based on the compliance state, an action

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

the endpoint, such that the computing system remotely ensures endpoint compliance with the

plurality of compliance policies stored in the data store of the computing system.

112.   Every '997 Accused Product practices a method for controlling the operation of an

endpoint. For example, the Trend Micro Apex One performs Vulnerability Protection on

endpoints.

VULNERABILITY PROTECTION

Backed by world-class vulnerability research, Apex One security's virtual patching delivers the most-timely vulnerability protection in the industry across a variety of endpoints.

Stop zero-day threats immediately on your endpoints—on and off the network.

Trend Micro Vulnerability Protection, along with Trend Micro's portfolio of endpoint capabilities extend protection to critical platforms, including legacy operating systems.

Defends Against Advanced Threats

- Blocks known and unknown vulnerability exploits before patches are deployed.
- Protects end-of-support and legacy operating systems, for which patches may never be provided.
- Dynamically adjusts security configuration based on the location of an endpoint.
- Protects endpoints with minimal impact on network throughput, performance, or user productivity.
- Shields endpoints against unwanted network traffic with multiple protection layers.
- Protects systems that hold sensitive data, critical to regulatory and corporate policy compliance.

Removes Bad Data from Business-Critical Traffic

- Applies control filters to alert/block specific traffic such as instant messaging and media streaming.
- Uses deep packet inspection to identify content that may harm the application layer.
- Filters forbidden network traffic and ensures allowed traffic through stateful inspection.

Provides Earlier Protection

- Provides protection before patches are deployed and often before patches are available.
- Shields operating system and common applications from known and unknown attacks.
- Detects malicious traffic that hides by using supported protocols over non-standard ports.
- Blocks traffic likely to damage at-risk components using vulnerability-facing network inspection.
- Prevents networking backdoors from penetrating into the corporate network.
- Blocks all known exploits with intrusion prevention signatures.
- Defends custom and legacy applications using custom filters that block user-defined parameters.

Software

Protection Points

- Endpoints

Threat Protection

- Vulnerability exploits
- Denial of service attacks
- Illegitimate network traffic
- Web threats

Features and Benefits

- Eliminates risk exposure due to missing patches
- Extends the life of legacy and end-of-support (EOS) operating systems
- Reduces down-time for recovery with incremental protection against zero-day attacks
- Allows patching on your own terms and timelines
- Lowers potential legal exposure by improving data security compliance
- Enhances firewall protection for remote and mobile enterprise endpoints

[49]

113.   Every '997 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies and maintaining the plurality of policies in a data store on the computing system. For example, Trend Micro Apex One allows configuration of a plurality of policies (*e.g.*, Intrusion Prevention rules) at a system remote from the endpoint through a provided user interface which are stored in a data store.

