




The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at [wvOASIS.gov](http://wvOASIS.gov). As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at [WVPurchasing.gov](http://WVPurchasing.gov) with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

## Header 5

 List View

## General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 591150

SO Doc Code: CRFQ

Procurement Type: Central Master Agreement

SO Dept: 0210

Vendor ID: 000000180526

SO Doc ID: ISC2000000002

Legal Name: SUN MANAGEMENT INC

Published Date: 7/22/19

Alias/DBA:

Close Date: 7/30/19

Total Bid: \$60,350.00

Close Time: 13:30

Response Date: 07/30/2019

Status: Closed

Response Time: 13:04

Solicitation Description: Addendum 1-EndPoint Detection  
and Response Software - OT1912

Total of Header Attachments: 5

Total of All Attachments: 5



Purchasing Division  
 2019 Washington Street East  
 Post Office Box 50130  
 Charleston, WV 25305-0130

**State of West Virginia  
 Solicitation Response**

**Proc Folder :** 591150

**Solicitation Description :** Addendum 1-EndPoint Detection and Response Software - OT1912

**Proc Type :** Central Master Agreement

| Date issued | Solicitation Closes    | Solicitation Response        | Version |
|-------------|------------------------|------------------------------|---------|
|             | 2019-07-30<br>13:30:00 | SR 0210 ESR07301900000000461 | 1       |

| <b>VENDOR</b>                      |
|------------------------------------|
| 000000180526<br>SUN MANAGEMENT INC |

**Solicitation Number:** CRFQ 0210 ISC2000000002

**Total Bid :** \$60,350.00      **Response Date:** 2019-07-30      **Response Time:** 13:04:03

**Comments:**

**FOR INFORMATION CONTACT THE BUYER**  
 Jessica S Chambers  
 (304) 558-0246  
 jessica.s.chambers@wv.gov

|                          |               |             |
|--------------------------|---------------|-------------|
| <b>Signature on File</b> | <b>FEIN #</b> | <b>DATE</b> |
|--------------------------|---------------|-------------|

All offers subject to all terms and conditions contained in this solicitation

| Line | Comm Ln Desc  | Qty     | Unit Issue | Unit Price      | Ln Total Or Contract Amount |
|------|---|---------|------------|-----------------|-----------------------------|
| 1    | Overall Total for Contract Items 1 & 2<br>with Opt Renewals | 1.00000 | LS         | \$60,350.000000 | \$60,350.00                 |

| Comm Code | Manufacturer | Specification | Model # |
|-----------|--------------|---------------|---------|
| 43233204  |              |               |         |

|                               |   |
|-------------------------------|---|
| <b>Extended Description :</b> | <p>4.1.1 Contract Item 1: Containment &amp; Remediation</p> <p>4.1.1.1 The Vendor must provide a software and/or service that is capable of supporting a minimum of 2,000 endpoints throughout the State of West Virginia</p> |
|-------------------------------|---|

**Comments:** Palo Alto # PAN-MGFR-XDR-1TB-1YR and # PAN-LGS-1TB-1YR. Including install svcs.  
Annual renewals = \$51,350

# Palo Alto Networks, Inc.

[RFP: EndPoint Detection & Response Software – OT19125]

**Technical Proposal**

**July 30, 2019**



## TABLE OF CONTENTS

|   |                                     |
|---|-------------------------------------|
| <b>4.1.1.1 CONTAINMENT &amp; REMEDIATION.....</b> | <b>ERROR! BOOKMARK NOT DEFINED.</b> |
| <b>4.1.1.5 REPORTING &amp; MONITORING .....</b>   | <b>7</b>                            |
| <b>4.2 TECHNICAL DETAILS.....</b>                 | <b>11</b>                           |

## SECTION 4: MANDATORY REQUIREMENTS

**4.1 Mandatory Contract Services Requirements and Deliverables:** Contract Services must meet or exceed the mandatory requirements listed below.

### 4.1.1 Contract Item: Endpoint Detection and Response Software

#### 4.1.1.1 Containment & Remediation

**4.1.1.2** The Vendor must provide a software and/or service that is capable of supporting a minimum of two thousand (2,000) endpoints throughout the State of West Virginia

*Palo Alto Networks Traps Endpoint Product supports massive scale, well over 100,000 agents can be supported in any given deployment.*

**4.1.1.3** The Vendor must provide a software and/or service that can be centrally managed by a West Virginia Office of Technology Administrator.

*Palo Alto Networks Traps employs a cloud-based management system that is also role-based, providing a centralized and granular management environment. With the Traps Management Service, a cloud-based endpoint security service, you save the time and cost of having to build out your own global security infrastructure. Deployment is simple and fast, requiring no server licenses, databases or other infrastructure to get started.*

**4.1.1.4** The Vendor must provide a software and/or service that shall feature the following:

**4.1.1.4.1** Automatically restrict potentially malicious activity to within an isolation container.

*Palo Alto Networks Traps can detect and stop malicious behavior automatically. Additionally, the offending endpoint can be isolated so as to protect other endpoints on the network. Once such isolation is invoked, security administrators can use the included Live Terminal function to do file and process exploration on the system in question. Additionally, the Live Terminal also allows the SecOps team to run commands or Python scripts to further investigate the isolated system.*

- 4.1.1.4.2 Automatically isolate applications interacting with untrusted content from more trusted portions of the device outside the container.

*Palo Alto Networks Traps can block untrusted applications from executing on selected systems.*

- 4.1.1.4.3 Automatically detect and isolate potentially malicious code behavior.

*Rather than focusing on individual attacks, Traps blocks the exploit techniques the attacks use. By doing so, at each step in an exploit attempt Traps breaks the attack lifecycle and renders threats ineffective.*

- 4.1.1.4.4 Continuously detect, and isolate threats based on machine learning, behavioral analytics, and custom detection rules.

*Unique in the breadth and depth of its endpoint protections, Traps stops malware, exploits and ransomware by observing attack techniques and behaviors. Traps uses machine learning and artificial intelligence (AI) to automatically detect and respond to sophisticated attacks. Included with Traps is WildFire, Palo Alto Networks malware prevention service to improve accuracy and coverage.*

- 4.1.1.4.5 Automatically capture necessary event details on all malicious activity, including but not limited to ports and protocols in use, running executables and services, and browser plugins occurring within the isolation container to support retrospective post-event analysis, threat analysis, and situational awareness.

*Traps captures a vast amount of relevant event details on all malicious activity, including but not limited to ports and protocols in use, running executables and services, and browser plugins occurring within the isolation container to support retrospective post-event analysis, threat analysis, and situational awareness as required by the State of West Virginia. To accomplish this, Traps uses the Palo Alto Networks Cortex Data Lake to store all event and incident data captured, allowing seamless integration with Cortex XDR for investigation and incident response. Cortex XDR, a cloud-based detection and response app, empowers SecOps to stop sophisticated attacks and adapt defenses in real time. By combining a rich network, endpoint, and cloud data with analytics, Cortex XDR allows you to: Automatically determine root cause to accelerate triage and incident response, reduce time and experience required from triage to threat hunting and respond to threats quicker and adapt defenses from knowledge gained, making the next response even faster.*



- 4.1.1.4.6** Be configurable to control the ability of applications running within the isolation container to access only specified system resources.

*Traps can be configured to allow or disallow access to certain system resources. In addition, Traps also offers a more sophisticated method for protecting said system resources without implementing said time consuming “blacklisting”. This method is called Behavioral Threat Protection (or BTP). BTP enables continuous monitoring of endpoint activity to identify and analyze chains of events—known as causality chains. This enables Traps to detect malicious activity that could otherwise appear legitimate if inspected as individual events.*

- 4.1.1.4.7** Provide the ability to restrict execution of high-risk applications and computer processing activities to an isolated environment.

*Traps allows the creation and use of policies that can be applied to specific systems. These policies can restrict execution of high-risk applications and computer processing activities to an isolated environment.*

- 4.1.1.4.8** Automatically eliminate and report all isolation container artifacts of compromise and intrusion remnants.

*When Traps detects malware on a Windows endpoint, you can take additional precautions to quarantine the file. When Traps quarantines malware, Traps can automatically move it from the location on a local or removable hard drive to a local quarantine folder where it isolates the file. This prevents the file from attempting to run again or causing any harm to your endpoints.*

- 4.1.1.4.9** Provide continual verification of the integrity of the isolation container to ensure there is no unauthorized/malicious access or persistent modification.

*Traps also offers a more sophisticated method for protecting said system resources and/or other files without implementing said time consuming integrity checking. This method is called Behavioral Threat Protection (or BTP). BTP enables continuous monitoring of endpoint activity to identify and analyze chains of events—known as causality chains. This enables Traps to detect malicious activity that could otherwise appear legitimate if inspected as individual events.*

- 4.1.1.4.10** Automatically report potentially malicious events detected within the isolation container and provide actionable information.

*Traps provides an intuitive interface that makes it easy to manage policies and events and accelerate incident response – helping to minimize the operational challenges associated with protecting your endpoints. From the Traps management service web console, you can manage the endpoint security policy, review security events as they occur, and perform additional analysis of associated logs.*

- 4.1.1.4.11** Be capable of containing operating system kernel-level vulnerability exploitation.

*Traps has several Kernel exploit prevention modules. By blocking processes from accessing injected malicious code, Traps is able to prevent the attacks early in the attack lifecycle without impacting legitimate processes.*

- 4.1.1.4.12** Provide options for configurable automated or manual remediation actions in response to detected potentially malicious events.

*Traps provides several options for Investigation and response, including our Live Terminal feature (which allows a SecOps team to initiate a remote connection to an endpoint). Live Terminal enables you to manage remote endpoints. Investigative and response actions that you can perform include the ability to navigate and manage files in the file system, manage active processes, and run Windows or Python commands).*

#### 4.1.1.5 Reporting & Monitoring

- 4.1.1.6** The Vendor must provide a software or service that shall interoperate with event monitoring and correlation systems to facilitate aggregated situational awareness.

*Traps allows for its event data to be used with the Palo Alto Networks Cortex XDR Platform. With Cortex XDR, your analysts can triage alerts from any source with a single click, reducing alert fatigue and dwell time. Cortex XDR automatically reveals the root cause and sequence of events associated with any threat, enabling analysts of all experience levels to quickly investigate an incident. Powerful search tools make threat hunting a snap. Additionally, the Traps logs stored are easily forwarded logs stored on the Cortex Data Lake to an external syslog receiver and email destination.*

- 4.1.1.7** The software shall support open standards for automated threat information sharing.

*Traps uses open standards to format and forward relevant threat logs to other systems.*

- 4.1.1.8** The software shall provide integrated and customizable search with, at minimum, the ability to search data from all systems for information relevant to an incident investigation or risk analysis.

