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

	§	
TAASERA LICENSING LLC,	§	Case No.
	§	
Plaintiff,	§	**JURY TRIAL DEMANDED**
	§	
v.	§	
	§	
PALO ALTO NETWORKS, INC.,	§	
	§	
Defendant.	§	
	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Taasera Licensing LLC ("Taasera Licensing" or "Plaintiff") for its Complaint against Defendant Palo Alto Networks, Inc. ("Palo Alto" or "Defendant") 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, Palo Alto is a corporation organized under the laws of the State of Delaware, with a regular and established place of business in this Judicial District at 3901 Dallas Parkway, Plano, Texas 75093. Defendant's Registered Agent for service of process in Texas is Corporation Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. Upon information and belief, Palo Alto does business in Texas and in the Eastern District of Texas, directly or through intermediaries, such as its subsidiaries.

JURISDICTION

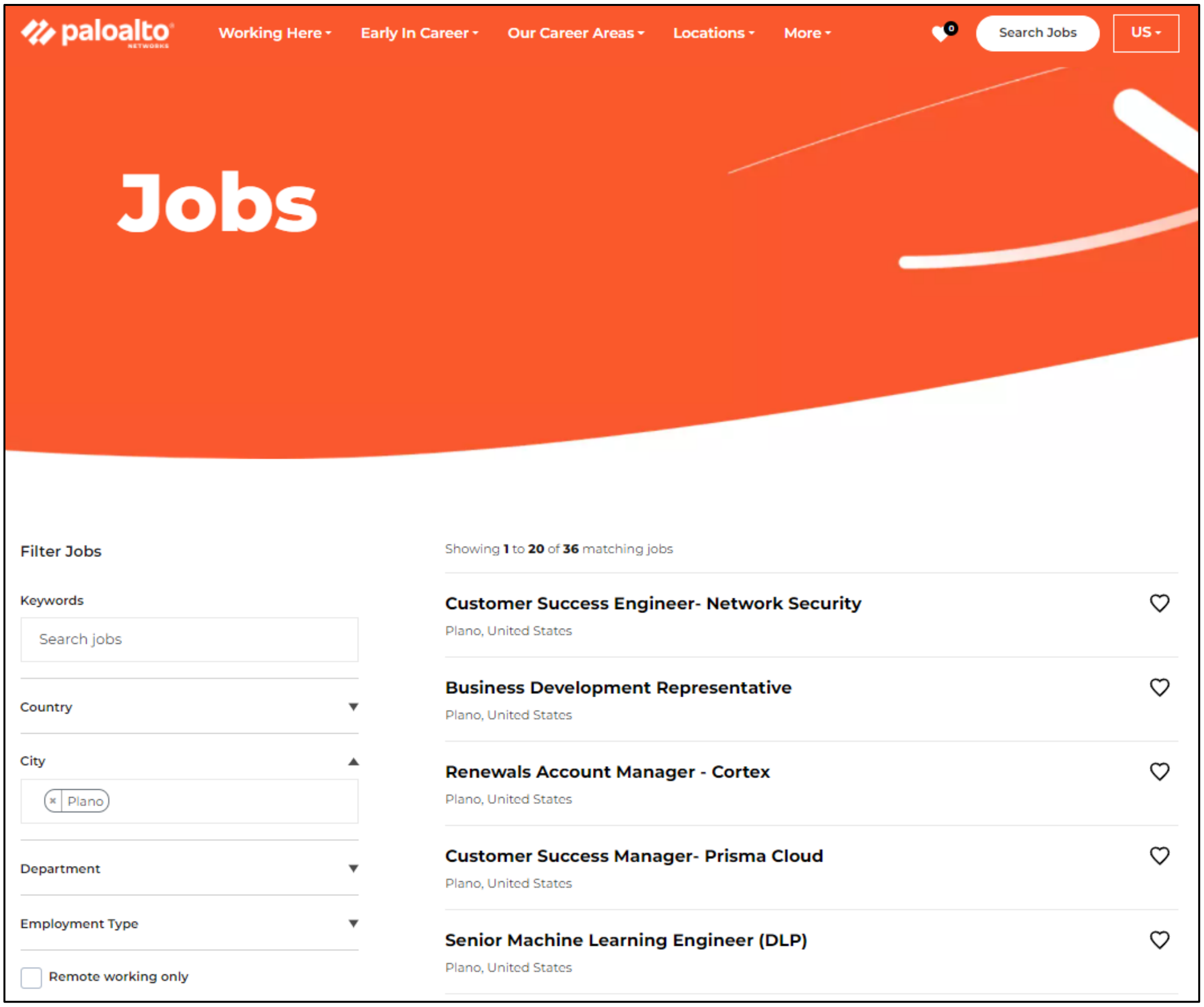
3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

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, Palo Alto conducts business at its regional office located at 3901 North Dallas Parkway, Plano, Texas 75093.

[1]

Defendant currently lists 36 open positions in Plano, Texas.

[1] https://www.google.com/maps/place/3901+Dallas+Pkwy,+Plano,+TX+75093/@33.0500257,-96.8305683,3a,75y,272.88h,88.92t/data=!3m6!1e1!3m4!1sppi-gdeX8kmdt4Sa6eDp4A!2e0!7i16384!8i8192!4m5!3m4!1s0x864c235e3c99c319:0x74e053e88e5db1f3!8m2!3d33.05023!4d-96.8314989



Jobs

Filter Jobs

Keywords

Search jobs

Country

City

Plano

Department

Employment Type

☐ Remote working only

Showing 1 to 20 of 36 matching jobs

Customer Success Engineer- Network Security
Plano, United States

Business Development Representative
Plano, United States

Renewals Account Manager - Cortex
Plano, United States

Customer Success Manager- Prisma Cloud
Plano, United States

Senior Machine Learning Engineer (DLP)
Plano, United States

[2]

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, Palo Alto directly or indirectly participated in the stream of commerce that results in products, including the accused products, being made, used,

[2] https://jobs.paloaltonetworks.com/en/jobs/?search=&location=Plano

offered for sale, and/or sold in the State of Texas and/or imported into the United States to the State of Texas.

6. Venue is also proper under 35 U.S.C. § 1400 (b) because Defendant has a regular and established place of business in this Judicial District, and Defendant has also committed acts of patent infringement in this Judicial District.

7. 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 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

8. 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 attached hereto as Exhibit A.

9. 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 attached hereto as Exhibit B.

10. On February 28, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,127,356 (the "'356 Patent") entitled "System, Method and Program Product for Detecting Unknown Computer Attacks." A true and correct copy of the '356 Patent is attached hereto as Exhibit C.

11. 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 attached hereto as Exhibit D.

12. 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 attached hereto as Exhibit E.

13. On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the "'038 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '038 Patent is attached hereto as Exhibit F.

14. 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 attached hereto as Exhibit G.

15. 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 attached hereto as Exhibit H.

16. 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 attached hereto as Exhibit I.

17. Taasera Licensing is the sole and exclusive owner of all right, title, and interest in the '796 Patent, the '137 Patent, the '356 Patent, the '441 Patent, the '517 Patent, the '038 Patent, the '948 Patent, the '616 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

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

19. Five of the Patents-in-Suit were invented by International Business Machines ("IBM"). IBM pioneered the field of network security. Every year, IBM spends billions of dollars on research and development to invent, market, and sell new technology, and IBM obtains patents on many of the novel inventions that come out of that work, including the Patents-in-Suit. The five patents invented by IBM are the result of the work from 8 different researchers, spanning over a decade.

20. 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.

21. 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 Mjkund Padmanabhan of IBM.

22. 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.

23. The ’356 Patent generally relates to technology that determines whether a packet is a new, exploit candidate. The technology described in the ’356 Patent was developed by Frederic G. Thiele and Michael A. Walter of IBM.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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 Palo Alto Cortex XDR, Pan-OS, and Next Generation Firewalls (NGFW).

31. 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.

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

COUNT I
(Infringement of the ’796 Patent)

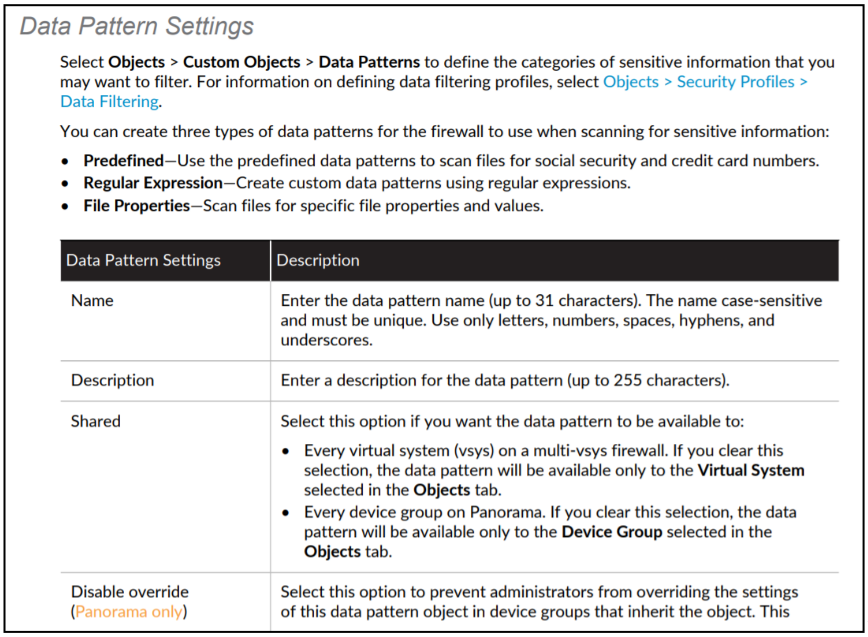
33. Paragraphs 1 through 32 are incorporated by reference as if fully set forth herein.

34. 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.

35. 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. Such products incorporate the Data Filtering based on Data Patterns feature and include at least all of the Palo Alto Next Generation Firewalls utilizing PAN-OS (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.

36. Every ’796 Accused Product practices automatically processing an input sequence of data symbols. For example, the Palo Alto PAN-OS performs Data Filtering based on Data Patterns.



Data Pattern Settings

Select **Objects** > **Custom Objects** > **Data Patterns** to define the categories of sensitive information that you may want to filter. For information on defining data filtering profiles, select Objects > Security Profiles > Data Filtering.

You can create three types of data patterns for the firewall to use when scanning for sensitive information:

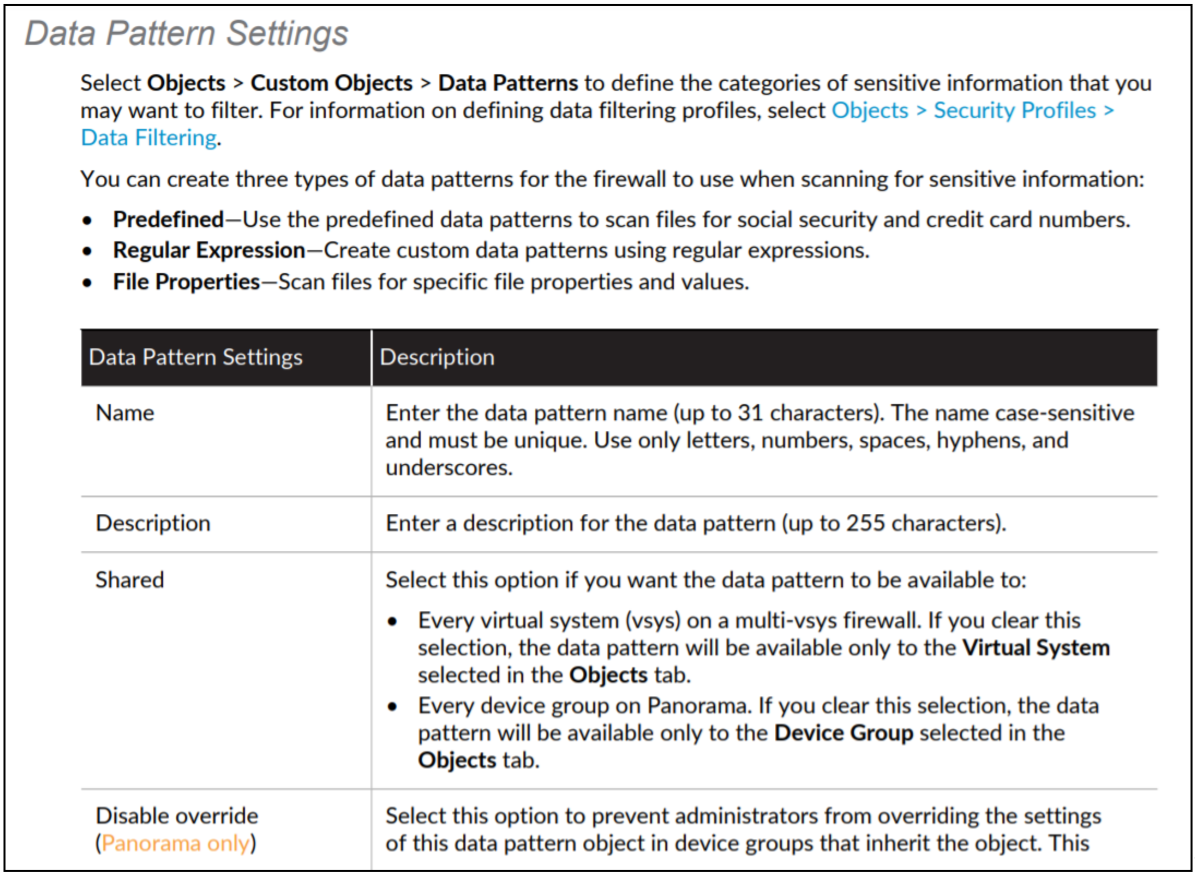
- **Predefined**—Use the predefined data patterns to scan files for social security and credit card numbers.
- **Regular Expression**—Create custom data patterns using regular expressions.
- **File Properties**—Scan files for specific file properties and values.

Data Pattern Settings	Description
Name	Enter the data pattern name (up to 31 characters). The name case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the data pattern (up to 255 characters).
Shared	Select this option if you want the data pattern to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the data pattern will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the data pattern will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this data pattern object in device groups that inherit the object. This

[3]

[3] https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/8-1/pan-os-web-interface-help/pan-os-web-interface-help.pdf

37. 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, Palo Alto PAN-OS enforces Data Filtering rules created using pre-defined and regular expressions.



Data Pattern Settings

Select **Objects** > **Custom Objects** > **Data Patterns** to define the categories of sensitive information that you may want to filter. For information on defining data filtering profiles, select Objects > Security Profiles > Data Filtering.

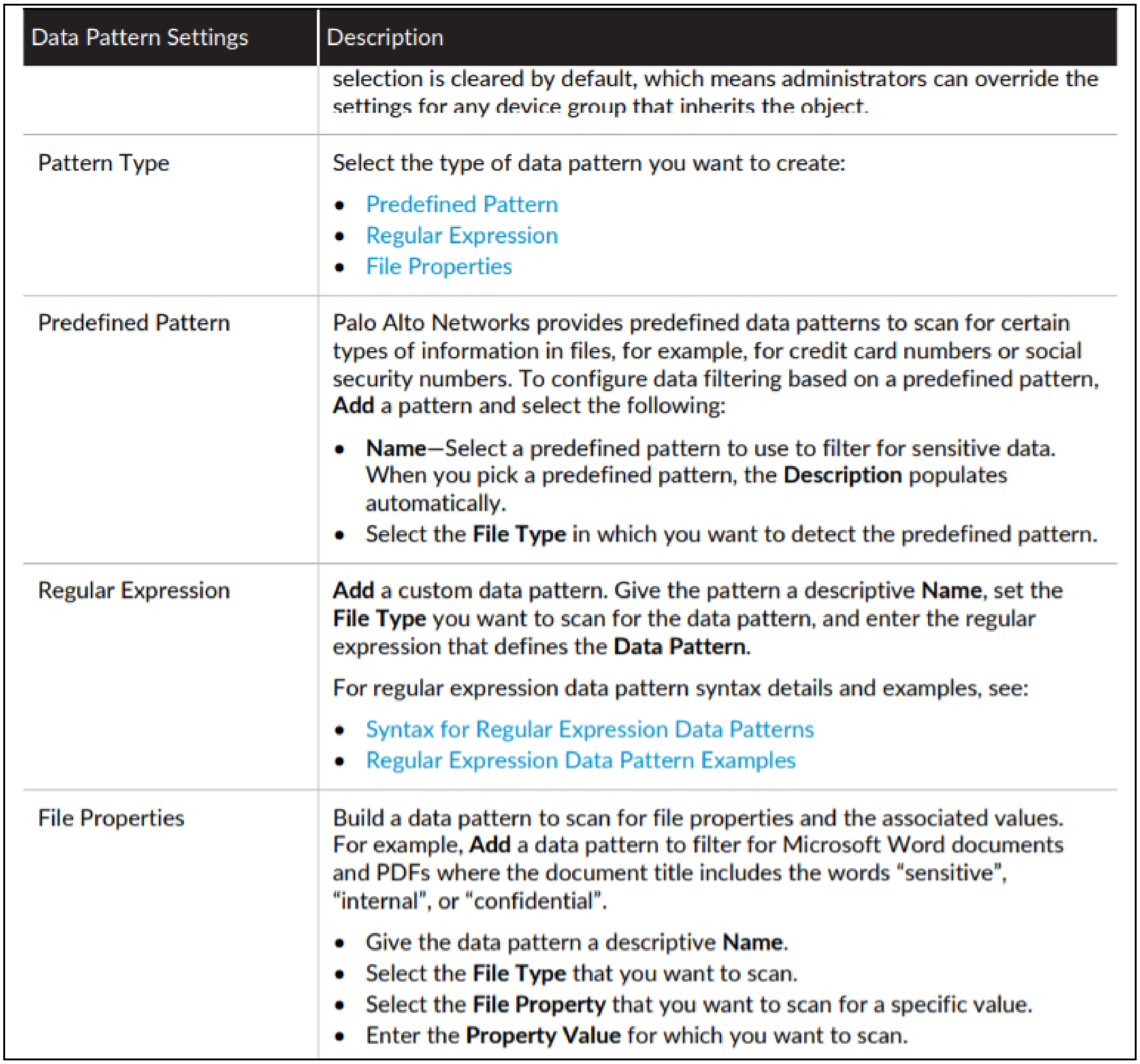
You can create three types of data patterns for the firewall to use when scanning for sensitive information:

- **Predefined**—Use the predefined data patterns to scan files for social security and credit card numbers.
- **Regular Expression**—Create custom data patterns using regular expressions.
- **File Properties**—Scan files for specific file properties and values.

Data Pattern Settings	Description
Name	Enter the data pattern name (up to 31 characters). The name case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
Description	Enter a description for the data pattern (up to 255 characters).
Shared	Select this option if you want the data pattern to be available to: • Every virtual system (vsys) on a multi-vsys firewall. If you clear this selection, the data pattern will be available only to the **Virtual System** selected in the **Objects** tab. • Every device group on Panorama. If you clear this selection, the data pattern will be available only to the **Device Group** selected in the **Objects** tab.
Disable override (Panorama only)	Select this option to prevent administrators from overriding the settings of this data pattern object in device groups that inherit the object. This

[4]

[4] *Id.*

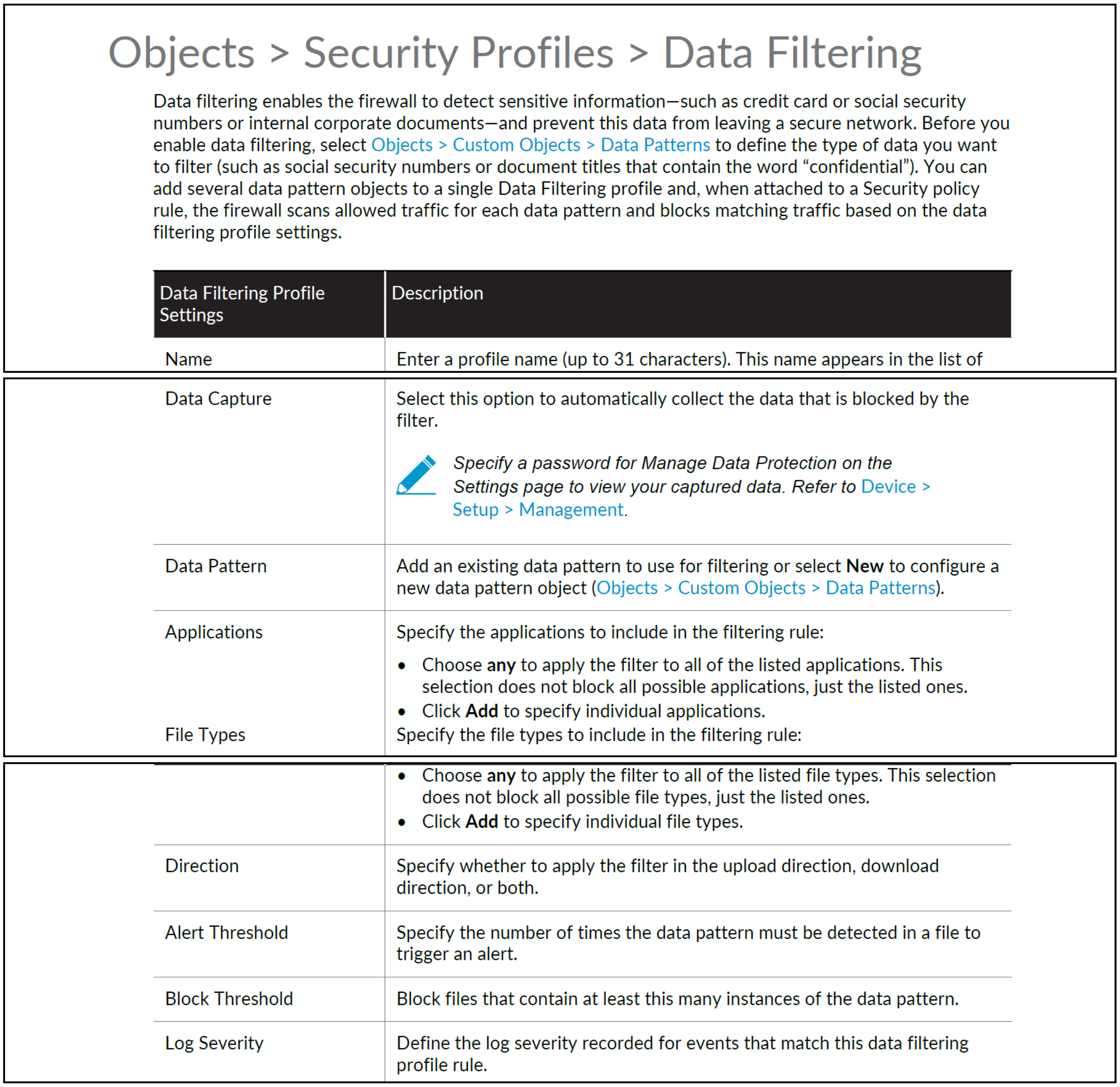


Data Pattern Settings	Description
	selection is cleared by default, which means administrators can override the settings for any device group that inherits the object.
Pattern Type	Select the type of data pattern you want to create: • Predefined Pattern • Regular Expression • File Properties
Predefined Pattern	Palo Alto Networks provides predefined data patterns to scan for certain types of information in files, for example, for credit card numbers or social security numbers. To configure data filtering based on a predefined pattern, **Add** a pattern and select the following: • **Name**—Select a predefined pattern to use to filter for sensitive data. When you pick a predefined pattern, the **Description** populates automatically. • Select the **File Type** in which you want to detect the predefined pattern.
Regular Expression	**Add** a custom data pattern. Give the pattern a descriptive **Name**, set the **File Type** you want to scan for the data pattern, and enter the regular expression that defines the **Data Pattern**. For regular expression data pattern syntax details and examples, see: • Syntax for Regular Expression Data Patterns • Regular Expression Data Pattern Examples
File Properties	Build a data pattern to scan for file properties and the associated values. For example, **Add** a data pattern to filter for Microsoft Word documents and PDFs where the document title includes the words "sensitive", "internal", or "confidential". • Give the data pattern a descriptive **Name**. • Select the **File Type** that you want to scan. • Select the **File Property** that you want to scan for a specific value. • Enter the **Property Value** for which you want to scan.

[5]

38. Every ’796 Accused Product practices identifying at least a portion of information associated with the at least one regularly identifiable expression and extracting the portion of information. For example, Palo Alto PAN-OS extracts filtered information for Data Capture.

[5] *Id.*



Objects > Security Profiles > Data Filtering

Data filtering enables the firewall to detect sensitive information—such as credit card or social security numbers or internal corporate documents—and prevent this data from leaving a secure network. Before you enable data filtering, select Objects > Custom Objects > Data Patterns to define the type of data you want to filter (such as social security numbers or document titles that contain the word "confidential"). You can add several data pattern objects to a single Data Filtering profile and, when attached to a Security policy rule, the firewall scans allowed traffic for each data pattern and blocks matching traffic based on the data filtering profile settings.

Data Filtering Profile Settings	Description
Name	Enter a profile name (up to 31 characters). This name appears in the list of
Data Capture	Select this option to automatically collect the data that is blocked by the filter. *Specify a password for Manage Data Protection on the Settings page to view your captured data. Refer to* Device > Setup > Management.
Data Pattern	Add an existing data pattern to use for filtering or select **New** to configure a new data pattern object (Objects > Custom Objects > Data Patterns).
Applications	Specify the applications to include in the filtering rule: • Choose **any** to apply the filter to all of the listed applications. This selection does not block all possible applications, just the listed ones. • Click **Add** to specify individual applications.
File Types	Specify the file types to include in the filtering rule: • Choose **any** to apply the filter to all of the listed file types. This selection does not block all possible file types, just the listed ones. • Click **Add** to specify individual file types.
Direction	Specify whether to apply the filter in the upload direction, download direction, or both.
Alert Threshold	Specify the number of times the data pattern must be detected in a file to trigger an alert.
Block Threshold	Block files that contain at least this many instances of the data pattern.
Log Severity	Define the log severity recorded for events that match this data filtering profile rule.

[6]

39. Defendant has and continues to indirectly infringe one or more claims of the '796 Patent by knowingly and intentionally inducing others, including Palo Alto 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

[6] *Id.*

include infringing technology, such as ’796 Accused Products (*e.g.*, products incorporating the Data Filtering based on Data Patterns feature).

40. Defendant, with the knowledge that these products, or the use thereof, infringe the ’796 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’796 Patent by providing these products to end-users for use in an infringing manner.

41. Defendant has 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.

42. 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.

43. 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.

COUNT II
(Infringement of the ’137 Patent)

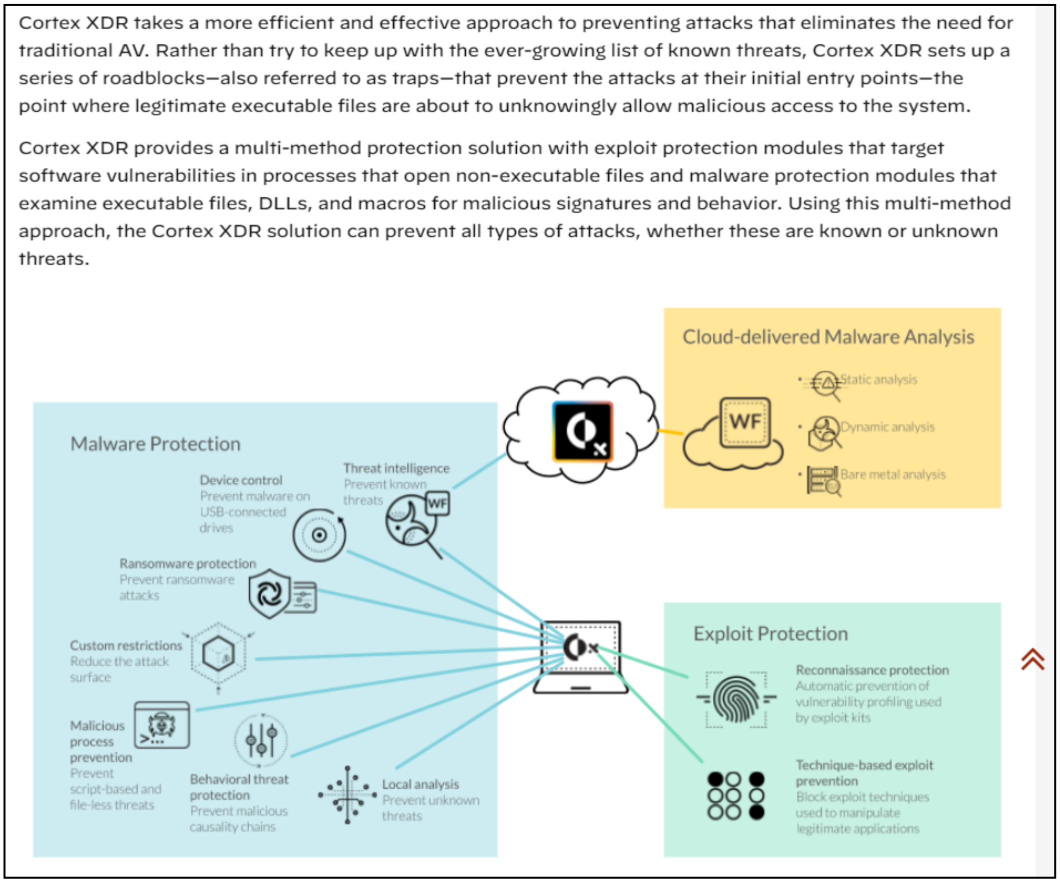
44. Paragraphs 1 through 32 are incorporated by reference as if fully set forth herein.

45. 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.

46. Defendant has and continues to directly infringe the ’137 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’137 Patent. Such products incorporate the

Malware Protection feature and include at least Palo Alto Cortex XDR (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.

47. Every '137 Accused Product practices implementing security for a computing device. For example, the Palo Alto Cortex XDR performs malware protection.



Cortex XDR takes a more efficient and effective approach to preventing attacks that eliminates the need for traditional AV. Rather than try to keep up with the ever-growing list of known threats, Cortex XDR sets up a series of roadblocks—also referred to as traps—that prevent the attacks at their initial entry points—the point where legitimate executable files are about to unknowingly allow malicious access to the system.

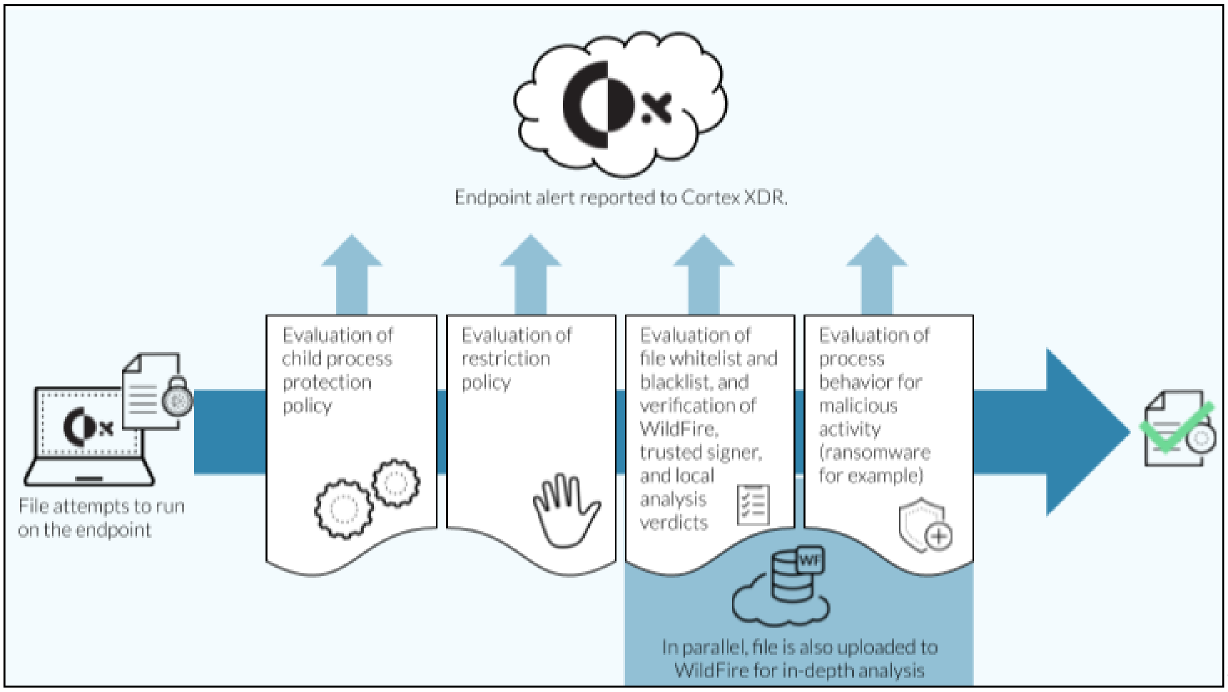
Cortex XDR provides a multi-method protection solution with exploit protection modules that target software vulnerabilities in processes that open non-executable files and malware protection modules that examine executable files, DLLs, and macros for malicious signatures and behavior. Using this multi-method approach, the Cortex XDR solution can prevent all types of attacks, whether these are known or unknown threats.

Cloud-delivered Malware Analysis
WF
Static analysis
Dynamic analysis
Bare metal analysis
Malware Protection
Device control
Prevent malware on USB-connected drives
Threat intelligence
Prevent known threats
WF
Ransomware protection
Prevent ransomware attacks
Custom restrictions
Reduce the attack surface
Malicious process prevention
Prevent script-based and file-less threats
Behavioral threat protection
Prevent malicious causality chains
Local analysis
Prevent unknown threats
Exploit Protection
Reconnaissance protection
Automatic prevention of vulnerability profiling used by exploit kits
Technique-based exploit prevention
Block exploit techniques used to manipulate legitimate applications

[7]

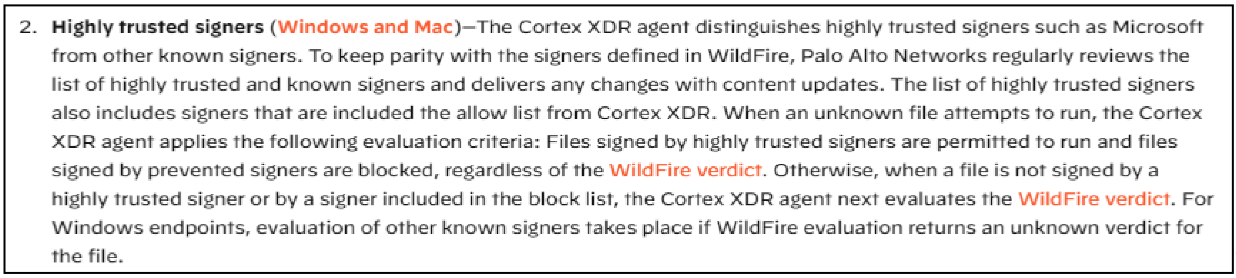
[7] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/endpoint-security-concepts/about-cortex-xdr-protection.html#

48. Every '137 Accused Product practices interrupting the loading of a new program for operation with the computing device. For example, when a new program is executed, the Palo Alto Cortex XDR first checks if the new program (or any of its child processes) is known malware.


Endpoint alert reported to Cortex XDR.
File attempts to run on the endpoint
Evaluation of child process protection policy
Evaluation of restriction policy
Evaluation of file whitelist and blacklist, and verification of WildFire, trusted signer, and local analysis verdicts
Evaluation of process behavior for malicious activity (ransomware for example)
WF
In parallel, file is also uploaded to WildFire for in-depth analysis

[8]

49. 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, Palo Alto Cortex XDR permits new programs to run if the new program was developed by a trusted installer.