---

[49] https://www.trenddefense.com/datasheets/sb-apex-one.pdf
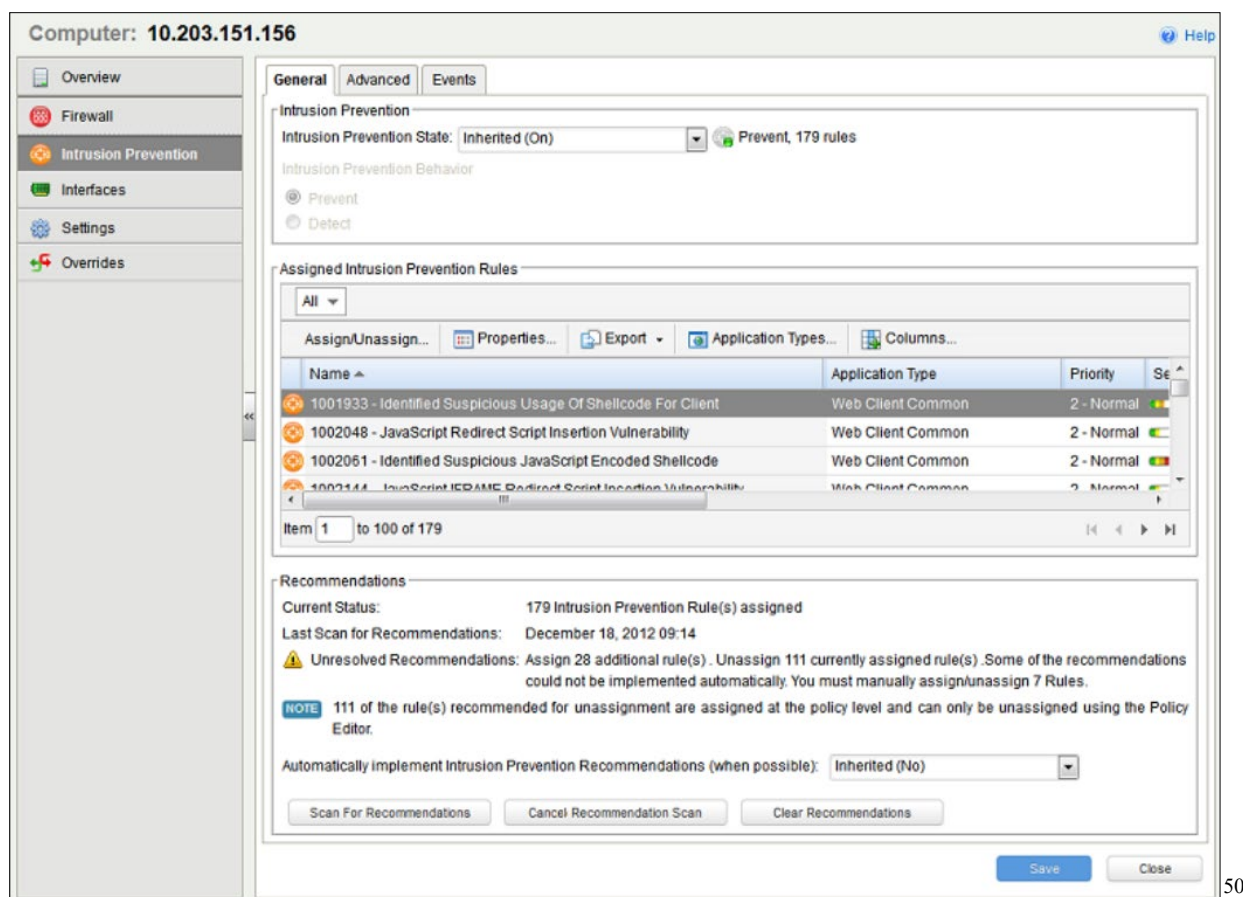
114.   Every '997 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Trend Micro Apex One (Vulnerability Protection) identifies, from the plurality of polices (*e.g.*, Intrusion Prevention rules), vulnerability attack indicators on the endpoint to monitor.

115.   Every '997 Accused Product practices configuring one or more software services on the endpoint to monitor the plurality of operating conditions. For example, Trend Micro Apex One configures at least the Vulnerability Protection module to monitor the plurality of operating conditions (*e.g.*, vulnerability attack indicators on the endpoint).

---

[50] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

116.   Every '997 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services. For example, Apex One receives information regarding whether vulnerability attacks have been detected, gathered by the one or more software services (*e.g.*, Vulnerability Protection module).
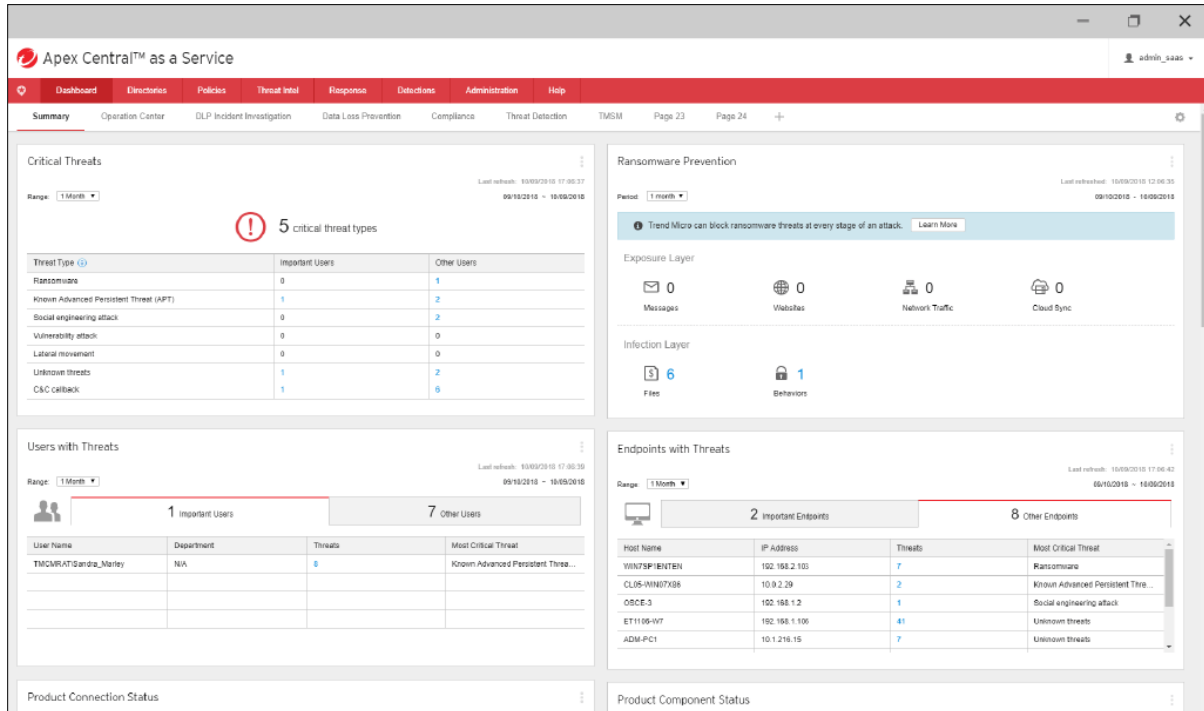
117.   Every '997 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, Trend Micro Apex One determines a compliance state of the endpoint based on the vulnerability attack information and the Intrusion Prevention rules.