*The Traps Management System and Cortex XDR automatically reveals the root cause and sequence of events associated with any threat, enabling analysts of all experience levels to quickly investigate an incident. Powerful search tools make threat hunting easy and available. With this rich set of capabilities, your team can automatically detect sophisticated attacks by analyzing network, endpoint and cloud data.*

- 4.1.1.9** The software shall have the ability to execute manual and scheduled scans of specified systems for indicators derived from threat intelligence or other sources.

*In addition to blocking the execution of malware, Traps can scan your endpoints and attached removable drives for dormant malware that is not actively attempting to run. If you enable Traps to quarantine malicious files, Traps can also automatically quarantine any malware it finds during the scan. Otherwise, Traps only reports the malware to Traps management service so that you can manually take additional action to remove the malware before it is triggered and attempts to harm the endpoint.*

- 4.1.1.10** The software shall provide integrated analytics (including visualization) and support the creation of custom analytics, in order to identify anomalous endpoint behaviors, support incident investigation, and perform event analysis.

*Cortex XDR Analytics is a cloud app that runs in Cortex by Palo Alto Networks. It automatically detects and reports on post-intrusion threats by identifying good (normal) behavior on your network, so that it can notice bad (anomalous) behavior. The analytics app uses an analytics engine to examine your network and VPN traffic, and endpoint activity data. This engine is built to process—in parallel—large amounts of data stored in Cortex Data Lake. The ultimate goal is to identify normal behavior so the Cortex apps can recognize and use alerts to notify you of that abnormal behavior.*

- 4.1.1.11** The software shall allow administrative functions to be delegated to users based on roles/permissions and or groupings of endpoints they are responsible for managing.

*Traps and Cortex XDR Role-based access control (RBAC) enables you to use preconfigured roles to assign access rights to administrative users. You can manage roles for all Cortex apps and services in the Cortex hub. By assigning roles, you enforce the separation of access among functional or regional areas of your organization. Each role extends specific privileges to users. The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access privileges to administrative user accounts. The built-in roles provide specific access rights that cannot be changed.*

- 4.1.1.12** The software shall support delegation (i.e., user-specified) of who can access/view collected endpoint data.

*Traps and Cortex XDR Role-based access control (RBAC) enables you to use preconfigured roles to assign access rights to administrative users. You can manage roles for all Cortex apps and services in the Cortex hub. By assigning roles, you enforce the separation of access among functional or regional areas of your organization. Each role extends specific privileges to users. The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access privileges to administrative user accounts. The built-in roles provide specific access rights that cannot be changed.*

- 4.1.1.13** The software shall have the capability to be tuned/configured to reduce alerts resulting from false positives.

*Traps uses a default, out-of-the-box policy to provide protection against malware and exploit. It is highly recommended to use content updates regularly to enjoy policy updates from Palo Alto Networks. In the case of a false positive, Traps can allow an administrator with the correct privileges to create an exception for the false positive.*

- 4.1.1.14** The software shall provide configurable alerting based upon administrator defined criteria.

*Both Traps and Cortex XDR, beyond raising alerts within their own user interfaces also sends alerts to Cortex Data Lake. This allows other Cortex apps to consume Cortex XDR – Analytics alerts and apply their own logic and actions. Specific alerts to specific SecOp operators are also available.*

- 4.1.1.15** The software shall send alerts at administrator-definable intervals.

*Specific alerts to specific SecOp operators is available.*

- 4.1.1.16** The software shall provide the ability to automatically discover and alert on previously unknown external and/or internal hardware/peripheral devices (such as storage) connected to endpoints for the purpose of retrospective/post-event analysis.

*Malicious code can gain access to endpoints through external media, such as removable drives and optical drives. To protect against this type of attack, you can define restriction rules that prevent executable files from running on external drives that are attached to your endpoints. Defining a restriction on external media protects against any attempt to launch an executable file from an external drive. As a near term roadmap feature Traps will be able to Monitor any plugged mass storage and portable devices to allow or deny their use on the endpoint.*

- 4.1.1.17** The software shall generate reports based on pre-saved user- defined formats and datasets to facilitate rapid analysis, decision making, and follow-up actions following events.

*From within Cortex XDR, the relevant Traps endpoint and Palo Alto Networks Firewall alerts can use pre-configured and used defined Behavioral indicators of compromise (BIOCs) to enable you to alert, report and respond to behaviors— tactics, techniques, and procedures. Instead of hashes and other traditional indicators of compromise, BIOC rules detect the behavior of processes, registry, files, and network activity.*

- 4.1.1.18** The software shall provide time stamping of all collected data and events based on a single time standard (e.g., coordinated universal time).

*Traps and Cortex XDR use a single, coordinated timestamp to facilitate correlation of security events.*

- 4.1.1.19** The software shall have the ability to pull locally stored data from specified endpoints in near real time to support high priority hunt and forensic operations.

*Traps reports up to its management system security events in near real time. Additionally, the Live terminal feature allows for real time access to the system(s) in question to support investigations.*

- 4.1.1.20** *The software shall provide automated analysis and visualization of an attack; including production of an event timeline and initial assessment of severity/impact.*

*Traps and Cortex XDR produce a timeline and visual representation of a security event, allowing for security investigation teams. When a malicious file, behavior, or technique is detected, Cortex XDR (Investigation and Response) correlates available data across your detection sensors to display the sequence of activity that led to the alert. This sequence of events is called the causality chain. The causality chain is built from processes, events, insights, and alerts associated with the activity. During alert investigation, you should review the entire causality chain to fully understand why the alert occurred.*

## 4.2 Technical Details

- 4.2.1.1** The Vendor must provide the minimum supported platforms including: Windows operating system, Linux operating system, and all virtual environments including but not limited to VMWare, Azure, and Hyper-V.

*Palo Alto Networks Traps runs in most environments including the Windows operating system, Linux operating system, and all virtual environments including but not limited to VMWare, Azure, AWS, GCP and Hyper-V.*

- 4.2.1.2** The software shall not impair authorized system operations nor shall it degrade managed system performance in any way, which may adversely impact a system's primary business/mission functions. The following authorize system operations include but not limited to:

- 4.1.2.2.1** Patching, Scanning, Business software usage

*Traps was designed to accommodate operating and application systems out of the box. In addition, Traps can accommodate other business functions such as scanning or remote desktop access. For the occasion where Traps does not have out of the box accommodation for a given activity, a Traps security administrator can provide exceptions on an as needed basis.*

- 4.1.2.2.2** The following Information Assurance Tools/Initiatives include but not limited to:

- 4.1.2.2.1** Secure host baseline, and assured compliance assessment software.

*The Traps endpoint agent consists of various drivers and services yet requires minimal memory and CPU usage to ensure a non-disruptive user experience.*

- 4.2.1.3** The software shall allow for patching and update of containerized applications through a means of automated verification (e.g., integration with automated patch management infrastructure/processes).

*Traps allows for the patching of protected systems either through a trusted signer or a customer created exception.*

- 4.2.1.4** All software components shall have the ability to be automatically deployed and configured based on predefined configurations.

*The Traps agent can be automatically deployed via the State of West Virginia's current software distribution system. After that initial deployment, the installed agent is completely managed by the Traps Management System, including all configurations.*

- 4.2.1.5** The software shall securely store and transmit data in a manner that ensures the confidentiality, integrity, availability, and source authenticity of the data.

*All customer data is encrypted both in transit as well as at rest via HTTPS and AES 256-bit encryption, using signed applications. This ensures the confidentiality, integrity, availability, and source authenticity of the data.*

- 4.2.1.6** The software shall encrypt all data in transit or data at rest with Federal Information Processing Standards (FIPS) 140-2 compliant cryptographic modules.

*All customer data is encrypted both in transit as well as at rest via HTTPS and AES 256-bit encryption. We are currently being certified for FedRAMP, which requirements include additional controls above the standard NIST baseline controls in NIST SP 800-53 Revision 4. These additional controls address the unique elements of cloud computing to ensure all data is secure in cloud environments. Note that FedRAMP requires that FIPS-140-2 validated encryption be deployed for all cryptographic functions so by default Traps and Cortex XDR will be FIPS 140-2 compliant.*



## END USER AGREEMENT (“EULA”)

THIS IS A LEGAL AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER”, “END USER”, “YOU” or “YOUR”) AND (A) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054 UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; OR (B) PALO ALTO NETWORKS (NETHERLANDS) B.V., OVAL TOWER, DE ENTRÉE 99-197, 5TH FLOOR, 1101 HE AMSTERDAM, IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA (“PALO ALTO NETWORKS”).

BY DOWNLOADING, INSTALLING, REGISTERING, ACCESSING, EVALUATING OR OTHERWISE USING PALO ALTO NETWORKS PRODUCTS, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE BOUND TO THIS EULA. IF YOU DO NOT ACCEPT ALL ITS TERMS, IMMEDIATELY CEASE USING OR ACCESSING THE PRODUCT. THIS EULA GOVERNS YOUR USE OF PALO ALTO NETWORKS PRODUCTS HOWEVER THEY WERE ACQUIRED INCLUDING WITHOUT LIMITATION VIA AN AUTHORIZED DISTRIBUTOR, RESELLER, ONLINE APP STORE, OR MARKETPLACE. MAINTENANCE AND SUPPORT SERVICES ARE GOVERNED BY THE END USER SUPPORT AGREEMENT (“EUSA”) FOUND AT [www.paloaltonetworks.com/legal/eusa](http://www.paloaltonetworks.com/legal/eusa) WHICH IS HEREBY INCORPORATED BY REFERENCE INTO THIS EULA.

### 1. DEFINITIONS

“**Affiliate**” means any entity that Controls, is Controlled by, or is under common Control with End User or Palo Alto Networks, as applicable, where “Control” means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

“**End User Data**” means data that may be accessed or collected by Products during the relationship governed by this EULA, in the form of logs, session data, telemetry, user data, usage data, threat intelligence data, and copies of potentially malicious files detected by the Product. End User Data may include confidential data and personal data, such as source and destination IP addresses, active directory information, file applications, URLs, file names, and file content.

“**Hardware**” means hardware-based products listed on Palo Alto Networks’ then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

“**Product**” means, collectively, Hardware, Software, Subscription, or any combination thereof.

“**Security Incident**” means any unauthorized access to any End User Data stored on Palo Alto Networks’ equipment or in Palo Alto Networks’ facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of End User Data that compromises the privacy, security or confidentiality of such End User Data.

“**Software**” means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

“**Subscription**” means cloud-hosted, SaaS offerings provided by Palo Alto Networks including, but not limited to, Aperture, AutoFocus, Evident, GlobalProtect Cloud, Logging, Magnifier, RedLock, Threat Prevention, URL Filtering, WildFire, regardless of whether a fee is charged for its use. Maintenance and support, and professional services are not considered Subscriptions under this EULA.