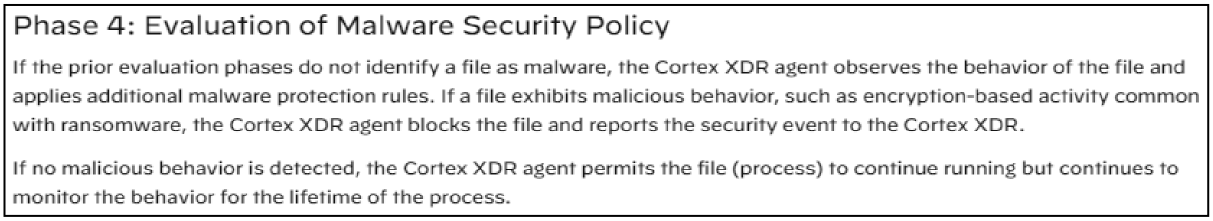
2. **Highly trusted signers** (Windows and Mac)—The Cortex XDR agent distinguishes highly trusted signers such as Microsoft from other known signers. To keep parity with the signers defined in WildFire, Palo Alto Networks regularly reviews the list of highly trusted and known signers and delivers any changes with content updates. The list of highly trusted signers also includes signers that are included the allow list from Cortex XDR. When an unknown file attempts to run, the Cortex XDR agent applies the following evaluation criteria: Files signed by highly trusted signers are permitted to run and files signed by prevented signers are blocked, regardless of the WildFire verdict. Otherwise, when a file is not signed by a highly trusted signer or by a signer included in the block list, the Cortex XDR agent next evaluates the WildFire verdict. For Windows endpoints, evaluation of other known signers takes place if WildFire evaluation returns an unknown verdict for the file.

[9]

[8] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/endpoint-security-concepts/analysis-and-protection-flow.html

[9] *Id.*

50. 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 is not validated, Palo Alto Cortex XDR first evaluates the Wildfire Verdict. If no malicious behavior is detected, Cortex XDR monitors the program while it loads and executes in connection with the endpoint.

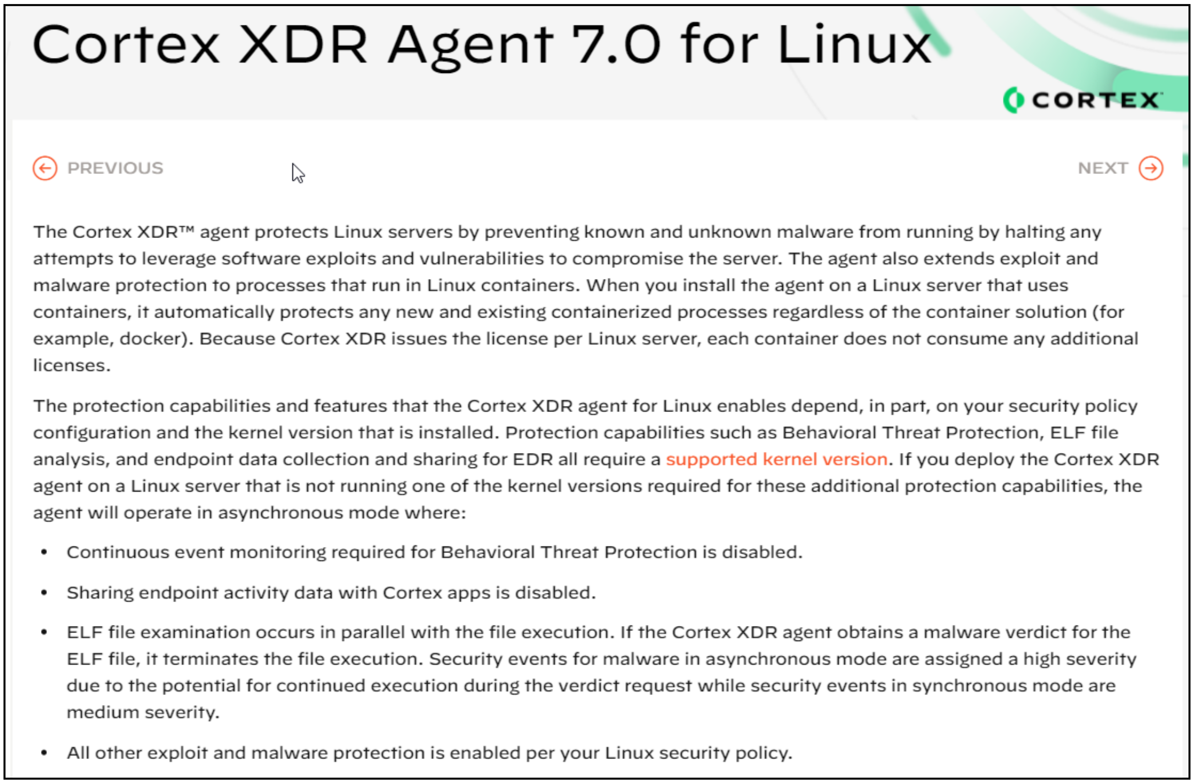


Phase 4: Evaluation of Malware Security Policy

If the prior evaluation phases do not identify a file as malware, the Cortex XDR agent observes the behavior of the file and applies additional malware protection rules. If a file exhibits malicious behavior, such as encryption-based activity common with ransomware, the Cortex XDR agent blocks the file and reports the security event to the Cortex XDR.

If no malicious behavior is detected, the Cortex XDR agent permits the file (process) to continue running but continues to monitor the behavior for the lifetime of the process. [10]

Monitoring the new program while it executes is performed at the operating kernel of the computing device.



Cortex XDR Agent 7.0 for Linux

The Cortex XDR™ agent protects Linux servers by preventing known and unknown malware from running by halting any attempts to leverage software exploits and vulnerabilities to compromise the server. The agent also extends exploit and malware protection to processes that run in Linux containers. When you install the agent on a Linux server that uses containers, it automatically protects any new and existing containerized processes regardless of the container solution (for example, docker). Because Cortex XDR issues the license per Linux server, each container does not consume any additional licenses.

The protection capabilities and features that the Cortex XDR agent for Linux enables depend, in part, on your security policy configuration and the kernel version that is installed. Protection capabilities such as Behavioral Threat Protection, ELF file analysis, and endpoint data collection and sharing for EDR all require a supported kernel version. If you deploy the Cortex XDR agent on a Linux server that is not running one of the kernel versions required for these additional protection capabilities, the agent will operate in asynchronous mode where:

- Continuous event monitoring required for Behavioral Threat Protection is disabled.
- Sharing endpoint activity data with Cortex apps is disabled.
- ELF file examination occurs in parallel with the file execution. If the Cortex XDR agent obtains a malware verdict for the ELF file, it terminates the file execution. Security events for malware in asynchronous mode are assigned a high severity due to the potential for continued execution during the verdict request while security events in synchronous mode are medium severity.
- All other exploit and malware protection is enabled per your Linux security policy.

[11]

[10] *Id.*

[11] https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/8-1/pan-os-web-interface-help/pan-os-web-interface-help.pdf

51. Defendant has and continues to indirectly infringe one or more claims of the '137 Patent by knowingly and intentionally inducing others, including Palo Alto 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 Malware Protection feature).

52. Defendant, with knowledge that these products, or the use thereof, infringe the '137 Patent at least as of the date of this 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.

53. Defendant has 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.

54. 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.

55. 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 '356 Patent)

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

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

58. Defendant has and continues to directly infringe the ’356 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’356 Patent. Such products incorporate the PAN-OS and Wildfire software and include at least Palo Alto VM and PA Series Firewalls (the “’356 Accused Products”) which are computer program products for automatically determining if a packet is a new, exploit candidate comprising: a computer-readable tangible storage device; first program instructions to determine if the packet is a known exploit; second program instructions to determine if the packet is addressed to a broadcast IP address of a network; third program instructions to determine if the packet is network administration traffic; fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a new, exploit candidate; and fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate; and wherein the first, second, third, fourth, and fifth program instructions are stored on the computer-readable tangible storage device.

59. Every ’356 Accused Product comprises a computer-readable tangible storage device. For example, the PA-7080 NGFW has two 240 GB solid state drives.

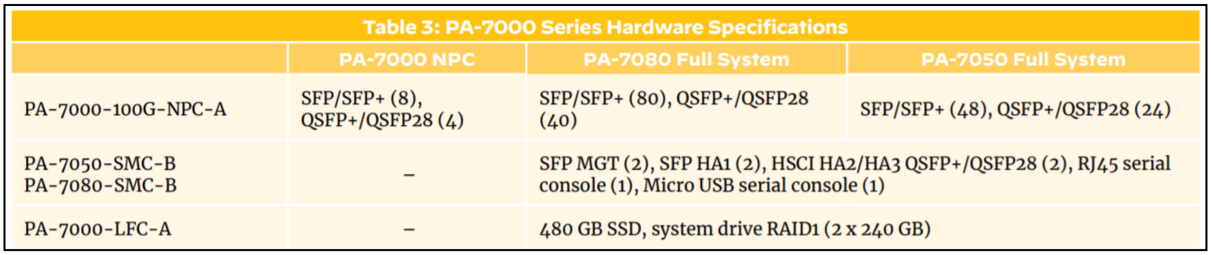
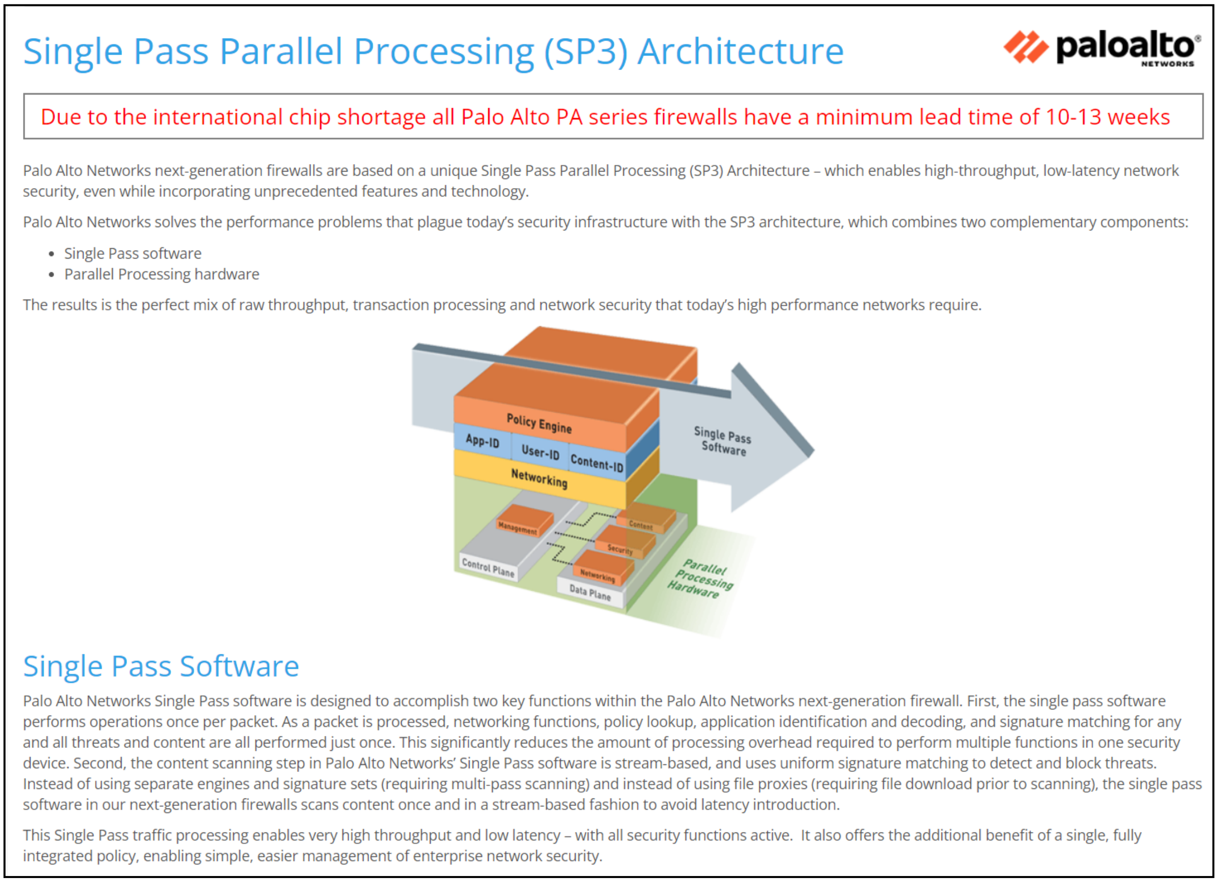


Table 3: PA-7000 Series Hardware Specifications

	PA-7000 NPC	PA-7080 Full System	PA-7050 Full System
PA-7000-100G-NPC-A	SFP/SFP+ (8), QSFP+/QSFP28 (4)	SFP/SFP+ (80), QSFP+/QSFP28 (40)	SFP/SFP+ (48), QSFP+/QSFP28 (24)
PA-7050-SMC-B PA-7080-SMC-B	–	SFP MGT (2), SFP HA1 (2), HSCI HA2/HA3 QSFP+/QSFP28 (2), RJ45 serial console (1), Micro USB serial console (1)	
PA-7000-LFC-A	–	480 GB SSD, system drive RAID1 (2 x 240 GB)	

[12]

60. Every ’356 Accused Product comprises first program instructions to determine if the packet is a known exploit. For example, the PA-7080 NGFW also includes PAN-OS software[13] and performs signature matching.



Single Pass Parallel Processing (SP3) Architecture

paloalto NETWORKS

Due to the international chip shortage all Palo Alto PA series firewalls have a minimum lead time of 10-13 weeks

Palo Alto Networks next-generation firewalls are based on a unique Single Pass Parallel Processing (SP3) Architecture – which enables high-throughput, low-latency network security, even while incorporating unprecedented features and technology.

Palo Alto Networks solves the performance problems that plague today's security infrastructure with the SP3 architecture, which combines two complementary components:

- Single Pass software
- Parallel Processing hardware

The results is the perfect mix of raw throughput, transaction processing and network security that today's high performance networks require.

Single Pass Software

Palo Alto Networks Single Pass software is designed to accomplish two key functions within the Palo Alto Networks next-generation firewall. First, the single pass software performs operations once per packet. As a packet is processed, networking functions, policy lookup, application identification and decoding, and signature matching for any and all threats and content are all performed just once. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device. Second, the content scanning step in Palo Alto Networks' Single Pass software is stream-based, and uses uniform signature matching to detect and block threats. Instead of using separate engines and signature sets (requiring multi-pass scanning) and instead of using file proxies (requiring file download prior to scanning), the single pass software in our next-generation firewalls scans content once and in a stream-based fashion to avoid latency introduction.

This Single Pass traffic processing enables very high throughput and low latency – with all security functions active. It also offers the additional benefit of a single, fully integrated policy, enabling simple, easier management of enterprise network security.

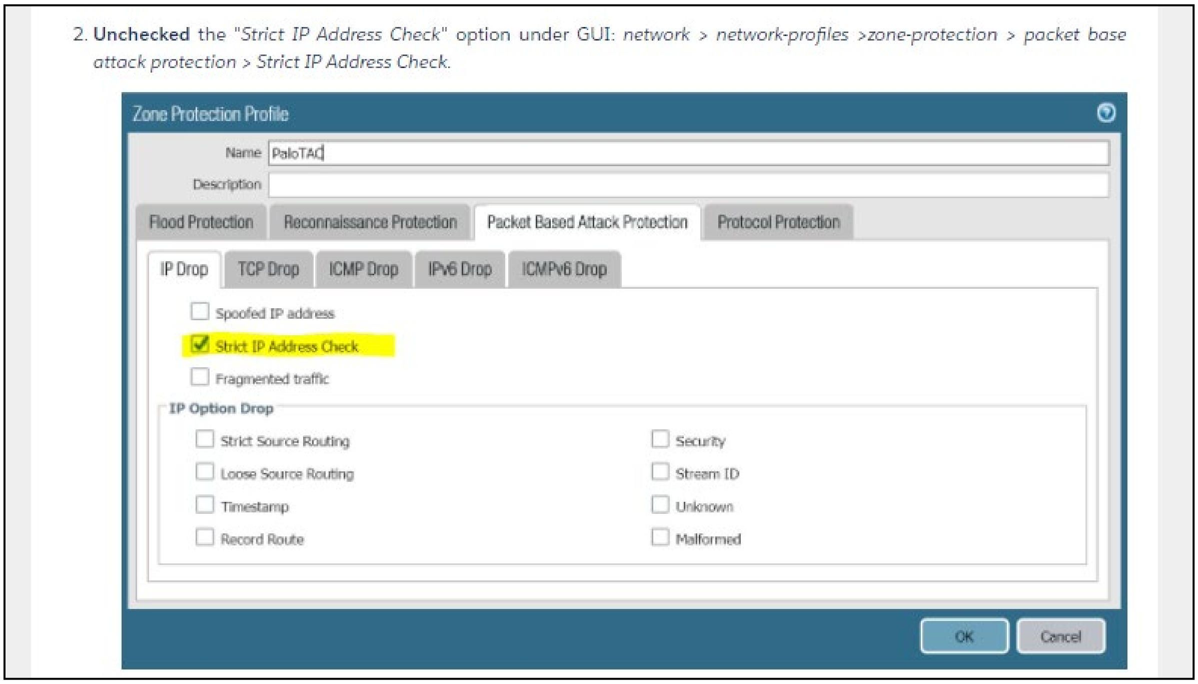
[14]

[12] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series

[13] *Id.*

[14] https://www.paloguard.com/SP3-Architecture.asp

61. Every ’356 Accused Product comprises second program instructions to determine if the packet is addressed to a broadcast IP address of a network. For example, the PA-7080 NGFW includes PAN-OS software[15] which performs Strict IP Address Checks.



2. **Unchecked** the "*Strict IP Address Check*" option under GUI: *network > network-profiles >zone-protection > packet base attack protection > Strict IP Address Check.*

Name PaloTAC

Description

□ Spoofed IP address

☑ Strict IP Address Check

□ Fragmented traffic

IP Option Drop

□ Strict Source Routing

□ Loose Source Routing

□ Timestamp

□ Record Route

□ Security

□ Stream ID

□ Unknown

□ Malformed

[16]

62. Every ’356 Accused Product comprises third program instructions to determine if the packet is network administration traffic. For example, the PA-7080 NGFW includes PAN-OS software[17] which scans the MGT port for administration traffic.[18]

63. Every ’356 Accused Product comprises fourth program instructions, responsive to the packet being a known exploit OR the packet being addressed to a broadcast IP address of a network OR the packet being network administration traffic, to determine that the packet is not a

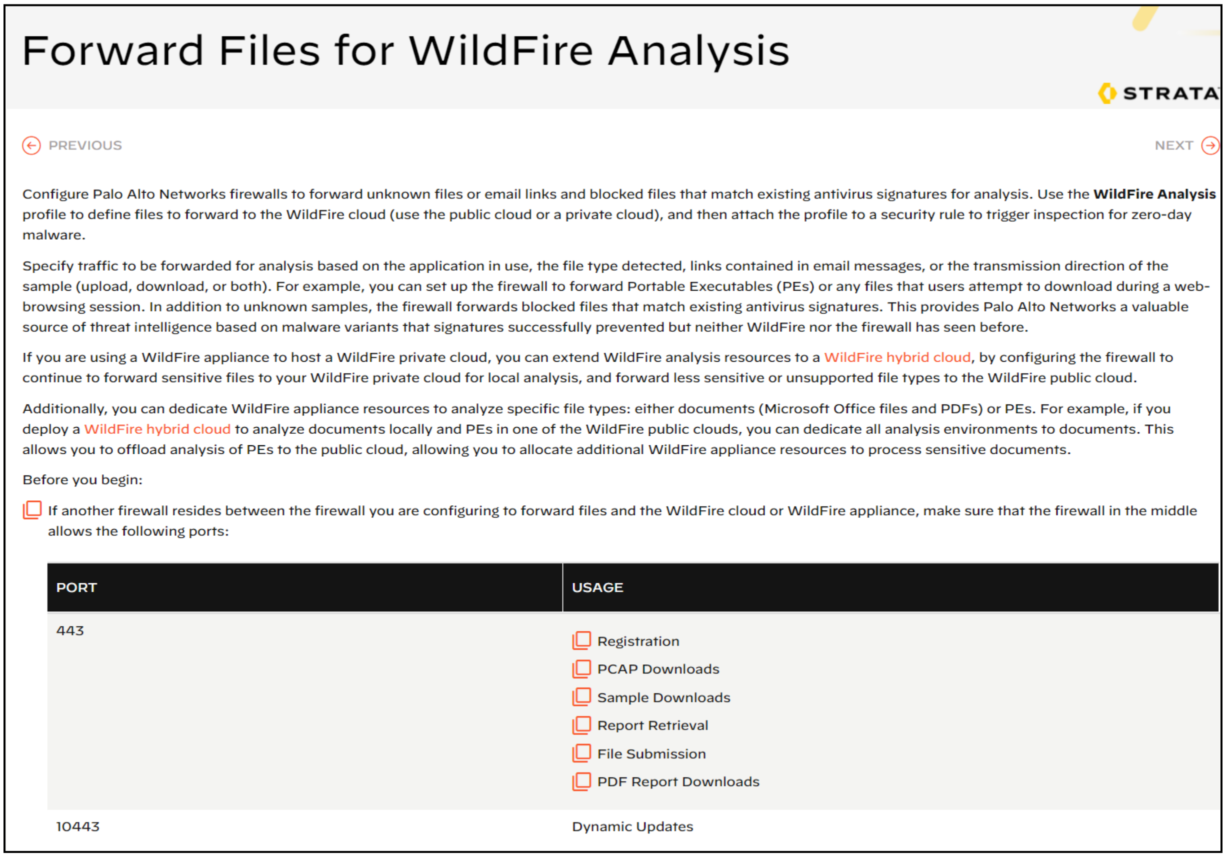
[15] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series

[16] https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000008U3FCAU&lang=en_US%E2%80%A9

[17] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series

[18] https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-1/pan-os-admin/pan-os-admin.pdf

new, exploit candidate. For example, the PA-7080 NGFW includes the Wildfire software[19] which has processes variants of known exploits.



Forward Files for WildFire Analysis

Configure Palo Alto Networks firewalls to forward unknown files or email links and blocked files that match existing antivirus signatures for analysis. Use the **WildFire Analysis** profile to define files to forward to the WildFire cloud (use the public cloud or a private cloud), and then attach the profile to a security rule to trigger inspection for zero-day malware.

Specify traffic to be forwarded for analysis based on the application in use, the file type detected, links contained in email messages, or the transmission direction of the sample (upload, download, or both). For example, you can set up the firewall to forward Portable Executables (PEs) or any files that users attempt to download during a web-browsing session. In addition to unknown samples, the firewall forwards blocked files that match existing antivirus signatures. This provides Palo Alto Networks a valuable source of threat intelligence based on malware variants that signatures successfully prevented but neither WildFire nor the firewall has seen before.

If you are using a WildFire appliance to host a WildFire private cloud, you can extend WildFire analysis resources to a WildFire hybrid cloud, by configuring the firewall to continue to forward sensitive files to your WildFire private cloud for local analysis, and forward less sensitive or unsupported file types to the WildFire public cloud.

Additionally, you can dedicate WildFire appliance resources to analyze specific file types: either documents (Microsoft Office files and PDFs) or PEs. For example, if you deploy a WildFire hybrid cloud to analyze documents locally and PEs in one of the WildFire public clouds, you can dedicate all analysis environments to documents. This allows you to offload analysis of PEs to the public cloud, allowing you to allocate additional WildFire appliance resources to process sensitive documents.

Before you begin:

□ If another firewall resides between the firewall you are configuring to forward files and the WildFire cloud or WildFire appliance, make sure that the firewall in the middle allows the following ports:

PORT	USAGE
443	□ Registration □ PCAP Downloads □ Sample Downloads □ Report Retrieval □ File Submission □ PDF Report Downloads
10443	Dynamic Updates

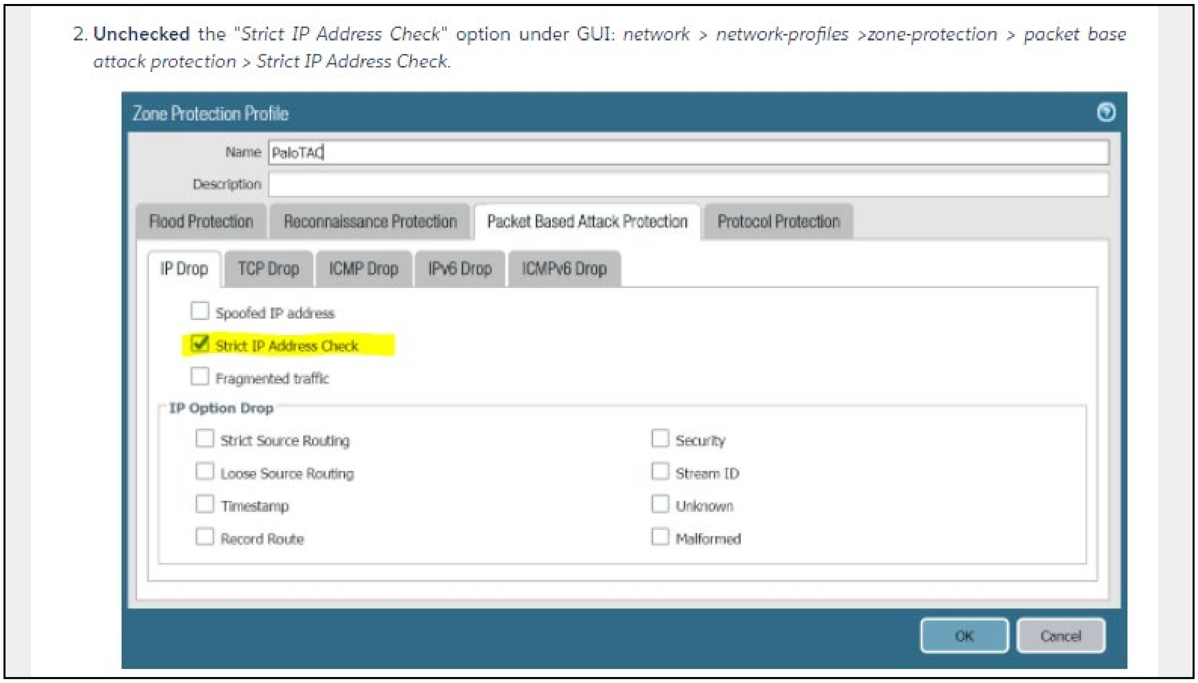
[20]

64. As another example, the PA-7080 NGFW includes PAN-OS software[21] which performs IP Drops.

[19] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series

[20] https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/forward-files-for-wildfire-analysis

[21] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series



2. **Unchecked** the "*Strict IP Address Check*" option under GUI: *network > network-profiles >zone-protection > packet base attack protection > Strict IP Address Check.*

Zone Protection Profile

Name PaloTAC

Description

□ Spoofed IP address
☑ Strict IP Address Check
□ Fragmented traffic

IP Option Drop

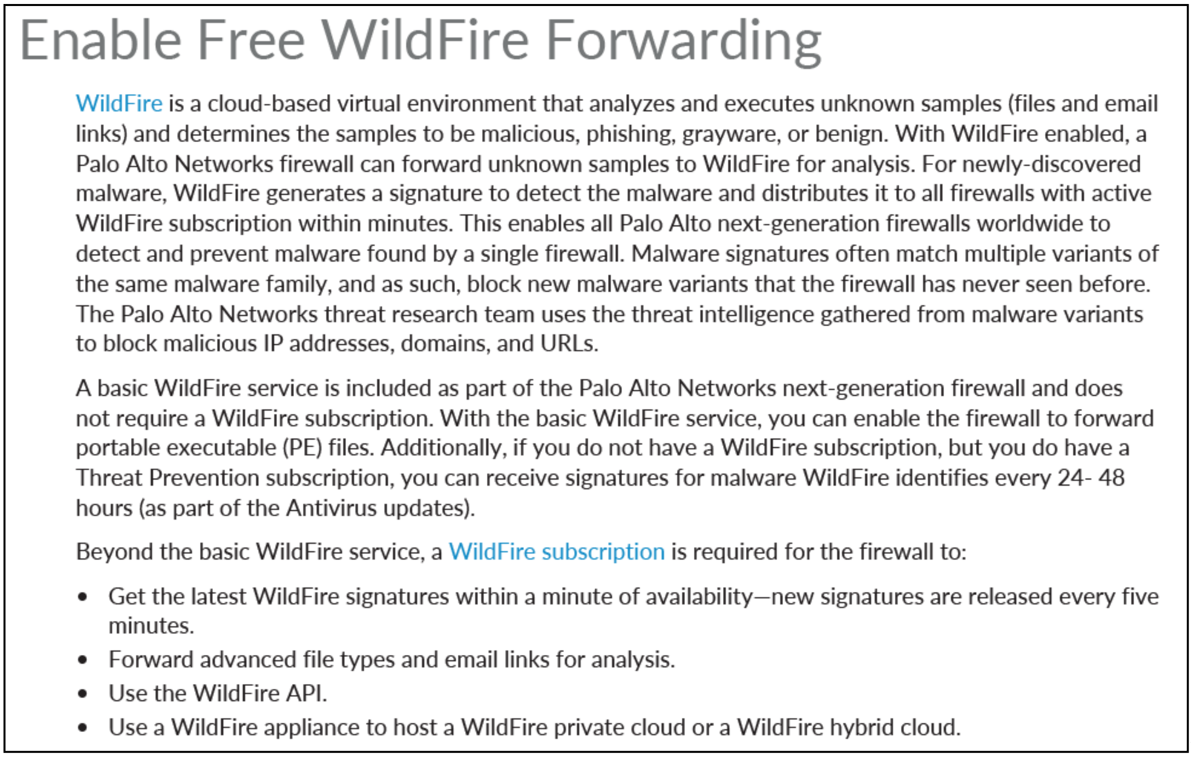
□ Strict Source Routing
□ Loose Source Routing
□ Timestamp
□ Record Route
□ Security
□ Stream ID
□ Unknown
□ Malformed

[22]

65. Every ’356 Accused Product comprises fifth program instructions, responsive to the packet not being a known exploit AND the packet not being addressed to a broadcast IP address of a network AND the packet not being network administration traffic AND the packet not being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate. For example, the PA-7080 NGFW includes Wildfire software[23] which determines whether the packet is a new, exploit candidate.

[22] https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g0000008U3FCAU&lang=en_US%E2%80%A9

[23] https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series



Enable Free WildFire Forwarding

WildFire is a cloud-based virtual environment that analyzes and executes unknown samples (files and email links) and determines the samples to be malicious, phishing, grayware, or benign. With WildFire enabled, a Palo Alto Networks firewall can forward unknown samples to WildFire for analysis. For newly-discovered malware, WildFire generates a signature to detect the malware and distributes it to all firewalls with active WildFire subscription within minutes. This enables all Palo Alto next-generation firewalls worldwide to detect and prevent malware found by a single firewall. Malware signatures often match multiple variants of the same malware family, and as such, block new malware variants that the firewall has never seen before. The Palo Alto Networks threat research team uses the threat intelligence gathered from malware variants to block malicious IP addresses, domains, and URLs.

A basic WildFire service is included as part of the Palo Alto Networks next-generation firewall and does not require a WildFire subscription. With the basic WildFire service, you can enable the firewall to forward portable executable (PE) files. Additionally, if you do not have a WildFire subscription, but you do have a Threat Prevention subscription, you can receive signatures for malware WildFire identifies every 24- 48 hours (as part of the Antivirus updates).

Beyond the basic WildFire service, a WildFire subscription is required for the firewall to:

- Get the latest WildFire signatures within a minute of availability—new signatures are released every five minutes.
- Forward advanced file types and email links for analysis.
- Use the WildFire API.
- Use a WildFire appliance to host a WildFire private cloud or a WildFire hybrid cloud.

[24]

66. In every ’356 Accused Product, the first, second, third, fourth, and fifth program instructions are stored on the computer-readable tangible storage device.

67. Defendant has and continues to indirectly infringe one or more claims of the ’356 Patent by knowingly and intentionally inducing others, including Palo Alto 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 ’356 Accused Products (*e.g.*, products incorporating the Palo Alto PAN-OS and Wildfire software).

68. Defendant, with knowledge that these products, or the use thereof, infringe the ’356 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues

[24] https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/9-1/pan-os-admin/pan-os-admin.pdf

to knowingly and intentionally induce, direct infringement of the ’356 Patent by providing these products to end-users for use in an infringing manner.

69. Defendant has induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’356 Patent, but while remaining willfully blind to the infringement.

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

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

COUNT IV
(Infringement of the ’441 Patent)

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

73. 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.

74. Defendant has and continues to directly infringe the ’441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’441 Patent. Such products incorporate the Malicious Process Prevention and Behavioral Threat Protection features and include at least the Palo Alto Cortex XDR (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.

75. 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, Palo Alto Cortex XDR incorporates malicious process prevention and behavioral threat protection to stop script-based threats and other attacks at runtime.

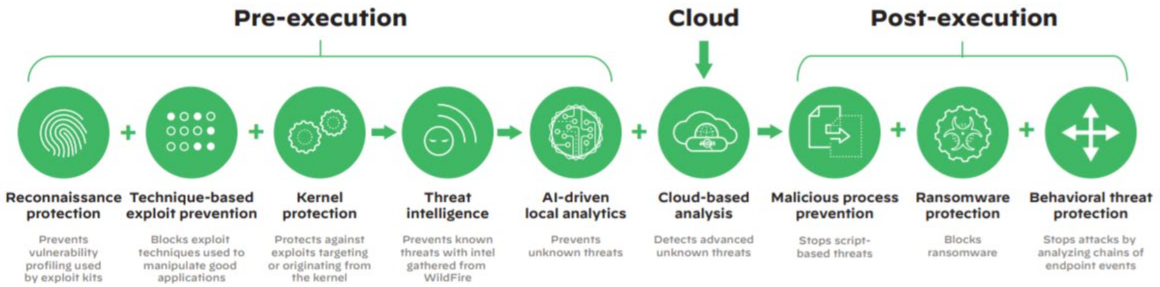
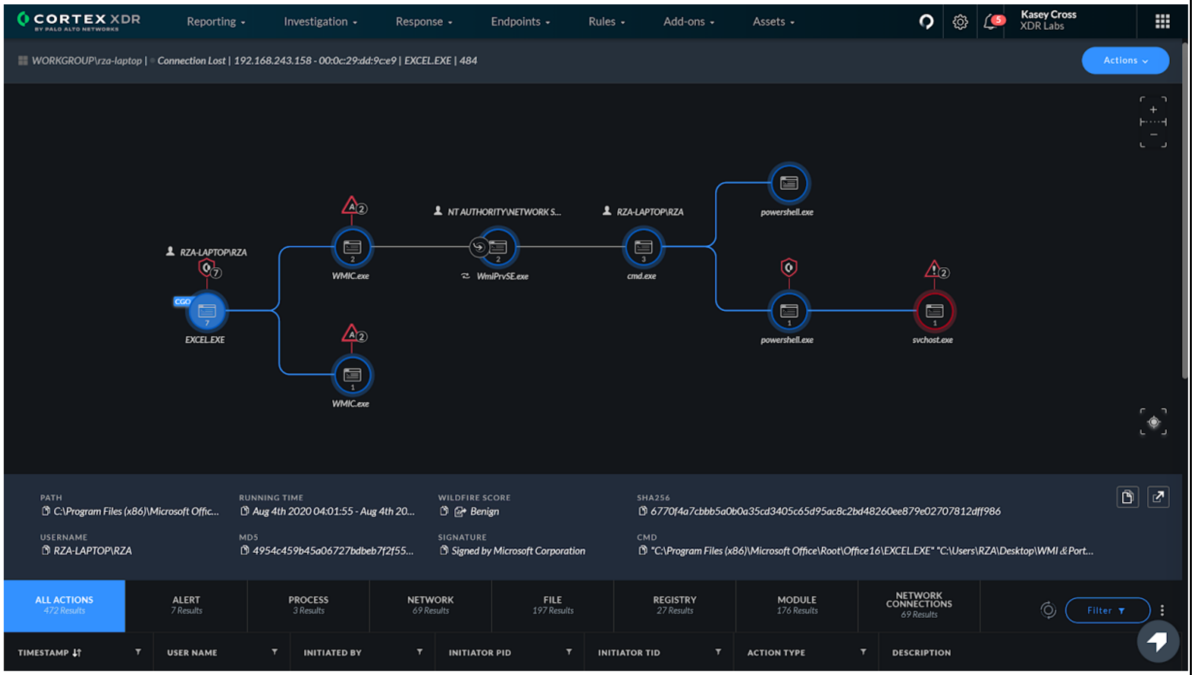

Pre-execution
Cloud
Post-execution
Reconnaissance protection
Prevents vulnerability profiling used by exploit kits
Technique-based exploit prevention
Blocks exploit techniques used to manipulate good applications
Kernel protection
Protects against exploits targeting or originating from the kernel
Threat intelligence
Prevents known threats with intel gathered from WildFire
AI-driven local analytics
Prevents unknown threats
Cloud-based analysis
Detects advanced unknown threats
Malicious process prevention
Stops script-based threats
Ransomware protection
Blocks ransomware
Behavioral threat protection
Stops attacks by analyzing chains of endpoint events

Figure 5: Automatically preventing malware, exploits, and fileless attacks [25]

76. 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

[25] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

PATH
C:\Program Files (x86)\Microsoft Offic...