118.   Every '997 Accused Product practices initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store,

---

51   https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ultimate-protection-against-vulnerabilities.png

wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. For example, Trend Micro Apex One Intrusion Prevention remotely initiates actions identified in the Intrusion Prevention rules (*e.g.*, controlling network traffic to the endpoint) based on the compliance state that are carried out by the endpoint processor.

Intrusion Prevention

The **Intrusion Prevention** module protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network.

Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.

Intrusion Prevention can be used for the following functions:

- **Virtual patching:** Intrusion Prevention rules can drop traffic designed to leverage unpatched vulnerabilities in certain applications or the operating system itself. This protects the host while awaiting the application of the relevant patches.
- **Protocol hygiene:** this detects and blocks traffic with malicious instructions
- **Application control:** this control can be used to block traffic associated with specific applications like Skype or file-sharing utilities [52]

119.   Defendant has and continues to indirectly infringe one or more claims of the '997 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '997 Accused Products (*e.g.*, products incorporating the Vulnerability Protection feature).

120.   Defendant has and continues to indirectly infringe one or more claims of the '997 Patent including, but not limited to, claim 21, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example,

---

[52] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

Defendant, with knowledge that these products, or the use thereof, infringe the '997 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '997 Patent by providing these products to end-users for use in an infringing manner.

121.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '997 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[53] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Vulnerability Protection feature.[54]

122.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '997 Patent in an amount to be proved at trial.

123.   Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '997 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT VIII
(Infringement of the '918 Patent)

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

125.   Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '918 Patent.

---

[53] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[54] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

126.   Defendant has and continues to directly infringe the '918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '918 Patent including, but not limited to, claim 17.[55] Such products incorporate the Vulnerability Protection module and include at least the Trend Micro Apex One and Trend Micro Vision One (the "'918 Accused Products") which comprise a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determine, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.

127.   Every '918 Accused Product comprises a system for controlling the operation of an endpoint. For example, the Trend Micro Trend Micro Apex One performs Vulnerability Protection on endpoints.

---

[55] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJO6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

VULNERABILITY PROTECTION

Backed by world-class vulnerability research, Apex One security's virtual patching delivers the most-timely vulnerability protection in the industry across a variety of endpoints.

Stop zero-day threats immediately on your endpoints—on and off the network.

Trend Micro Vulnerability Protection, along with Trend Micro's portfolio of endpoint capabilities extend protection to critical platforms, including legacy operating systems.

Defends Against Advanced Threats

- Blocks known and unknown vulnerability exploits before patches are deployed.
- Protects end-of-support and legacy operating systems, for which patches may never be provided.
- Dynamically adjusts security configuration based on the location of an endpoint.
- Protects endpoints with minimal impact on network throughput, performance, or user productivity.
- Shields endpoints against unwanted network traffic with multiple protection layers.
- Protects systems that hold sensitive data, critical to regulatory and corporate policy compliance.