### 2. USE AND RESTRICTIONS

#### a. Software Use Grant

This section 2.a applies to Software only. Palo Alto Networks grants you a limited, non-exclusive right to use the Software:

- i. in accordance with published specifications for the Product;
- ii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and
- iii. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this EULA. All other rights in the Software are expressly reserved by Palo Alto Networks.

#### b. Access to Subscriptions

This section 2.b applies to Subscriptions only. During the period for which you purchased Subscriptions, Palo Alto Networks will use commercially reasonable efforts to make them available 24 hours a day, 7 days a week except for published downtime or any unavailability caused by circumstances beyond our control including, but not limited to, a force majeure event described in section 13.g below. Palo Alto Networks grants you a non-exclusive right to access the Subscriptions:

- i. in accordance with published specifications for the Subscriptions;

- ii. solely for your internal use, unless agreed otherwise in a separate written contract with Palo Alto Networks; and
- iii. through your third-party contractor providing IT services solely for your benefit, subject to their compliance with this EULA.

All other rights to the Subscriptions are expressly reserved by Palo Alto Networks.

c. Use Restrictions

You shall not:

- i. modify, translate or create derivative works from the Products, in whole or in part;
- ii. disassemble, decompile, reverse engineer or otherwise attempt to derive the source code of the Products, in whole or in part, unless expressly permitted by applicable law in the jurisdiction of use despite this prohibition;
- iii. disclose, publish or otherwise make publicly available any benchmark, performance or comparison tests that you (or a third-party contracted by you) run on the Products, in whole or in part;
- iv. interfere with, disrupt the integrity or performance of, or attempt to gain unauthorized access to the Subscriptions, their related systems or networks, or any third-party data contained therein;
- v. use the Subscriptions in any manner not authorized by the published specifications for the applicable Subscriptions;
- vi. duplicate the Software, except for making a reasonable number of archival or backup copies, provided that you reproduce in your copy the copyright, trademark and other proprietary notices or markings that appear on the original copy of the Software (if any) as delivered to you;
- vii. sell, resell, distribute, transfer, publish, disclose, rent, lend, lease or sublicense the Products, except in accordance with Palo Alto Networks license transfer procedure (<https://www.paloaltonetworks.com/support/support-policies/secondary-market-policy.html>); or
- viii. make the functionality of the Products available to any third party through any means, including without limitation, by uploading the Software to a network or file-sharing service or through any hosting, application services provider, service bureau or other type of services unless agreed otherwise in a separate managed services agreement with Palo Alto Networks.

d. Affiliates

If you purchase Product for use by your Affiliate, you shall:

- i. provide the Affiliate with a copy of this EULA;
- ii. ensure that the affiliate complies with the terms and conditions therein; and
- iii. be responsible for any breach of this EULA by such affiliate.

e. Authentication Credentials and Security Incidents

You shall keep accounts and authentication credentials providing access to Products secure and confidential. You must notify Palo Alto Networks without undue delay about any actual or suspected misuse of your accounts or authentication credentials or of any Security Incident you become aware of.

### 3. OWNERSHIP

Palo Alto Networks and its suppliers retain all rights to intellectual and intangible property relating to the Product, including but not limited to copyrights, patents, trade secret rights, and trademarks and any other intellectual property rights therein unless otherwise indicated. You shall not delete or alter the copyright, trademark, or other proprietary rights notices or markings that appear on the Product. To the extent you provide any suggestions or comments related to the Products, Palo Alto Networks shall have the right to retain and use any such suggestions or comments in current or future products or subscriptions, without your approval or compensation to you.

### 4. PAYMENT AND TAXES

a. Fees

Applicable fees will be set forth on the website at the time of purchase or in the applicable invoice. Note, however, that fees which are payable in advance for volume or capacity usage (e.g., terabytes of data, # of accounts, endpoints, devices, seats, users, workloads, etc.) must be reconciled with actual usage at the end of each month or applicable service period. Palo Alto Networks reserves the right to perform true-up reconciliation and charge for any usage above the volume or capacity purchased. Unless you have chosen monthly billing, fees will be due net thirty (30) days from invoice date. All sums due and payable that remain unpaid after any applicable cure period herein will accrue interest at the highest rate permissible by applicable law. Palo Alto Networks reserves the right to assign its right to receive payments hereunder to a third party with notice but without your consent. For purposes of such assignment, such third party shall be considered a third-party beneficiary of the payment obligation under this EULA. All fees are non-refundable unless otherwise specified.

b. Taxes

Prices quoted are exclusive of all sales, use, value-added, good and services, withholding and other taxes or duties. You will pay or self-assess all taxes and duties assessed in connection with this EULA and its performance, except for taxes payable on Palo Alto Networks' net income. To the extent that any amounts payable by you are subject to withholding taxes, the amount payable shall be grossed up such that the amount paid to Palo Alto Networks net of withholding taxes equals the amount invoiced by Palo Alto Networks. If you pay any withholding taxes based on payments made by you to Palo Alto Networks hereunder, you will furnish Palo Alto Networks with written documentation of all such tax payments, including receipts and other customary documentation, to demonstrate to the relevant tax authorities that you have paid such taxes. If applicable, you shall also provide Palo Alto Networks with appropriate VAT/GST registration numbers and other documentation satisfactory to the applicable taxing authorities to substantiate any claim of exemption from any tax or duties. You agree to indemnify Palo Alto Networks from liabilities, damage, costs, fees and expenses, arising out of or resulting from any third-party claims based on or otherwise attributable to your breach of this section 4.b.

The entirety of this section 4 does not apply to you if you purchased Product from an authorized reseller.

**5. THIRD-PARTY PRODUCTS AND SERVICES**

Through its Security Operating Platform, Palo Alto Networks may make available to you third-party products or services ("**third-party apps**") which may contain features designed to interoperate with our Products. To use such features, you must obtain access to such third-party apps from their respective providers. All third-party apps are optional and if you choose to utilize such third-party apps:

- i. all governing terms and conditions, including data processing terms, shall be entered into between you and the applicable app provider;
- ii. you may be required to grant Palo Alto Networks access to your account on such third-party apps; and
- iii. you instruct Palo Alto Networks to allow the app provider to access your data as required for the interoperation with our Products.

In the event the operation of the third-party app requires the processing of personal data to which the General Data Protection Regulation ("**GDPR**") applies in a country that does not provide adequate data protection safeguards, then you and the app provider will put in place an adequate data transfer mechanism as set out in Arts. 46 or 47 of the GDPR, including executing appropriate Standard Contractual Clauses, as needed. Palo Alto Networks shall not be responsible for any disclosure, modification, or deletion of your data resulting from access by such app providers. App providers do not operate as sub-processors to Palo Alto Networks, as that term is defined in the GDPR. Palo Alto Networks is not liable for and does not warrant or support any such third-party apps, whether or not they are designated as "Palo Alto Networks-certified" or otherwise. Similarly, Palo Alto Networks cannot guarantee the continued availability of such third-party apps, and may cease providing them without entitling you to any refund, credit, or other compensation, if for example the provider of the third-party app ceases to make its product or service available in a manner acceptable to Palo Alto Networks.

**6. TERM; TERMINATION; AND EFFECT OF TERMINATION**

This EULA is effective until terminated. You may terminate this EULA at any time by notifying Palo Alto Networks. Palo Alto Networks may terminate this EULA at any time in the event you breach any material term of this EULA and fail to cure such breach within thirty (30) days following notice. Upon termination, you shall immediately cease using the Product.

**7. WARRANTY, EXCLUSIONS AND DISCLAIMERS**

a. Warranty

Palo Alto Networks warrants that:

- i. the Hardware shall be free from defects in material and workmanship for one (1) year from the date of shipment;
- ii. the Software will substantially conform to Palo Alto Networks' published specifications for three (3) months from the date of shipment; and
- iii. the Subscriptions shall perform materially to published specifications for the Product. As your sole and exclusive remedy, and Palo Alto Networks' and its suppliers' sole and exclusive liability for breach of warranty, Palo Alto Networks shall, at its option and expense, repair or replace the Hardware or correct the Software or the Subscriptions, as applicable.

All warranty claims must be made on or before the expiration of the warranty period specified herein, if any. Replacement Products may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or

any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not. You will pay the shipping costs for return of Products to Palo Alto Networks. Palo Alto Networks will pay the shipping costs for repaired or replaced Products back to you.

**b. Exclusions**

The warranty set forth above shall not apply if the failure of the Product results from or is otherwise attributable to:

- i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks or a Palo Alto Networks-authorized party;
- ii. accident, negligence, abuse or misuse of a Product;
- iii. use of the Product other than in accordance with Palo Alto Networks' published specifications;
- iv. improper installation or site preparation or your failure to comply with environmental and storage requirements set forth in the published specifications including, without limitation, temperature or humidity ranges; or
- v. causes external to the Product such as, but not limited to, failure of electrical systems, fire or water damage.

**c. Disclaimers**

EXCEPT FOR THE WARRANTIES EXPRESSLY STATED AND TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCTS ARE PROVIDED "AS IS". PALO ALTO NETWORKS AND ITS SUPPLIERS MAKE NO OTHER WARRANTIES AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. PALO ALTO NETWORKS DOES NOT WARRANT THAT (A) THE PRODUCTS WILL MEET YOUR REQUIREMENTS, (B) USE THEREOF SHALL BE UNINTERRUPTED OR ERROR-FREE, OR (C) THE PRODUCTS WILL PROTECT AGAINST ALL POSSIBLE THREATS WHETHER KNOWN OR UNKNOWN.

**8. LIMITATION OF LIABILITY**

**a. Disclaimer of Indirect Damages**

To the fullest extent permitted by applicable law, in no event shall either party or Palo Alto Networks' suppliers be liable for any special, indirect, incidental, punitive, exemplary or consequential damages of any kind (including but not limited to loss of use, data, business or profits, or for the cost of procuring substitute products, services or other goods), arising out of or relating to this EULA, regardless of the theory of liability and whether or not the other party was advised of the possibility of such damage or loss.

**b. Direct Damages**

To the fullest extent permitted by applicable law, in no event shall the total liability of either party or Palo Alto Networks' suppliers, from all claims or causes of action and under all theories of liability arising out of or relating to this EULA, exceed the greater of one million United States dollars or the total amount paid by End User for the entire term of the subscription or enterprise agreement on which the claim is based. The foregoing limitation in this section 8.b shall not apply to liability arising from:

- i. death or bodily injury;
- ii. sections 2 (Use and Restrictions) and 9 (Indemnification); and
- iii. End User's payment obligations for the Product.