RUNNING TIME
Aug 4th 2020 04:01:55 - Aug 4th 20...

WILDFIRE SCORE
Benign

SHA256
6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986

USERNAME
RZA-LAPTOP\RZA

MD5
4954c459b45a06727bdbeb7f2f55...

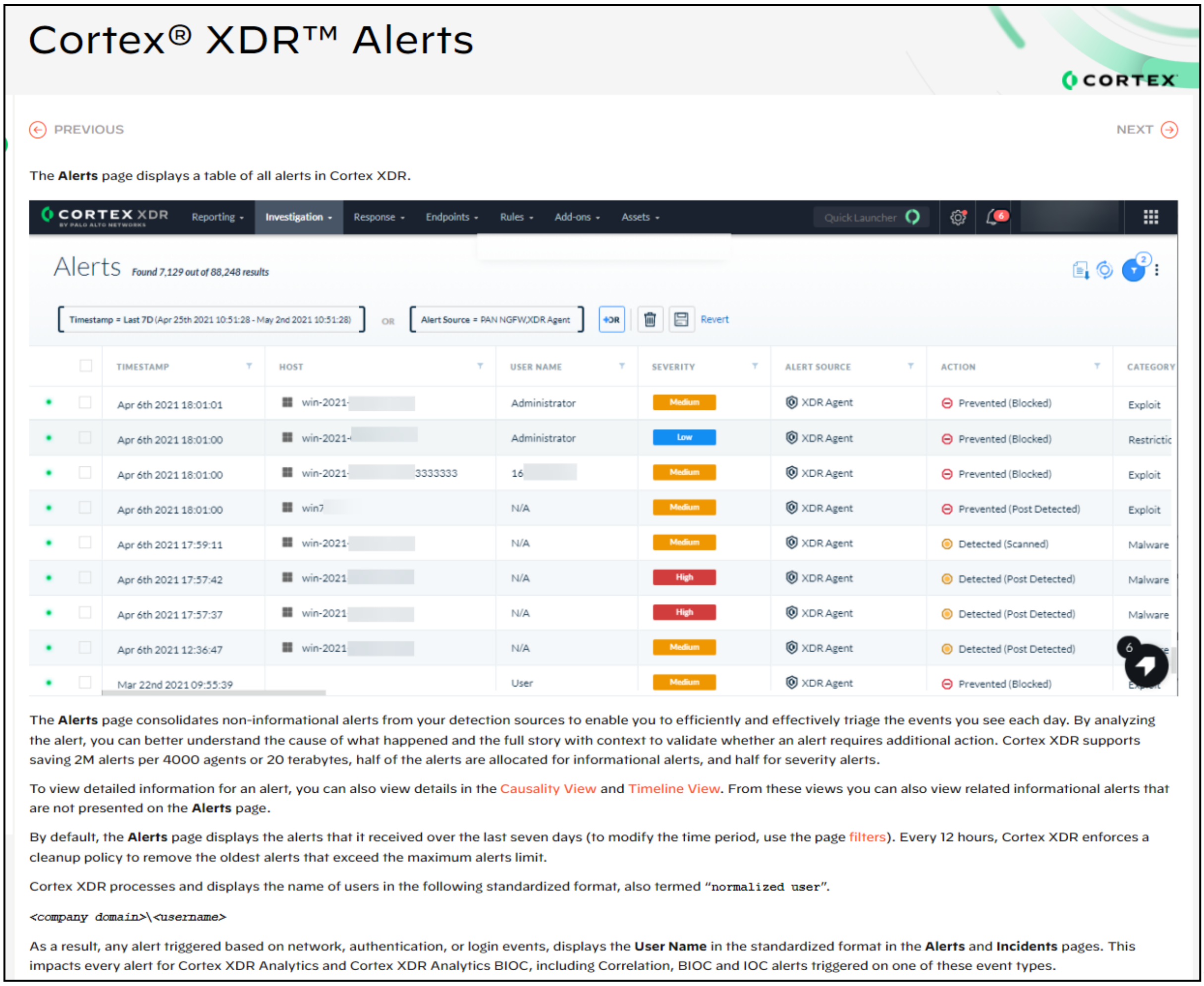
SIGNATURE
Signed by Microsoft Corporation

CMD
"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR[26]

77. Every ’441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result and sending, by the attestation server, the attestation result associated with the application. For example, Palo Alto Cortex XDR generates alerts and logs information related to each detected threat, including the result of the detected threat.

[26] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



Cortex® XDR™ Alerts

The **Alerts** page displays a table of all alerts in Cortex XDR.

Alerts *Found 7,129 out of 88,248 results*

Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28) OR Alert Source = PAN NGFW,XDR Agent

	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
● □	Apr 6th 2021 18:01:01	win-2021-[redacted]	Administrator	Medium	XDR Agent	Prevented (Blocked)	Exploit
● □	Apr 6th 2021 18:01:00	win-2021-[redacted]	Administrator	Low	XDR Agent	Prevented (Blocked)	Restrictic
● □	Apr 6th 2021 18:01:00	win-2021-[redacted]3333333	16[redacted]	Medium	XDR Agent	Prevented (Blocked)	Exploit
● □	Apr 6th 2021 18:01:00	win7[redacted]	N/A	Medium	XDR Agent	Prevented (Post Detected)	Exploit
● □	Apr 6th 2021 17:59:11	win-2021-[redacted]	N/A	Medium	XDR Agent	Detected (Scanned)	Malware
● □	Apr 6th 2021 17:57:42	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
● □	Apr 6th 2021 17:57:37	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
● □	Apr 6th 2021 12:36:47	win-2021[redacted]	N/A	Medium	XDR Agent	Detected (Post Detected)	Malware
● □	Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	Prevented (Blocked)	Exploit

The **Alerts** page consolidates non-informational alerts from your detection sources to enable you to efficiently and effectively triage the events you see each day. By analyzing the alert, you can better understand the cause of what happened and the full story with context to validate whether an alert requires additional action. Cortex XDR supports saving 2M alerts per 4000 agents or 20 terabytes, half of the alerts are allocated for informational alerts, and half for severity alerts.

To view detailed information for an alert, you can also view details in the Causality View and Timeline View. From these views you can also view related informational alerts that are not presented on the **Alerts** page.

By default, the **Alerts** page displays the alerts that it received over the last seven days (to modify the time period, use the page filters). Every 12 hours, Cortex XDR enforces a cleanup policy to remove the oldest alerts that exceed the maximum alerts limit.

Cortex XDR processes and displays the name of users in the following standardized format, also termed "`normalized user`".

`<company domain>\<username>`

As a result, any alert triggered based on network, authentication, or login events, displays the **User Name** in the standardized format in the **Alerts** and **Incidents** pages. This impacts every alert for Cortex XDR Analytics and Cortex XDR Analytics BIOC, including Correlation, BIOC and IOC alerts triggered on one of these event types.[27]

78. Defendant has and continues to indirectly infringe one or more claims of the '441 Patent by knowingly and intentionally inducing others, including Palo Alto 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 malicious process prevention and behavioral threat protection features).

79. Defendant, with knowledge that these products, or the use thereof, infringe the '441 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues

[27] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/cortex-xdr-alerts.html

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

80. Defendant has 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.

81. 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.

82. 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 V
(Infringement of the ’038 Patent)

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

84. 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.

85. Defendant has and continues to directly infringe the ’038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’038 Patent. Such products incorporate the Malicious Process Prevention and Behavioral Threat Protection features and include at least the Palo Alto Cortex XDR (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.

86. Every ’038 Accused Product practices a method for controlling the operation of an endpoint. For example, the Palo Alto Cortex XDR performs Malicious Process Prevention and Behavioral Threat Protection on endpoints.

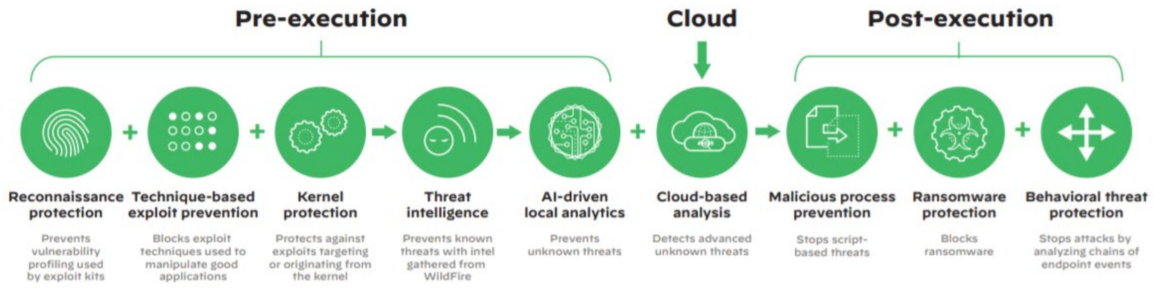
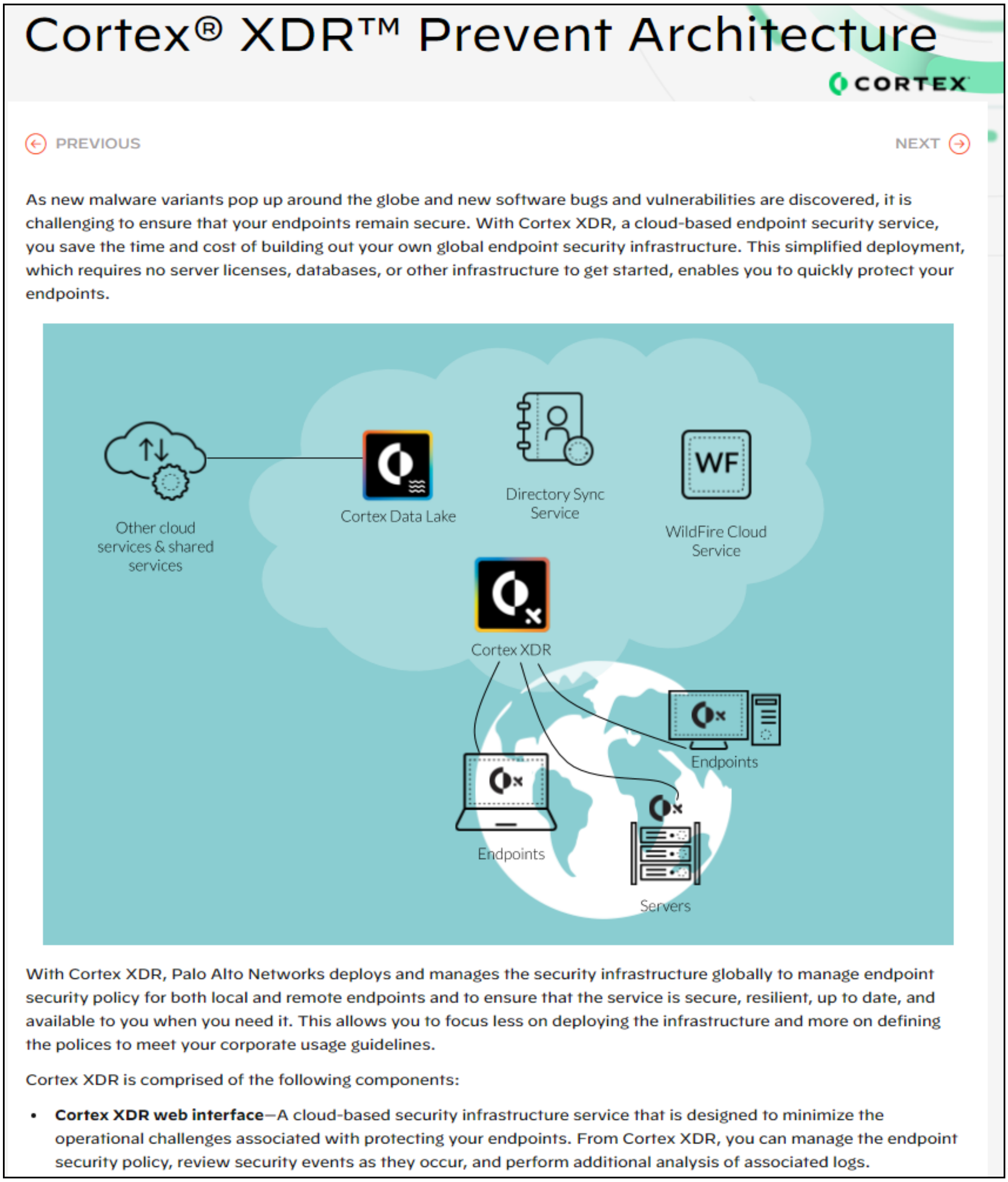

Pre-execution
Cloud
Post-execution
Reconnaissance protection
Prevents vulnerability profiling used by exploit kits
Technique-based exploit prevention
Blocks exploit techniques used to manipulate good applications
Kernel protection
Protects against exploits targeting or originating from the kernel
Threat intelligence
Prevents known threats with intel gathered from WildFire
AI-driven local analytics
Prevents unknown threats
Cloud-based analysis
Detects advanced unknown threats
Malicious process prevention
Stops script-based threats
Ransomware protection
Blocks ransomware
Behavioral threat protection
Stops attacks by analyzing chains of endpoint events

Figure 5: Automatically preventing malware, exploits, and fileless attacks [28]

87. 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, Palo

[28] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

Alto Cortex XDR allows configuration of a plurality of policies (*e.g.*, endpoint security policies, rules, profiles) at a system remote from the endpoint through a provided user interface which are stored in a data store (*e.g.*, Cortex XDR).



Cortex® XDR™ Prevent Architecture

As new malware variants pop up around the globe and new software bugs and vulnerabilities are discovered, it is challenging to ensure that your endpoints remain secure. With Cortex XDR, a cloud-based endpoint security service, you save the time and cost of building out your own global endpoint security infrastructure. This simplified deployment, which requires no server licenses, databases, or other infrastructure to get started, enables you to quickly protect your endpoints.

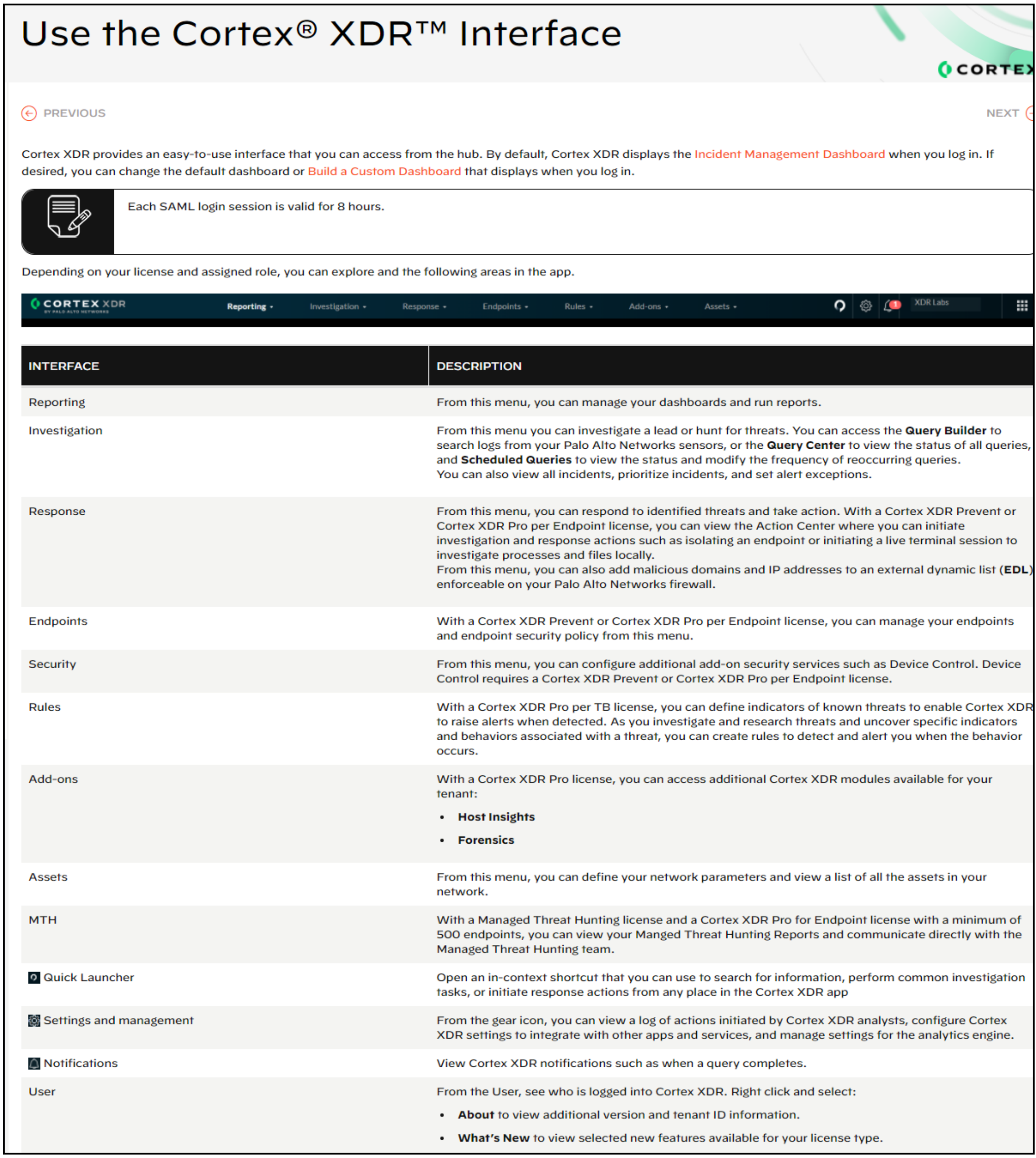
With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

[29]

[29] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html



Use the Cortex® XDR™ Interface

Cortex XDR provides an easy-to-use interface that you can access from the hub. By default, Cortex XDR displays the Incident Management Dashboard when you log in. If desired, you can change the default dashboard or Build a Custom Dashboard that displays when you log in.

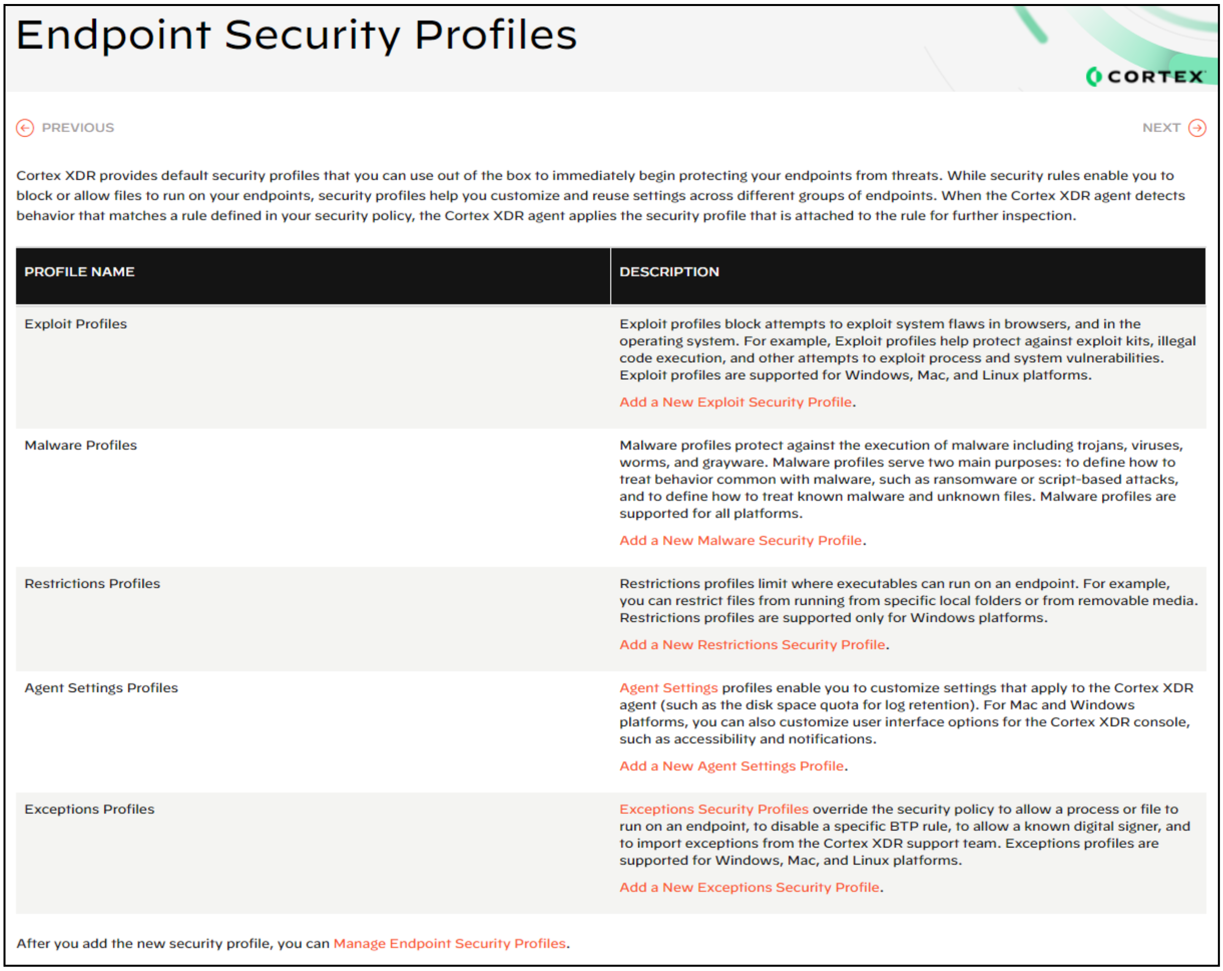
Each SAML login session is valid for 8 hours.

Depending on your license and assigned role, you can explore and the following areas in the app.

INTERFACE	DESCRIPTION
Reporting	From this menu, you can manage your dashboards and run reports.
Investigation	From this menu you can investigate a lead or hunt for threats. You can access the **Query Builder** to search logs from your Palo Alto Networks sensors, or the **Query Center** to view the status of all queries, and **Scheduled Queries** to view the status and modify the frequency of reoccurring queries. You can also view all incidents, prioritize incidents, and set alert exceptions.
Response	From this menu, you can respond to identified threats and take action. With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can view the Action Center where you can initiate investigation and response actions such as isolating an endpoint or initiating a live terminal session to investigate processes and files locally. From this menu, you can also add malicious domains and IP addresses to an external dynamic list (**EDL**) enforceable on your Palo Alto Networks firewall.
Endpoints	With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can manage your endpoints and endpoint security policy from this menu.
Security	From this menu, you can configure additional add-on security services such as Device Control. Device Control requires a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license.
Rules	With a Cortex XDR Pro per TB license, you can define indicators of known threats to enable Cortex XDR to raise alerts when detected. As you investigate and research threats and uncover specific indicators and behaviors associated with a threat, you can create rules to detect and alert you when the behavior occurs.
Add-ons	With a Cortex XDR Pro license, you can access additional Cortex XDR modules available for your tenant: • **Host Insights** • **Forensics**
Assets	From this menu, you can define your network parameters and view a list of all the assets in your network.
MTH	With a Managed Threat Hunting license and a Cortex XDR Pro for Endpoint license with a minimum of 500 endpoints, you can view your Manged Threat Hunting Reports and communicate directly with the Managed Threat Hunting team.
Quick Launcher	Open an in-context shortcut that you can use to search for information, perform common investigation tasks, or initiate response actions from any place in the Cortex XDR app
Settings and management	From the gear icon, you can view a log of actions initiated by Cortex XDR analysts, configure Cortex XDR settings to integrate with other apps and services, and manage settings for the analytics engine.
Notifications	View Cortex XDR notifications such as when a query completes.
User	From the User, see who is logged into Cortex XDR. Right click and select: • **About** to view additional version and tenant ID information. • **What's New** to view selected new features available for your license type.

[30]

[30] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/get-started-with-cortex-xdr-pro/use-cortex-xdr.html



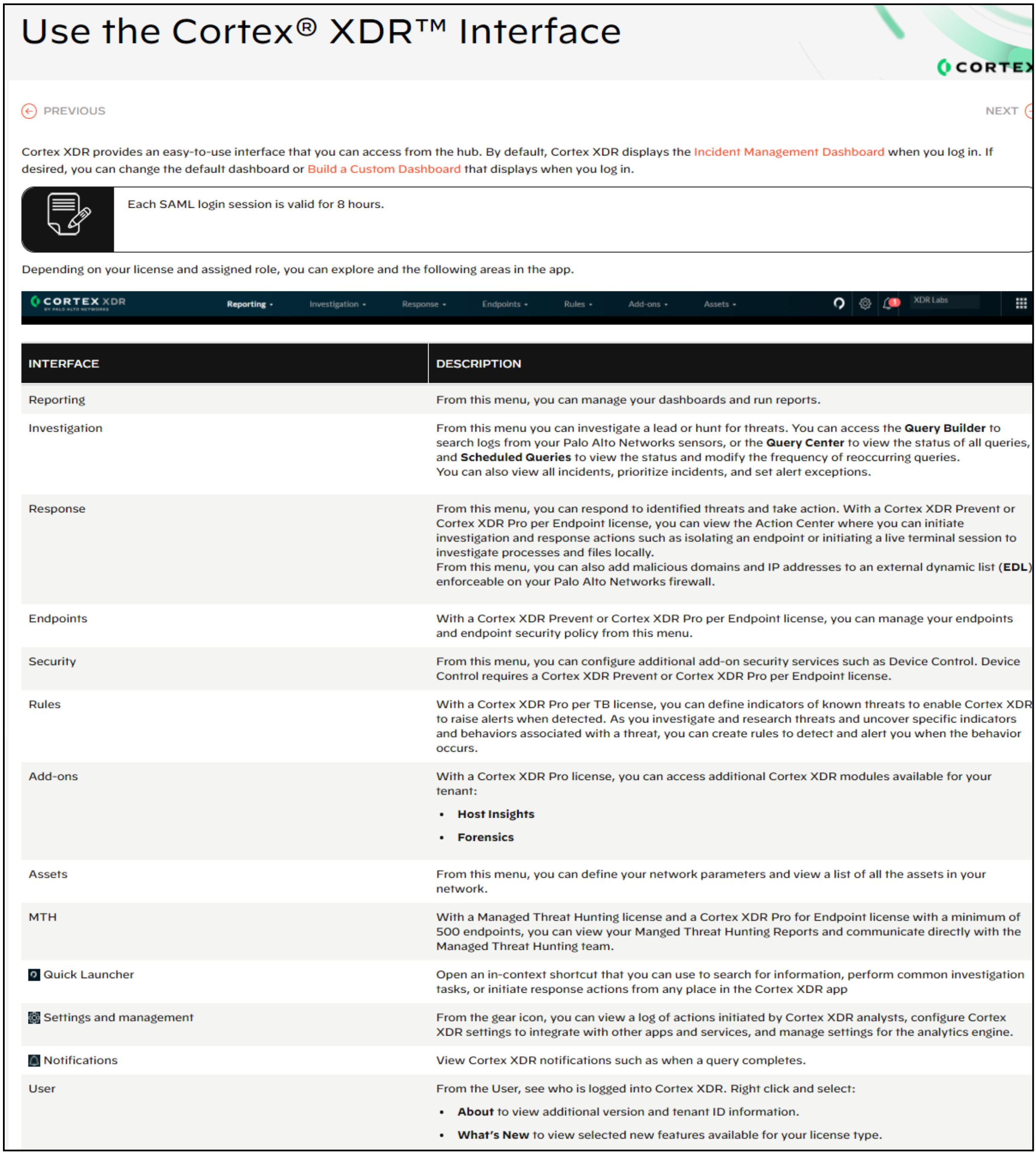
Endpoint Security Profiles

Cortex XDR provides default security profiles that you can use out of the box to immediately begin protecting your endpoints from threats. While security rules enable you to block or allow files to run on your endpoints, security profiles help you customize and reuse settings across different groups of endpoints. When the Cortex XDR agent detects behavior that matches a rule defined in your security policy, the Cortex XDR agent applies the security profile that is attached to the rule for further inspection.

PROFILE NAME	DESCRIPTION
Exploit Profiles	Exploit profiles block attempts to exploit system flaws in browsers, and in the operating system. For example, Exploit profiles help protect against exploit kits, illegal code execution, and other attempts to exploit process and system vulnerabilities. Exploit profiles are supported for Windows, Mac, and Linux platforms. Add a New Exploit Security Profile.
Malware Profiles	Malware profiles protect against the execution of malware including trojans, viruses, worms, and grayware. Malware profiles serve two main purposes: to define how to treat behavior common with malware, such as ransomware or script-based attacks, and to define how to treat known malware and unknown files. Malware profiles are supported for all platforms. Add a New Malware Security Profile.
Restrictions Profiles	Restrictions profiles limit where executables can run on an endpoint. For example, you can restrict files from running from specific local folders or from removable media. Restrictions profiles are supported only for Windows platforms. Add a New Restrictions Security Profile.
Agent Settings Profiles	Agent Settings profiles enable you to customize settings that apply to the Cortex XDR agent (such as the disk space quota for log retention). For Mac and Windows platforms, you can also customize user interface options for the Cortex XDR console, such as accessibility and notifications. Add a New Agent Settings Profile.
Exceptions Profiles	Exceptions Security Profiles override the security policy to allow a process or file to run on an endpoint, to disable a specific BTP rule, to allow a known digital signer, and to import exceptions from the Cortex XDR support team. Exceptions profiles are supported for Windows, Mac, and Linux platforms. Add a New Exceptions Security Profile.

After you add the new security profile, you can Manage Endpoint Security Profiles.[31]

[31] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-security-profiles.html



Use the Cortex® XDR™ Interface

Cortex XDR provides an easy-to-use interface that you can access from the hub. By default, Cortex XDR displays the Incident Management Dashboard when you log in. If desired, you can change the default dashboard or Build a Custom Dashboard that displays when you log in.

Each SAML login session is valid for 8 hours.

Depending on your license and assigned role, you can explore and the following areas in the app.

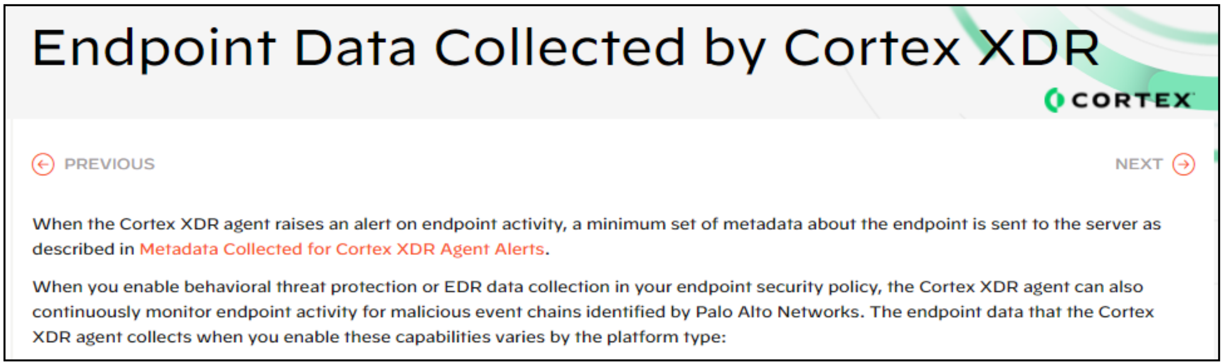
INTERFACE	DESCRIPTION
Reporting	From this menu, you can manage your dashboards and run reports.
Investigation	From this menu you can investigate a lead or hunt for threats. You can access the **Query Builder** to search logs from your Palo Alto Networks sensors, or the **Query Center** to view the status of all queries, and **Scheduled Queries** to view the status and modify the frequency of reoccurring queries. You can also view all incidents, prioritize incidents, and set alert exceptions.
Response	From this menu, you can respond to identified threats and take action. With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can view the Action Center where you can initiate investigation and response actions such as isolating an endpoint or initiating a live terminal session to investigate processes and files locally. From this menu, you can also add malicious domains and IP addresses to an external dynamic list (**EDL**) enforceable on your Palo Alto Networks firewall.
Endpoints	With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can manage your endpoints and endpoint security policy from this menu.
Security	From this menu, you can configure additional add-on security services such as Device Control. Device Control requires a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license.
Rules	With a Cortex XDR Pro per TB license, you can define indicators of known threats to enable Cortex XDR to raise alerts when detected. As you investigate and research threats and uncover specific indicators and behaviors associated with a threat, you can create rules to detect and alert you when the behavior occurs.
Add-ons	With a Cortex XDR Pro license, you can access additional Cortex XDR modules available for your tenant: • **Host Insights** • **Forensics**
Assets	From this menu, you can define your network parameters and view a list of all the assets in your network.
MTH	With a Managed Threat Hunting license and a Cortex XDR Pro for Endpoint license with a minimum of 500 endpoints, you can view your Manged Threat Hunting Reports and communicate directly with the Managed Threat Hunting team.
Quick Launcher	Open an in-context shortcut that you can use to search for information, perform common investigation tasks, or initiate response actions from any place in the Cortex XDR app
Settings and management	From the gear icon, you can view a log of actions initiated by Cortex XDR analysts, configure Cortex XDR settings to integrate with other apps and services, and manage settings for the analytics engine.
Notifications	View Cortex XDR notifications such as when a query completes.
User	From the User, see who is logged into Cortex XDR. Right click and select: • **About** to view additional version and tenant ID information. • **What's New** to view selected new features available for your license type.