Removes Bad Data from Business-Critical Traffic

- Applies control filters to alert/block specific traffic such as instant messaging and media streaming.
- Uses deep packet inspection to identify content that may harm the application layer.
- Filters forbidden network traffic and ensures allowed traffic through stateful inspection.

Provides Earlier Protection

- Provides protection before patches are deployed and often before patches are available.
- Shields operating system and common applications from known and unknown attacks.
- Detects malicious traffic that hides by using supported protocols over non-standard ports.
- Blocks traffic likely to damage at-risk components using vulnerability-facing network inspection.
- Prevents networking backdoors from penetrating into the corporate network.
- Blocks all known exploits with intrusion prevention signatures.
- Defends custom and legacy applications using custom filters that block user-defined parameters.

Software

Protection Points

- Endpoints

Threat Protection

- Vulnerability exploits
- Denial of service attacks
- Illegitimate network traffic
- Web threats

Features and Benefits

- Eliminates risk exposure due to missing patches
- Extends the life of legacy and end-of-support (EOS) operating systems
- Reduces down-time for recovery with incremental protection against zero-day attacks
- Allows patching on your own terms and timelines
- Lowers potential legal exposure by improving data security compliance
- Enhances firewall protection for remote and mobile enterprise endpoints

[56]

128.   Every '918 Accused Product comprises a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, Trend Micro Apex One comprises a user interface that allows configuration of a plurality of policies (*e.g.*, Intrusion Prevention rules) at a system remote from the endpoint which are stored in the Apex One data store.

---

[56] https://www.trenddefense.com/datasheets/sb-apex-one.pdf
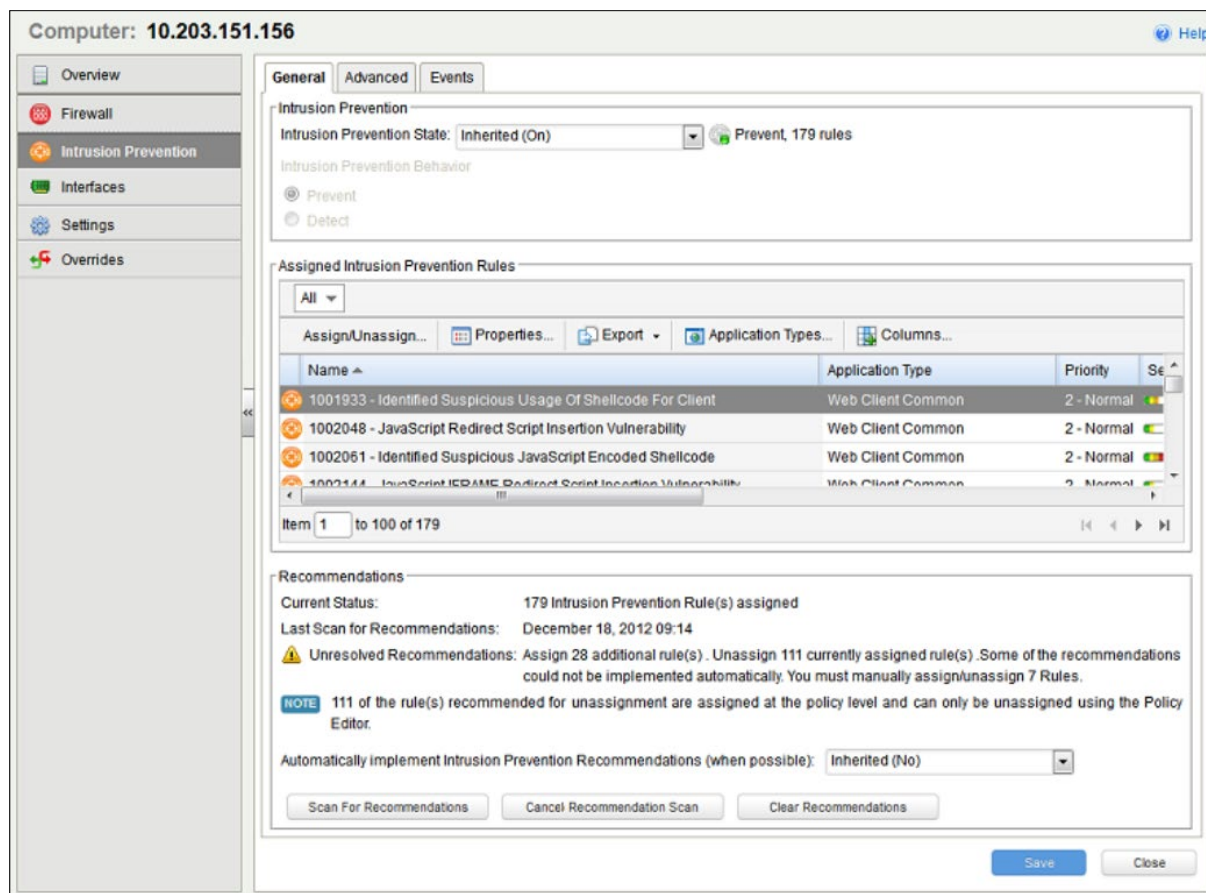
129.   Every '918 Accused Product comprises one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. For example, at least the Trend Micro Apex One Vulnerability Protection module is configured to evaluate the plurality of operating conditions (*e.g.*, vulnerability attack indicators on the endpoint) identified in the plurality of policies (*e.g.*, Intrusion Prevention rules).