**9. INDEMNIFICATION**

**a. Indemnification and Procedure**

Palo Alto Networks will defend, at its expense, any third-party action or suit against you alleging that the Product infringes or misappropriates such third party's patent, copyright, trademark, or trade secret (a "**Claim**"), and Palo Alto Networks will pay damages awarded in final judgment against you or agreed to in settlement by Palo Alto Networks that are attributable to any such Claim; provided that you (a) promptly notify Palo Alto Networks in writing of the Claim; (b) give Palo Alto Networks sole control of the defense and settlement of the Claim; and (c) reasonably cooperate with Palo Alto Networks' requests for assistance with the defense and settlement of the Claim. Palo Alto Networks will not be bound by any settlement or compromise that you enter into without Palo Alto Networks' prior written consent.

**b. Remedy**

If the Product becomes, or in Palo Alto Networks' opinion is likely to become, the subject of a Claim, then Palo Alto Networks may, at its sole option and expense:

- i. procure the right for you to continue using the Product;
- ii. replace or modify the Product to avoid the Claim; or
- iii. if options (i) and (ii) cannot be accomplished despite Palo Alto Networks' reasonable efforts, then Palo Alto Networks may accept return of the Product and grant you credit for the price of the Product as depreciated on a straight-line five (5) year basis, commencing on the date you received such Product or, for Subscriptions, grant you credit for the portion of the Subscription paid but not used.

c. Exceptions

Palo Alto Networks' obligations under this section shall not apply to the extent any Claim results from or is based on:

- i. modifications to the Product made by a party other than Palo Alto Networks or its designee;
- ii. the combination, operation, or use of the Product with hardware or software not supplied by Palo Alto Networks, if a Claim would not have occurred but for such combination, operation or use;
- iii. failure to use the most recent version or release of the Product;
- iv. Palo Alto Networks' compliance with your explicit or written designs, specifications or instructions; or
- v. use of the Product not in accordance with published specifications.

THE FOREGOING TERMS STATE PALO ALTO NETWORKS' SOLE AND EXCLUSIVE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY THIRD-PARTY CLAIMS OF INTELLECTUAL PROPERTY INFRINGEMENT OR MISAPPROPRIATION.

## 10. CONFIDENTIALITY

"**Confidential Information**" means the non-public information that is exchanged between the parties, provided that such information is identified as confidential at the time of disclosure by the disclosing party ("**Discloser**"), or disclosed under circumstances that would indicate to a reasonable person that the information ought to be treated as confidential by the party receiving such information ("**Recipient**").

Notwithstanding the foregoing, Confidential Information is exclusive of information or data that Recipient can prove by credible evidence:

- a. Was in the public domain at the time it was communicated to Recipient;
- b. Entered the public domain subsequent to the time it was communicated to Recipient through no fault of Recipient;
- c. Was in Recipient's possession not in violation of any obligation of confidentiality at the time it was communicated to Recipient;
- d. Was disclosed to Recipient not in any violation of any obligation of confidentiality; or
- e. Was developed by employees or agents of Recipient without use of or reference to the Confidential Information of Discloser.

Each party will not use the other party's Confidential Information, except as necessary for the performance of this EULA, and will not disclose such Confidential Information to any third party, except to those of its employees and subcontractors that need to know such Confidential Information for the performance of this EULA, provided that each such employee and subcontractor is subject to a written agreement that includes binding use and disclosure restrictions that are at least as protective as those set forth herein. Each party will use all reasonable efforts to maintain the confidentiality of all of the other party's Confidential Information in its possession or control, but in no event shall each party use less effort than it ordinarily uses with respect to its own confidential information of similar nature and importance.

The foregoing obligations will not restrict either party from disclosing the other party's Confidential Information or the terms and conditions of this EULA:

- a. Pursuant to the order or requirement of a court, administrative agency, or other governmental body, provided that the party required to make such a disclosure gives reasonable notice to the other party to enable it to contest such order or requirement;
- b. On a confidential basis to its legal or professional financial advisors; or
- c. As required under applicable securities regulations.

The foregoing obligations of each Party shall continue for the period terminating three (3) years from the date on which the Confidential Information is last disclosed, or the date of termination of this EULA, whichever is later.

## 11. END USER DATA AND DATA PROTECTION

a. Sharing Data

Palo Alto Networks provides End User the ability to configure the Products to share End User Data (including type thereof) with Palo Alto Networks for threat analysis and prevention as described in the applicable Product documentation, which contains details regarding the processing of End User Data and End User's options for sharing such data.

b. Data Processing

End User acknowledges, agrees and grants to Palo Alto Networks the right, to the extent permitted by applicable law, to process and retain data, including End User Data, shared by End User related to a security event, for the legitimate interest of operating, providing, maintaining, developing, and improving security technologies and services, including for purposes compatible with providing such services. To the extent Palo Alto Networks processes personal data on behalf of End User as a processor in the meaning given in EU data protection law, it will do so in accordance with section 12.

c. Subcontractors

Palo Alto Networks will take appropriate measures to safeguard the confidentiality of End User Data. Except where required by law, Palo Alto Networks will not share End User Data with third parties other than with selected subcontractors. Palo Alto Networks will impose appropriate contractual obligations upon such subcontractors that are no less protective than this section 11 and Palo Alto Networks will remain responsible for the subcontractor's compliance with this EULA and for any acts or omissions of the subcontractor that cause Palo Alto Networks to breach any of its obligations under this EULA.

d. Regional Data Centers

For some Products, End Users may configure the Products to have End User Data remain in facilities located within the European Economic Area or another available region. If so, Palo Alto Networks will not transfer data out of the selected region, unless compelled by law or a binding order of a governmental body.

e. Compliance with Laws

Palo Alto Networks will process End User Data in accordance with applicable data protection laws, including, where applicable, the EU General Data Protection Regulation. End User represents and warrants that its use of the Products, its authorization for Palo Alto Networks' access to data, and any related submission of data to Palo Alto Networks, including any End User Data contained therein, complies with all applicable laws, including those related to data privacy, data security, electronic communication and the export of technical, personal or sensitive data.

f. PCI Compliance

Palo Alto Networks is not a payment processor and as such is not subject to compliance with PCI standards. However, Palo Alto Networks acknowledges that credit card information may be provided by End User during the performance or use of Products and therefore Palo Alto Networks shall use information data security controls that are compliant with PCI standards.

g. Audit

Palo Alto Networks will select an independent, qualified third-party auditor to conduct, at Palo Alto Networks' expense, at least annual audits of the security of its data centers, its systems, and its computing environments used to process End User Data, in accordance with the SOC2 Type II standards or its equivalent. At End User's request and under non-disclosure agreement Palo Alto Networks will provide such audit report to End User so that it may verify Palo Alto Networks' compliance with the adopted security framework.

## **12. PROCESSING AS DATA PROCESSOR**

a. Data Processor

To the extent Palo Alto Networks processes personal data on behalf of End User as a processor as defined by EU data protection law, it shall do so only on instructions from End User pursuant to this EULA and as permitted by applicable law.

b. Confidentiality of Personal Data

Palo Alto Networks will ensure that personnel it authorizes to process personal data have committed themselves to confidentiality or are under appropriate statutory obligation of confidentiality.

c. Sub-Processors

End User authorizes Palo Alto Networks to engage sub-processors, as described in the applicable Product documentation for the relevant Product, to process personal data. In the event Palo Alto Networks engages any new sub-processor it will:

- i. update the applicable documentation;
- ii. notify End Users that have opted in to receive compliance notifications of such change to give End User the opportunity to object to such sub-processing;
- iii. impose appropriate contractual obligations upon the sub-processor that are no less protective than this section 12; and
- iv. remain responsible for the sub-processor's compliance with this EULA and for any acts or omissions of the sub-processor that cause Palo Alto Networks to breach any of its obligations under this EULA.

If End User objects to a new sub-processor, it must do so in writing within fifteen (15) days of such update and Palo Alto Networks will then endeavor to offer alternate options for the delivery of Products that do not involve the new sub-processor without prejudice to any of End User's termination rights.

d. Security

Palo Alto Networks has implemented practices and policies to maintain appropriate organizational, physical and technical measures to safeguard the confidentiality and security of personal data to comply with applicable laws.

e. Security Incident Notification

In the event of a Security Incident affecting End User personal data, Palo Alto Networks will without undue delay:

- i. inform End User of the Security Incident pursuant to section 13.j below;
- ii. investigate and provide End User with detailed information about the Security Incident; and
- iii. take reasonable steps to mitigate the effects and minimize any damage resulting from the Security Incident as required by applicable law.

f. Assistance to Data Subjects

Palo Alto Networks shall provide reasonable assistance to End User to comply with its obligations with regard to data subject rights under applicable data protection law and any other legal requirements, as appropriate, taking into account the nature of the data processing and the information available to Palo Alto Networks.

g. Data Retention

Palo Alto Networks shall process and retain personal data no longer than necessary for the purposes which it is processed. Upon termination of this EULA, Palo Alto Networks shall, upon End User's request, delete End User Data that is no longer necessary to carry out any of the purposes under section 11.b.

h. International Transfer of Data

End User personal data may be sent to facilities hosted outside of the country where End User purchased or utilizes the Products. Palo Alto Networks will comply with the European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland, including the execution of EU Standard Contractual Clauses for data transfer, where applicable.