[32]

88. Every '038 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Palo Alto Cortex XDR

[32] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/get-started-with-cortex-xdr-pro/use-cortex-xdr.html

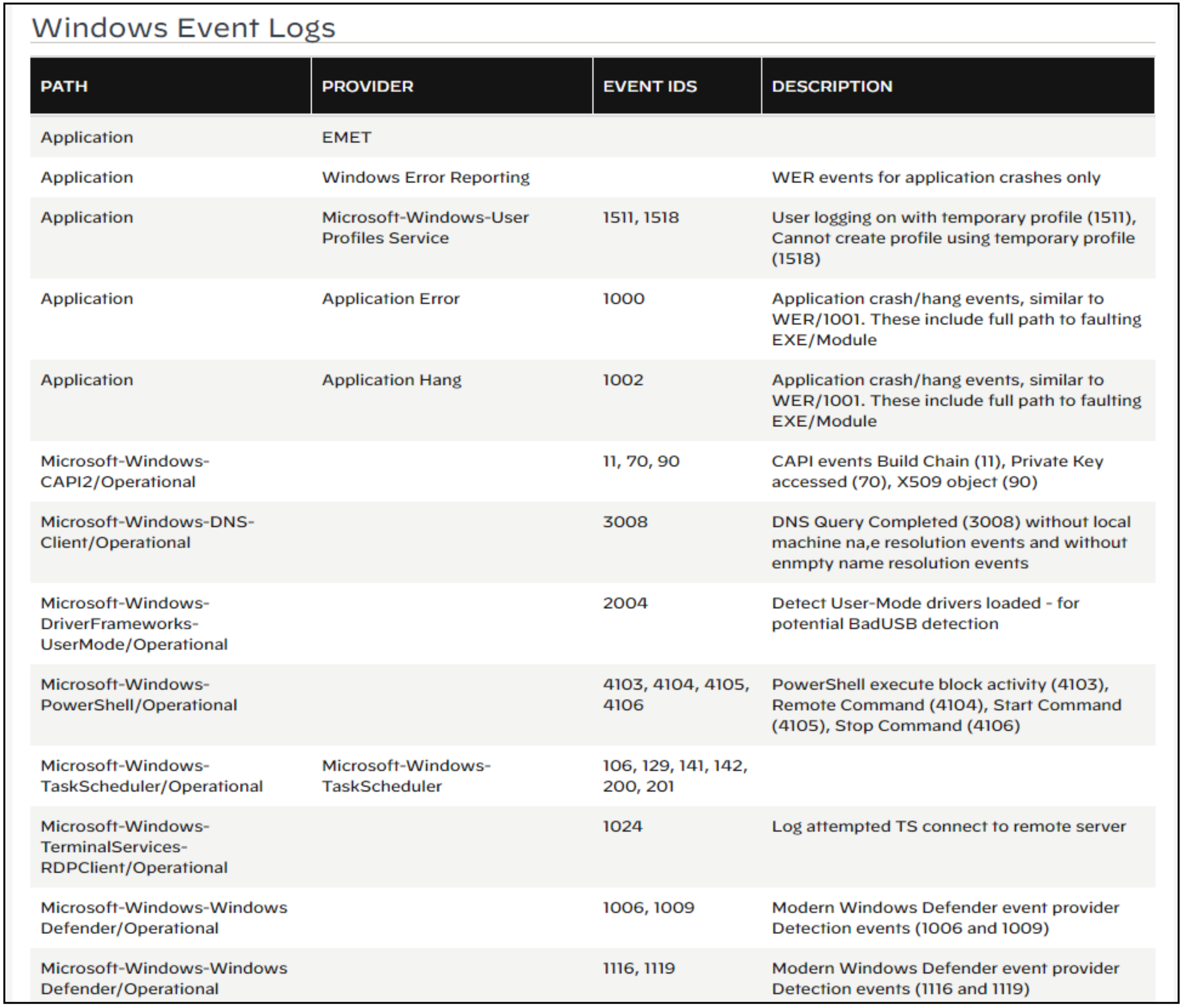
Agents identify, from the plurality of policies, operating conditions (*e.g.*, events) on the endpoint to monitor.



Endpoint Data Collected by Cortex XDR

When the Cortex XDR agent raises an alert on endpoint activity, a minimum set of metadata about the endpoint is sent to the server as described in Metadata Collected for Cortex XDR Agent Alerts.

When you enable behavioral threat protection or EDR data collection in your endpoint security policy, the Cortex XDR agent can also continuously monitor endpoint activity for malicious event chains identified by Palo Alto Networks. The endpoint data that the Cortex XDR agent collects when you enable these capabilities varies by the platform type:

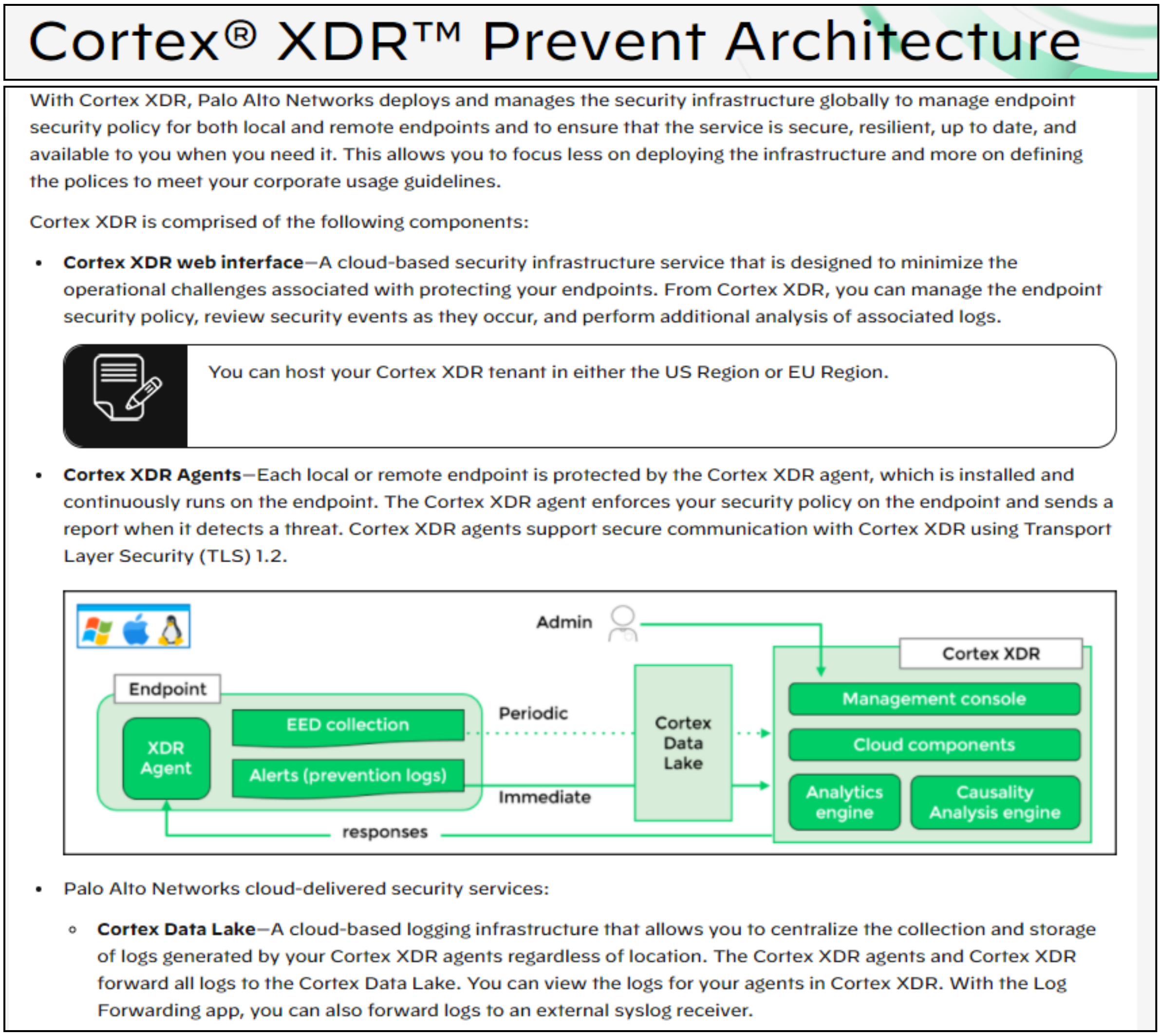


Windows Event Logs

PATH	PROVIDER	EVENT IDS	DESCRIPTION
Application	EMET		
Application	Windows Error Reporting		WER events for application crashes only
Application	Microsoft-Windows-User Profiles Service	1511, 1518	User logging on with temporary profile (1511), Cannot create profile using temporary profile (1518)
Application	Application Error	1000	Application crash/hang events, similar to WER/1001. These include full path to faulting EXE/Module
Application	Application Hang	1002	Application crash/hang events, similar to WER/1001. These include full path to faulting EXE/Module
Microsoft-Windows-CAPI2/Operational		11, 70, 90	CAPI events Build Chain (11), Private Key accessed (70), X509 object (90)
Microsoft-Windows-DNS-Client/Operational		3008	DNS Query Completed (3008) without local machine na,e resolution events and without enmpty name resolution events
Microsoft-Windows-DriverFrameworks-UserMode/Operational		2004	Detect User-Mode drivers loaded - for potential BadUSB detection
Microsoft-Windows-PowerShell/Operational		4103, 4104, 4105, 4106	PowerShell execute block activity (4103), Remote Command (4104), Start Command (4105), Stop Command (4106)
Microsoft-Windows-TaskScheduler/Operational	Microsoft-Windows-TaskScheduler	106, 129, 141, 142, 200, 201	
Microsoft-Windows-TerminalServices-RDPClient/Operational		1024	Log attempted TS connect to remote server
Microsoft-Windows-Windows Defender/Operational		1006, 1009	Modern Windows Defender event provider Detection events (1006 and 1009)
Microsoft-Windows-Windows Defender/Operational		1116, 1119	Modern Windows Defender event provider Detection events (1116 and 1119)

[33]

[33] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/customizable-agent-settings/endpoint-data-collected-by-cortex-xdr.html



Cortex® XDR™ Prevent Architecture

With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

  You can host your Cortex XDR tenant in either the US Region or EU Region.

- **Cortex XDR Agents**—Each local or remote endpoint is protected by the Cortex XDR agent, which is installed and continuously runs on the endpoint. The Cortex XDR agent enforces your security policy on the endpoint and sends a report when it detects a threat. Cortex XDR agents support secure communication with Cortex XDR using Transport Layer Security (TLS) 1.2.

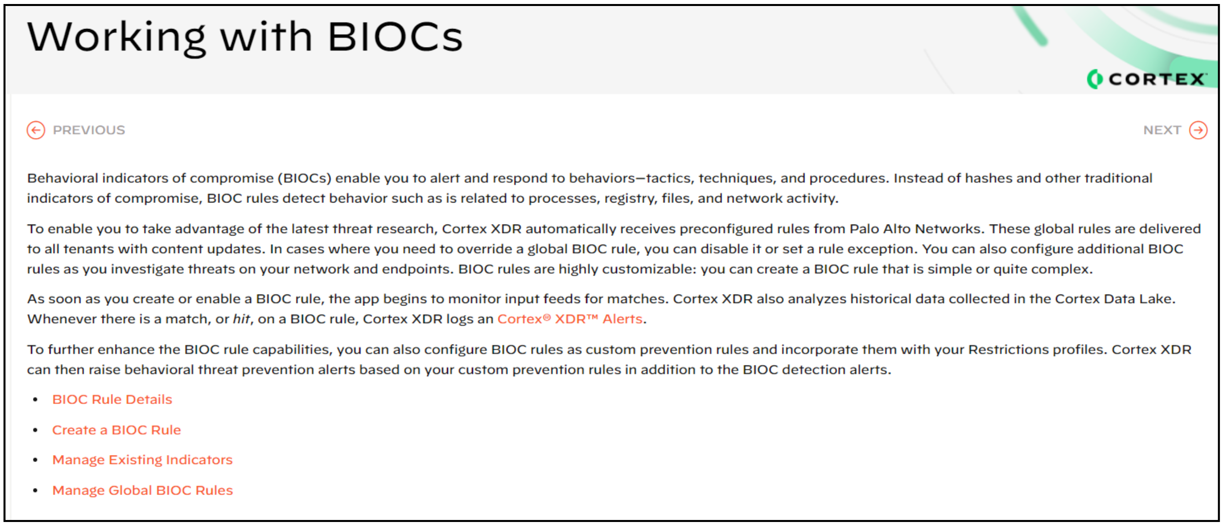
- Palo Alto Networks cloud-delivered security services:
  - **Cortex Data Lake**—A cloud-based logging infrastructure that allows you to centralize the collection and storage of logs generated by your Cortex XDR agents regardless of location. The Cortex XDR agents and Cortex XDR forward all logs to the Cortex Data Lake. You can view the logs for your agents in Cortex XDR. With the Log Forwarding app, you can also forward logs to an external syslog receiver.

[34]

89. Every ’038 Accused Product practices configuring one or more software agents on the endpoint to monitor the plurality of operating conditions. For example, Palo Alto Cortex XDR configures the Cortex XDR Agents to monitor the plurality of operating conditions.[35]

[34] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html

[35] *Id*.



Working with BIOCs

Behavioral indicators of compromise (BIOCs) enable you to alert and respond to behaviors—tactics, techniques, and procedures. Instead of hashes and other traditional indicators of compromise, BIOC rules detect behavior such as is related to processes, registry, files, and network activity.

To enable you to take advantage of the latest threat research, Cortex XDR automatically receives preconfigured rules from Palo Alto Networks. These global rules are delivered to all tenants with content updates. In cases where you need to override a global BIOC rule, you can disable it or set a rule exception. You can also configure additional BIOC rules as you investigate threats on your network and endpoints. BIOC rules are highly customizable: you can create a BIOC rule that is simple or quite complex.

As soon as you create or enable a BIOC rule, the app begins to monitor input feeds for matches. Cortex XDR also analyzes historical data collected in the Cortex Data Lake. Whenever there is a match, or *hit*, on a BIOC rule, Cortex XDR logs an Cortex® XDR™ Alerts.

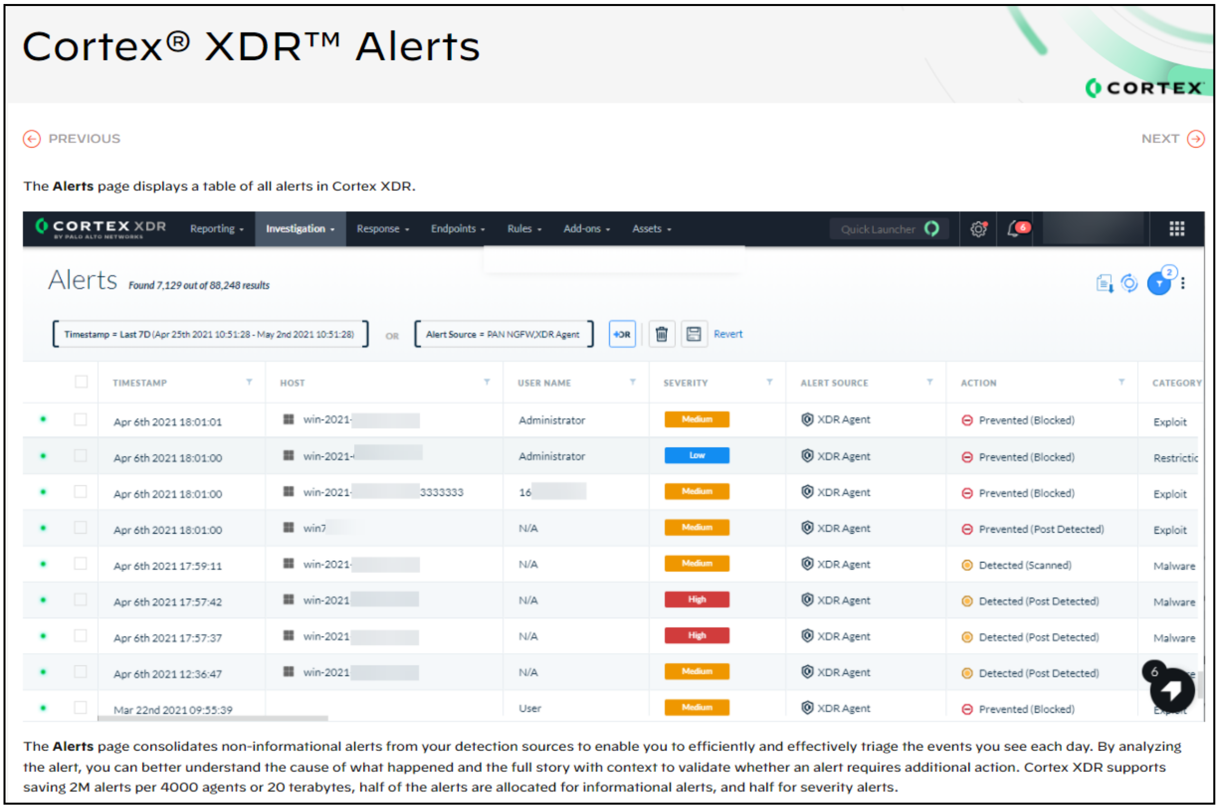
To further enhance the BIOC rule capabilities, you can also configure BIOC rules as custom prevention rules and incorporate them with your Restrictions profiles. Cortex XDR can then raise behavioral threat prevention alerts based on your custom prevention rules in addition to the BIOC detection alerts.

- BIOC Rule Details
- Create a BIOC Rule
- Manage Existing Indicators
- Manage Global BIOC Rules

[36]

90. 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, Cortex XDR receives information regarding whether threats have been detected, gathered by the one or more software agents (*e.g.*, Cortex XDR Agents).

[36] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs.html



Cortex® XDR™ Alerts

The **Alerts** page displays a table of all alerts in Cortex XDR.

Alerts *Found 7,129 out of 88,248 results*

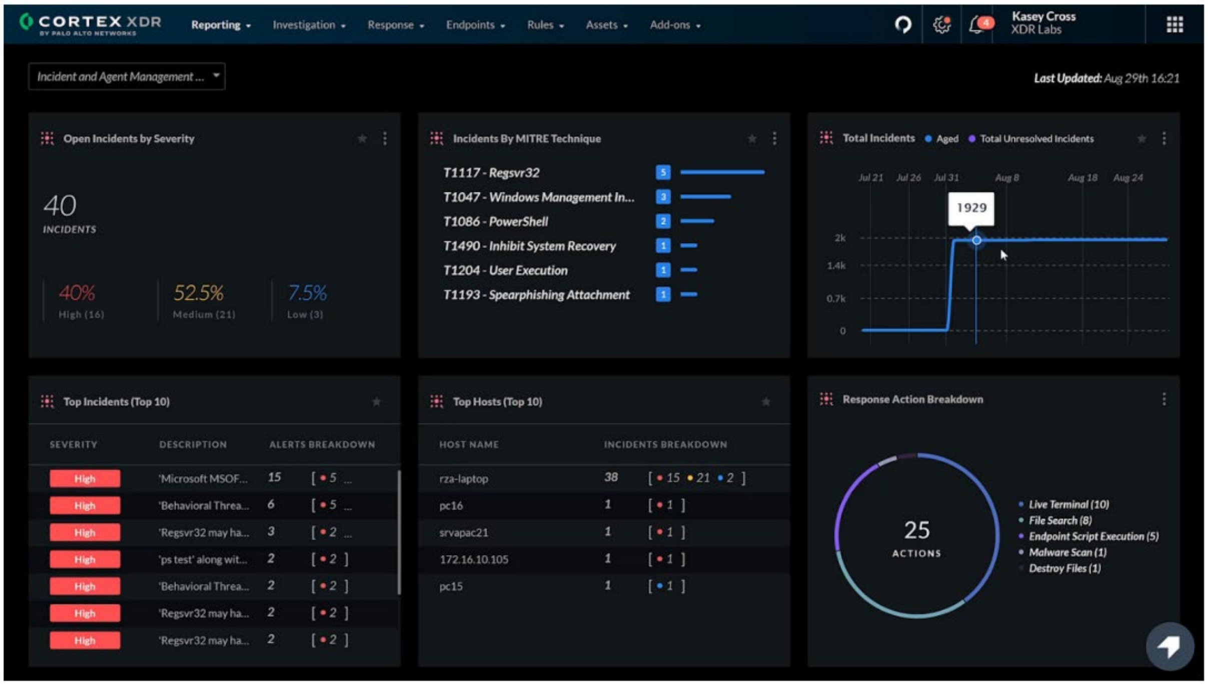
Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28) OR Alert Source = PAN NGFW,XDR Agent

		TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
●	□	Apr 6th 2021 18:01:01	win-2021-[redacted]	Administrator	Medium	XDR Agent	⊖ Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]	Administrator	Low	XDR Agent	⊖ Prevented (Blocked)	Restrictic
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]3333333	16[redacted]	Medium	XDR Agent	⊖ Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win7[redacted]	N/A	Medium	XDR Agent	⊖ Prevented (Post Detected)	Exploit
●	□	Apr 6th 2021 17:59:11	win-2021-[redacted]	N/A	Medium	XDR Agent	● Detected (Scanned)	Malware
●	□	Apr 6th 2021 17:57:42	win-2021[redacted]	N/A	High	XDR Agent	● Detected (Post Detected)	Malware
●	□	Apr 6th 2021 17:57:37	win-2021[redacted]	N/A	High	XDR Agent	● Detected (Post Detected)	Malware
●	□	Apr 6th 2021 12:36:47	win-2021[redacted]	N/A	Medium	XDR Agent	● Detected (Post Detected)	[illegible]
●	□	Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	⊖ Prevented (Blocked)	Exploit

The **Alerts** page consolidates non-informational alerts from your detection sources to enable you to efficiently and effectively triage the events you see each day. By analyzing the alert, you can better understand the cause of what happened and the full story with context to validate whether an alert requires additional action. Cortex XDR supports saving 2M alerts per 4000 agents or 20 terabytes, half of the alerts are allocated for informational alerts, and half for severity alerts.[37]

91. Every '038 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information (*e.g.*, whether attacks have been detected) and a plurality of compliance policies in the data store. For example, Palo Alto Cortex XDR determines a compliance state of the endpoint (*e.g.*, endpoints/hosts with the most incidents) based on the status information and the policies.

[37] https://es.coursera.org/lecture/palo-alto-networks-security-operations-center-fundamentals/cortex-and-secops-SJOWf



Last Updated: Aug 29th 16:21

40 INCIDENTS

40%	52.5%	7.5%
High (16)	Medium (21)	Low (3)

Technique	Count
T1117 - Regsvr32	5
T1047 - Windows Management In...	3
T1086 - PowerShell	2
T1490 - Inhibit System Recovery	1
T1204 - User Execution	1
T1193 - Spearphishing Attachment	1

Top Incidents (Top 10)

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[• 5 ...
High	'Behavioral Threa...	6	[• 5 ...
High	'Regsvr32 may ha...	3	[• 2 ...
High	'ps test' along wit...	2	[• 2]
High	'Behavioral Threa...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]

Top Hosts (Top 10)

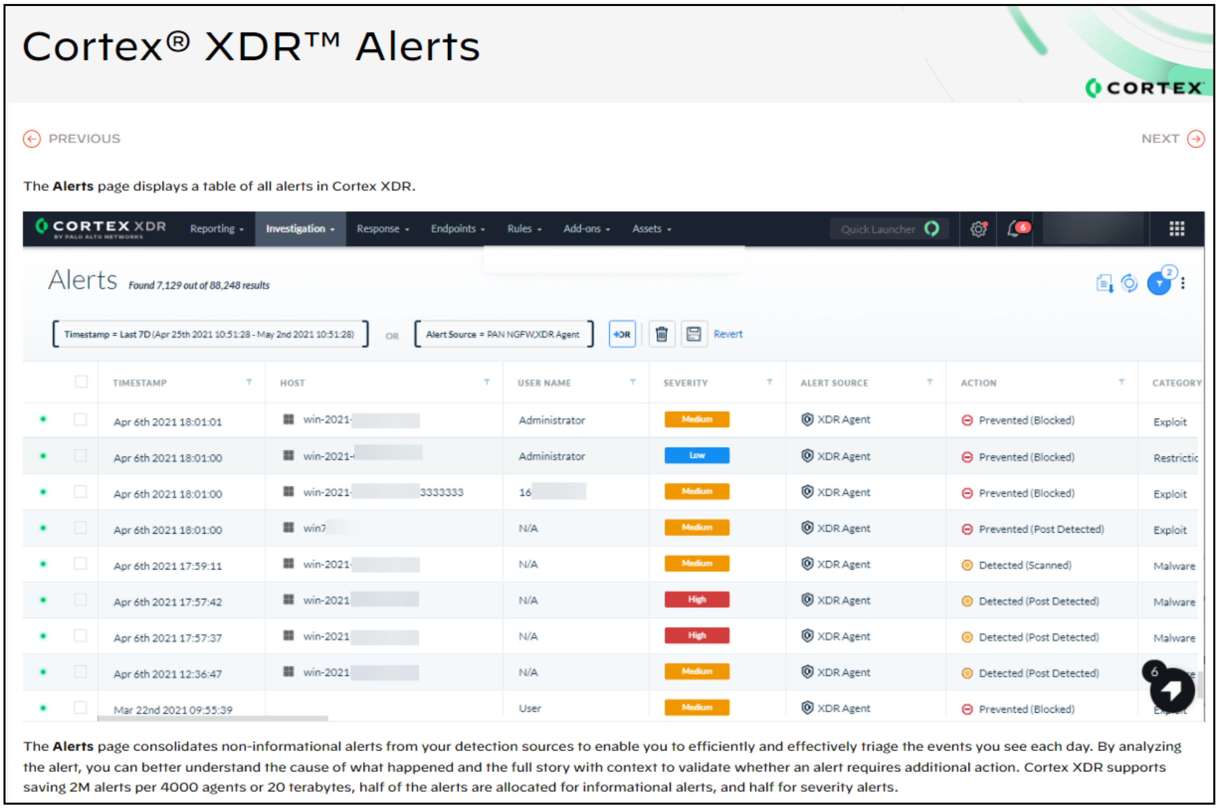
HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[• 15 • 21 • 2]
pc16	1	[• 1]
srvapac21	1	[• 1]
172.16.10.105	1	[• 1]
pc15	1	[• 1]

- Live Terminal (10)
- File Search (8)
- Endpoint Script Execution (5)
- Malware Scan (1)
- Destroy Files (1)

Figure 12: Cortex XDR dashboard[38]

92. 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, Palo Alto Cortex XDR initiates actions (*e.g.*, Actions) identified in the rules based on the compliance state which are carried out by the endpoint processor.

[38] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



Cortex® XDR™ Alerts

The **Alerts** page displays a table of all alerts in Cortex XDR.

Alerts *Found 7,129 out of 88,248 results*

Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28) OR Alert Source = PAN NGFW,XDR Agent

	□	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
●	□	Apr 6th 2021 18:01:01	win-2021-[redacted]	Administrator	Medium	XDR Agent	Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]	Administrator	Low	XDR Agent	Prevented (Blocked)	Restrictic
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]3333333	16[redacted]	Medium	XDR Agent	Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win7[redacted]	N/A	Medium	XDR Agent	Prevented (Post Detected)	Exploit
●	□	Apr 6th 2021 17:59:11	win-2021-[redacted]	N/A	Medium	XDR Agent	Detected (Scanned)	Malware
●	□	Apr 6th 2021 17:57:42	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
●	□	Apr 6th 2021 17:57:37	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
●	□	Apr 6th 2021 12:36:47	win-2021[redacted]	N/A	Medium	XDR Agent	Detected (Post Detected)	[illegible]
●	□	Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	Prevented (Blocked)	Exploit

The **Alerts** page consolidates non-informational alerts from your detection sources to enable you to efficiently and effectively triage the events you see each day. By analyzing the alert, you can better understand the cause of what happened and the full story with context to validate whether an alert requires additional action. Cortex XDR supports saving 2M alerts per 4000 agents or 20 terabytes, half of the alerts are allocated for informational alerts, and half for severity alerts.

[39]

93. Defendant has and continues to indirectly infringe one or more claims of the '038 Patent by knowingly and intentionally inducing others, including Palo Alto 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 Malicious Process Prevention and Behavioral Threat Protection features).

94. Defendant, with knowledge that these products, or the use thereof, infringe the '038 Patent at least as of the date of this 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.

[39] https://es.coursera.org/lecture/palo-alto-networks-security-operations-center-fundamentals/cortex-and-secops-SJOWf

95. Defendant has 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.

96. 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.

97. 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.

COUNT VI
(Infringement of the ’948 Patent)

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

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

100. Defendant has and continues to directly infringe the ’948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’948 Patent. Such products incorporate the Malicious Process Prevention and Behavioral Threat Protection features and include at least the Palo Alto Cortex 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.

101. Every ’948 Accused Product practices a method of providing real-time operational integrity of an application on a native computing environment. For example, the Palo Alto Cortex XDR incorporates Malicious Process Prevention and Behavioral Threat Protection.

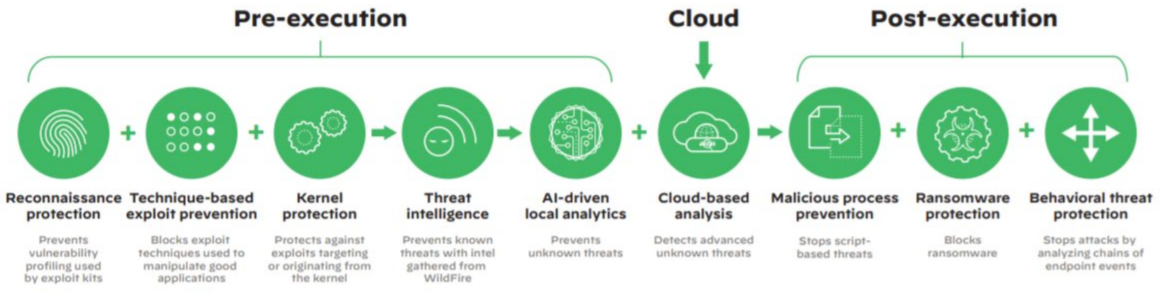
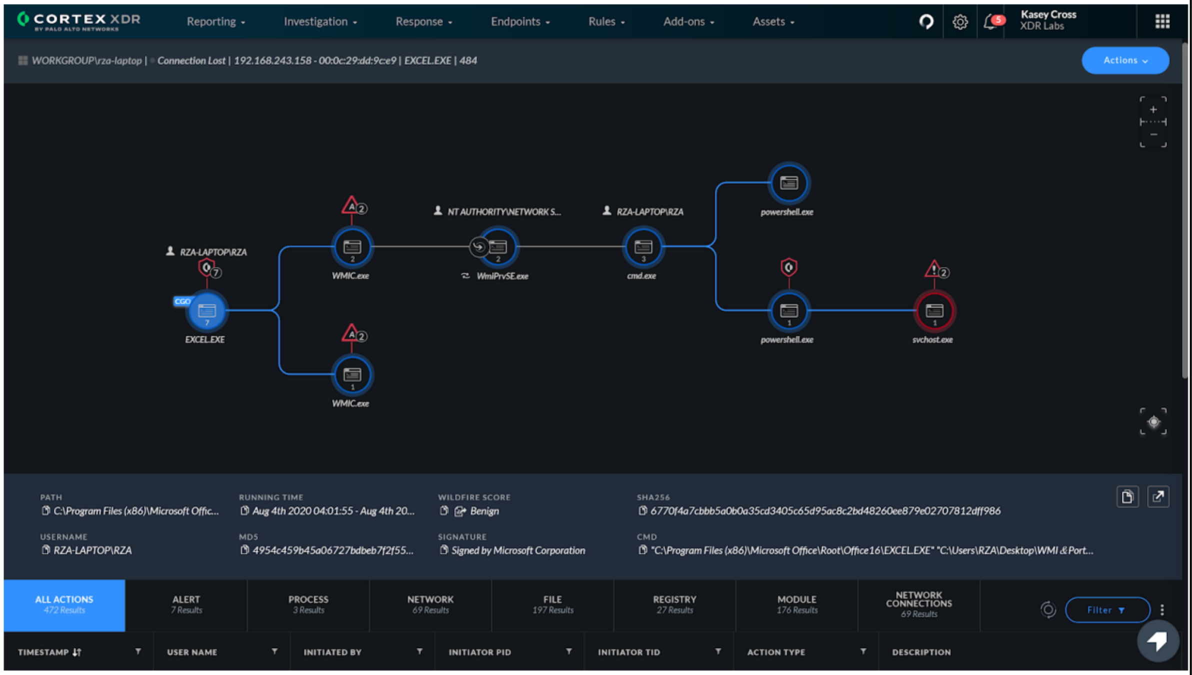

Pre-execution
Cloud
Post-execution
Reconnaissance protection
Prevents vulnerability profiling used by exploit kits
Technique-based exploit prevention
Blocks exploit techniques used to manipulate good applications
Kernel protection
Protects against exploits targeting or originating from the kernel
Threat intelligence
Prevents known threats with intel gathered from WildFire
AI-driven local analytics
Prevents unknown threats
Cloud-based analysis
Detects advanced unknown threats
Malicious process prevention
Stops script-based threats
Ransomware protection
Blocks ransomware
Behavioral threat protection
Stops attacks by analyzing chains of endpoint events

Figure 5: Automatically preventing malware, exploits, and fileless attacks [40]

[40] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

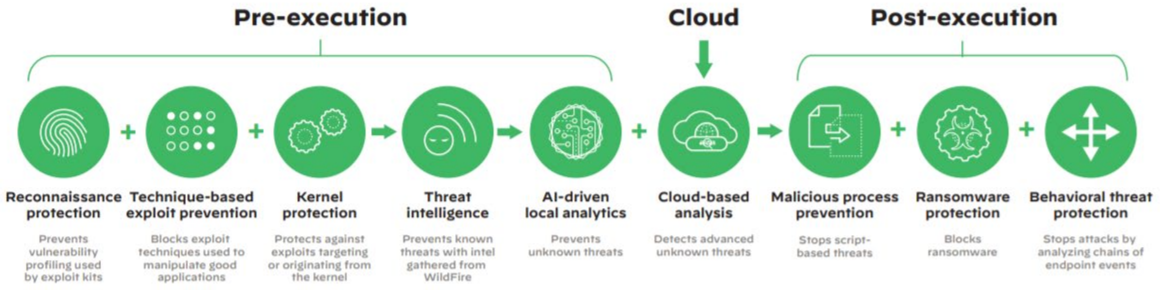
PATH: C:\Program Files (x86)\Microsoft Offic...
RUNNING TIME: Aug 4th 2020 04:01:55 - Aug 4th 20...
WILDFIRE SCORE: Benign
SHA256: 6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986
USERNAME: RZA-LAPTOP\RZA
MD5: 4954c459b45a06727bdbeb7f2f55...
SIGNATURE: Signed by Microsoft Corporation
CMD: "C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

ALL ACTIONS	ALERT	PROCESS	NETWORK	FILE	REGISTRY	MODULE	NETWORK CONNECTIONS
472 Results	7 Results	3 Results	69 Results	197 Results	27 Results	176 Results	69 Results

TIMESTAMP	USER NAME	INITIATED BY	INITIATOR PID	INITIATOR TID	ACTION TYPE	DESCRIPTION

Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR[41]

102. 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, Palo Alto Cortex XDR monitors for malware, exploits, and fileless attacks and follows defined application policies.