130.   Every '918 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identified a user of the

---

[57] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

endpoint. For example, Apex One receives information regarding whether vulnerability attacks have been detected, gathered by the one or more software services (*e.g.*, Vulnerability Protection module), and identification of a user of the endpoint.
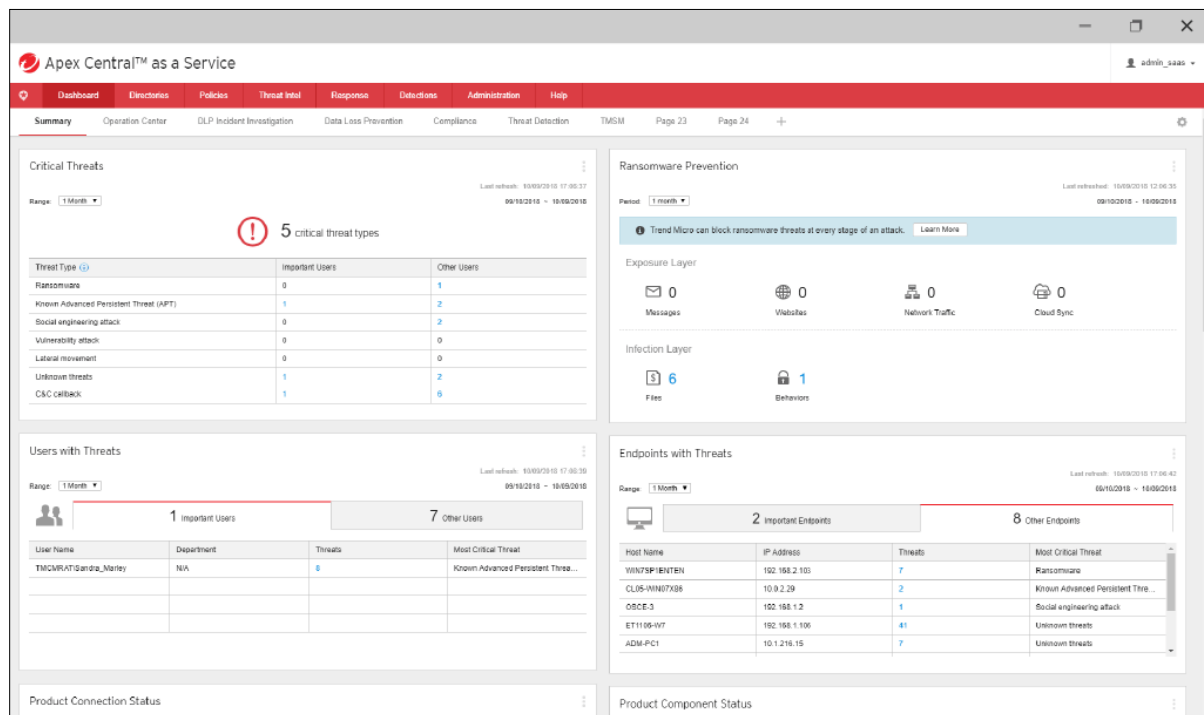
131.   Every '918 Accused Product determines, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store. For example, Trend Micro Apex One determines a compliance state of the endpoint based on the user information, vulnerability attack information, and the Intrusion Prevention rules.