### 13. GENERAL

a. Assignment

Neither party may assign or transfer this EULA or any obligation hereunder without the prior written consent of the other party, except that, upon written notice, Palo Alto Networks may assign or transfer this EULA or any obligation hereunder to its subsidiary or Affiliate, or an entity acquiring all or substantially all of the assets of Palo Alto Networks, whether by acquisition of assets or shares, or by merger or consolidation without your consent. Any attempt to assign or transfer this EULA shall be null and of no effect. For purposes of this EULA, a change of control will be deemed to be an assignment. Subject to the foregoing, this EULA shall be binding upon and inure to the benefit of the successors and assigns of the parties.

b. Auditing End User Compliance

You grant to Palo Alto Networks and its independent advisors the right to examine your books, records, and accounts during normal business hours to verify compliance with this EULA. In the event such audit discloses non-compliance with this EULA, you shall promptly pay the appropriate license fees, plus reasonable audit costs.

c. Authorization Codes, Grace Periods and Registration

Your Product may require an authorization code to activate or access Subscriptions and support. The authorization codes will be issued at the time of order fulfillment. Where applicable, you will be able to download Software via the server network located closest to you. The subscription or support term will commence in accordance with the grace period policy at <https://www.paloaltonetworks.com/support/support-policies/grace-period.html>. You are hereby notified that, upon applicable grace period expiration, if any, Palo Alto Networks reserves the right to register and/or activate your Product and support services (if purchased) on your behalf without further notification to you.

d. Compliance with Laws; Export Control

You shall comply with all applicable laws in connection with your use of the Product. You further agree that you will not engage in any illegal activity in any relevant jurisdiction, and you acknowledge that Palo Alto Networks reserves the right to notify its customers or appropriate law enforcement in the event of such illegal activity. Both parties shall comply with the U.S. Export Administration Regulations, and any other export laws, restrictions, and regulations to ensure that the Product and any technical data related thereto is not exported or re-exported directly or indirectly in violation of or used for any purposes prohibited by such laws and regulations.

e. Cumulative Remedies

Except as expressly set forth in this EULA, the exercise by either party of any of its remedies will be without prejudice to any other remedies under this EULA or otherwise.

f. Entire Agreement

This EULA constitutes the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior written or oral agreements, understandings and communications between them with respect to the subject matter hereof. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with or in addition to the terms and conditions of this EULA are hereby rejected by Palo Alto Networks and shall be deemed null and of no effect.

g. Force Majeure

Palo Alto Networks shall not be responsible for any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, terrorism, armed conflict, labor strike, lockout, boycott or other similar events beyond its reasonable control.

h. Governing Law

If you are located in North or Latin America, this EULA shall be governed by and construed in accordance with the laws of the state of California, excluding its conflict of laws principles. Any legal action or proceeding arising under this EULA will be brought exclusively in the state or federal courts located in Santa Clara, California, or the Northern District of California, as applicable. If you are located outside North or Latin America, this EULA shall be governed by and construed in accordance with the laws of the Netherlands, excluding its conflict of laws principles. Any legal action or proceeding arising under this EULA will be brought exclusively before the District Court of Amsterdam, the Netherlands. The United Nations Convention on Contracts for the International Sale of Goods shall not apply.

i. Headings

The headings, including section titles, are given solely as a convenience to facilitate reference. Such headings shall not be deemed in any way material or relevant to the construction or interpretation of this document or any of its provisions.

j. Notices

All notices shall be in writing and delivered by overnight delivery service or by certified mail sent to the address published on the respective parties' websites or the address specified on the relevant order document (attention: Legal Department), and in each instance will be deemed given upon receipt.

k. Open Source Software

The Products may contain or be provided with components subject to the terms and conditions of open source software licenses ("**Open Source Software**"). A list of Open Source Software can be found at <https://www.paloaltonetworks.com/documentation/oss-listings/oss-listings.html>. These Open Source Software license terms are consistent with the license granted in section 2 (Use and Restrictions) and may contain additional rights benefitting you. Palo Alto Networks represents and warrants that the Product, when used in conformance with this EULA, does not include Open Source Software that restricts your ability to use the Product nor requires you to disclose, license, or make available at no charge any material proprietary source code that embodies any of your intellectual property rights.

l. Reciprocal Waiver of Claims Related to United States SAFETY Act

Where a Qualified Anti-terrorism Technology (the "**QATT**") has been deployed in defense against, response to or recovery from an "act of terrorism" as that term is defined under the SAFETY Act, Palo Alto Networks and End User agree to waive all claims against each other, including their officers, directors, agents or other representatives, arising out of the manufacture, sale, use or operation of the QATT, and further agree that each is responsible for losses, including business interruption losses, that it sustains, or for losses sustained by its own employees resulting from an activity arising out of such act of terrorism.

m. Survival

Sections regarding license restrictions, ownership, term and termination, U.S. Government End Users, limitations of liability, governing law, and this General section shall survive termination of this EULA.

n. U.S. Government End Users

This section applies to United States Government End Users only and does not apply to any other End Users. The Software and its documentation are "commercial computer software" and "commercial computer software documentation," respectively; as such terms are used in FAR 12.212 and DFARS 227.7202. If the Software and its documentation are being acquired by or on behalf of the U.S. Government, then, as provided in FAR 12.212 and DFARS 227.7202-1 through 227.7202-4, as applicable, the U.S. Government's rights in the Software and its documentation shall be as specified in this EULA.

If any term or condition set forth in this EULA:

- i. allows for the automatic termination of the Government's license rights or maintenance of services;
- ii. allows for the automatic renewal of services and/or fees;



iii. allows for the Government to pay audit costs; and/or

iv. requires the governing law to be anything other than Federal law, then such term and condition shall not apply to the United States Government, but shall continue to apply to prime contractors and subcontractors of the Government.

Furthermore, nothing contained in this EULA is meant to diminish the rights of the United States Department of Justice as identified in 28 U.S.C. Section 516. Finally, to the extent any term and condition set forth in this EULA is contrary to United States Federal procurement law, then such term and condition shall not apply to the United States Government, but shall continue to apply to prime contractors and subcontractors of the government.

o. Waiver and Severability

The failure by either party to enforce any provision of this EULA will not constitute a waiver of future enforcement of that or any other provision. Any waiver or amendment of any provision of this EULA will be effective only if in writing and signed by authorized representatives of both parties. If any provision of this EULA is held to be unenforceable or invalid, that provision will be enforced to the maximum extent possible and the other provisions will remain in full force and effect.

## END USER SUPPORT AGREEMENT (“EUSA”)

THIS EUSA SUPPLEMENTS THE END USER AGREEMENT BETWEEN YOU (REFERRED TO HEREIN AS “CUSTOMER,” “END USER,” “YOU” or “YOUR”) AND (I) PALO ALTO NETWORKS, INC., 3000 TANNERY WAY, SANTA CLARA, CALIFORNIA 95054 UNITED STATES, IF YOU ARE LOCATED IN NORTH OR LATIN AMERICA; OR (II) PALO ALTO NETWORKS (NETHERLANDS) B.V., OVAL TOWER, DE ENTRÉE 99-197, 5<sup>TH</sup> FLOOR, 1101 HE AMSTERDAM, IF YOU ARE LOCATED OUTSIDE NORTH OR LATIN AMERICA (“PALO ALTO NETWORKS”).

This EUSA sets forth the terms and conditions under which Palo Alto Networks will provide technical support services for the Palo Alto Networks products sold and/or licensed pursuant to the Palo Alto Networks End User Agreement (“EULA”). Palo Alto Networks is willing to provide technical support services only if you accept these terms. By checking the box labeled “I accept”, you are indicating that you understand and accept these terms and conditions. If you are entering into this agreement on behalf of a company or other legal entity, you represent that you have the authority to bind such entity to this agreement, in which case the terms “you” or “your” shall refer to such company or other legal entity. Palo Alto Networks reserves the right not to support products which were not purchased via an authorized Palo Alto Networks distributor or reseller.

### 1. SUPPORT PLANS AND SERVICES OFFERED

| Support Offerings  | 4-HR Premium Support   | Premium Support  | Standard Support  |
|--|--|------------------|-------------------|
| Business Hours Availability  | Mon – Fri, 7am to 6pm PT   |                  |                   |
| After Hours Availability   | Yes - 24x7x365   | Yes - 24x7x365   | No                |
| Focused Services (Regular, Plus, Elite)  | Optional   | Optional         | No                |
| <b>Hardware Support</b>  |  |                  |                   |
| Advance Replacement Service: 4-Hour Replacement (available only for Hardware located within a specified range of a Palo Alto Networks service location)        | Yes  | No               | No                |
| Advance Replacement Service: Next Business Day Service   | N/A  | Yes              | No                |
| Return and Repair  | N/A  | N/A              | Yes               |
| <b>Call Response Times</b>   |  |                  |                   |
| Severity 1 – Critical<br>Product is down, critically affects Customer production environment. No workaround available yet.                                     | < 1 hour   | < 1 hour         | < 1 Business Hour |
| Severity 2 – High<br>Product is impaired, Customer production up, but impacted. No workaround available yet.   | 2 Hours  | 2 Hours          | 2 Business Hours  |
| Severity 3 – Medium<br>A Product function has failed, Customer production not affected. Support is aware of the issue and a workaround is available.           | 4 Hours  | 4 Hours          | 4 Business Hours  |
| Severity 4 – Low<br>Non-critical issue. Does not impact Customer business. Feature, information, documentation, how-to and enhancement requests from Customer. | 8 Business Hours   | 8 Business Hours | 8 Business Hours  |
| Contact Support:   | Website: <a href="http://support.paloaltonetworks.com">support.paloaltonetworks.com</a><br>Toll Free US: 1.866.898.9087<br>Outside the US: +1.408.738.7799 |                  |                   |

## 2. DEFINITIONS

**"Affiliate"** means any entity that Controls, is Controlled by, or is under common Control with End User or Palo Alto Networks, as applicable, where "Control" means having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of voting securities, by contract or otherwise.

**"Business Hours"** means Mondays through Fridays, 7:00 am – 6:00 pm PT, excluding US and California holidays.

**"Hardware"** means hardware-based products listed on Palo Alto Networks then-current price list or supplied by Palo Alto Networks regardless of whether a fee is charged for such hardware.

**"Maintenance Releases"** means bug fixes to the Software that: (i) are designated by a change in the 3rd set of digits of the version release number (e.g., v5.00.01 to v5.00.02); and (ii) are generally made available by Palo Alto Networks to its customers under valid support contracts, at no additional cost.

**"Major Releases"** means significant modifications or improvements to the Software that: (i) are designated by a change in the 1st digit of the version release number (e.g., v5.0 to v6.0); and (ii) are generally made available by Palo Alto Networks to its customers under valid support contracts, at no additional cost.

**"Minor Releases"** means minor modifications or improvements to the Software, cumulative bug fixes from Maintenance Releases since the last Minor Release and new bug fixes, as applicable, that: (i) are designated by a change in the 2nd set of digits of the version release number (e.g., v5.00 to v5.01); and (ii) are generally made available by Palo Alto Networks to its customers under valid support contracts, at no additional cost.

**"Product"** means, collectively, Hardware, Software, Subscription, or any combination thereof.

**"Software"** means any software embedded in Hardware and any standalone software that is provided without Hardware, including updates, regardless of whether a fee is charged for the use of such software.

**"Standard Support," "Premium Support," "4-Hour Premium Support,"** and **"Support Plans"** refer to the various support programs offered by Palo Alto Networks, as further detailed in section 3 below.

**"Subscription-based Offering"** or **"Subscription"** means cloud-hosted offerings provided by Palo Alto Networks including, but not limited to, Aperture, AutoFocus, Evident, GlobalProtect Cloud, Logging, Magnifier, RedLock, Threat Prevention, URL Filtering, WildFire, regardless of whether a fee is charged for its use.

**"Support Website"** means the website currently located at <https://support.paloaltonetworks.com>, or any successor site thereto, as specified by Palo Alto Networks.