Pre-execution

Cloud

Post-execution

Reconnaissance protection
Prevents vulnerability profiling used by exploit kits

Technique-based exploit prevention
Blocks exploit techniques used to manipulate good applications

Kernel protection
Protects against exploits targeting or originating from the kernel

Threat intelligence
Prevents known threats with intel gathered from WildFire

AI-driven local analytics
Prevents unknown threats

Cloud-based analysis
Detects advanced unknown threats

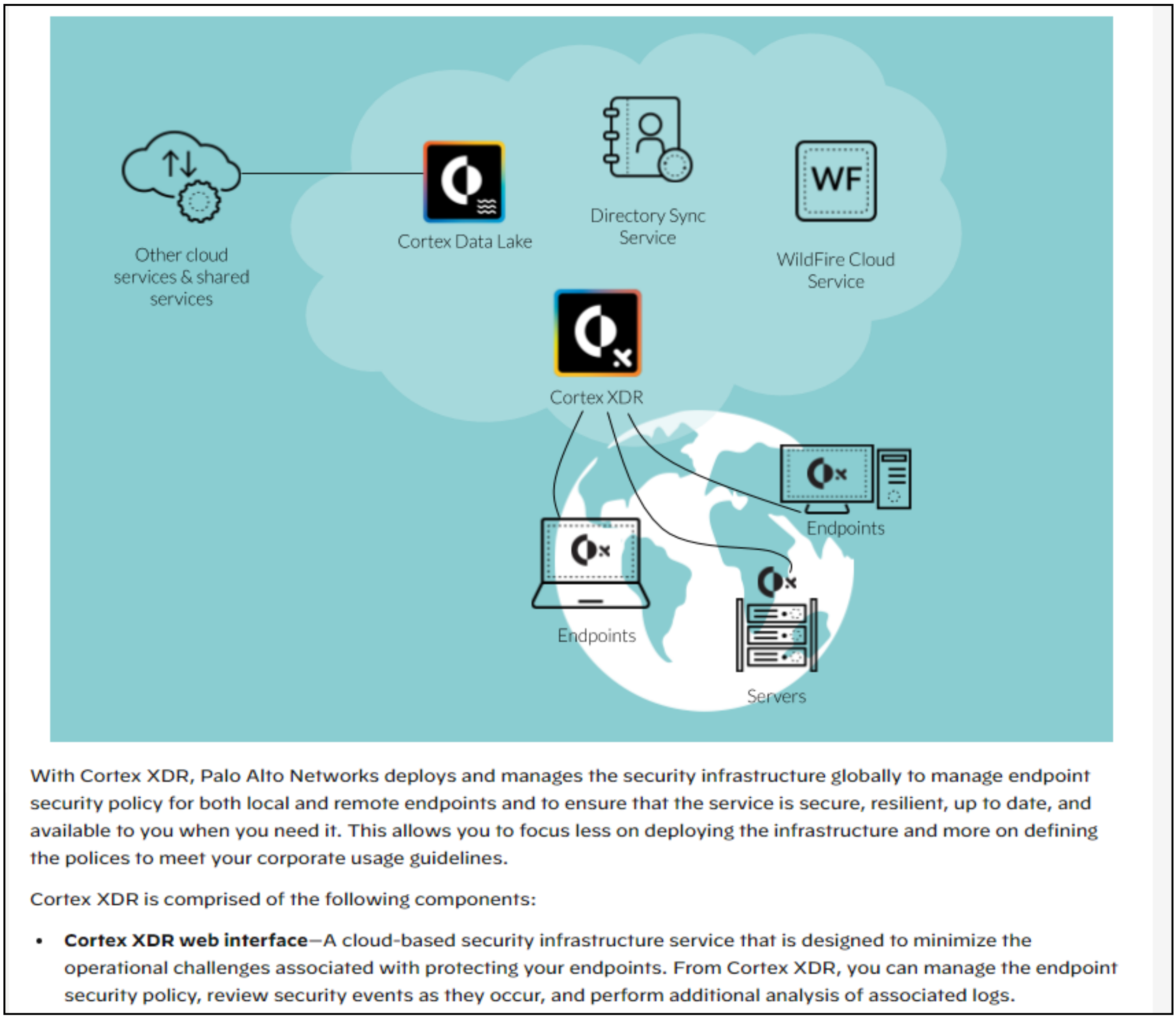
Malicious process prevention
Stops script-based threats

Ransomware protection
Blocks ransomware

Behavioral threat protection
Stops attacks by analyzing chains of endpoint events

Figure 5: Automatically preventing malware, exploits, and fileless attacks[42]

[41] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf
[42] *Id.*



With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

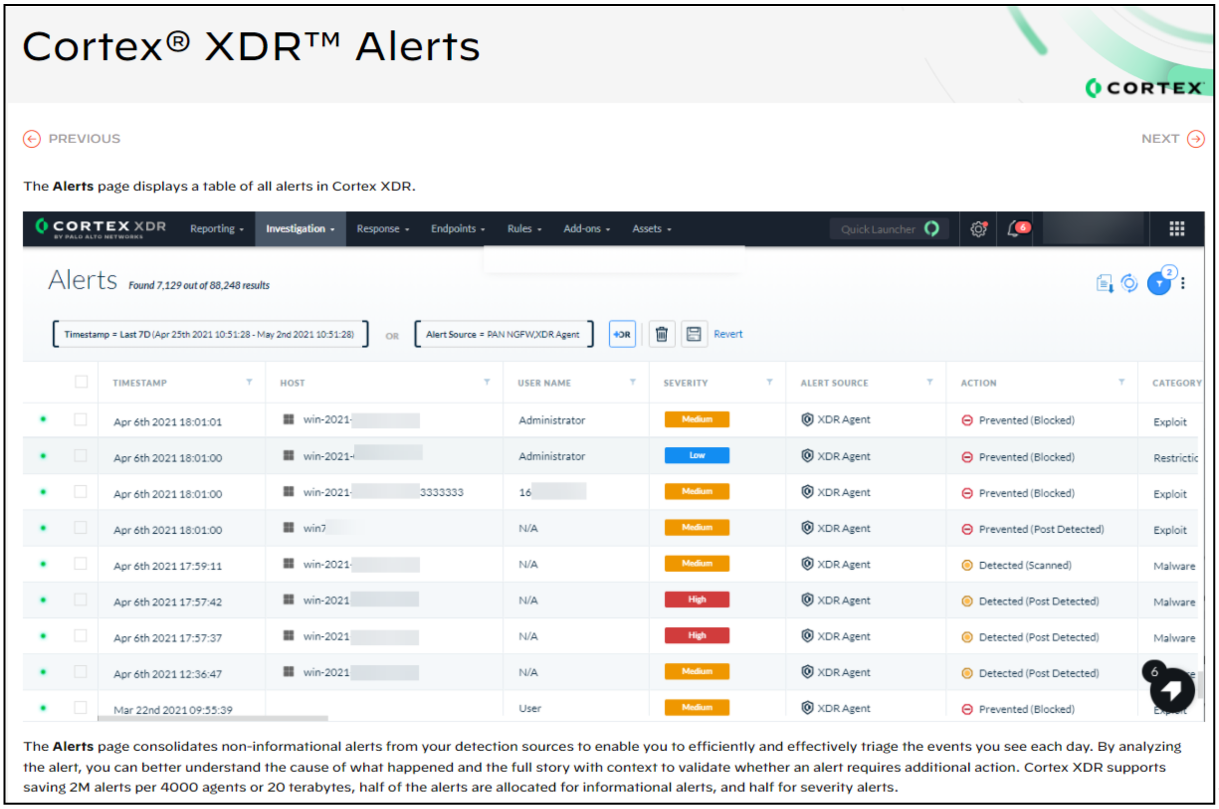
Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

[43]

103. 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, Palo Alto Cortex XDR security agents generate behavior based events for determining the real-time operational integrity of the application executing on the native computer environment.

[43] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html



Cortex® XDR™ Alerts

The **Alerts** page displays a table of all alerts in Cortex XDR.

Alerts *Found 7,129 out of 88,248 results*

[Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28)] OR [Alert Source = PAN NGFW,XDR Agent] +OR

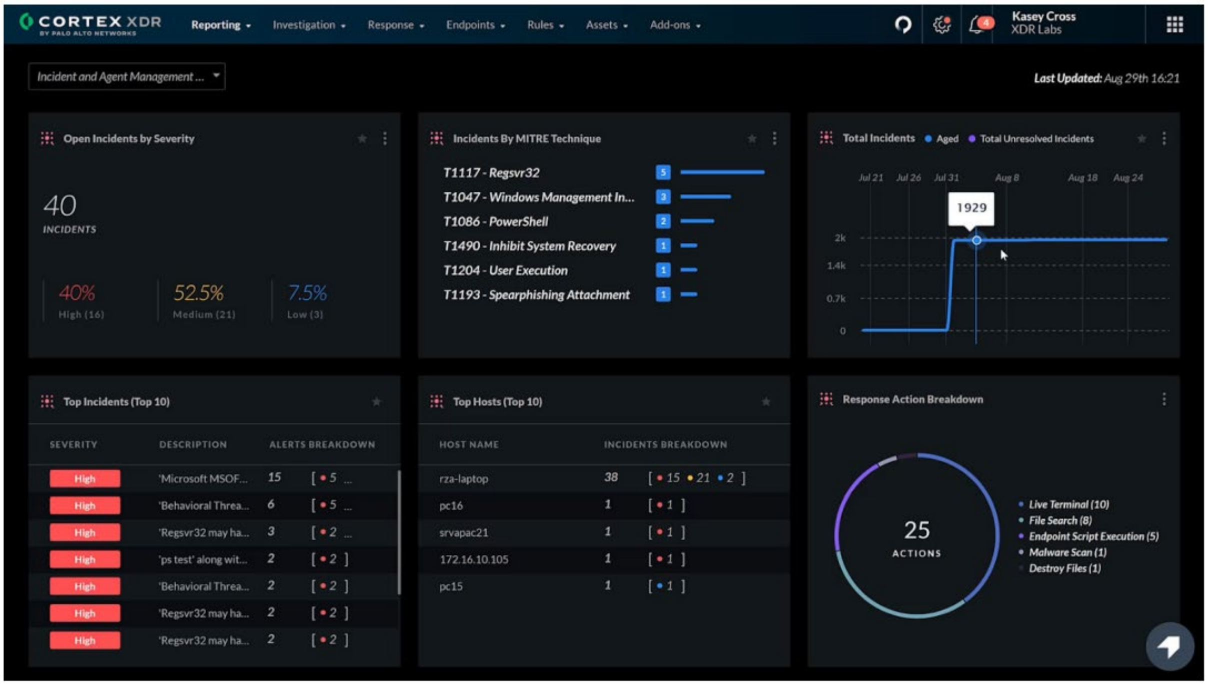
	□	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
●	□	Apr 6th 2021 18:01:01	win-2021-[redacted]	Administrator	Medium	XDR Agent	Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]	Administrator	Low	XDR Agent	Prevented (Blocked)	Restrictic
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]3333333	16[redacted]	Medium	XDR Agent	Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win7[redacted]	N/A	Medium	XDR Agent	Prevented (Post Detected)	Exploit
●	□	Apr 6th 2021 17:59:11	win-2021-[redacted]	N/A	Medium	XDR Agent	Detected (Scanned)	Malware
●	□	Apr 6th 2021 17:57:42	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
●	□	Apr 6th 2021 17:57:37	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
●	□	Apr 6th 2021 12:36:47	win-2021[redacted]	N/A	Medium	XDR Agent	Detected (Post Detected)	[illegible]
●	□	Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	Prevented (Blocked)	Exploit

The **Alerts** page consolidates non-informational alerts from your detection sources to enable you to efficiently and effectively triage the events you see each day. By analyzing the alert, you can better understand the cause of what happened and the full story with context to validate whether an alert requires additional action. Cortex XDR supports saving 2M alerts per 4000 agents or 20 terabytes, half of the alerts are allocated for informational alerts, and half for severity alerts.

[44]

104. 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.

[44] https://es.coursera.org/lecture/palo-alto-networks-security-operations-center-fundamentals/cortex-and-secops-SJOWf



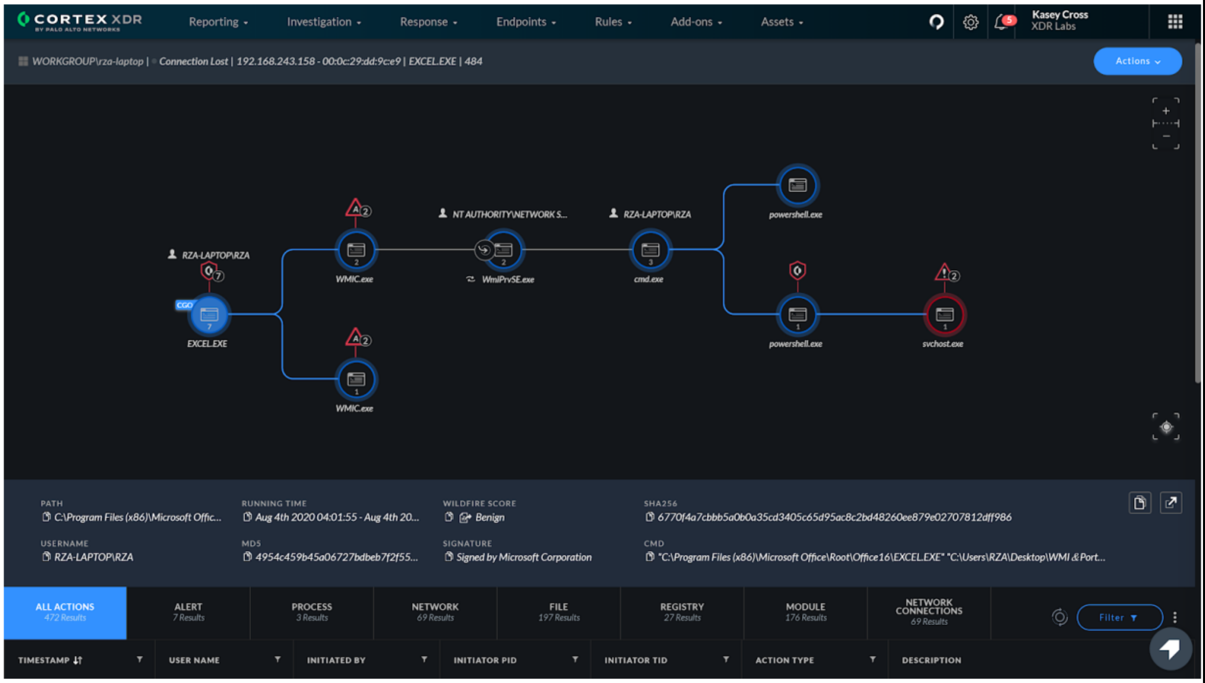
SEVERITY	DESCRIPTION	ALERTS BREAKDOWN
High	'Microsoft MSOF...	15 [● 5 ...
High	'Behavioral Threa...	6 [● 5 ...
High	'Regsvr32 may ha...	3 [● 2 ...
High	'ps test' along wit...	2 [● 2]
High	'Behavioral Threa...	2 [● 2]
High	'Regsvr32 may ha...	2 [● 2]
High	'Regsvr32 may ha...	2 [● 2]

HOST NAME	INCIDENTS BREAKDOWN
rza-laptop	38 [● 15 ● 21 ● 2]
pc16	1 [● 1]
srvapac21	1 [● 1]
172.16.10.105	1 [● 1]
pc15	1 [● 1]

Figure 12: Cortex XDR dashboard [45]

105. 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, Palo Alto Cortex XDR includes several display options for showing real-time status indications for the operational integrity of the application.

[45] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



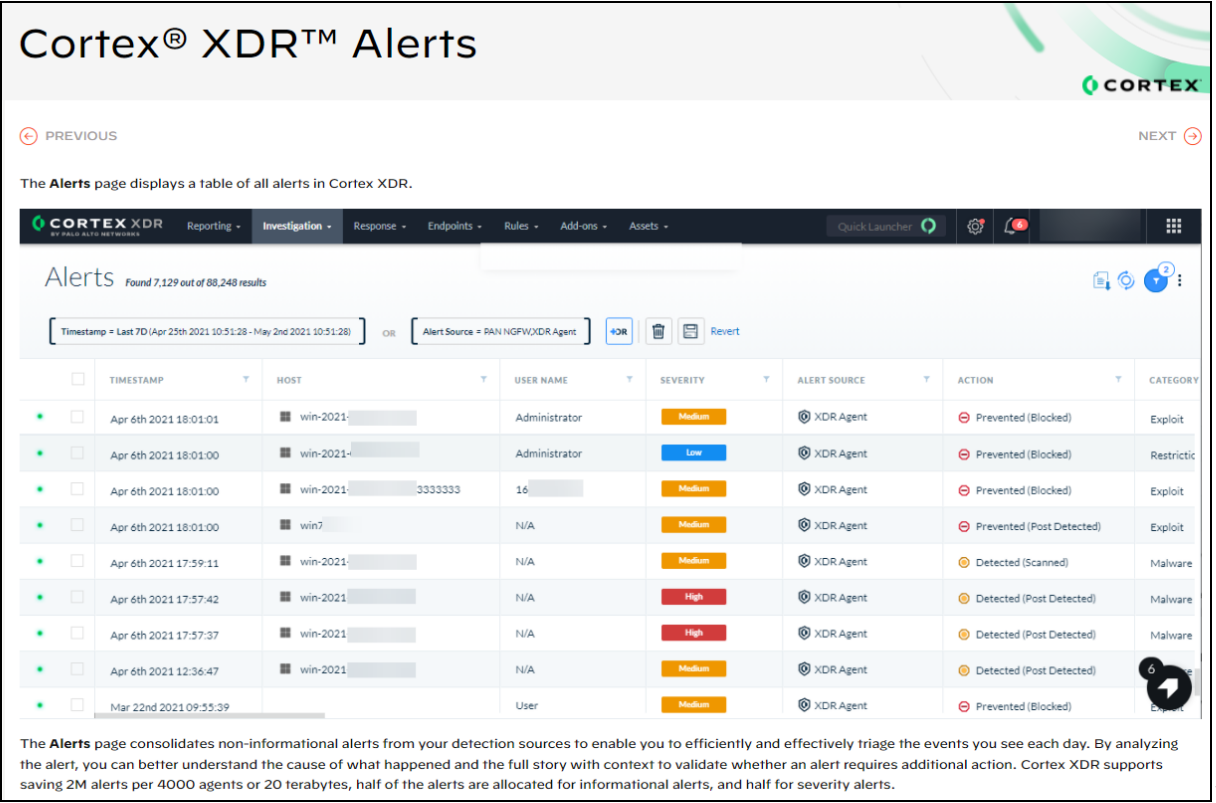
WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

PATH: C:\Program Files (x86)\Microsoft Offic...
RUNNING TIME: Aug 4th 2020 04:01:55 - Aug 4th 20...
WILDFIRE SCORE: Benign
SHA256: 6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986
USERNAME: RZA-LAPTOP\RZA
MD5: 4954c459b45a06727bdbeb7f2f55...
SIGNATURE: Signed by Microsoft Corporation
CMD: "C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

ALL ACTIONS	ALERT	PROCESS	NETWORK	FILE	REGISTRY	MODULE	NETWORK CONNECTIONS
472 Results	7 Results	3 Results	69 Results	197 Results	27 Results	176 Results	69 Results

TIMESTAMP	USER NAME	INITIATED BY	INITIATOR PID	INITIATOR TID	ACTION TYPE	DESCRIPTION

Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR [46]



Cortex® XDR™ Alerts

The **Alerts** page displays a table of all alerts in Cortex XDR.

Alerts Found 7,129 out of 88,248 results

Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28) OR Alert Source = PAN NGFW,XDR Agent

TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
Apr 6th 2021 18:01:01	win-2021-[redacted]	Administrator	Medium	XDR Agent	Prevented (Blocked)	Exploit
Apr 6th 2021 18:01:00	win-2021-[redacted]	Administrator	Low	XDR Agent	Prevented (Blocked)	Restrictic
Apr 6th 2021 18:01:00	win-2021-[redacted]3333333	16[redacted]	Medium	XDR Agent	Prevented (Blocked)	Exploit
Apr 6th 2021 18:01:00	win7[redacted]	N/A	Medium	XDR Agent	Prevented (Post Detected)	Exploit
Apr 6th 2021 17:59:11	win-2021-[redacted]	N/A	Medium	XDR Agent	Detected (Scanned)	Malware
Apr 6th 2021 17:57:42	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
Apr 6th 2021 17:57:37	win-2021[redacted]	N/A	High	XDR Agent	Detected (Post Detected)	Malware
Apr 6th 2021 12:36:47	win-2021[redacted]	N/A	Medium	XDR Agent	Detected (Post Detected)	[illegible]
Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	Prevented (Blocked)	Exploit

The **Alerts** page consolidates non-informational alerts from your detection sources to enable you to efficiently and effectively triage the events you see each day. By analyzing the alert, you can better understand the cause of what happened and the full story with context to validate whether an alert requires additional action. Cortex XDR supports saving 2M alerts per 4000 agents or 20 terabytes, half of the alerts are allocated for informational alerts, and half for severity alerts. [47]

[46] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

[47] https://es.coursera.org/lecture/palo-alto-networks-security-operations-center-fundamentals/cortex-and-secops-SJOWf

106. Defendant has and continues to indirectly infringe one or more claims of the ’948 Patent by knowingly and intentionally inducing others, including Palo Alto 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 ’948 Accused Products (*e.g.*, products incorporating the Malicious Process Prevention and Behavioral Threat Protection features).

107. Defendant, with knowledge that these products, or the use thereof, infringe the ’948 Patent at least as of the date of this 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.

108. Defendant has 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.

109. 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.

110. 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 VII
(Infringement of the ’616 Patent)

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

112. 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.

113. Defendant has and continues to directly infringe the ’616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’616 Patent. Such products incorporate the Malicious Process Prevention and Behavioral Threat Protection features and include at least the Palo Alto Cortex XDR (the "’616 Accused Products") which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

114. 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, Palo Alto Cortex XDR Agents provide operational integrity of a system.

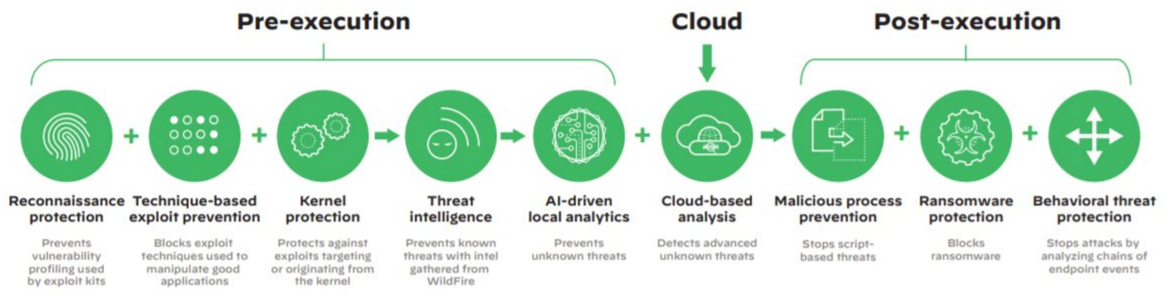
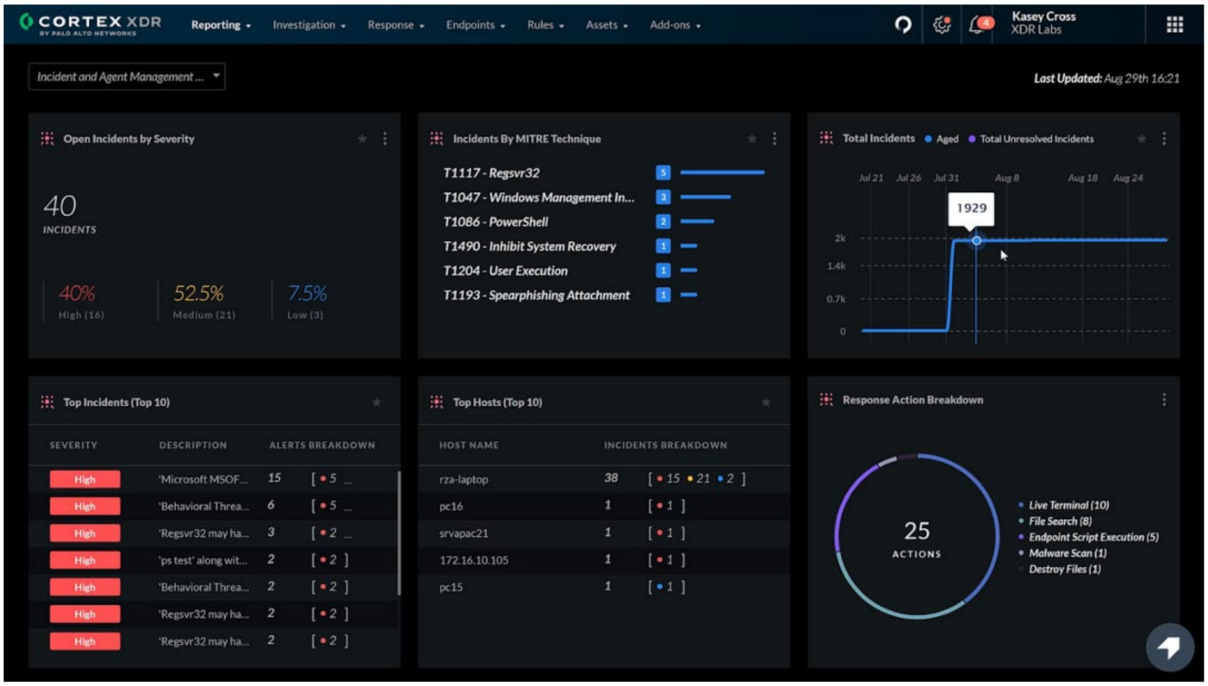

Pre-execution
Cloud
Post-execution
Reconnaissance protection
Prevents vulnerability profiling used by exploit kits
Technique-based exploit prevention
Blocks exploit techniques used to manipulate good applications
Kernel protection
Protects against exploits targeting or originating from the kernel
Threat intelligence
Prevents known threats with intel gathered from WildFire
AI-driven local analytics
Prevents unknown threats
Cloud-based analysis
Detects advanced unknown threats
Malicious process prevention
Stops script-based threats
Ransomware protection
Blocks ransomware
Behavioral threat protection
Stops attacks by analyzing chains of endpoint events

Figure 5: Automatically preventing malware, exploits, and fileless attacks [48]



Last Updated: Aug 29th 16:21

Open Incidents by Severity

40 INCIDENTS

40% High (16) 52.5% Medium (21) 7.5% Low (3)

Incidents By MITRE Technique

T1117 - Regsvr32	5
T1047 - Windows Management In...	3
T1086 - PowerShell	2
T1490 - Inhibit System Recovery	1
T1204 - User Execution	1
T1193 - Spearphishing Attachment	1

Total Incidents ● Aged ● Total Unresolved Incidents

Top Incidents (Top 10)

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[● 5 ...
High	'Behavioral Threa...	6	[● 5 ...
High	'Regsvr32 may ha...	3	[● 2 ...
High	'ps test' along wit...	2	[● 2]
High	'Behavioral Threa...	2	[● 2]
High	'Regsvr32 may ha...	2	[● 2]
High	'Regsvr32 may ha...	2	[● 2]

Top Hosts (Top 10)

HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[● 15 ● 21 ● 2]
pc16	1	[● 1]
srvapac21	1	[● 1]
172.16.10.105	1	[● 1]
pc15	1	[● 1]

Response Action Breakdown

25 ACTIONS

- Live Terminal (10)
- File Search (8)
- Endpoint Script Execution (5)
- Malware Scan (1)
- Destroy Files (1)

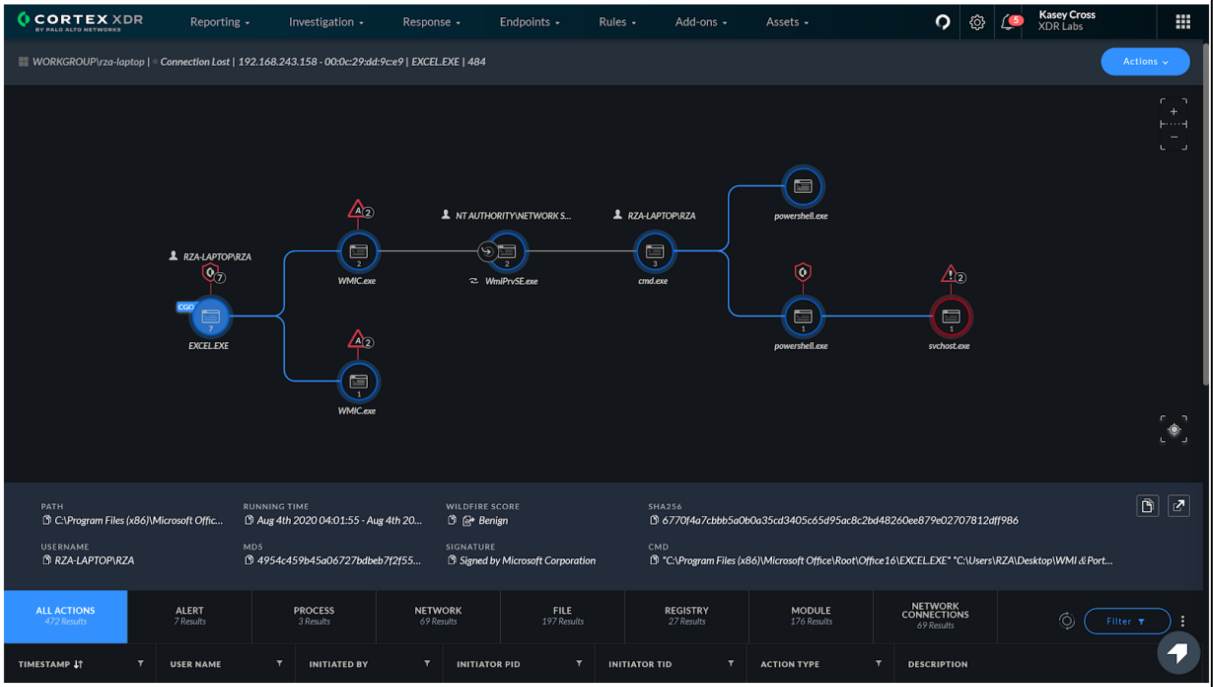
Figure 12: Cortex XDR dashboard [49]

115. Every ’616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime. For example, the security agents send events, context, and status information.

[48] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

[49] *Id.*

116. 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, Palo Alto Cortex XDR receives dynamic context including endpoint events and the applications executing on the monitored device in runtime.



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

PATH
C:\Program Files (x86)\Microsoft Offic...

RUNNING TIME
Aug 4th 2020 04:01:55 - Aug 4th 20...

WILDFIRE SCORE
Benign

SHA256
6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986

USERNAME
RZA-LAPTOP\RZA

MD5
4954c459b45a06727bdbeb7f2f55...

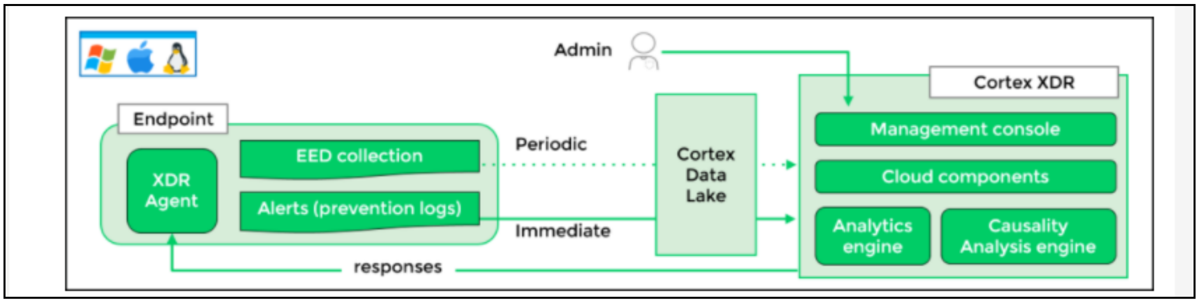
SIGNATURE
Signed by Microsoft Corporation

CMD
"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

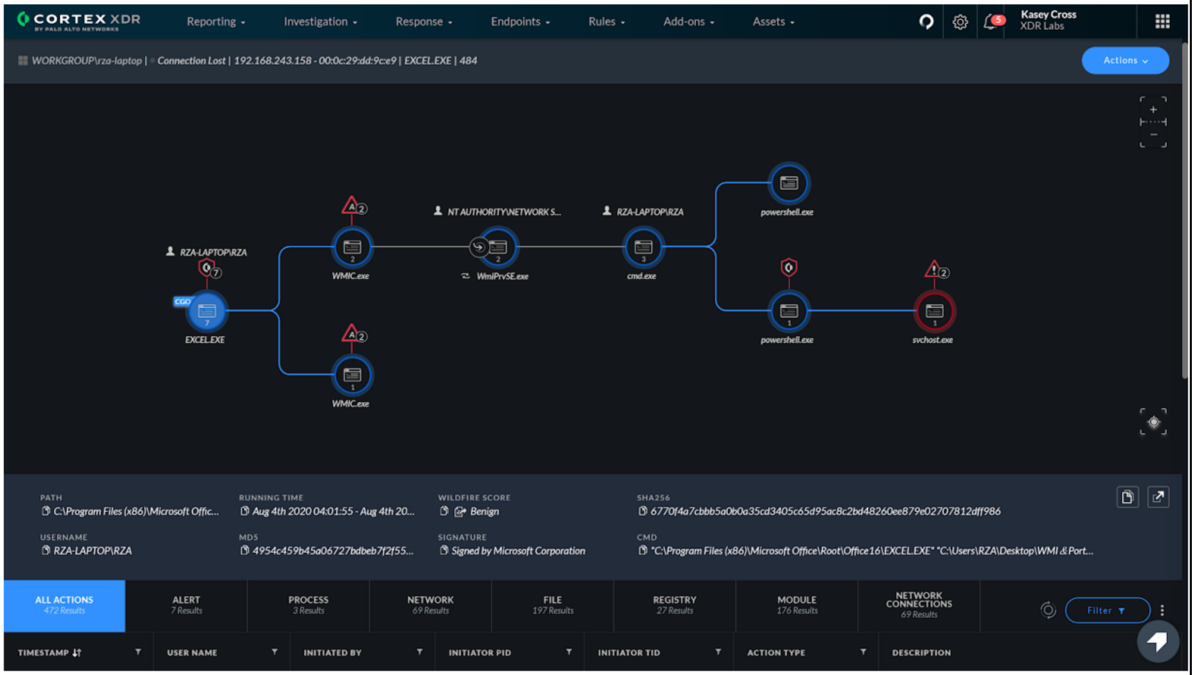
Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR [50]

117. Every ’616 Accused Product practices analyzing, by the trust orchestration server, the received endpoint events. For example, Palo Alto Cortex XDR receives endpoint events (*i.e.*, data related to potential security threats).

[50] *Id.*



[51]



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

PATH
C:\Program Files (x86)\Microsoft Offic...

RUNNING TIME
Aug 4th 2020 04:01:55 - Aug 4th 20...

WILDFIRE SCORE
Benign

SHA256
6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986

USERNAME
RZA-LAPTOP\RZA

MD5
4954c459b45a06727bdbeb7f2f55...

