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

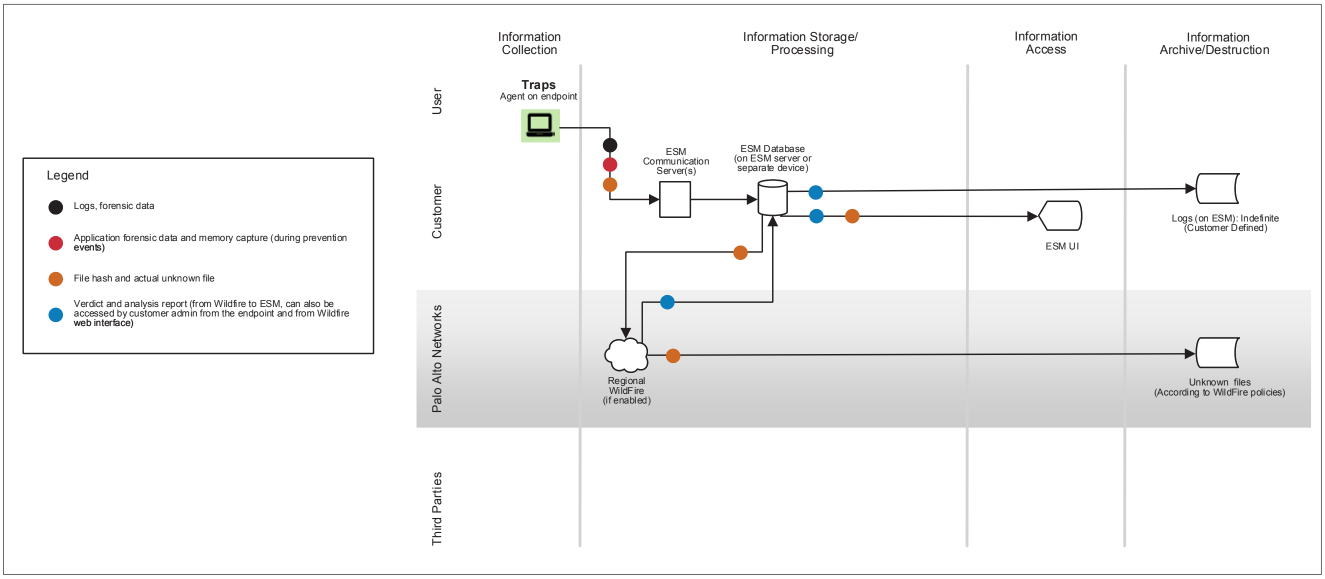
ESM Communication Servers act as proxies between Traps agents and the ESM database. Communications from Traps agents to the ESM Communication Servers, and from the ESM to WildFire, occur over HTTPS-encrypted channels.

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


Legend
● Logs, forensic data
● Application forensic data and memory capture (during prevention events)
● File hash and actual unknown file
● Verdict and analysis report (from Wildfire to ESM, can also be accessed by customer admin from the endpoint and from Wildfire web interface)
Information Collection
Information Storage/ Processing
Information Access
Information Archive/Destruction
User
Customer
Palo Alto Networks
Third Parties
Traps
Agent on endpoint
ESM Communication Server(s)
ESM Database (on ESM server or separate device)
ESM UI
Logs (on ESM): Indefinite (Customer Defined)
Regional WildFire (if enabled)
Unknown files (According to WildFire policies)

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