## 3. DESCRIPTION OF SUPPORT PLANS

You must register each Product for which you have purchased support on the Support Website to access the features and benefits available to such Product. In consideration of your purchase of a Support Plan, Palo Alto Networks shall provide the services as set forth in the table entitled "Support Plans and Services Offered" above, including:

- a. Remote Technical Support
  - i. Telephone support available during the times specified for the Support Plan purchased.
  - ii. Support cases created via the web will have a response time based on the severity classification as set forth in the table entitled "Support Plans and Services Offered" above.
- b. Secure Web Access
  - i. Access to the Support Website to acquire the latest software versions, fixes, feature releases, software release notes, signature updates, FAQs, case management and technical documentation.
  - ii. Palo Alto Networks will use commercially reasonable efforts to ensure that the Support Website is available 24x7.

Palo Alto Networks reserves the right to modify the Support Plans offered so long as such modification does not result in degradation of service. Please refer to the Support Website for the most current support plan descriptions.

## 4. SUPPORT OPTIONS

You shall choose from these support plans: Standard Support, Premium Support, and 4-Hour Premium Support. Based upon your selection and payment of applicable fees, Palo Alto Networks must:

- a. Standard Support
  - i. maintain and support the list of releases defined as the currently-supported releases on the Support Website.
  - ii. make available all supported Maintenance Releases, Minor Releases and Major Releases.
  - iii. verify defects in the Software identified and submitted by customers.
  - iv. correct material defects in the Software for the currently-supported Maintenance Releases.
  - v. provide access to Palo Alto Networks online support through the Support Website including, but not limited to, knowledge base/FAQ, case management and software downloads.

- vi. provide technical telephone support during Business Hours.
- vii. provide a return and repair service for Hardware defects.

b. Premium Support

Includes all the benefits of Standard Support and the following:

- i. after-hours technical telephone support on a 7x24 basis.
- ii. advance replacement for defective Hardware. Please refer to section 5 (RMA Policy and Process), subsection b (Advance Replacement) below for additional details.

c. 4-Hour Premium Support

Includes all the benefits of Premium Support and delivery of replacement Hardware to you within four hours from the issuance of a RMA. This support option is available only for Hardware located within a specified range of a Palo Alto Networks service location. Eligibility must be determined, and the service sold, on a per-device basis. When covered, Palo Alto Networks will use commercially reasonable efforts to deliver replacements within the designated time frame.

## 5. RMA POLICY AND PROCESS

In situations when it is necessary for you to return a Product to Palo Alto Networks, you must ask Palo Alto Networks to issue a Return Material Authorization (“RMA”) number prior to shipment. Each RMA number will be uniquely identified to track the processing of the returned Product, pursuant to the RMA Process and Policy found at [https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/datasheets/support/rma-process-policy.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/rma-process-policy.pdf).

a. Return and Repair

You shall obtain a RMA number for the Product that you wish to return to Palo Alto Networks by contacting Support via telephone or email or via the Support Website. Support will work with you to confirm the Hardware problem and issue a RMA number to be used to ship the Product back to Palo Alto Networks. You shall repackage the Product in the original packaging (shipping damage that occurs from insufficient packaging is not covered under this agreement), note the RMA number on the shipping label and ship the Product to the specified Palo Alto Networks location. You will be responsible for all shipping costs incurred in returning the defective Product to Palo Alto Networks. Products will be repaired (or replaced) and shipped within 10 business days from receipt of the defective Product by Palo Alto Networks. Palo Alto Networks will pay all shipping costs incurred in shipping the repaired or replacement Product to you, except that if you are located outside the United States, you will be responsible for any taxes, duties, fees or other charges assessed in connection with importing the repaired or replaced Product into your country of destination.

b. Advance Replacement

You shall obtain a RMA number for the Product that you wish to return to Palo Alto Networks by contacting Support via telephone or via the Support Website. Support will work with you to confirm the Hardware problem and issue a RMA number to be used to ship the Product back to Palo Alto Networks. Palo Alto Networks will use commercially reasonable efforts to have a replacement Product delivered to you by the next business day. Palo Alto Networks will pay all shipping costs incurred in shipping the replacement Product to you. Upon receipt of a replacement Product, you shall return the defective Product to Palo Alto Networks in the replacement Product’s packaging (shipping damage that occurs from insufficient packaging is not covered under this agreement), using the prepaid return airbill affixed to the exterior of the shipping carton, and arranging for the designated courier service for pickup. If Palo Alto Networks does not receive the returned Product within 10 business days after the delivered date of the replacement Product, you will be charged current list price of the replacement Product.

c. 4-Hour Replacement

You shall obtain a RMA number for the Product that you wish to return to Palo Alto Networks. Support will work with you to confirm the Hardware problem and issue a RMA number. Palo Alto Networks will use commercially reasonable efforts to have a replacement Product delivered to you within four hours after issuance of the RMA number. You must have an authorized representative available to accept delivery of the replacement Product. If Palo Alto Networks (or its subcontractor) is unable to complete delivery because you did not have an authorized representative available, Palo Alto Networks reserves the right to charge you for costs incurred in making a subsequent delivery.

## 6. YOUR OBLIGATIONS

During the term of this agreement, you must:

- a. Operate at the then-supported Maintenance Release;
  - b. Use reasonable efforts to isolate, collect all error and log files to enable Palo Alto Networks to fulfill its obligations herein;
- and

c. Notify Palo Alto Networks if you physically relocate device(s) covered by 4-Hour Replacement service to new location(s), including verification that the relocated device(s) remain within the geographical area covered by 4-Hour Replacement service.

## **7. LIMITATIONS**

The following services are expressly excluded from the Support Plans:

- a. Repair or replacement of Product required as a result of causes other than normal use, including without limitation:
  - i. repair, maintenance or modification of the Product by persons other than Palo Alto Networks-authorized personnel;
  - ii. accident or negligence of your fault;
  - iii. user error or misuse of the Product; or
  - iv. causes external to the Product such as, but not limited to, failure of electrical systems or fire or water damage or hardware failure, operation system software failure or any other damage and failure not caused by Palo Alto Networks.
- b. Maintenance or technical services for any third-party software or hardware, where such third-party software or hardware was not provided by Palo Alto Networks.

## **8. TERM AND TERMINATION**

This agreement will begin on the Effective Date and, unless terminated earlier in accordance with its terms, will remain in effect for the one, two or other multi-year support contract purchased. Palo Alto Networks will send you renewal reminders in advance of the expiration date(s). At the end of such term (and each renewal term thereafter, if any), this agreement will automatically expire unless you renew. Either party may terminate this agreement at any time in the event the other party breaches any material term of this agreement and fails to cure such breach within thirty (30) days following notice thereof from the non-breaching party.

## **9. NO WARRANTY**

Nothing in this agreement shall be construed as expanding or adding to the warranty set forth in the EULA. PALO ALTO NETWORKS MAKES, AND YOU RECEIVE, NO WARRANTIES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, ARISING IN ANY WAY OUT OF, RELATED TO, OR UNDER THIS AGREEMENT OR THE PROVISION OF MATERIALS OR SERVICES THEREUNDER, AND PALO ALTO NETWORKS SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE. Note that replacement Products under section 5 may consist of new or remanufactured parts that are equivalent to new. All Products that are returned to Palo Alto Networks and replaced become the property of Palo Alto Networks. Palo Alto Networks shall not be responsible for your or any third party's software, firmware, information, or memory data contained in, stored on, or integrated with any Product returned to Palo Alto Networks for repair or upon termination, whether under warranty or not.

## **10. CONFLICT**

In the event of any conflict between this EUSA and the End User Agreement, this EUSA shall take precedence, but only with respect to the subject matter specified above.

# TRAPS PRIVACY DATASHEET

Palo Alto Networks® engaged independent data privacy risk management provider TRUSTe® to review and document the data flows and practices described in this datasheet. This document provides customers of Palo Alto Networks with information needed to assess the impact of Traps on their overall privacy posture by detailing how personal information may be captured, processed and stored by and within Traps and its associated components.



## PRODUCT SUMMARY

Palo Alto Networks Traps advanced endpoint protection replaces traditional antivirus with a multi-method approach to malware prevention – a proprietary combination of purpose-built malware and exploit prevention methods that protects endpoints from known and unknown threats. Traps prevents the execution of malicious executables as well as exploits contained in weaponized data files or network data streams.

## Information Processed by Traps

In order to prevent security breaches caused by malware and exploits, Traps™ advanced endpoint protection collects and processes information about the executable programs that run on any protected endpoint. This information is primarily limited to the forensic information that Traps logs on an ongoing basis for each application (such as program filenames and hashes, time of execution, computer and usernames, and IP addresses), as well as additional forensics collected during a prevention event (such as a full memory capture for offending applications, file paths and URLs, and process execution trees). In the case of exploit preventions, the memory capture will likely include the contents of the weaponized file that contained the exploit. In the case of malware preventions, Traps will retain and quarantine the offending malware files. Administrators can disable this behavior.

Traps processes, stores and transmits the forensic information it collects among its core components: the agent installed on the protected endpoint or server, and the Endpoint Security Manager (ESM), which includes its Management Console, central Policy Database, and ESM Communication Servers. Ongoing logs and forensic information collected from each endpoint reside on the endpoint itself and are also transmitted to the ESM for reporting, administration and security operations. Administrators can configure the ESM to transmit forensic information and system logs to other services via “syslog” protocol.

When encountering certain unknown files, such as executables and macro-enabled Office files, Traps computes and transmits the hash of the file to Palo Alto Networks WildFire™ cloud-based threat analysis service. If the hash of the suspect file is unknown to WildFire, Traps transmits the file to WildFire for full analysis (administrators can disable this behavior). Included in this transmission to WildFire is the unique identifier of the ESM submitting the file, which serves to limit access to submitted files to the customer who submitted them.

## Customer Privacy Options

Traps customers configure by policy which types of files to transmit to the ESM and WildFire for analysis. Customers can also choose between the US- and EU-based WildFire service if they want to further limit the geographic location of the unknown files transmitted to WildFire for analysis.

## Access and Disclosure

The ESM server stores operational logs locally and can write logs to external logging platforms (e.g., a syslog server). Internal logs can be viewed through the ESM Management Console. For organizations that deploy multiple ESMs, external logging platforms allow an aggregated view of such log databases. Customers retain and control access to all logs. Access to any files submitted to WildFire for analysis is restricted to customers who have submitted those files, as well as to authorized Palo Alto Networks employees when necessary to complete their WildFire system administration duties.

## Retention

Logs captured by the ESM are subject to retention policies established by the customer administrator and may be stored indefinitely. Files that Traps submits to WildFire for analysis are retained in accordance with the WildFire retention policies.