SIGNATURE
Signed by Microsoft Corporation

CMD
"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

ALL ACTIONS	ALERT	PROCESS	NETWORK	FILE	REGISTRY	MODULE	NETWORK CONNECTIONS
472 Results	7 Results	3 Results	69 Results	197 Results	27 Results	176 Results	69 Results

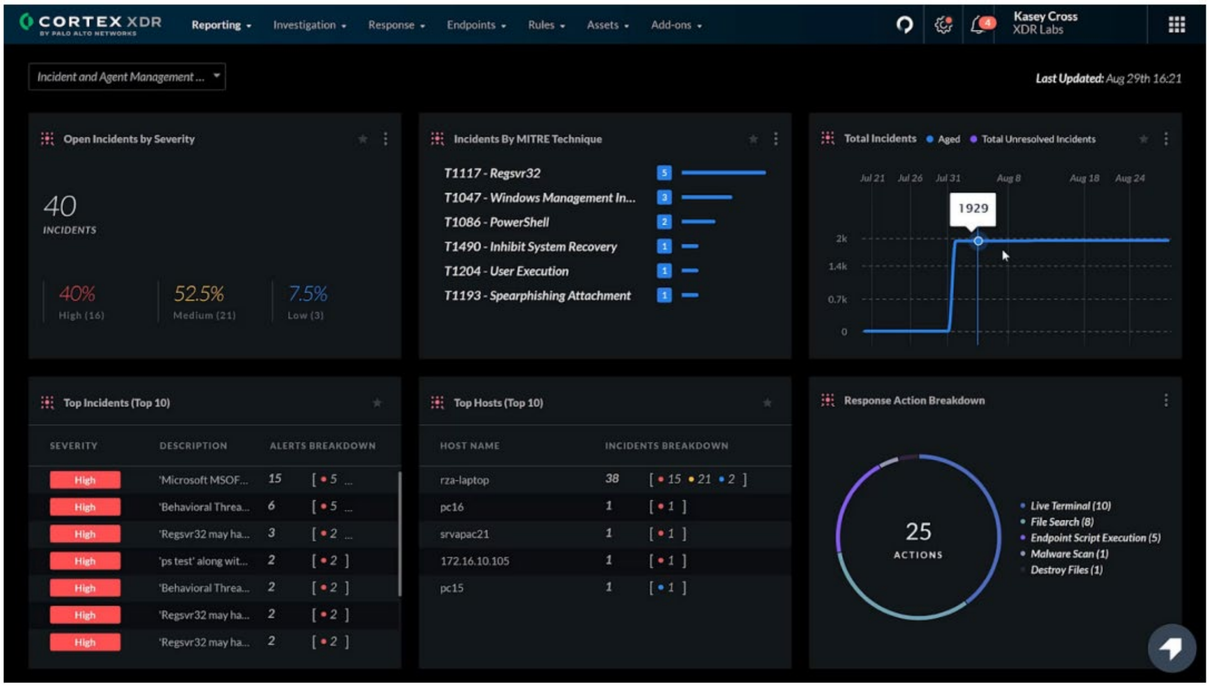
TIMESTAMP	USER NAME	INITIATED BY	INITIATOR PID	INITIATOR TID	ACTION TYPE	DESCRIPTION

Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR [52]

118. Every ’616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, Palo Alto Cortex XDR receives MITRE ATT&CK data and other third-party network endpoint assessments.

[51] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html

[52] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



Incidents By MITRE Technique	
T1117 - Regsvr32	5
T1047 - Windows Management In...	3
T1086 - PowerShell	2
T1490 - Inhibit System Recovery	1
T1204 - User Execution	1
T1193 - Spearphishing Attachment	1

Top Incidents (Top 10)

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[● 5 ...
High	'Behavioral Threa...	6	[● 5 ...
High	'Regsvr32 may ha...	3	[● 2 ...
High	'ps test' along wit...	2	[● 2]
High	'Behavioral Threa...	2	[● 2]
High	'Regsvr32 may ha...	2	[● 2]
High	'Regsvr32 may ha...	2	[● 2]

Top Hosts (Top 10)

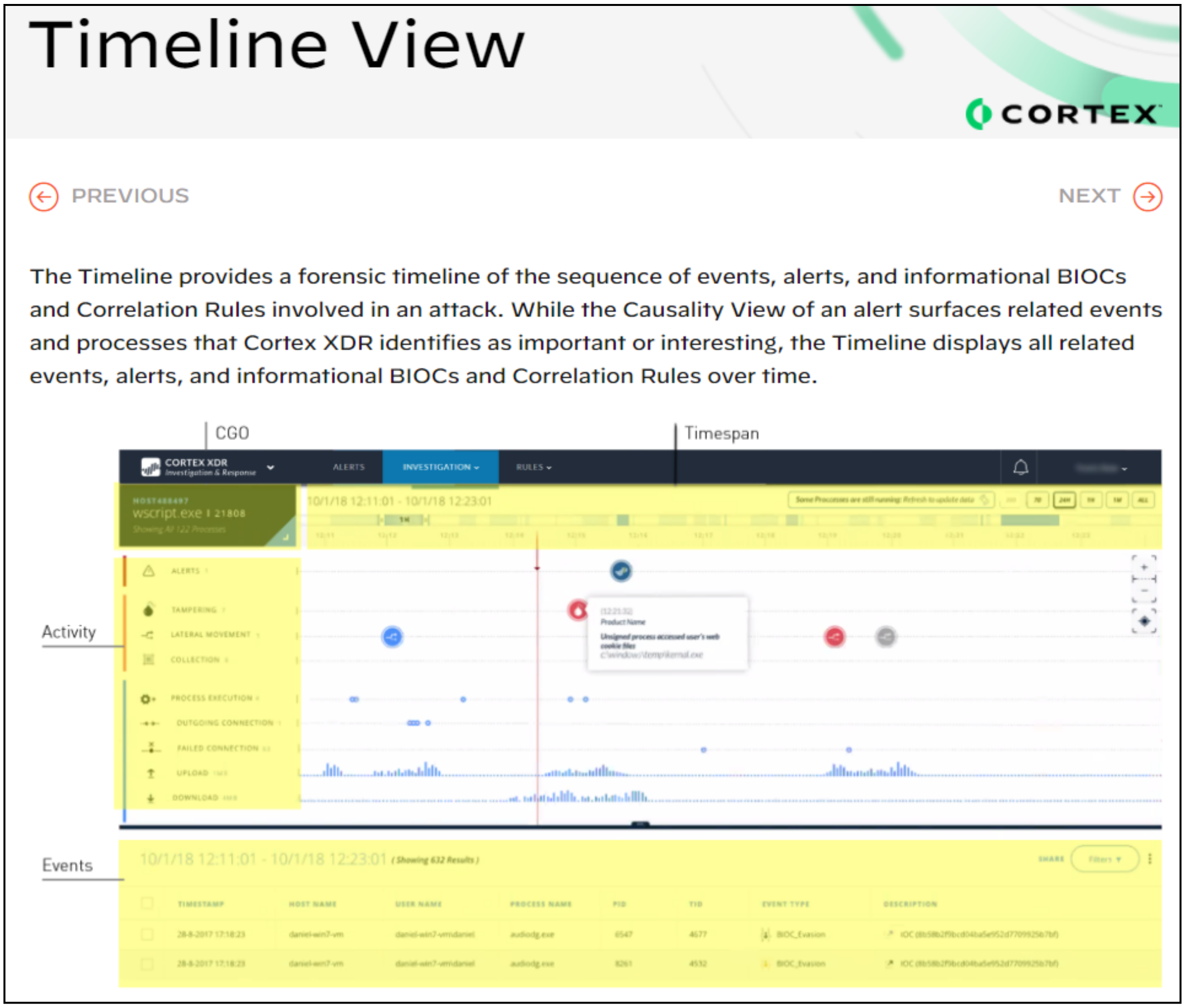
HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[● 15 ● 21 ● 2]
pc16	1	[● 1]
srvapac21	1	[● 1]
172.16.10.105	1	[● 1]
pc15	1	[● 1]

Figure 12: Cortex XDR dashboard [53]

119. 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, Palo Alto Cortex XDR generates event 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).[54]

[53] *Id.*

[54] *Id.*



Timeline View

CORTEX

PREVIOUS NEXT

The Timeline provides a forensic timeline of the sequence of events, alerts, and informational BIOCs and Correlation Rules involved in an attack. While the Causality View of an alert surfaces related events and processes that Cortex XDR identifies as important or interesting, the Timeline displays all related events, alerts, and informational BIOCs and Correlation Rules over time.

10/1/18 12:11:01 - 10/1/18 12:23:01 *(Showing 632 Results)*

TIMESTAMP	HOST NAME	USER NAME	PROCESS NAME	PID	TID	EVENT TYPE	DESCRIPTION
28-8-2017 17:18:23	daniel-win7-vm	daniel-win7-vm\daniel	audiodg.exe	6547	4677	BIOC_Evasion	IOC (8b58b2f9bcd04ba5e952d7709925b7bf)
28-8-2017 17:18:23	daniel-win7-vm	daniel-win7-vm\daniel	audiodg.exe	8261	4532	BIOC_Evasion	IOC (8b58b2f9bcd04ba5e952d7709925b7bf)

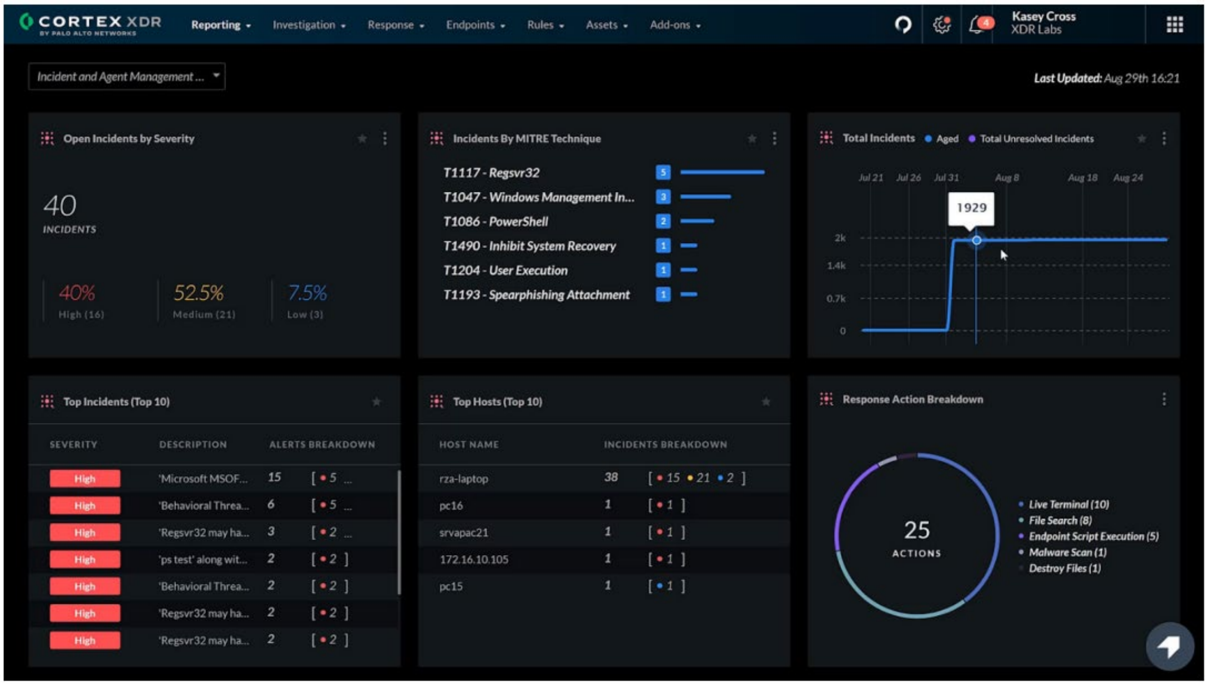
[55]

120. Every ’616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, Palo Alto Cortex XDR correlates the received endpoint events and the generated temporal events (*e.g.*, event data and assessed severity scores).[56]

121. Every ’616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, Palo Alto Cortex XDR generates an integrity profile for the system in displaying detected MITRE ATT&CK tactics and techniques.

[55] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/timeline-view.html

[56] *Id.*



Top Incidents (Top 10)

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[• 5 ...
High	'Behavioral Threa...	6	[• 5 ...
High	'Regsvr32 may ha...	3	[• 2 ...
High	'ps test' along wit...	2	[• 2]
High	'Behavioral Threa...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]

Top Hosts (Top 10)

HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[• 15 • 21 • 2]
pc16	1	[• 1]
srvapac21	1	[• 1]
172.16.10.105	1	[• 1]
pc15	1	[• 1]

Figure 12: Cortex XDR dashboard[57]

122. Defendant has and continues to indirectly infringe one or more claims of the ’616 Patent by knowingly and intentionally inducing others, including Palo Alto 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 ’616 Accused Products (*e.g.*, products incorporating the Malicious Process Prevention and Behavioral Threat Protection features).

123. Defendant, with knowledge that these products, or the use thereof, infringe the ’616 Patent at least as of the date of this 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.

[57] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

124. Defendant has 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.

125. 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.

126. 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.

COUNT VIII
(Infringement of the ’918 Patent)

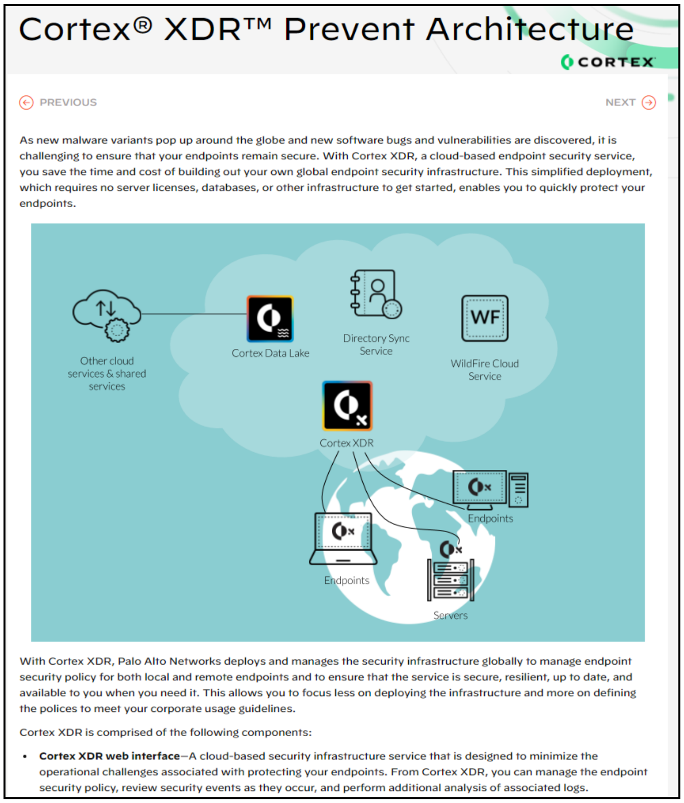
127. Paragraphs 1 through 32 are incorporated by reference as if fully set forth herein.

128. 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.

129. Defendant has and continues to directly infringe the ’918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’918 Patent. Such products incorporate the Endpoint Protection and include at least the Palo Alto Cortex XDR (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.

130. Every ’918 Accused Product is a system for controlling the operation of an endpoint. For example, the Palo Alto Cortex XDR controls the operation of endpoints through security profiles.



Cortex® XDR™ Prevent Architecture

As new malware variants pop up around the globe and new software bugs and vulnerabilities are discovered, it is challenging to ensure that your endpoints remain secure. With Cortex XDR, a cloud-based endpoint security service, you save the time and cost of building out your own global endpoint security infrastructure. This simplified deployment, which requires no server licenses, databases, or other infrastructure to get started, enables you to quickly protect your endpoints.

With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

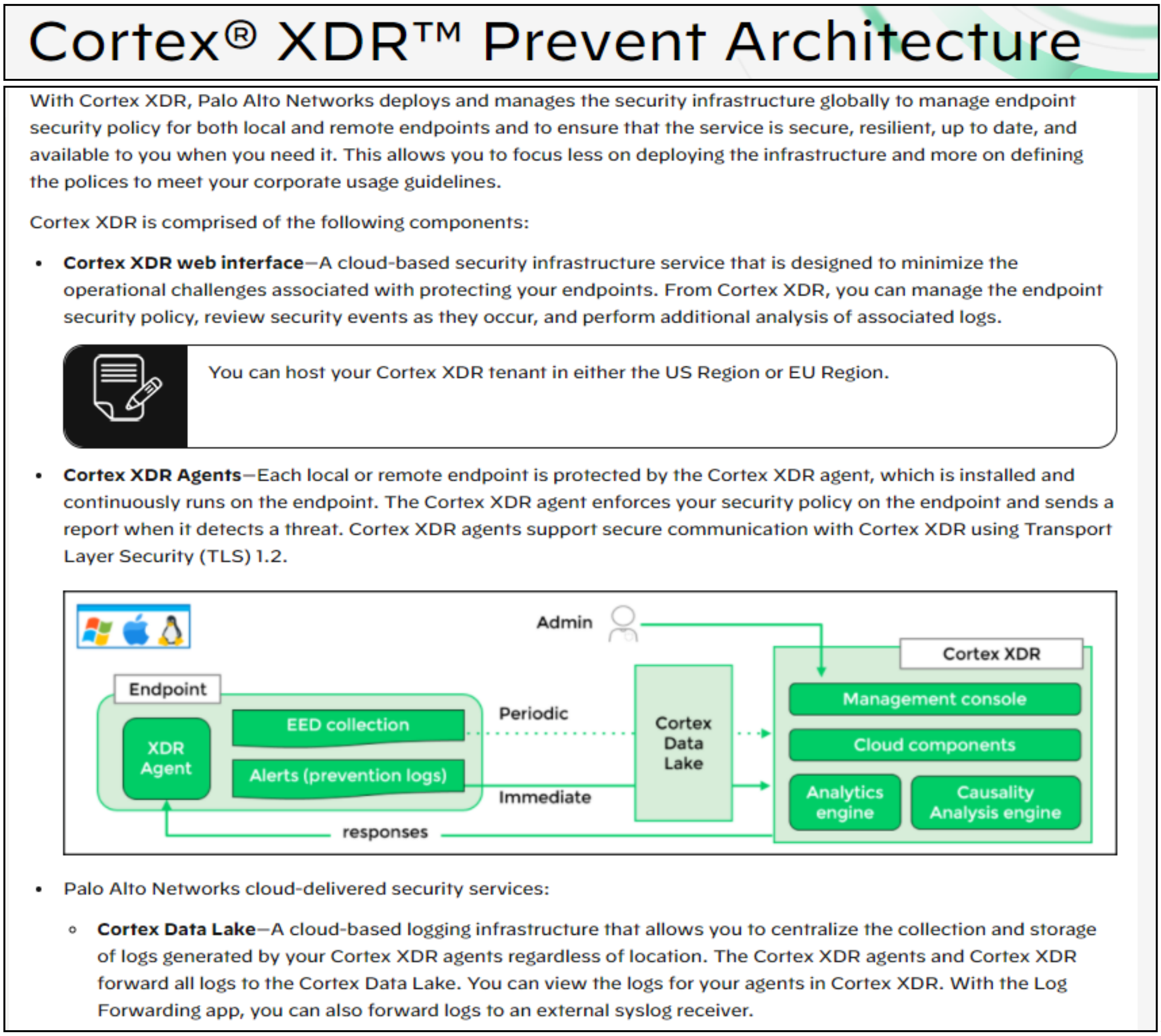
Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

[58]

[58] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html

131. 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, Palo Alto Cortex XDR comprises a user interface that allows configuration of a plurality of policies (*e.g.*, endpoint security policies, rules, profiles) at a system remote from the endpoint which are stored in the Cortex Data Lake data store.



Cortex® XDR™ Prevent Architecture

With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

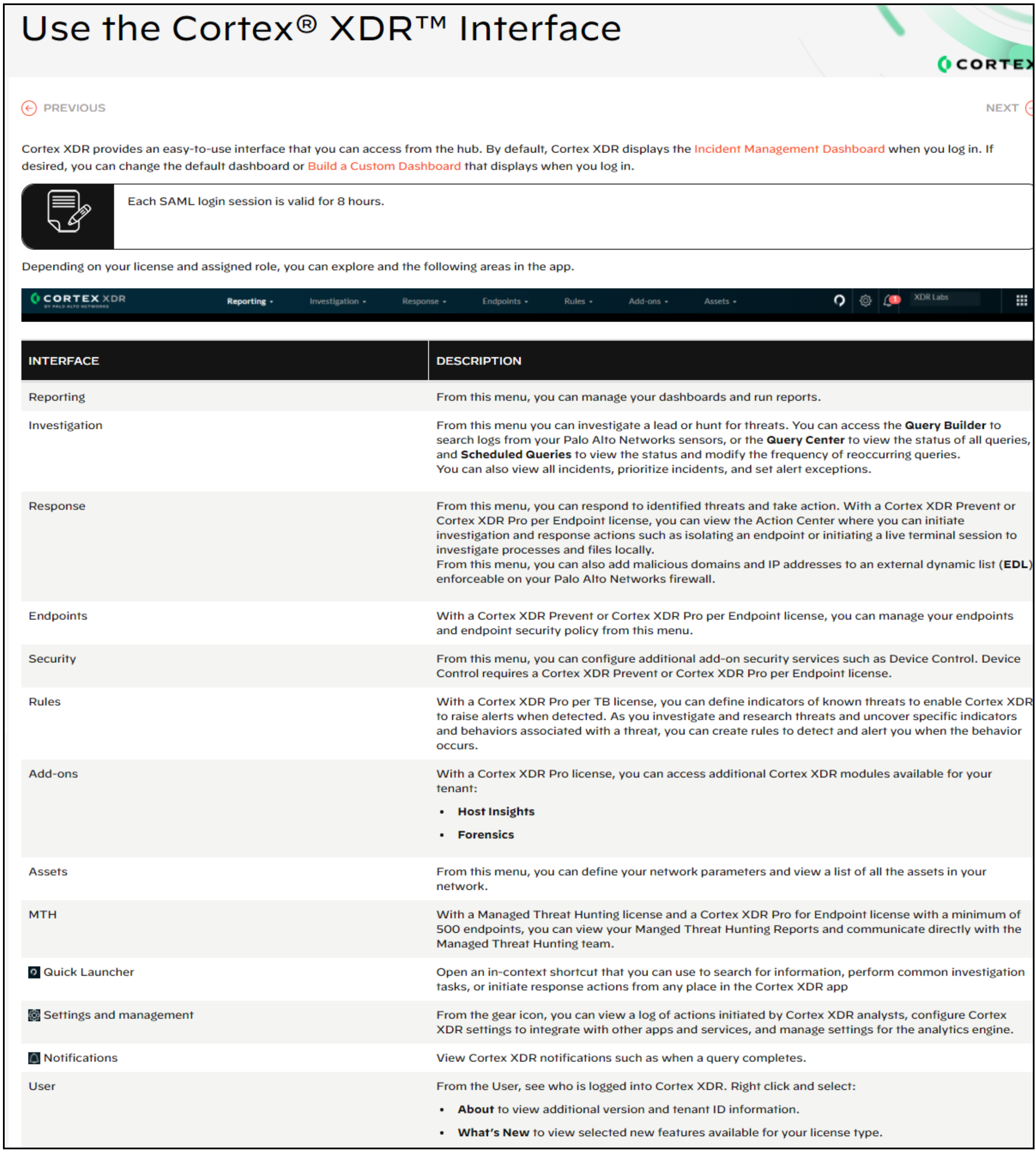
  You can host your Cortex XDR tenant in either the US Region or EU Region.

- **Cortex XDR Agents**—Each local or remote endpoint is protected by the Cortex XDR agent, which is installed and continuously runs on the endpoint. The Cortex XDR agent enforces your security policy on the endpoint and sends a report when it detects a threat. Cortex XDR agents support secure communication with Cortex XDR using Transport Layer Security (TLS) 1.2.

- Palo Alto Networks cloud-delivered security services:
  - **Cortex Data Lake**—A cloud-based logging infrastructure that allows you to centralize the collection and storage of logs generated by your Cortex XDR agents regardless of location. The Cortex XDR agents and Cortex XDR forward all logs to the Cortex Data Lake. You can view the logs for your agents in Cortex XDR. With the Log Forwarding app, you can also forward logs to an external syslog receiver.

[59]

[59] *Id.*



Use the Cortex® XDR™ Interface

Cortex XDR provides an easy-to-use interface that you can access from the hub. By default, Cortex XDR displays the Incident Management Dashboard when you log in. If desired, you can change the default dashboard or Build a Custom Dashboard that displays when you log in.

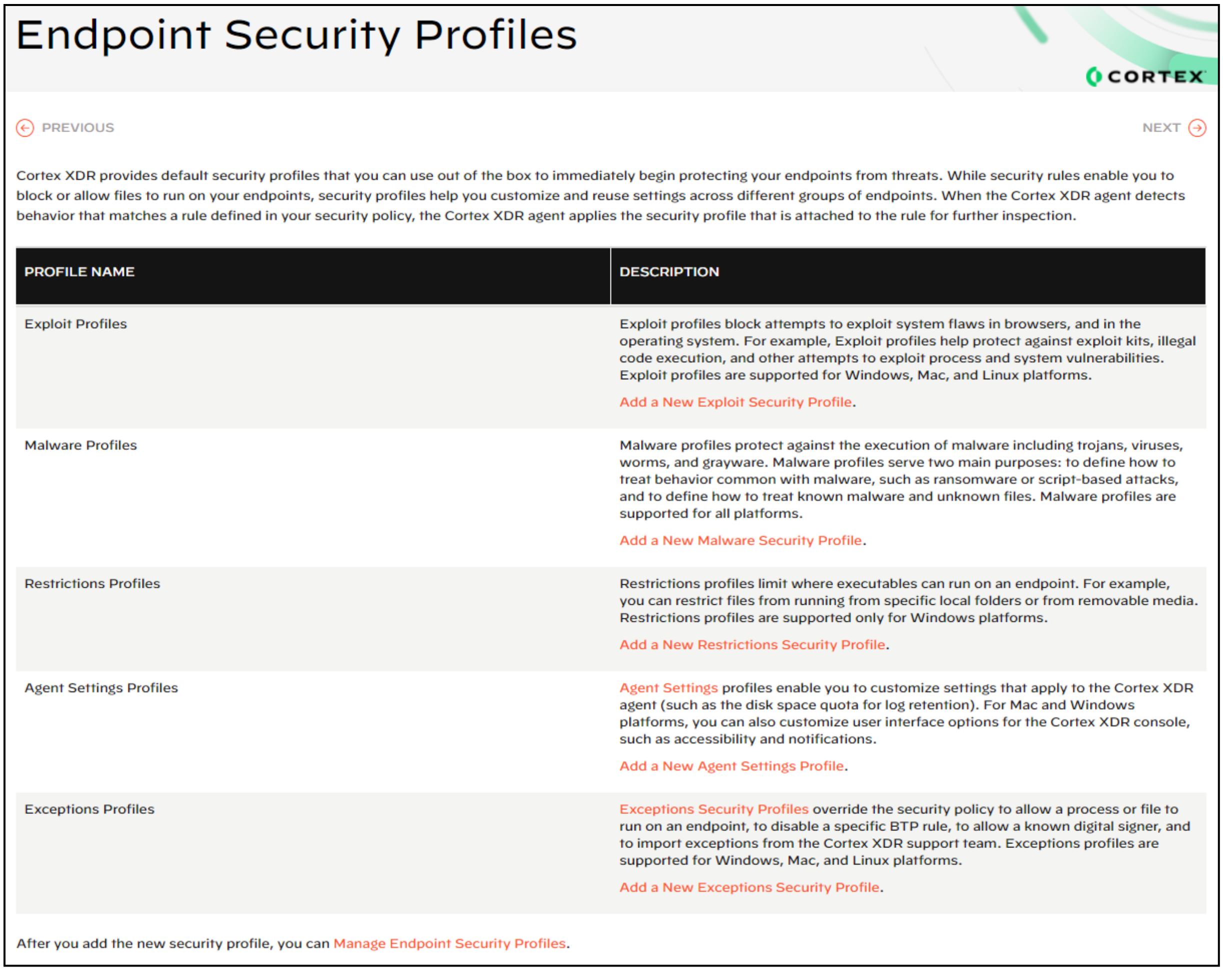
Each SAML login session is valid for 8 hours.

Depending on your license and assigned role, you can explore and the following areas in the app.

INTERFACE	DESCRIPTION
Reporting	From this menu, you can manage your dashboards and run reports.
Investigation	From this menu you can investigate a lead or hunt for threats. You can access the **Query Builder** to search logs from your Palo Alto Networks sensors, or the **Query Center** to view the status of all queries, and **Scheduled Queries** to view the status and modify the frequency of reoccurring queries. You can also view all incidents, prioritize incidents, and set alert exceptions.
Response	From this menu, you can respond to identified threats and take action. With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can view the Action Center where you can initiate investigation and response actions such as isolating an endpoint or initiating a live terminal session to investigate processes and files locally. From this menu, you can also add malicious domains and IP addresses to an external dynamic list (**EDL**) enforceable on your Palo Alto Networks firewall.
Endpoints	With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can manage your endpoints and endpoint security policy from this menu.
Security	From this menu, you can configure additional add-on security services such as Device Control. Device Control requires a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license.
Rules	With a Cortex XDR Pro per TB license, you can define indicators of known threats to enable Cortex XDR to raise alerts when detected. As you investigate and research threats and uncover specific indicators and behaviors associated with a threat, you can create rules to detect and alert you when the behavior occurs.
Add-ons	With a Cortex XDR Pro license, you can access additional Cortex XDR modules available for your tenant: • **Host Insights** • **Forensics**
Assets	From this menu, you can define your network parameters and view a list of all the assets in your network.
MTH	With a Managed Threat Hunting license and a Cortex XDR Pro for Endpoint license with a minimum of 500 endpoints, you can view your Manged Threat Hunting Reports and communicate directly with the Managed Threat Hunting team.
Quick Launcher	Open an in-context shortcut that you can use to search for information, perform common investigation tasks, or initiate response actions from any place in the Cortex XDR app
Settings and management	From the gear icon, you can view a log of actions initiated by Cortex XDR analysts, configure Cortex XDR settings to integrate with other apps and services, and manage settings for the analytics engine.
Notifications	View Cortex XDR notifications such as when a query completes.
User	From the User, see who is logged into Cortex XDR. Right click and select: • **About** to view additional version and tenant ID information. • **What's New** to view selected new features available for your license type.

[60]

[60] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/get-started-with-cortex-xdr-pro/use-cortex-xdr.html



Endpoint Security Profiles

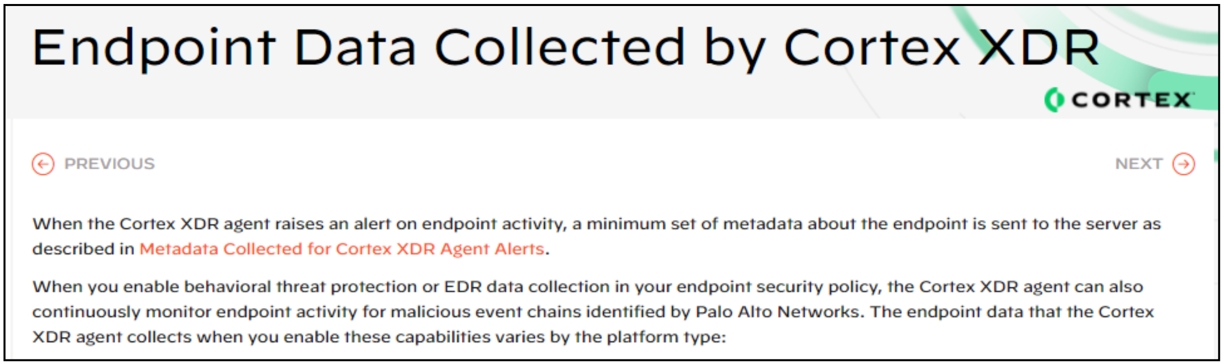
Cortex XDR provides default security profiles that you can use out of the box to immediately begin protecting your endpoints from threats. While security rules enable you to block or allow files to run on your endpoints, security profiles help you customize and reuse settings across different groups of endpoints. When the Cortex XDR agent detects behavior that matches a rule defined in your security policy, the Cortex XDR agent applies the security profile that is attached to the rule for further inspection.

PROFILE NAME	DESCRIPTION
Exploit Profiles	Exploit profiles block attempts to exploit system flaws in browsers, and in the operating system. For example, Exploit profiles help protect against exploit kits, illegal code execution, and other attempts to exploit process and system vulnerabilities. Exploit profiles are supported for Windows, Mac, and Linux platforms. Add a New Exploit Security Profile.
Malware Profiles	Malware profiles protect against the execution of malware including trojans, viruses, worms, and grayware. Malware profiles serve two main purposes: to define how to treat behavior common with malware, such as ransomware or script-based attacks, and to define how to treat known malware and unknown files. Malware profiles are supported for all platforms. Add a New Malware Security Profile.
Restrictions Profiles	Restrictions profiles limit where executables can run on an endpoint. For example, you can restrict files from running from specific local folders or from removable media. Restrictions profiles are supported only for Windows platforms. Add a New Restrictions Security Profile.
Agent Settings Profiles	Agent Settings profiles enable you to customize settings that apply to the Cortex XDR agent (such as the disk space quota for log retention). For Mac and Windows platforms, you can also customize user interface options for the Cortex XDR console, such as accessibility and notifications. Add a New Agent Settings Profile.
Exceptions Profiles	Exceptions Security Profiles override the security policy to allow a process or file to run on an endpoint, to disable a specific BTP rule, to allow a known digital signer, and to import exceptions from the Cortex XDR support team. Exceptions profiles are supported for Windows, Mac, and Linux platforms. Add a New Exceptions Security Profile.

After you add the new security profile, you can Manage Endpoint Security Profiles.[61]

132. 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, Palo Alto Cortex XDR Agents are configured to evaluate the plurality of operating conditions (*e.g.*, events) identified in the plurality of policies (*e.g.*, endpoint security policies, rules, profiles).

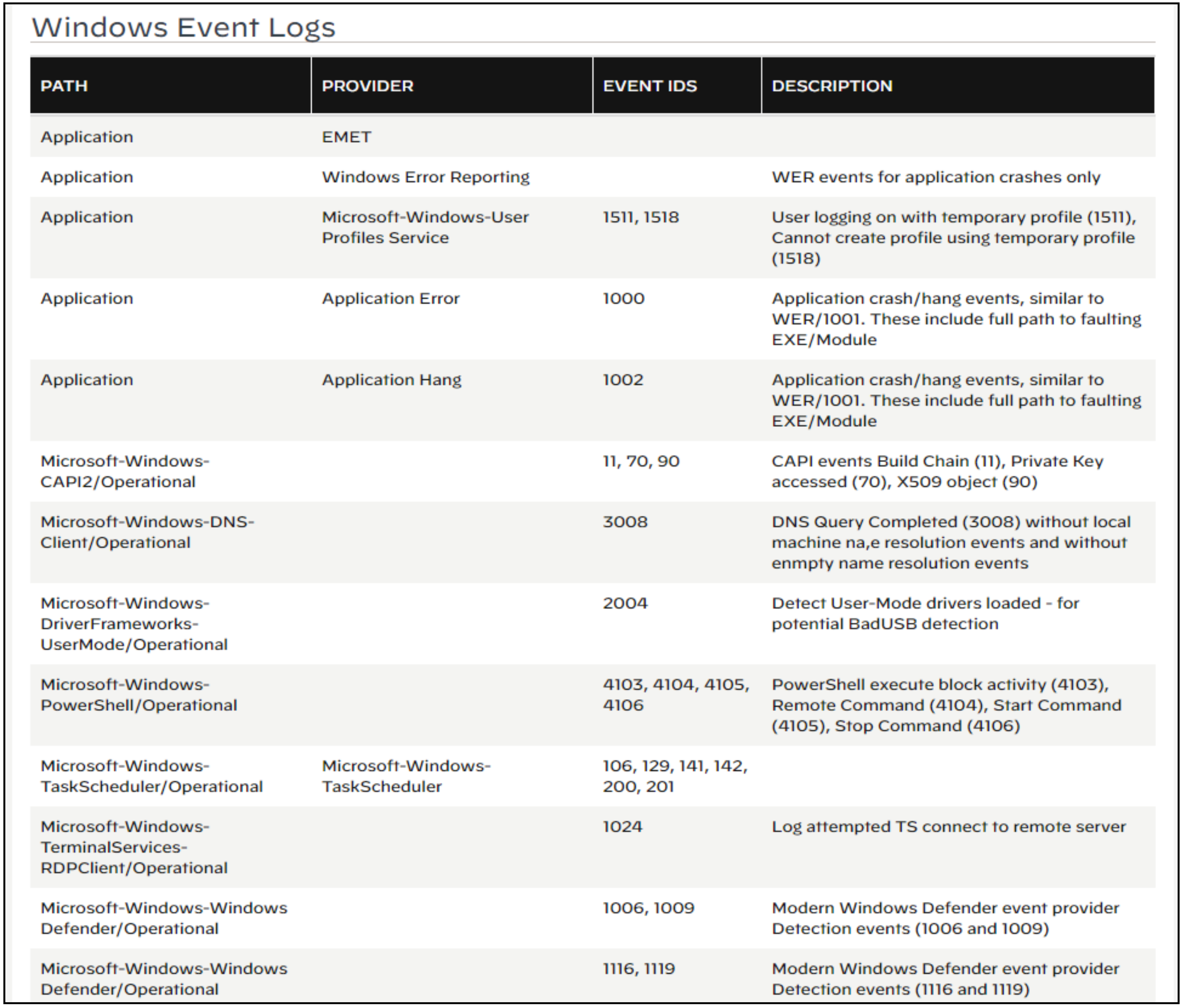
[61] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-security-profiles.html



Endpoint Data Collected by Cortex XDR

When the Cortex XDR agent raises an alert on endpoint activity, a minimum set of metadata about the endpoint is sent to the server as described in Metadata Collected for Cortex XDR Agent Alerts.