132.   Every '918 Accused Product authorizes access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state. For example, Trend Micro Apex One Intrusion Prevention

---

[58] https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ultimate-protection-against-vulnerabilities.png

authorizes access by the endpoint to a computing resource on the network (*e.g.*, controls network traffic at the endpoint), authorization being determined by Trend Micro Apex One in response to the compliance state.

Intrusion Prevention

The **Intrusion Prevention** module protects computers from being exploited by attacks against known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed. It identifies malicious software accessing the network and increases visibility into, or control over, applications accessing the network.

Intrusion Prevention prevents attacks by detecting malicious instructions in network traffic and dropping relevant packets.

Intrusion Prevention can be used for the following functions:

- **Virtual patching:** Intrusion Prevention rules can drop traffic designed to leverage unpatched vulnerabilities in certain applications or the operating system itself. This protects the host while awaiting the application of the relevant patches.
- **Protocol hygiene:** this detects and blocks traffic with malicious instructions
- **Application control:** this control can be used to block traffic associated with specific applications like Skype or file-sharing utilities [59]

133.   Defendant has and continues to indirectly infringe one or more claims of the '918 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '918 Accused Products (*e.g.*, products incorporating the Vulnerability Protection feature).

134.   Defendant has and continues to indirectly infringe one or more claims of the '918 Patent including, but not limited to, claim 17, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '918 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to

---

[59] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

knowingly and intentionally induce, direct infringement of the '918 Patent by providing these products to end-users for use in an infringing manner.

135.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '918 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[60] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an infringing manner, including specifically how to use the Vulnerability Protection module.[61]

136.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '918 Patent in an amount to be proved at trial.

137.   Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '918 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT IX
(Infringement of the '517 Patent)

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

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

140.   Defendant has and continues to directly infringe the '517 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making,

---

[60] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/
[61] https://docs.trendmicro.com/all/ent/vp/v2.0/en-us/sp2/Vulnerability_Protection_2_SP2_Admin_Guide_EN.pdf

using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '517 Patent including, but not limited to, claim 1.[62] Such products incorporate the Correlated Rule and/or Targeted Attack Campaign features and include at least the Trend Micro Deep Discovery Inspector, Trend Micro Apex Central, Trend Micro Apex One, and Trend Micro Vision One (the "'517 Accused Products") which practice a method for assessing runtime risk for an application program that executes on a device, comprising: storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence; storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules; identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application; and identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action.

141.   Every '517 Accused Product practices a method for assessing runtime risk for an application program that executes on a device. For example, the Trend Micro Trend Micro Vison One with XDR assesses runtime risk for applications that execute on endpoints.

---

[62] Trend Micro distributes its Accused Products to customers and end-users in Texas and this District through its website at https://resources.trendmicro.com/vision-one-trial.html?_ga=2.203102545.1797687026.1660610776-1305895883.1660610776&_gac=1.27718350.1660662015.Cj0KCQjwgO2XBhCaARIsANrW2X0FZxAma7nWuafJO6-_scbCKpduoB9vFi_m5v0_IzEE3ZhQIcT8VvkaAsujEALw_wcB

TREND MICRO VISION ONE

- Offers a threat defense platform featuring XDR and risk visibility.
- Simplifies and accelerates threat detection and response by connecting email, endpoints, servers, cloud workloads, and network.
- Provides automatic indicator of compromise (IoC) sweeping with included Trend Micro threat intelligence feed.
- Hunt, detect, and contain threats.
- Quickly see all aspects of an attack and respond from a single place.
- Optional Trend Micro™ Managed XDR service for threat hunting and investigation by Trend Micro threat experts.

[63]

142.   Every '517 Accused Product practices storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence. For example, Trend Micro Deep Discovery Inspector stores a plurality of Correlation Rules and Targeted Attack Campaigns where each rule identifies an action sequence.

143.   Every '517 Accused Product practices storing, in a policy database, a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules. For example, at least the Trend Micro Apex Central stores a plurality of assessment polices which comprise at least one rule of the plurality or rules.