## Security of Data in Traps

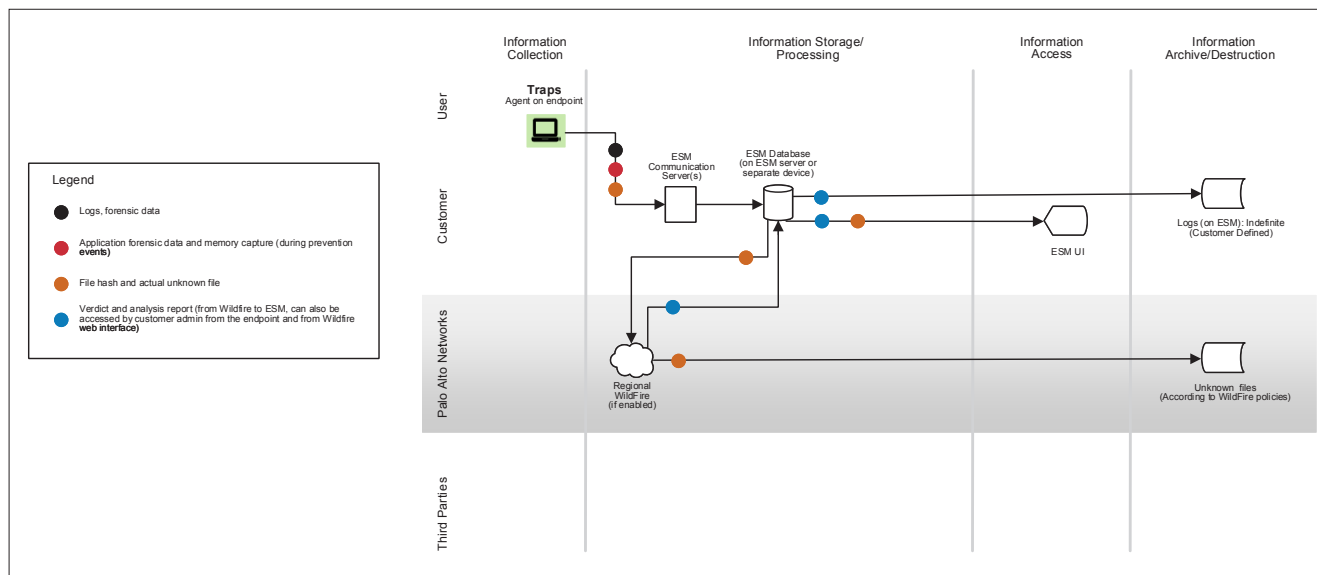
ESM Communication Servers act as proxies between Traps agents and the ESM database. Communications from Traps agents to the ESM Communication Servers, and from the ESM to WildFire, occur over HTTPS-encrypted channels.

## Resources

Additional information about Traps is available in the following resources:

- **Traps Datasheet** – <http://Go.PaloAltoNetworks.com/TrapsDS>
- **Traps Technology Overview** – <http://Go.PaloAltoNetworks.com/TrapsTechOverview>
- **Traps Live Demos** – <https://www.paloaltonetworks.com/events/next-generation-firewall-demos.html#endpoint>

### Data Flow



## About This Datasheet

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described herein. The discovery process relied upon the good faith accuracy of the information provided; TRUSTe has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.



4401 Great America Parkway  
Santa Clara, CA 95054  
Main: +1.408.753.4000  
Sales: +1.866.320.4788  
Support: +1.866.898.9087  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.  
traps-privacy-ds-053117

# CORTEX XDR PRIVACY

---

## Product Summary

Cortex XDR™ detection and response consists of two cloud-based applications that use the industry-leading Palo Alto Networks Security Operating Platform® to perform analytics on network, endpoint, and cloud data in Cortex Data Lake.

- **Cortex XDR – Analytics** analyzes customers' logs in Cortex Data Lake to identify patterns in users' and devices' network activity as well as to create alerts when it detects deviations from such patterns, with the purpose of detecting activities that may constitute attacks.
- **Cortex XDR – Investigation & Response** allows customers to investigate security alerts, search security threats, and remotely respond when an endpoint is confirmed as a threat.

When Cortex XDR – Analytics detects anomalous network activity, it automatically scans and analyzes the endpoint through an on-premises virtual machine called Pathfinder. Cortex XDR – Analytics also provides a web-based user interface through which to perform triage and investigate alerts provided by the tool. Alerts in the user interface include information about the anomalous network activity as well as the user or endpoint responsible. Optionally, user and device information can be displayed through the Directory Sync Service.

Cortex XDR – Investigation & Response provides a user interface through which to view all alerts the Security Operating Platform generates. The interface also gives customers the ability to view descriptions of alerts, with options to analyze alerts in more detail by using information in Cortex Data Lake or the Cortex XDR – Analytics interface. The interface also allows customers to search through logs in Cortex Data Lake and create as well as apply rules that can generate alerts by analyzing such logs.

## Information Processed by Cortex XDR

Cortex XDR performs analytics and searches from multiple sources, primarily logs from the Security Operating Platform. This includes logs from Palo Alto Networks Next-Generation Firewalls and endpoint activity logs from Traps™ endpoint protection and response agents. Pathfinder collects additional information from endpoints.

### *Information from Firewall Logs*

Logs from each firewall are encrypted in transit and stored in a data center in the region the customer selects. The customer can fully configure which of the available types of logs to send to Cortex Data Lake.



---

Cortex XDR analyzes traffic logs, which contain basic information about internal and external network connections from the IP addresses of devices and users. Cortex XDR also analyzes URL Filtering logs, which contain information about websites accessed by devices and users. Finally, Cortex XDR analyzes enhanced application logs, which contain information about how devices are connected to the internal network, such as Dynamic Host Configuration Protocol logs when a device joins a Wi-Fi network, and the types of requests devices make to other hosts, such as DNS queries and responses.

Analysis identifies network connectivity patterns from users and devices. Alerts are triggered using detection algorithms that compare current network and application patterns against historical and peer-group patterns.

### *Information from Endpoints*

When Cortex XDR identifies changes in patterns—particularly changes that may indicate attacks—it triggers alerts and Pathfinder scans. Pathfinder automatically logs in to endpoints to collect the information shown in Figure 1 when anomalous network activity is detected or an administrator performs an on-demand scan. Pathfinder analyzes the collected information and sends select processes, executables, and modules to WildFire® malware prevention service for threat intelligence lookups.

Traps agents installed on select endpoints, if enabled, continuously collect endpoint activity logs and forward them to Cortex Data Lake for processing by Cortex XDR – Analytics and Cortex XDR – Investigation & Response. The information in the events includes the following:

- **Process activity logs** contain data about users and how the process is executed. This includes the user who started the process, with name and directory path. The data also contains unique information about the process to help with analytics, including its hash values, thread IDs, and any command line arguments the process uses on execution.
- **File activity logs** contain information on operations to specific binaries and applications. This information includes the user or process that renamed or wrote information of the file.
- **Network activities logs** contain information about outgoing and incoming network connections performed by a user, process, or network. This includes information such as user, process, source and destination IP addresses, ports, protocol, local hostname, remote hostname, and destination country.
- **Registry activity logs** contain information about Windows® registry keys, including the value, type of key, and any name of the key. Information about users or processes that create or change the registry key is also logged.
- **Miscellaneous information** that describes the operating system and hashes of files on the endpoint is also collected. Change events related to user logins or logouts, and changes to the Windows OS, such as reboots and agent restarts, are also collected.

For more information about these logs, consult the [Traps management service privacy datasheet](#).

### *Information from Active Directory via Directory Sync Service*

Optionally, customers can configure Cortex XDR to read information from the Directory Sync Service, which allows Cortex XDR to display more accurate information about devices and users.

### **Purpose of Information Processed by Cortex XDR**

The information Cortex XDR processes can be grouped into five categories, described here. Cortex XDR uses these categories to identify user and device patterns across the network as well as detect anomalies from such patterns. This information provides context for security analysts investigating alerts.

1. **User information** is used to associate patterns of activity with a specific user's network account. This helps security teams attribute anomalous network activity or processes to a more reliable source, whether an individual or a shared account, rather than relying only on the IP address.
2. **Device information**—in the form of hostnames, fully qualified hostnames, and MAC addresses—is used to identify the source and destination of anomalous network activity, which could be a laptop, workstation, server, internet-connected device, or network infrastructure device. This helps security teams investigate anomalous activity even when it cannot be attributed to a specific user.
3. **Network addresses**, in the form of IP subnets or IP addresses, are used to identify the sources and destinations of anomalies. This helps security teams investigate anomalous activity even when it cannot be attributed to a specific user account or network device. It also helps security teams investigate possible attacks targeting high-risk servers or parts of the network.
4. **Endpoint information**—in the form of executable files, loaded modules and processes, and file and registry activity—is used to identify the digital source of anomalous network activity and alert security teams to potential zero-day attacks. This also helps security teams authorize network activity related to software or users performing their job functions, such as administrators using specific tools.
5. **Other information**, such as URLs, can help identify the destination or possible source of network activity. Websites often contain malicious payloads or can be used as servers to control internal devices.

| Category          | Source  | Info Processed by Cortex XDR   | Example(s)  | May Be Considered or Contain Personal Information |
|-------------------|---|--|---|---|
| User info         | Firewall logs, Traps logs, and Directory Sync Service     | Domain and username  | company\johnsmith   | Yes   |
|                   | Directory Sync Service                                    | User distinguished name  | CN=Username1, OU=Americas, OU=Users, OU=Company, DC=Company, DC=Local   | Yes   |
|                   | Directory Sync Service                                    | Full name or display name  | John W. Smith   | Yes   |
|                   | Firewall logs and Directory Sync Service                  | Email address  | Username1@company.com   | Yes   |
|                   | Directory Sync Service                                    | Organization unit from Active Directory  | Company/Users/Americas  | Yes   |
|                   | Directory Sync Service                                    | Phone number   | 444-555-6666  | Yes   |
|                   | Pathfinder  | Username   | Johnsmith   | Yes   |
| Device info       | Firewall logs (enhanced application log)                  | MAC address  | 00-11-22-AA-BB-CC   | Yes   |
|                   | Traps agents and Firewall logs (enhanced application log) | Hostname of devices  | ABCD-WINDOWS-LAPTOP<br>123-MACBOOK                                      | Yes   |
|                   | Firewall logs (enhanced application log)                  | Domain name  | www.google.com<br>www.suspicioussite.com<br>internalserver.company.com  | Yes   |
|                   | Firewall logs   | Name of firewall   | NA-Firewall or DC1-Firewall   | Yes   |
|                   | Firewall logs   | Other names used by firewall configuration   | vsys1 or trust-zone or untrust-zone or US-DMZ                           | No  |
|                   | Directory Sync Service                                    | Host distinguished name  | CN=Computer1, OU=Region, OU=Computers, OU=Company, DC=Company, DC=Local | Yes   |
|                   | Directory Sync Service                                    | Organizational unit  | Company/Computers/Region  | Yes   |
|                   | Directory Sync Service                                    | Operating system   | Windows 10 Enterprise   | No  |
| Network addresses | Firewall logs and Traps agent logs                        | IP address or subnet (e.g., source device, destination device)   | 10.1.1.10, 10.10.10.10,<br>192.168.1.16<br>172.16.0.0/16                | Yes   |
|                   | Firewall logs and Traps agent logs                        | IP address of network infrastructure devices (e.g., NAT devices, routers, DNS servers, DHCP servers, domain controllers, mail servers) | 10.1.1.1<br>192.168.1.254   | Yes   |