When you enable behavioral threat protection or EDR data collection in your endpoint security policy, the Cortex XDR agent can also continuously monitor endpoint activity for malicious event chains identified by Palo Alto Networks. The endpoint data that the Cortex XDR agent collects when you enable these capabilities varies by the platform type:

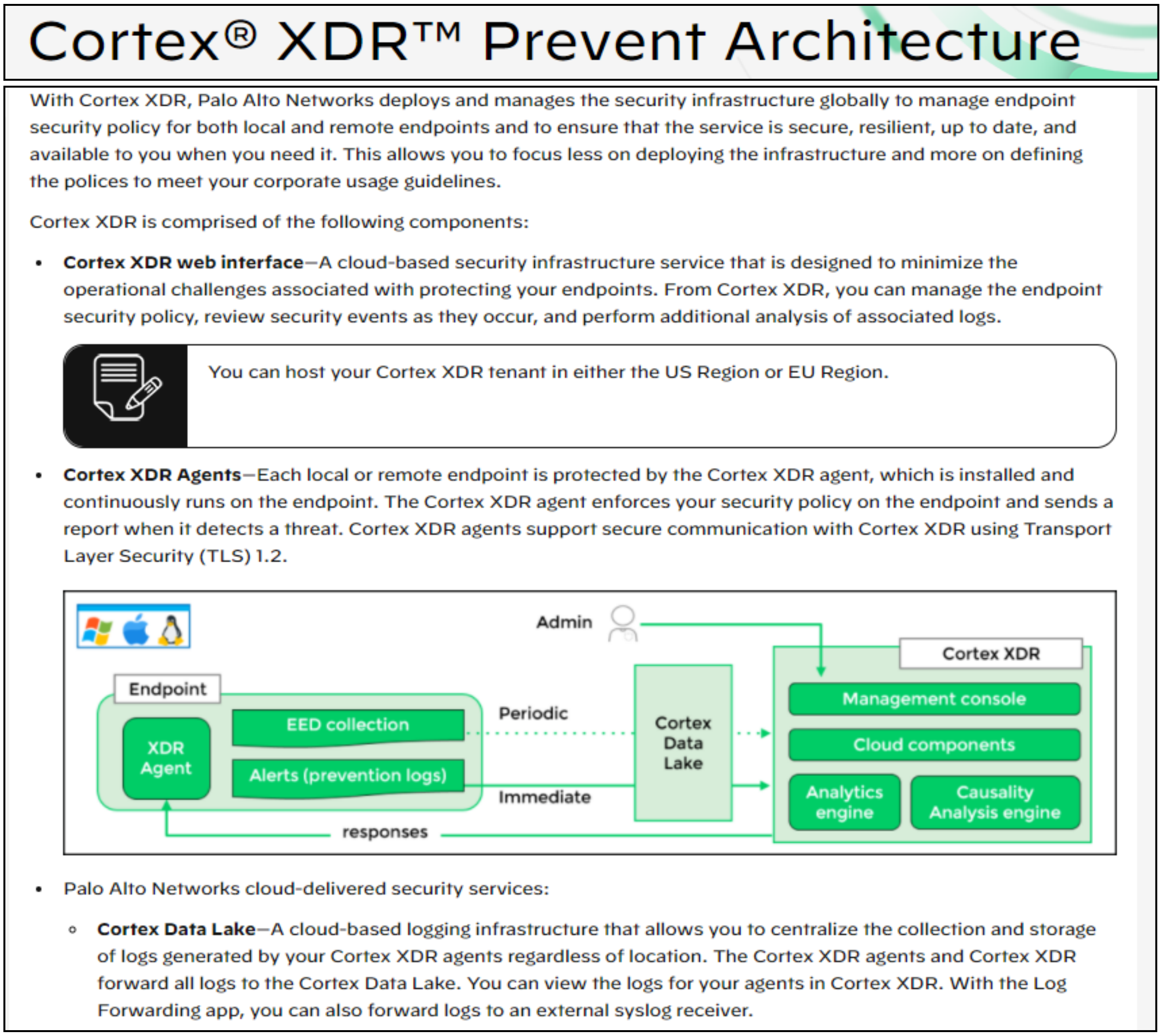


Windows Event Logs

PATH	PROVIDER	EVENT IDS	DESCRIPTION
Application	EMET		
Application	Windows Error Reporting		WER events for application crashes only
Application	Microsoft-Windows-User Profiles Service	1511, 1518	User logging on with temporary profile (1511), Cannot create profile using temporary profile (1518)
Application	Application Error	1000	Application crash/hang events, similar to WER/1001. These include full path to faulting EXE/Module
Application	Application Hang	1002	Application crash/hang events, similar to WER/1001. These include full path to faulting EXE/Module
Microsoft-Windows-CAPI2/Operational		11, 70, 90	CAPI events Build Chain (11), Private Key accessed (70), X509 object (90)
Microsoft-Windows-DNS-Client/Operational		3008	DNS Query Completed (3008) without local machine na,e resolution events and without enmpty name resolution events
Microsoft-Windows-DriverFrameworks-UserMode/Operational		2004	Detect User-Mode drivers loaded - for potential BadUSB detection
Microsoft-Windows-PowerShell/Operational		4103, 4104, 4105, 4106	PowerShell execute block activity (4103), Remote Command (4104), Start Command (4105), Stop Command (4106)
Microsoft-Windows-TaskScheduler/Operational	Microsoft-Windows-TaskScheduler	106, 129, 141, 142, 200, 201	
Microsoft-Windows-TerminalServices-RDPClient/Operational		1024	Log attempted TS connect to remote server
Microsoft-Windows-Windows Defender/Operational		1006, 1009	Modern Windows Defender event provider Detection events (1006 and 1009)
Microsoft-Windows-Windows Defender/Operational		1116, 1119	Modern Windows Defender event provider Detection events (1116 and 1119)

[62]

[62] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/customizable-agent-settings/endpoint-data-collected-by-cortex-xdr.html



Cortex® XDR™ Prevent Architecture

With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

  You can host your Cortex XDR tenant in either the US Region or EU Region.

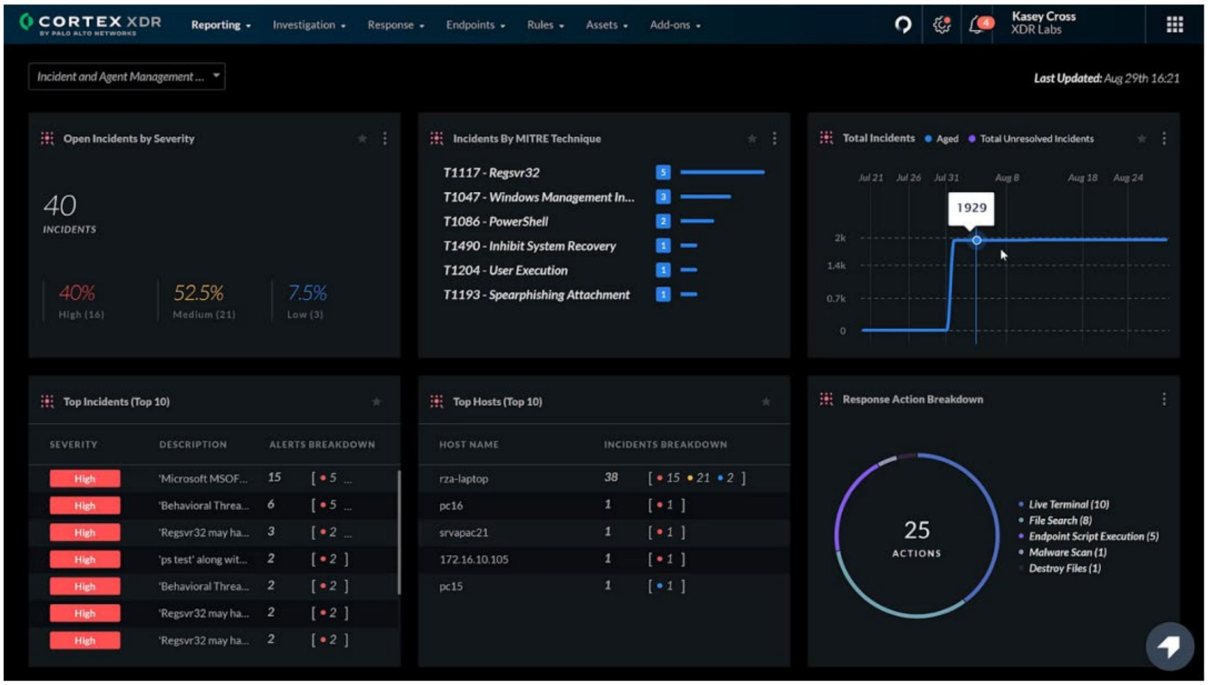
- **Cortex XDR Agents**—Each local or remote endpoint is protected by the Cortex XDR agent, which is installed and continuously runs on the endpoint. The Cortex XDR agent enforces your security policy on the endpoint and sends a report when it detects a threat. Cortex XDR agents support secure communication with Cortex XDR using Transport Layer Security (TLS) 1.2.

- Palo Alto Networks cloud-delivered security services:
  - **Cortex Data Lake**—A cloud-based logging infrastructure that allows you to centralize the collection and storage of logs generated by your Cortex XDR agents regardless of location. The Cortex XDR agents and Cortex XDR forward all logs to the Cortex Data Lake. You can view the logs for your agents in Cortex XDR. With the Log Forwarding app, you can also forward logs to an external syslog receiver.

[63]

133. 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 endpoint. For example, Cortex XDR receives information including what attacks have been detected, top infected endpoints, and number of incidents over time, gathered by the one or more software services (*e.g.*, Cortex XDR Agent), and identification of a user of the endpoint.

[63] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html



Last Updated: Aug 29th 16:21

40 INCIDENTS

40% High (16) 52.5% Medium (21) 7.5% Low (3)

T1117 - Regsvr32	5
T1047 - Windows Management In...	3
T1086 - PowerShell	2
T1490 - Inhibit System Recovery	1
T1204 - User Execution	1
T1193 - Spearphishing Attachment	1

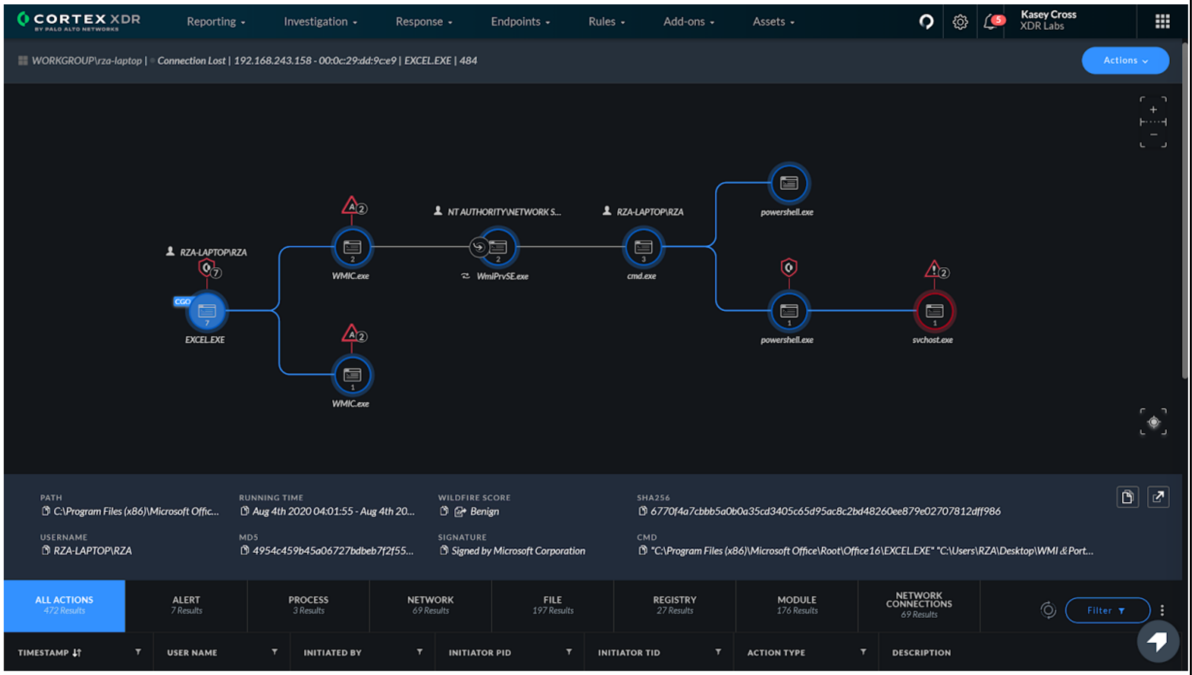
SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[• 5 ...
High	'Behavioral Threa...	6	[• 5 ...
High	'Regsvr32 may ha...	3	[• 2 ...
High	'ps test' along wit...	2	[• 2]
High	'Behavioral Threa...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]

HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[• 15 • 21 • 2]
pc16	1	[• 1]
srvapac21	1	[• 1]
172.16.10.105	1	[• 1]
pc15	1	[• 1]

25 ACTIONS

- Live Terminal (10)
- File Search (8)
- Endpoint Script Execution (5)
- Malware Scan (1)
- Destroy Files (1)

Figure 12: Cortex XDR dashboard [64]



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

PATH: C:\Program Files (x86)\Microsoft Offic...

RUNNING TIME: Aug 4th 2020 04:01:55 - Aug 4th 20...

WILDFIRE SCORE: Benign

SHA256: 6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986

USERNAME: RZA-LAPTOP\RZA

MD5: 4954c459b45a06727bdbeb7f2f55...

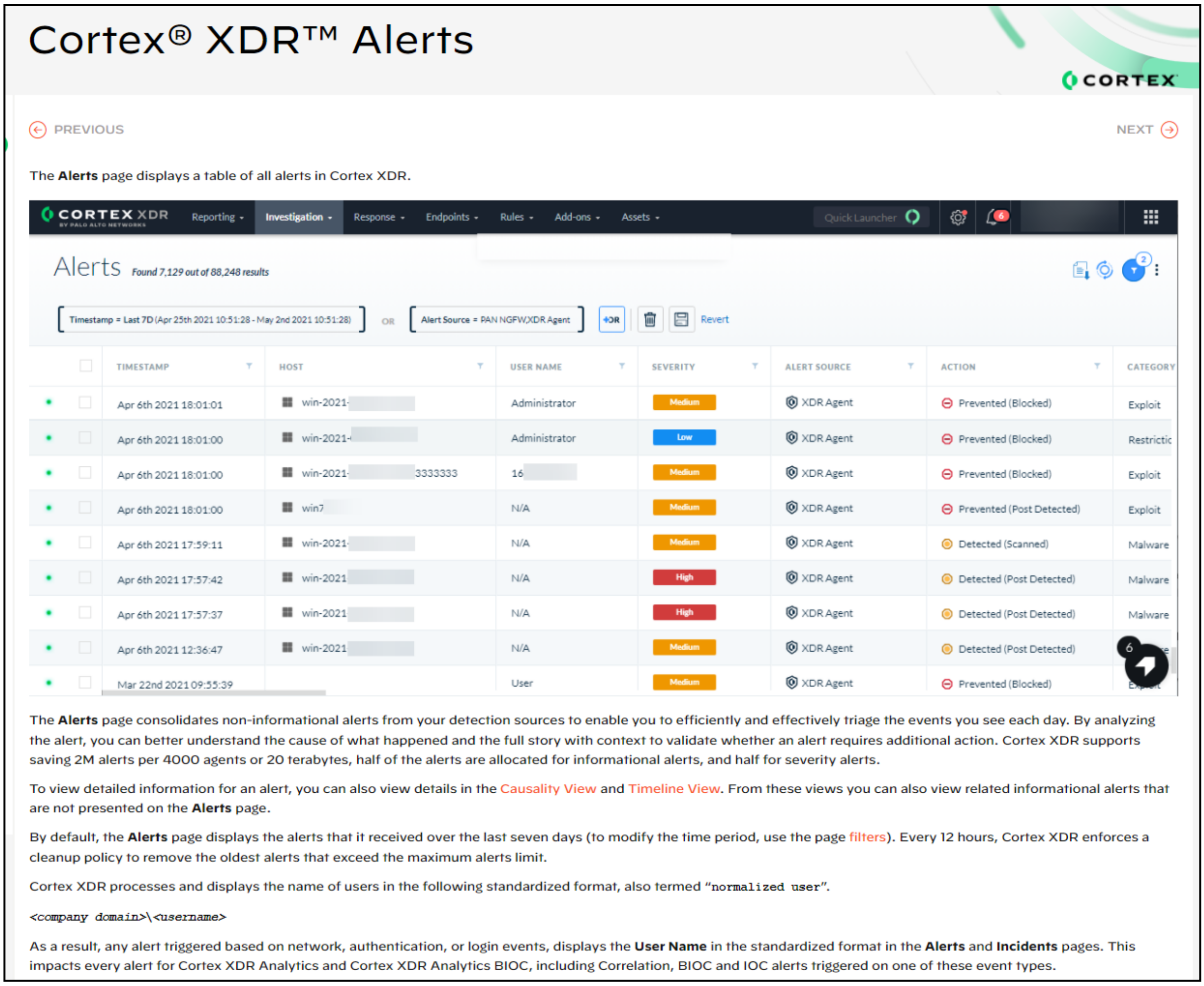
SIGNATURE: Signed by Microsoft Corporation

CMD: "C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI & Port...

Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR [65]

[64] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

[65] *Id.*



Cortex® XDR™ Alerts

The **Alerts** page displays a table of all alerts in Cortex XDR.

Alerts *Found 7,129 out of 88,248 results*

[Timestamp = Last 7D (Apr 25th 2021 10:51:28 - May 2nd 2021 10:51:28)] OR [Alert Source = PAN NGFW,XDR Agent] +OR

	□	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
●	□	Apr 6th 2021 18:01:01	win-2021-[redacted]	Administrator	Medium	XDR Agent	⊖ Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]	Administrator	Low	XDR Agent	⊖ Prevented (Blocked)	Restrictic
●	□	Apr 6th 2021 18:01:00	win-2021-[redacted]3333333	16[redacted]	Medium	XDR Agent	⊖ Prevented (Blocked)	Exploit
●	□	Apr 6th 2021 18:01:00	win7[redacted]	N/A	Medium	XDR Agent	⊖ Prevented (Post Detected)	Exploit
●	□	Apr 6th 2021 17:59:11	win-2021-[redacted]	N/A	Medium	XDR Agent	○ Detected (Scanned)	Malware
●	□	Apr 6th 2021 17:57:42	win-2021[redacted]	N/A	High	XDR Agent	○ Detected (Post Detected)	Malware
●	□	Apr 6th 2021 17:57:37	win-2021[redacted]	N/A	High	XDR Agent	○ Detected (Post Detected)	Malware
●	□	Apr 6th 2021 12:36:47	win-2021[redacted]	N/A	Medium	XDR Agent	○ Detected (Post Detected)	[illegible]
●	□	Mar 22nd 2021 09:55:39		User	Medium	XDR Agent	⊖ Prevented (Blocked)	Exploit

The **Alerts** page consolidates non-informational alerts from your detection sources to enable you to efficiently and effectively triage the events you see each day. By analyzing the alert, you can better understand the cause of what happened and the full story with context to validate whether an alert requires additional action. Cortex XDR supports saving 2M alerts per 4000 agents or 20 terabytes, half of the alerts are allocated for informational alerts, and half for severity alerts.

To view detailed information for an alert, you can also view details in the Causality View and Timeline View. From these views you can also view related informational alerts that are not presented on the **Alerts** page.

By default, the **Alerts** page displays the alerts that it received over the last seven days (to modify the time period, use the page filters). Every 12 hours, Cortex XDR enforces a cleanup policy to remove the oldest alerts that exceed the maximum alerts limit.

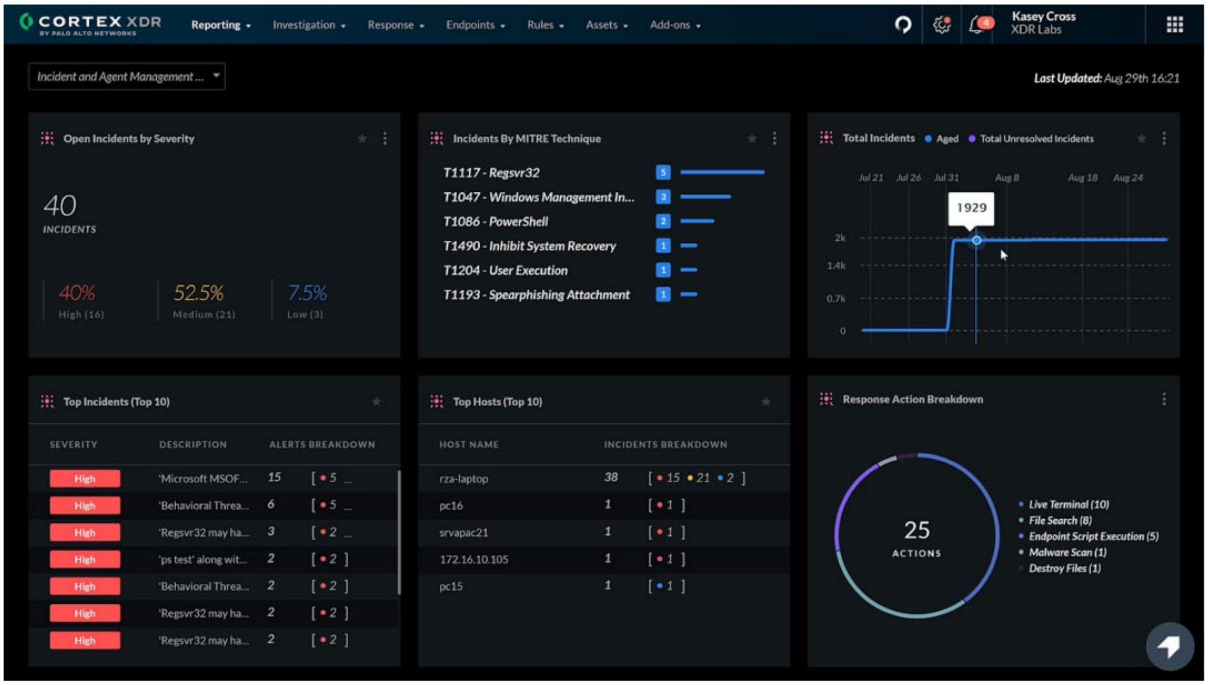
Cortex XDR processes and displays the name of users in the following standardized format, also termed "`normalized user`".

`<company domain>\<username>`

As a result, any alert triggered based on network, authentication, or login events, displays the **User Name** in the standardized format in the **Alerts** and **Incidents** pages. This impacts every alert for Cortex XDR Analytics and Cortex XDR Analytics BIOC, including Correlation, BIOC and IOC alerts triggered on one of these event types.[66]

134. 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, Palo Alto Cortex XDR determines a compliance state of the endpoint based on the user information, attack information, and the rules.

[66] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/cortex-xdr-alerts.html



Last Updated: Aug 29th 16:21

Open Incidents by Severity

40
INCIDENTS

40% High (16)
52.5% Medium (21)
7.5% Low (3)

Incidents By MITRE Technique

T1117 - Regsvr32	5
T1047 - Windows Management In...	3
T1086 - PowerShell	2
T1490 - Inhibit System Recovery	1
T1204 - User Execution	1
T1193 - Spearphishing Attachment	1

Top Incidents (Top 10)

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[• 5 ...
High	'Behavioral Threa...	6	[• 5 ...
High	'Regsvr32 may ha...	3	[• 2 ...
High	'ps test' along wit...	2	[• 2]
High	'Behavioral Threa...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]

Top Hosts (Top 10)

HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[• 15 • 21 • 2]
pc16	1	[• 1]
srvapac21	1	[• 1]
172.16.10.105	1	[• 1]
pc15	1	[• 1]

Response Action Breakdown

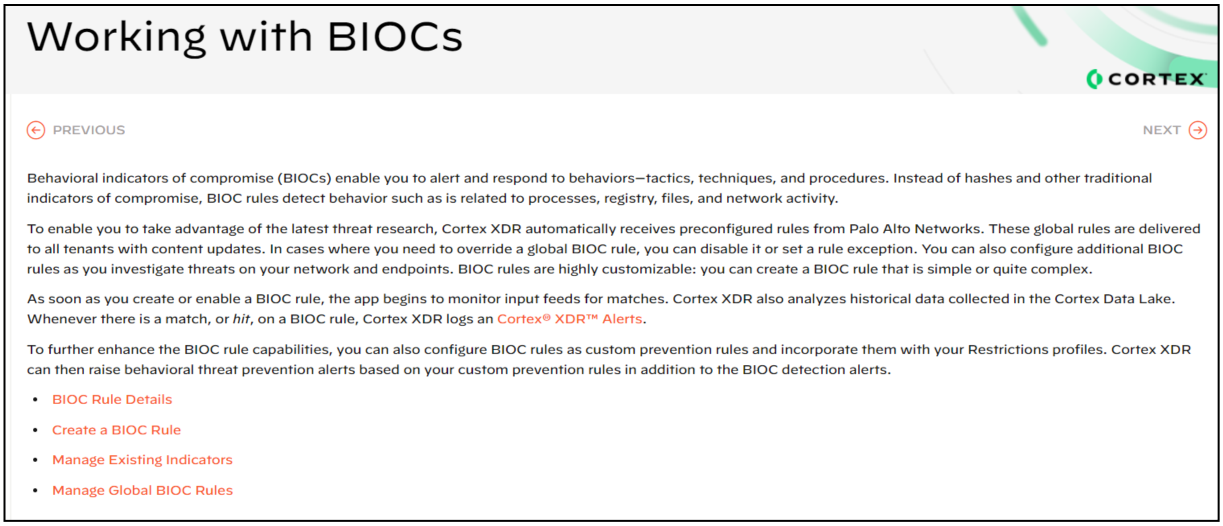
25
ACTIONS

- Live Terminal (10)
- File Search (8)
- Endpoint Script Execution (5)
- Malware Scan (1)
- Destroy Files (1)

Figure 12: Cortex XDR dashboard [67]

135. 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, Palo Alto Cortex XDR authorizes access by the endpoint to a computing resource on the network (*e.g.*, controls network traffic at the endpoint), authorization being determined by Palo Alto Cortex XDR in response to the compliance state.

[67] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf



Working with BIOCs

Behavioral indicators of compromise (BIOCs) enable you to alert and respond to behaviors—tactics, techniques, and procedures. Instead of hashes and other traditional indicators of compromise, BIOC rules detect behavior such as is related to processes, registry, files, and network activity.

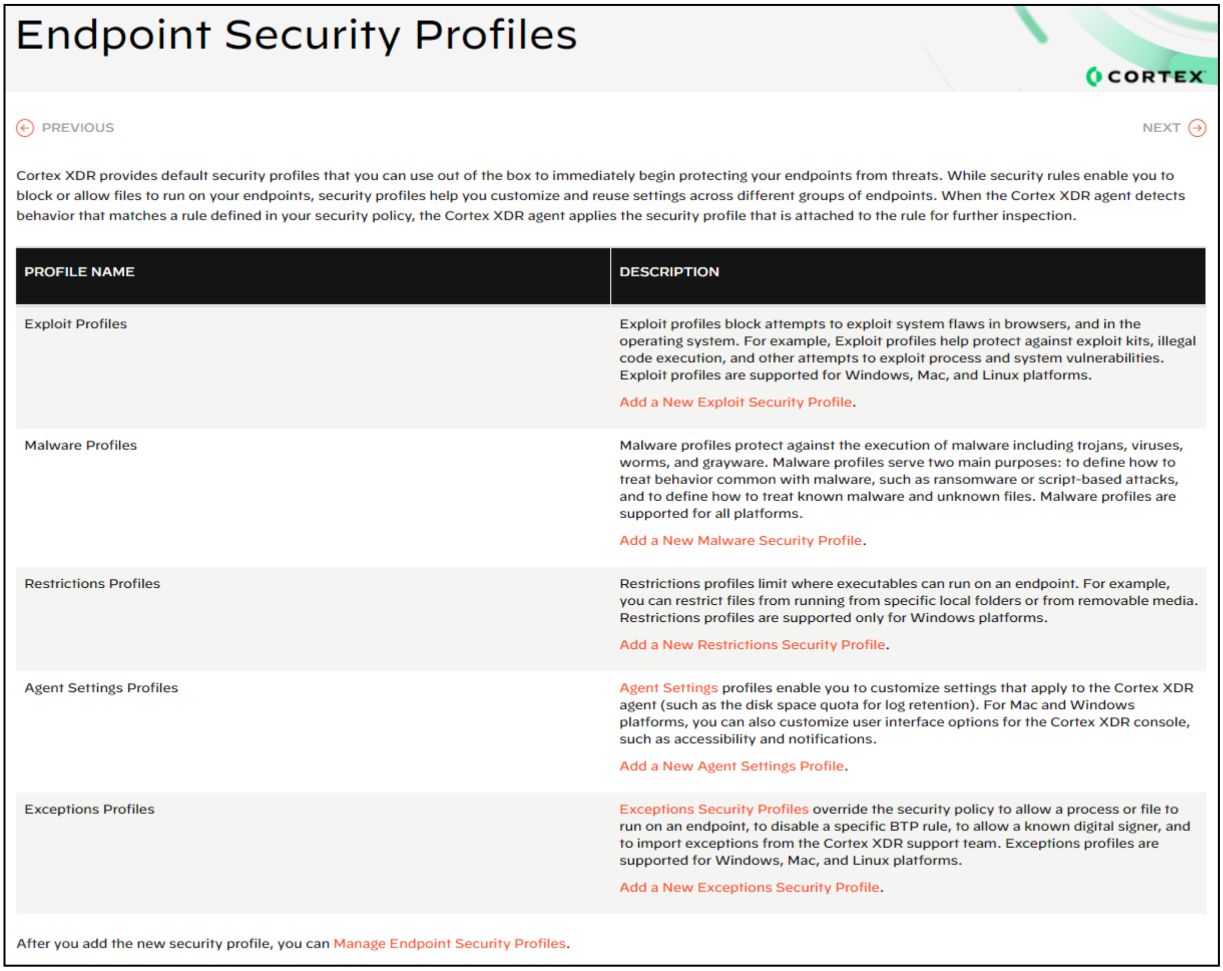
To enable you to take advantage of the latest threat research, Cortex XDR automatically receives preconfigured rules from Palo Alto Networks. These global rules are delivered to all tenants with content updates. In cases where you need to override a global BIOC rule, you can disable it or set a rule exception. You can also configure additional BIOC rules as you investigate threats on your network and endpoints. BIOC rules are highly customizable: you can create a BIOC rule that is simple or quite complex.

As soon as you create or enable a BIOC rule, the app begins to monitor input feeds for matches. Cortex XDR also analyzes historical data collected in the Cortex Data Lake. Whenever there is a match, or *hit*, on a BIOC rule, Cortex XDR logs an Cortex® XDR™ Alerts.

To further enhance the BIOC rule capabilities, you can also configure BIOC rules as custom prevention rules and incorporate them with your Restrictions profiles. Cortex XDR can then raise behavioral threat prevention alerts based on your custom prevention rules in addition to the BIOC detection alerts.

- BIOC Rule Details
- Create a BIOC Rule
- Manage Existing Indicators
- Manage Global BIOC Rules

[68]



Endpoint Security Profiles

Cortex XDR provides default security profiles that you can use out of the box to immediately begin protecting your endpoints from threats. While security rules enable you to block or allow files to run on your endpoints, security profiles help you customize and reuse settings across different groups of endpoints. When the Cortex XDR agent detects behavior that matches a rule defined in your security policy, the Cortex XDR agent applies the security profile that is attached to the rule for further inspection.

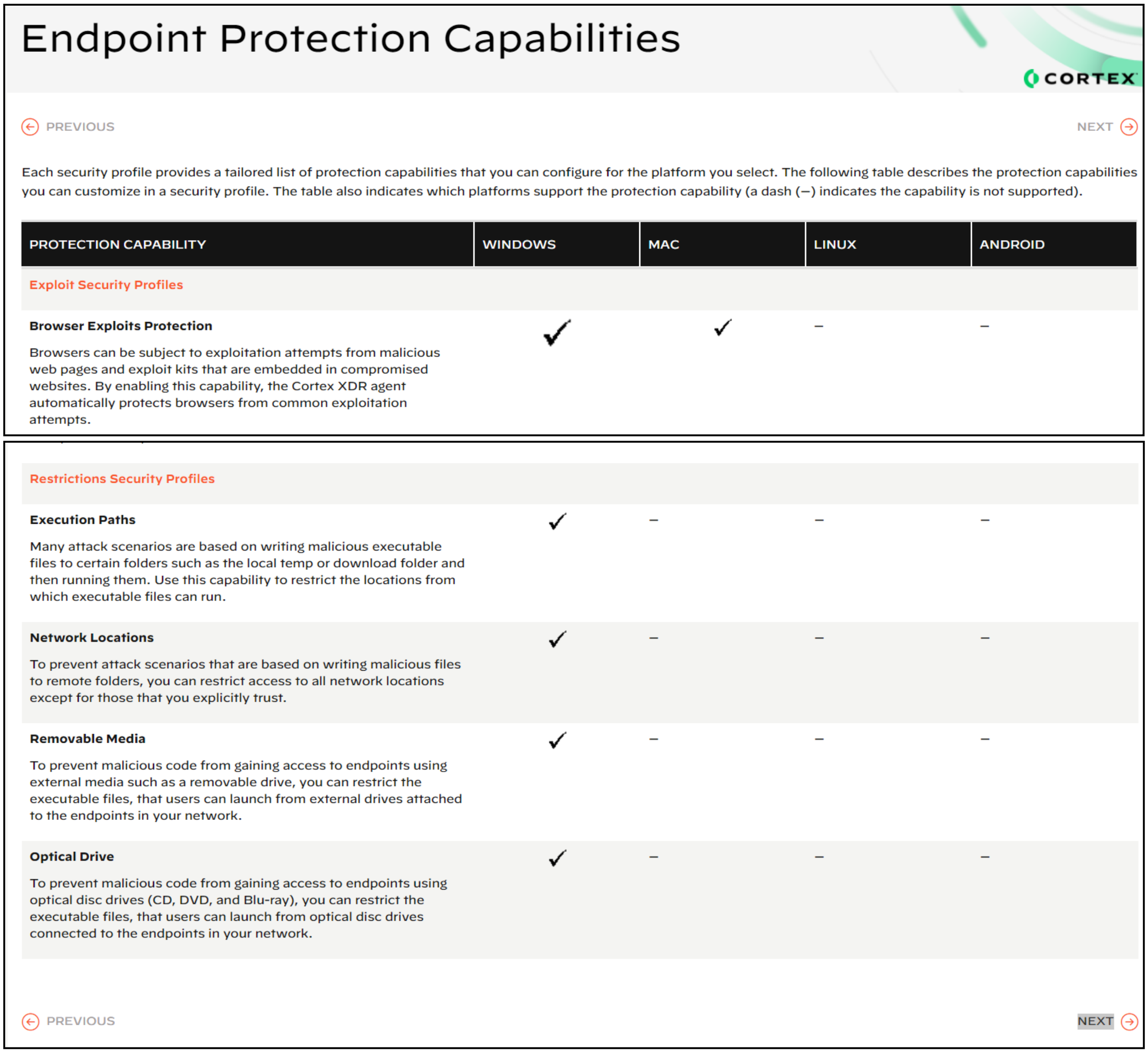
PROFILE NAME	DESCRIPTION
Exploit Profiles	Exploit profiles block attempts to exploit system flaws in browsers, and in the operating system. For example, Exploit profiles help protect against exploit kits, illegal code execution, and other attempts to exploit process and system vulnerabilities. Exploit profiles are supported for Windows, Mac, and Linux platforms. Add a New Exploit Security Profile.
Malware Profiles	Malware profiles protect against the execution of malware including trojans, viruses, worms, and grayware. Malware profiles serve two main purposes: to define how to treat behavior common with malware, such as ransomware or script-based attacks, and to define how to treat known malware and unknown files. Malware profiles are supported for all platforms. Add a New Malware Security Profile.
Restrictions Profiles	Restrictions profiles limit where executables can run on an endpoint. For example, you can restrict files from running from specific local folders or from removable media. Restrictions profiles are supported only for Windows platforms. Add a New Restrictions Security Profile.
Agent Settings Profiles	Agent Settings profiles enable you to customize settings that apply to the Cortex XDR agent (such as the disk space quota for log retention). For Mac and Windows platforms, you can also customize user interface options for the Cortex XDR console, such as accessibility and notifications. Add a New Agent Settings Profile.
Exceptions Profiles	Exceptions Security Profiles override the security policy to allow a process or file to run on an endpoint, to disable a specific BTP rule, to allow a known digital signer, and to import exceptions from the Cortex XDR support team. Exceptions profiles are supported for Windows, Mac, and Linux platforms. Add a New Exceptions Security Profile.

After you add the new security profile, you can Manage Endpoint Security Profiles.

[69]

[68] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs.html

[69] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-security-profiles.html



Endpoint Protection Capabilities

Each security profile provides a tailored list of protection capabilities that you can configure for the platform you select. The following table describes the protection capabilities you can customize in a security profile. The table also indicates which platforms support the protection capability (a dash (—) indicates the capability is not supported).

PROTECTION CAPABILITY	WINDOWS	MAC	LINUX	ANDROID
Exploit Security Profiles				
Browser Exploits Protection Browsers can be subject to exploitation attempts from malicious web pages and exploit kits that are embedded in compromised websites. By enabling this capability, the Cortex XDR agent automatically protects browsers from common exploitation attempts.	✓	✓	–	–
Restrictions Security Profiles				
Execution Paths Many attack scenarios are based on writing malicious executable files to certain folders such as the local temp or download folder and then running them. Use this capability to restrict the locations from which executable files can run.	✓	–	–	–
Network Locations To prevent attack scenarios that are based on writing malicious files to remote folders, you can restrict access to all network locations except for those that you explicitly trust.	✓	–	–	–
Removable Media To prevent malicious code from gaining access to endpoints using external media such as a removable drive, you can restrict the executable files, that users can launch from external drives attached to the endpoints in your network.	✓	–	–	–
Optical Drive To prevent malicious code from gaining access to endpoints using optical disc drives (CD, DVD, and Blu-ray), you can restrict the executable files, that users can launch from optical disc drives connected to the endpoints in your network.	✓	–	–	–

[70]

136. Defendant has and continues to indirectly infringe one or more claims of the ’918 Patent by knowingly and intentionally inducing others, including Palo Alto 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 Endpoint Protection feature).

[70] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-protection-capabilities.html

137. Defendant, with knowledge that these products, or the use thereof, infringe the ’918 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’918 Patent by providing these products to end-users for use in an infringing manner.

138. Defendant has 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.

139. 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.

140. 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)

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

142. 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.

143. Defendant has and continues to directly infringe the ’517 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’517 Patent. Such products incorporate the Malicious Process Prevention and Behavioral Threat Protection features and include at least the Palo Alto Cortex XDR (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.

144. Every ’517 Accused Product practices a method for assessing runtime risk for an application program that executes on a device. For example, the Palo Alto Cortex XDR Malicious Process Prevention and Behavioral Threat Protection features assess runtime risk for applications that execute on endpoints.

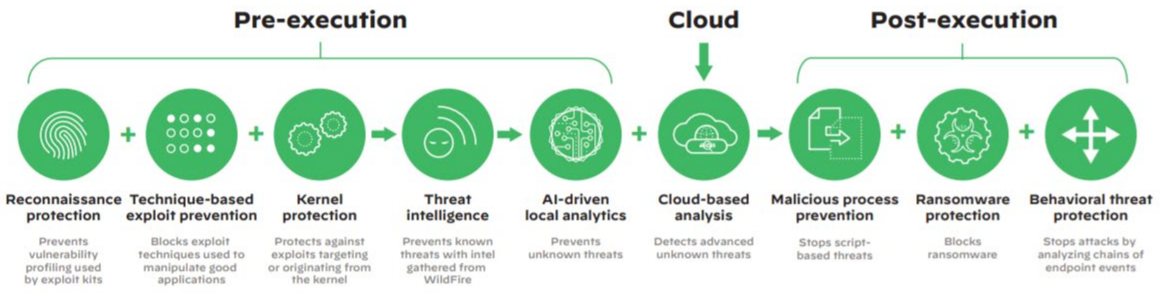
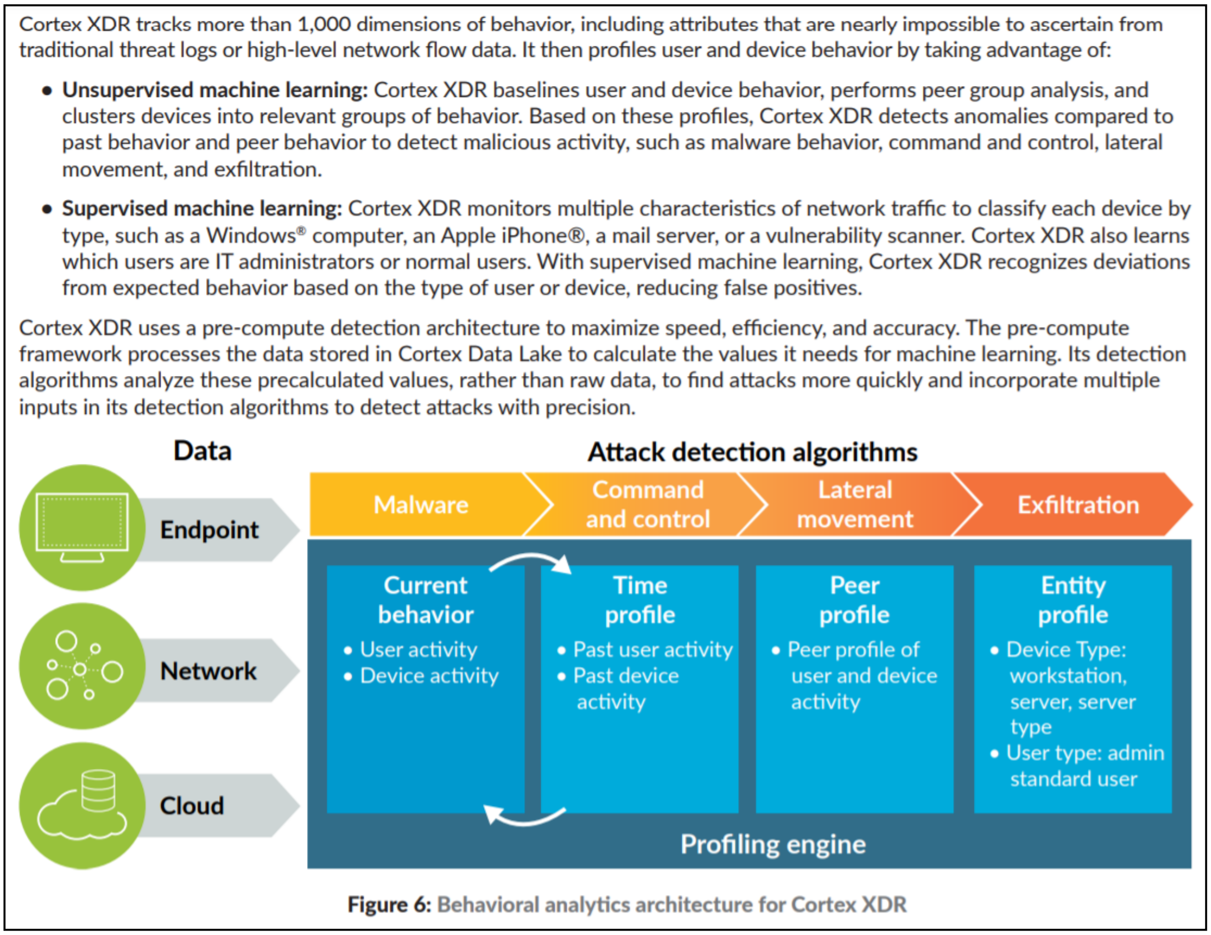

Pre-execution
Cloud
Post-execution
Reconnaissance protection
Prevents vulnerability profiling used by exploit kits
Technique-based exploit prevention
Blocks exploit techniques used to manipulate good applications
Kernel protection
Protects against exploits targeting or originating from the kernel
Threat intelligence
Prevents known threats with intel gathered from WildFire
AI-driven local analytics
Prevents unknown threats
Cloud-based analysis
Detects advanced unknown threats
Malicious process prevention
Stops script-based threats
Ransomware protection
Blocks ransomware
Behavioral threat protection
Stops attacks by analyzing chains of endpoint events

Figure 5: Automatically preventing malware, exploits, and fileless attacks [71]

[71] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

145. Every '517 Accused Product practices storing, in a rules database, a plurality of rules, wherein each rule identifies an action sequence. For example, Palo Alto Cortex XDR stores a plurality of behavior-related rules where each rule identifies an action sequence.



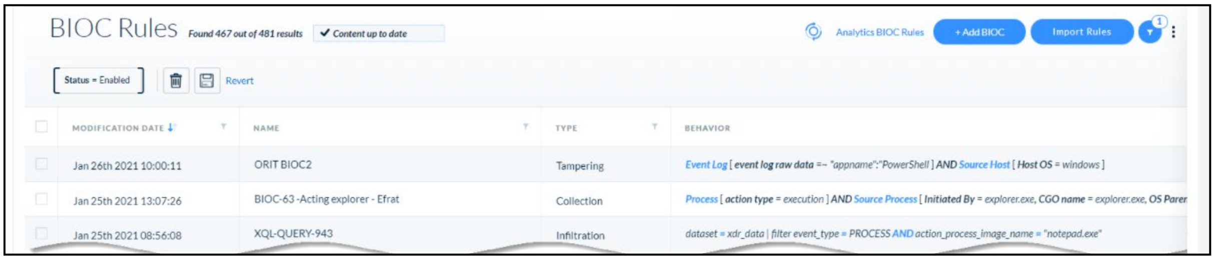
Cortex XDR tracks more than 1,000 dimensions of behavior, including attributes that are nearly impossible to ascertain from traditional threat logs or high-level network flow data. It then profiles user and device behavior by taking advantage of:

- **Unsupervised machine learning:** Cortex XDR baselines user and device behavior, performs peer group analysis, and clusters devices into relevant groups of behavior. Based on these profiles, Cortex XDR detects anomalies compared to past behavior and peer behavior to detect malicious activity, such as malware behavior, command and control, lateral movement, and exfiltration.
- **Supervised machine learning:** Cortex XDR monitors multiple characteristics of network traffic to classify each device by type, such as a Windows® computer, an Apple iPhone®, a mail server, or a vulnerability scanner. Cortex XDR also learns which users are IT administrators or normal users. With supervised machine learning, Cortex XDR recognizes deviations from expected behavior based on the type of user or device, reducing false positives.

Cortex XDR uses a pre-compute detection architecture to maximize speed, efficiency, and accuracy. The pre-compute framework processes the data stored in Cortex Data Lake to calculate the values it needs for machine learning. Its detection algorithms analyze these precalculated values, rather than raw data, to find attacks more quickly and incorporate multiple inputs in its detection algorithms to detect attacks with precision.

Figure 6: Behavioral analytics architecture for Cortex XDR

[72]



BIOC Rules Found 467 out of 481 results ✓ Content up to date

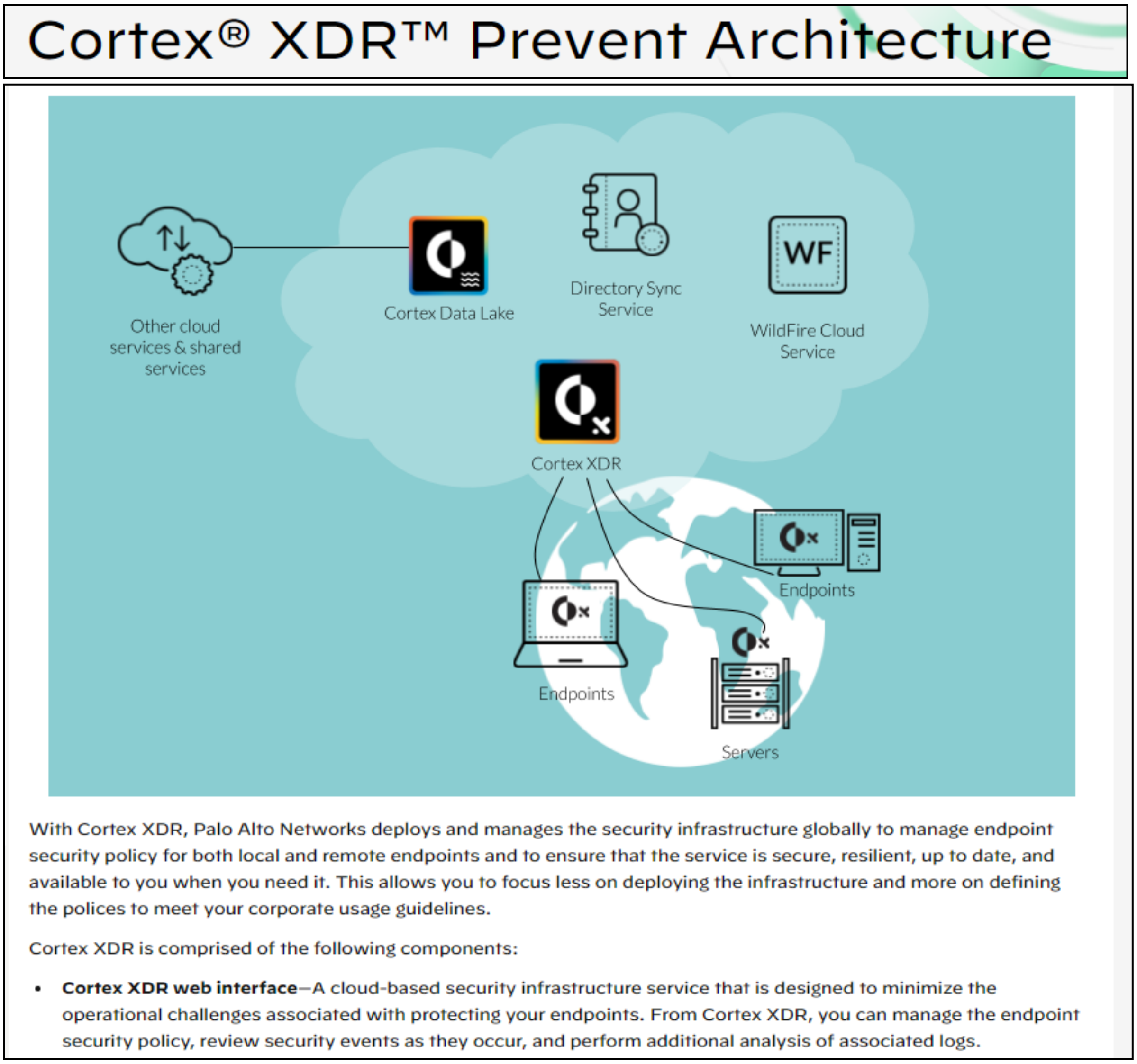
Status = Enabled

□	MODIFICATION DATE	NAME	TYPE	BEHAVIOR
□	Jan 26th 2021 10:00:11	ORIT BIOC2	Tampering	Event Log [event log raw data =~ "appname":"PowerShell] AND Source Host [Host OS = windows]
□	Jan 25th 2021 13:07:26	BIOC-63 -Acting explorer - Efrat	Collection	Process [action type = execution] AND Source Process [Initiated By = explorer.exe, CGO name = explorer.exe, OS Paren
□	Jan 25th 2021 08:56:08	XQL-QUERY-943	Infiltration	dataset = xdr_data | filter event_type = PROCESS AND action_process_image_name = "notepad.exe"

[73]

[72] https://www.exclusive-networks.com/nl/wp-content/uploads/sites/21/2020/12/cortex-xdr-whitepaper.pdf
[73] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/bioc-rules-details.html

146. 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 Palo Alto Cortex XDR stores a plurality of assessment policies which comprise at least one rule of the plurality or rules.



Cortex® XDR™ Prevent Architecture

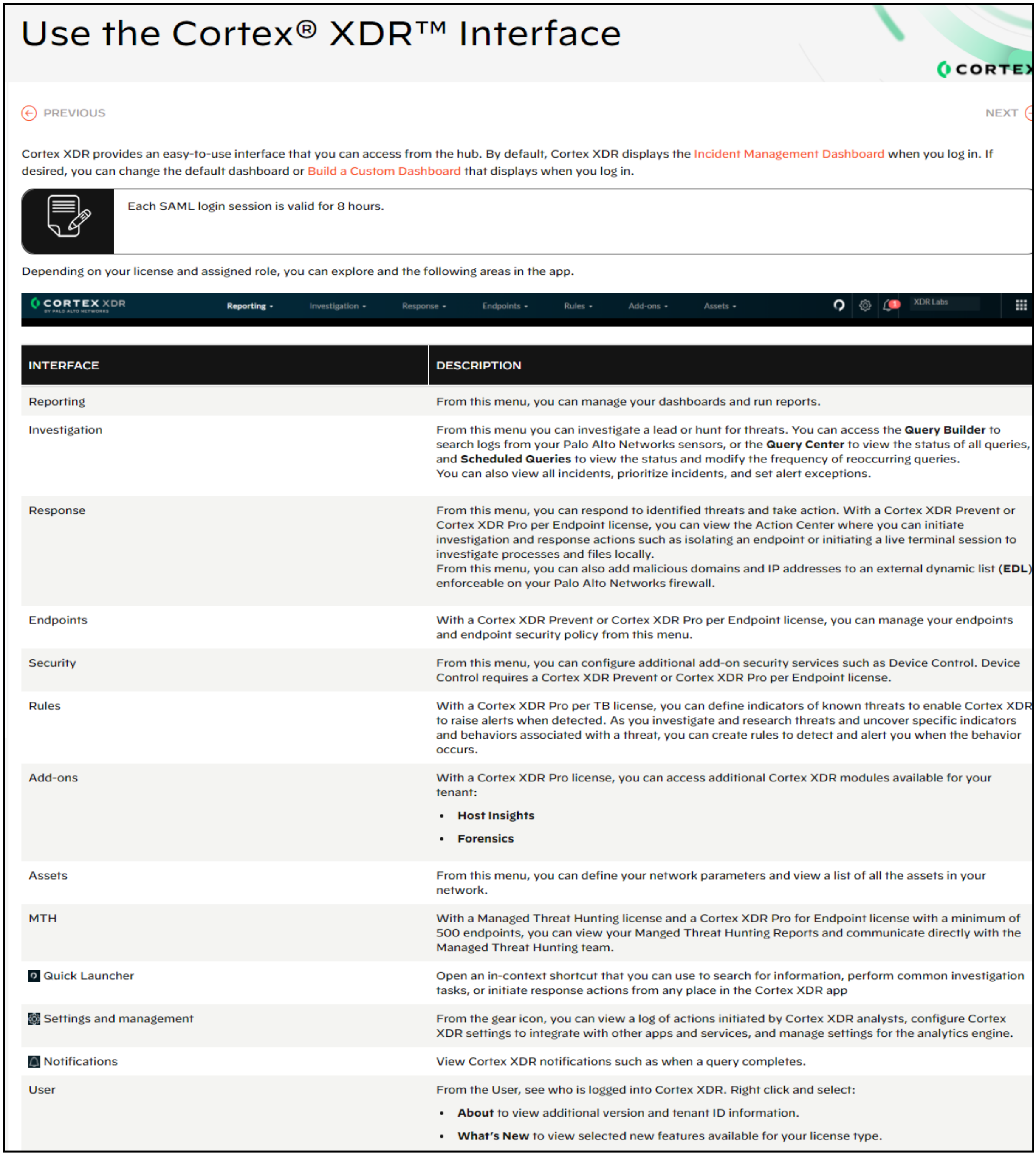
With Cortex XDR, Palo Alto Networks deploys and manages the security infrastructure globally to manage endpoint security policy for both local and remote endpoints and to ensure that the service is secure, resilient, up to date, and available to you when you need it. This allows you to focus less on deploying the infrastructure and more on defining the polices to meet your corporate usage guidelines.

Cortex XDR is comprised of the following components:

- **Cortex XDR web interface**—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your endpoints. From Cortex XDR, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.

[74]

[74] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture.html



Use the Cortex® XDR™ Interface

Cortex XDR provides an easy-to-use interface that you can access from the hub. By default, Cortex XDR displays the Incident Management Dashboard when you log in. If desired, you can change the default dashboard or Build a Custom Dashboard that displays when you log in.

Each SAML login session is valid for 8 hours.

Depending on your license and assigned role, you can explore and the following areas in the app.

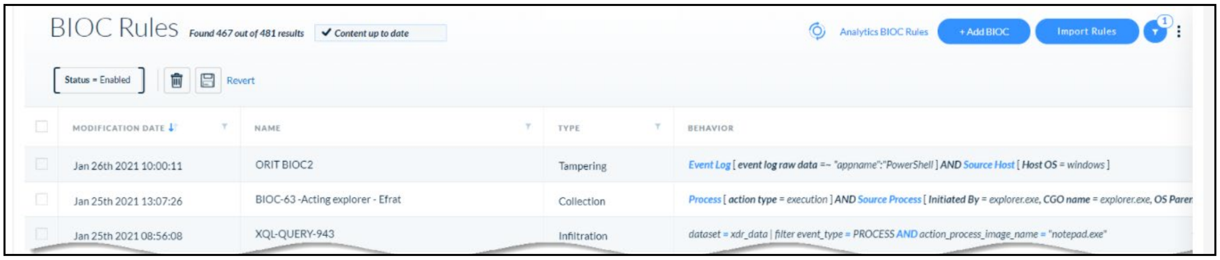
INTERFACE	DESCRIPTION
Reporting	From this menu, you can manage your dashboards and run reports.
Investigation	From this menu you can investigate a lead or hunt for threats. You can access the **Query Builder** to search logs from your Palo Alto Networks sensors, or the **Query Center** to view the status of all queries, and **Scheduled Queries** to view the status and modify the frequency of reoccurring queries. You can also view all incidents, prioritize incidents, and set alert exceptions.
Response	From this menu, you can respond to identified threats and take action. With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can view the Action Center where you can initiate investigation and response actions such as isolating an endpoint or initiating a live terminal session to investigate processes and files locally. From this menu, you can also add malicious domains and IP addresses to an external dynamic list (**EDL**) enforceable on your Palo Alto Networks firewall.
Endpoints	With a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license, you can manage your endpoints and endpoint security policy from this menu.
Security	From this menu, you can configure additional add-on security services such as Device Control. Device Control requires a Cortex XDR Prevent or Cortex XDR Pro per Endpoint license.
Rules	With a Cortex XDR Pro per TB license, you can define indicators of known threats to enable Cortex XDR to raise alerts when detected. As you investigate and research threats and uncover specific indicators and behaviors associated with a threat, you can create rules to detect and alert you when the behavior occurs.
Add-ons	With a Cortex XDR Pro license, you can access additional Cortex XDR modules available for your tenant: • **Host Insights** • **Forensics**
Assets	From this menu, you can define your network parameters and view a list of all the assets in your network.
MTH	With a Managed Threat Hunting license and a Cortex XDR Pro for Endpoint license with a minimum of 500 endpoints, you can view your Manged Threat Hunting Reports and communicate directly with the Managed Threat Hunting team.
Quick Launcher	Open an in-context shortcut that you can use to search for information, perform common investigation tasks, or initiate response actions from any place in the Cortex XDR app
Settings and management	From the gear icon, you can view a log of actions initiated by Cortex XDR analysts, configure Cortex XDR settings to integrate with other apps and services, and manage settings for the analytics engine.
Notifications	View Cortex XDR notifications such as when a query completes.
User	From the User, see who is logged into Cortex XDR. Right click and select: • **About** to view additional version and tenant ID information. • **What's New** to view selected new features available for your license type.

[75]

147. 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

[75] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/get-started-with-cortex-xdr-pro/use-cortex-xdr.html

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, Palo Alto Cortex XDR 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). Palo Alto Cortex XDR 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.


BIOC Rules Found 467 out of 481 results ✓ Content up to date

□	MODIFICATION DATE	NAME	TYPE	BEHAVIOR
□	Jan 26th 2021 10:00:11	ORIT BIOC2	Tampering	Event Log [event log raw data =~ "appname":"PowerShell] AND Source Host [Host OS = windows]
□	Jan 25th 2021 13:07:26	BIOC-63 -Acting explorer - Efrat	Collection	Process [action type = execution] AND Source Process [Initiated By = explorer.exe, CGO name = explorer.exe, OS Parer
□	Jan 25th 2021 08:56:08	XQL-QUERY-943	Infiltration	dataset = xdr_data | filter event_type = PROCESS AND action_process_image_name = "notepad.exe"

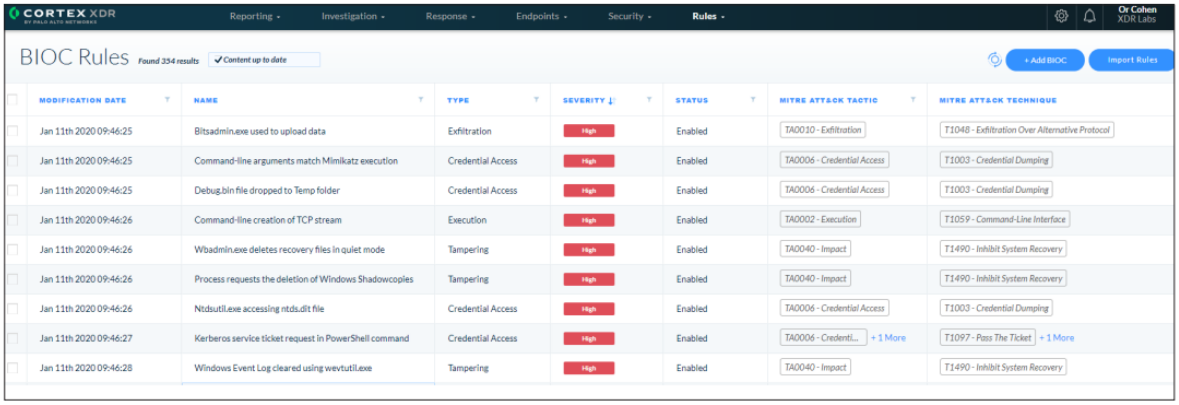
[76]

[76] https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/bioc-rules-details.html

Extended Detection and Response (XDR) Capabilities

XDR, or extended detection and response, describes detection and response systems that can ingest and analyze data from multiple sources, such as endpoint, network, and cloud. Gartner has listed XDR as one of the top security and risk management trends of 2020.

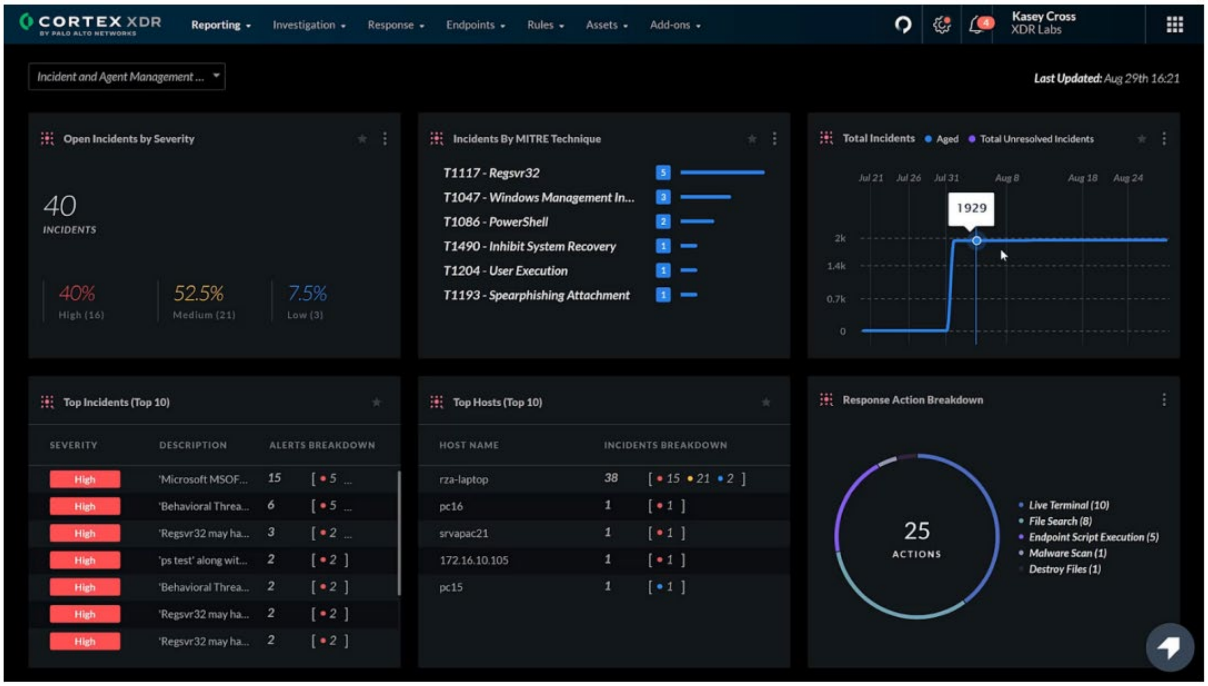
XDR is gaining traction rapidly among security operations teams not only because it helps consolidate the security technology stack and broaden visibility into the full scope of an attack, but also because it allows for better alerts. XDR can combine softer signals from multiple components to detect events that might otherwise be ignored. At the same time, XDR solutions can validate alerts by analyzing them with much broader context, resulting in higher fidelity. The net result of all this data stitching is that organizations have greater visibility, faster investigations, more comprehensive and more accurate alerts, and lots of good data feeding into their machine learning models to continue improving their analytics.



BIOC Rules Found 354 results ✓ Content up to date

	MODIFICATION DATE	NAME	TYPE	SEVERITY	STATUS	MITRE ATT&CK TACTIC	MITRE ATT&CK TECHNIQUE
□	Jan 11th 2020 09:46:25	Bitsadmin.exe used to upload data	Exfiltration	High	Enabled	TA0010 - Exfiltration	T1048 - Exfiltration Over Alternative Protocol
□	Jan 11th 2020 09:46:25	Command-line arguments match Mimikatz execution	Credential Access	High	Enabled	TA0006 - Credential Access	T1003 - Credential Dumping
□	Jan 11th 2020 09:46:25	Debug.bin file dropped to Temp folder	Credential Access	High	Enabled	TA0006 - Credential Access	T1003 - Credential Dumping
□	Jan 11th 2020 09:46:26	Command-line creation of TCP stream	Execution	High	Enabled	TA0002 - Execution	T1059 - Command-Line Interface
□	Jan 11th 2020 09:46:26	Wbadmin.exe deletes recovery files in quiet mode	Tampering	High	Enabled	TA0040 - Impact	T1490 - Inhibit System Recovery
□	Jan 11th 2020 09:46:26	Process requests the deletion of Windows Shadowcopies	Tampering	High	Enabled	TA0040 - Impact	T1490 - Inhibit System Recovery
□	Jan 11th 2020 09:46:26	Ntdsutil.exe accessing ntds.dit file	Credential Access	High	Enabled	TA0006 - Credential Access	T1003 - Credential Dumping
□	Jan 11th 2020 09:46:27	Kerberos service ticket request in PowerShell command	Credential Access	High	Enabled	TA0006 - Credenti... + 1 More	T1097 - Pass The Ticket + 1 More
□	Jan 11th 2020 09:46:28	Windows Event Log cleared using wevtutil.exe	Tampering	High	Enabled	TA0040 - Impact	T1490 - Inhibit System Recovery

Figure 10: Cortex XDR stitches log data together to display attack scope and root cause [77]



Top Incidents (Top 10)

SEVERITY	DESCRIPTION	ALERTS BREAKDOWN	
High	'Microsoft MSOF...	15	[• 5 ...
High	'Behavioral Threa...	6	[• 5 ...
High	'Regsvr32 may ha...	3	[• 2 ...
High	'ps test' along wit...	2	[• 2]
High	'Behavioral Threa...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]
High	'Regsvr32 may ha...	2	[• 2]

Top Hosts (Top 10)

HOST NAME	INCIDENTS BREAKDOWN	
rza-laptop	38	[• 15 • 21 • 2]
pc16	1	[• 1]
srvapac21	1	[• 1]
172.16.10.105	1	[• 1]
pc15	1	[• 1]

Figure 12: Cortex XDR dashboard [78]

[77] https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/palo-alto-networks/palo-alto-mitre-attack-round-2-edr-evaluation.pdf

[78] https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xdr.pdf

148. Defendant has and continues to indirectly infringe one or more claims of the ’517 Patent by knowingly and intentionally inducing others, including Palo Alto 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 the ’517 Accused Products (*e.g.*, products that incorporate the Malicious Process Prevention and Behavioral Threat Protection features).

149. Defendant, with knowledge that these products, or the use thereof, infringe the ’517 Patent at least as of the date of this 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.

150. Defendant has 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.

151. 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.

152. 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

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;

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: February 25, 2021

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**