Apex Central

Trend Micro Apex Central is a software management solution that simplifies the administration of your corporate antivirus and content security policies. Apex Central provides the following features:

- Centrally manages the following:
    - Suspicious objects, user-defined lists, and exception lists
    - Multiple Deep Discovery Inspector system statuses
    - Antivirus and content security programs, regardless of the program's physical location or platform

[64]

- Consolidates multiple Deep Discovery Inspector logs [65]

---

[63] https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/user-protection/sps/endpoint-security-apex-one/ds-apex-one.pdf
[64] https://docs.trendmicro.com/all/ent/ddi/v5.7/en-us/ddi_5.7_ag.pdf
[65] *Id.*

144.   Every '517 Accused Product practices identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application; and identifying, by a runtime monitor including a processing device, a behavior score for the application program that executes on the device based on the identified runtime risk wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action. For example, Trend Micro Vision One uses assessment policies to identify a runtime risk for an application program that executes on an endpoint. The identified runtime risk indicates a risk or threat of the identified action sequence of the application (*e.g.*, correlated rule or targeted attack campaign). Trend Micro Vision One identifies a behavior score for the application program based on the identified runtime risk. The action sequence is a sequence of at least two performed actions and each action is at least one of a user action, an application action, and a system action.

145.   Defendant has and continues to indirectly infringe one or more claims of the '517 Patent by knowingly and intentionally inducing others, including Trend Micro subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as '517 Accused Products (*e.g.*, products that incorporate the Correlated Rule and/or Targeted Attack Campaign features).

146.   Defendant has and continues to indirectly infringe one or more claims of the '517 Patent including, but not limited to, claim 1, by knowingly and intentionally inducing others to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States the infringing Accused Products. For example, Defendant, with knowledge that these products, or the use thereof, infringe the '517 Patent at least as of the date of the original Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '517 Patent by providing these products to end-users for use in an infringing manner.

147.   Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '517 Patent, but while remaining willfully blind to the infringement. Defendant provides detailed information about how to use the Accused Products in an infringing manner in the Trend Micro Online Help Center and/or in the Trend Micro Knowledge Base at the Trend Micro website.[67] Defendant provides product manuals and documentation that instruct customers and end-users how to use the Accused Products in an

---

[67] https://docs.trendmicro.com/en-us/home.aspx; https://helpcenter.trendmicro.com/en-us/

infringing manner, including specifically how to use the Correlated Rule and/or Targeted Attack Campaign features.[68]

148.   Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '517 Patent in an amount to be proved at trial. Upon information and belief, Taasera and prior assignees of the '517 Patent, prior assignees' affiliates, and prior assignees' sublicensees to the '517 Patent, complied with the marking statute 35 U.S.C. § 287. Accordingly, Taasera is entitled to pre-suit damages.

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

DEMAND FOR JURY TRIAL

150.   Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

 WHEREFORE, Taasera Licensing prays for relief against Defendant as follows:

a.   Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b.   An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;

c.   An order awarding damages sufficient to compensate Taasera Licensing for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

---

[68] https://docs.trendmicro.com/all/ent/ddi/v5.8/en-us/ddi_5.8_olh/All-Detections---Det_002.html;
https://docs.trendmicro.com/all/ent/ddi/v5.7/en-us/ddi_5.7_ag.pdf

d.   Entry of judgment declaring that this case is exceptional and awarding Taasera

Licensing its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e.   Such other and further relief as the Court deems just and proper.

Dated: August 19, 2022   Respectfully submitted,

                                                  /s/ *Alfred R. Fabricant*
                                                 Alfred R. Fabricant
                                                 NY Bar No. 2219392
                                                 Email: ffabricant@fabricantllp.com
                                                 Peter Lambrianakos
                                                 NY Bar No. 2894392
                                                 Email: plambrianakos@fabricantllp.com
                                                 Vincent J. Rubino, III
                                                 NY Bar No. 4557435
                                                 Email: vrubino@fabricantllp.com
                                                 Joseph M. Mercadante
                                                 NY Bar No. 4784930
                                                 Email: jmercadante@fabricantllp.com
                                                 FABRICANT LLP
                                                 411 Theodore Fremd Avenue,
                                                 Suite 206 South
                                                 Rye, New York 10580
                                                 Telephone: (212) 257-5797
                                                 Facsimile: (212) 257-5796

                                                 Justin Kurt Truelove
                                                 Texas Bar No. 24013653
                                                 Email: kurt@truelovelawfirm.com
                                                 TRUELOVE LAW FIRM, PLLC
                                                 100 West Houston Street
                                                 Marshall, Texas 75670
                                                 Telephone: (903) 938-8321
                                                 Facsimile: (903) 215-851

                                                 ATTORNEYS FOR PLAINTIFF
                                                 TAASERA LICENSING LLC

65

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on August 19, 2022, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3).

/s/ Alfred R. Fabricant
Alfred R. Fabricant