|               |  |  |   |     |
|---------------|--|--|---|-----|
| Endpoint info | Pathfinder   | List of running processes, loaded modules, installed executables, and their command arguments, if applicable                                       | c:\windows\system32\svchost.exe<br>c:\program files\microsoft office\office15\excel.exe -dde  | Yes |
|               | Pathfinder   | Executables, including portable executable files, installed executable files, loaded modules, autoruns, and their command arguments, if applicable | c:\windows\system32\ping.exe<br>server.company.com<br>c:\program files\realtek\audio\hda\ravbg64.exe /im  | Yes |
|               | Traps agent logs   | Process activity logs  | Process: C:\Program Files\7-Zip\7zFM.exe<br>Started with CMD: "C:\Program Files\7-Zip\7zFM.exe"<br>"C:\Users\MarySmith\Downloads\suspicious_file.zip"   | Yes |
|               | Traps agent logs   | File activity logs   | Type: File Create<br>Path: C:\Users\JDo\Desktop\Data.zip.tmp<br>Type: File Rename<br>Path: C:\Users\JDo\Desktop\Data.zip  | Yes |
|               | Traps agent logs   | Network activity logs  | Type: Network Outgoing<br>Source: 10.201.113.22:2563 to 192.168.1.100:443 (server.company.com)  | Yes |
|               | Traps agent logs   | Registry activity logs   | Type: Registry Key Create Key: HKEY_USERS\S-1-5-21-937295531-4040087734-563264647-1111\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU Value : null   | No  |
|               | Traps agent logs   | Miscellaneous logs   | Host Status: Logon<br>Host Status: Logoff   | No  |
| Other info    | Firewall logs (URL filtering logs and enhanced application logs) | URLs   | https://outlook.office365.com/EWS/Exchange.asmx<br>https://mg.mail.yahoo.com/neo/m/launch?&filterBy=&fid=Inbox&fidx=1&ac=DSTVMBzTbaVaamXPZAndcVWZ22g-&rand=1966219345&nsc<br>https://www.linkedin.com/johnsmith | Yes |

**Figure 1: Information processed by Cortex XDR**

### How Cortex XDR Addresses EU Data Protection Laws

Processing personal data to ensure network and information security—for instance, through the Security Operating Platform and Cortex products—is broadly recognized as a legitimate interest and is specifically called out as such in the EU General Data Protection Regulation:

*(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.<sup>1</sup>*

1. GDPR, recital 49; see also Article 29 Working Party Opinion 06/2014 on the notion of legitimate interest of the data controller, WP217, adopted 9 April 2014, p. 24–25.

---

Where a service provider, such as Palo Alto Networks, processes personal data to ensure network and information security, this is a legitimate interest of the service provider and its customers. Such legitimate interest provides a basis for the processing of personal data by Palo Alto Networks under EU data protection laws. This legitimate interest generally also provides a basis for customers analyzing personal data through Cortex XDR, in accordance with privacy or regulatory requirements that may prevent customers from sharing certain data. In such an event, customers can limit data processing or access to data by using their privacy options, as described herein, when configuring their firewalls.

### **How Palo Alto Networks Complies with Data Protection Rules**

Palo Alto Networks is committed to protecting personal data processed by Cortex XDR. We will not access the content of the information in a way that would allow us to acquire meaningful information about natural persons except where it is necessary for identifying security threats or investigating suspicious activities indicative of attacks.

Any logs stored on or processed by Palo Alto Networks systems are secured with state-of-the-art technologies, and Palo Alto Networks operates rigorous technical and organizational security controls. Logs and information forwarded to a given regional data center will be kept in that region. As Palo Alto Networks is a multinational company, there may be a need, in some cases, to share logs and information with Palo Alto Networks offices in other regions. We will do so in compliance with applicable requirements for transfer of personal data, including the EU Standard Contractual Clauses as approved by the European Commission or other legal instruments for the transfer of personal data, provided for in EU data protection law.

### **Sub-Processors**

Data processed by Cortex XDR and Traps agent data in Cortex Data Lake is hosted in Google Cloud Platform data centers in the regions the customer selects.

### **Retention**

Cortex XDR applies retention policies that purge data once it is no longer needed for the purpose for which it was collected. Cortex XDR – Analytics retains copies of the most recent three days of logs. It also aggregates logs into summary logs for efficient processing and stores these for 30 days. To enable customers to perform queries in a timely manner, Cortex XDR – Investigation & Response processes and stores copies of query results. Older copies will be deleted as the temporary storage reaches capacity, and all copies are deleted upon termination of the service.

If an algorithm triggers an alert, Cortex XDR – Analytics retains the processed information for 180 days for the purposes of investigation. If enabled, endpoint and user information collected by Pathfinder will be available in Cortex XDR – Analytics for 30 days if there are no alerts attributed to that endpoint or user. If alerts are attributed to an endpoint, information collected by Pathfinder will be available for 180 days to give security analysts the information they need for investigation at a later time. If enabled, endpoint activity logs from Traps agents will be available in the Cortex Data Lake for the same amount of time.

Upon termination of Cortex XDR service, the information generated by Pathfinder as well as all data in Cortex XDR will be marked for deletion. Unless Cortex Data Lake service is terminated at the same time, data in Cortex Data Lake will be maintained. Upon termination, after 30 days data in active systems in Cortex XDR will be marked inactive and may be recovered for up to 30 days, after which it will be deleted from the active systems. Deletion of backup data may take up to an additional 150 days.

### **Access and Disclosure**

#### ***Access by Customers***

Customers can access the information about the alerts through the Cortex XDR user interface, including WildFire reports if applicable to the alert. Customers can also access information about endpoint activity logs through the Cortex XDR user interface. To access firewall and Prisma Access logs in Cortex Data Lake, customers can use the Panorama™ network security management interface.

If enabled, Cortex XDR processes enhanced application logs separately from other logs within Cortex Data Lake. Customers can view the results of such processing through the Cortex XDR user interface.

#### ***Access by Palo Alto Networks***

Access to information in Cortex XDR and Cortex Data Lake is restricted to Palo Alto Networks Site Reliability Engineers (SREs), threat research and analytics teams, and—when a support case is opened—customer support teams. Access is allowed for the purposes of troubleshooting, solving issues, and improving the effectiveness of security protections. All access is recorded and audited. Access privileges are managed by Engineering leadership.

#### ***Security of Data***

Palo Alto Networks has achieved SOC 2 Type II certification for Cortex Data Lake and Cortex XDR – Analytics to demonstrate its strong security policies and internal controls environment.

For information about security protections in the data centers where Cortex XDR data resides, please consult [cloud.google.com/security/compliance](https://cloud.google.com/security/compliance).

Information processed by Cortex XDR is encrypted both in transit and at rest.

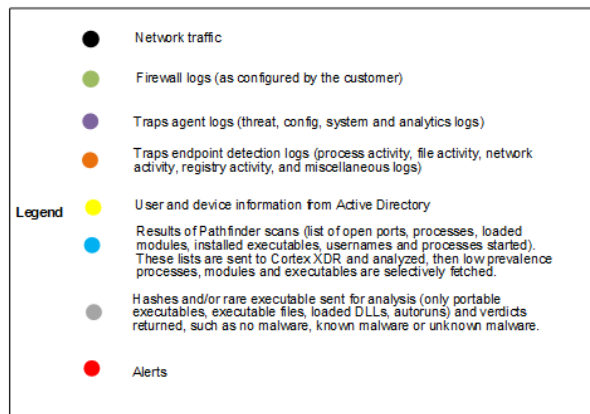
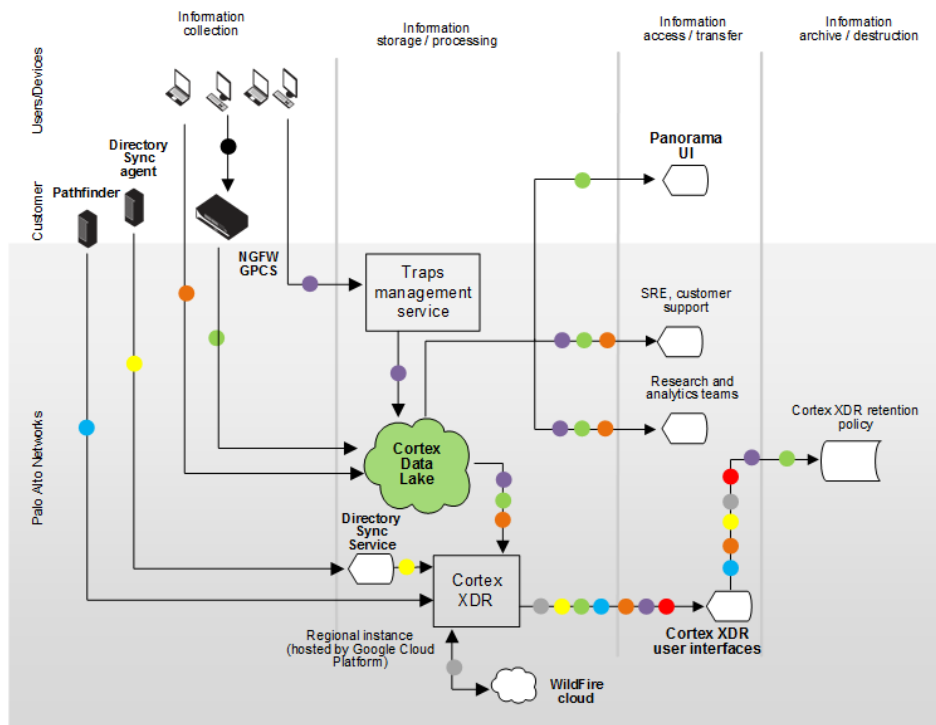


Figure 2: Data flow diagram

## Resources

See the following resources for additional information about Cortex and related Palo Alto Networks services:

- [Cortex XDR](#)
- [Cortex Data Lake](#)
- [Panorama](#)
- [Cortex hub](#)
- [Directory Sync service](#)
- [Security Operating Platform](#)

## About This Datasheet

Please note that the information provided with this paper concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws.