WILDFIRE PRIVACY

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

Product Summary

WildFire is an advanced, cloud-based threat analysis service that identifies unknown malware, zero-day exploits, and advanced persistent threats in a scalable, virtual environment. Once deployed, WildFire automatically disseminates updated protections in near-real time to stop threats from spreading. This closed-loop, automated process gives organizations the assurance that their networks, endpoints, and clouds are armed with the absolute latest threat intelligence at all times.

Information Processed by WildFire

WildFire is built on Palo Alto Networks industry-leading Security Operating Platform® and receives threat data from various sources, including:

Next-Generation Firewall

The firewall inspects traffic for threat indicators or policy violations. Our Next-Generation Firewall, Threat Prevention, URL Filtering, Traps™ endpoint protection and response and Prisma™ SaaS security service proactively block known threats, while WildFire analyzes unknown files and email links in a scalable sandbox environment. WildFire identifies new threats and automatically delivers protections to customers in the form of signatures and verdict updates.

While Palo Alto Networks is not interested in the content of the files analyzed in the WildFire cloud, apart from any malicious code such files may contain, some files may contain personal data. However, such data is generally irrelevant for analysis and thus not included in verdicts or updates.

A critical aspect of the Next-Generation Firewall is the ability to decrypt SSL/TLS traffic for analysis. However, decryption of traffic is turned off by default. Customers must activate decryption and specify the traffic to be decrypted.

Once decrypted, the traffic stream may be analyzed within the firewall using a variety of tools and methods, depending on the customer's Palo Alto Networks service subscriptions. After the firewall has confirmed the traffic as safe, it re-encrypts the traffic and sends it forward to its destination. In some instances, if the firewall may require additional information to properly analyze the traffic

and may transmit certain data to Palo Alto Networks to facilitate such analysis. Data transmitted in this way provides context for malware events, producing more accurate reporting and correlation for the customer.

The types of files submitted to WildFire are highly configurable. For instance, customers can decide to submit all types of unknown files on all traffic passing through a firewall or just unknown executable files within incoming web-based traffic. The same control applies to various pieces of information that can optionally be shared with WildFire to contextualize the malware event, giving the customer more accurate reporting and correlation.

Data Type	May Be Considered or Contain Personal Information
Source IP address that sent the unknown file	Yes
Destination IP address for the unknown file	Yes
Source port that sent the unknown file	No
Virtual system that detected the unknown file	No
Targeted user/user group	Yes
Name of the unknown file	Yes
Sender, recipient and subject of an unknown email link (the sender's name also appears in WildFire logs and reports)	Yes
Application/User that transmitted the unknown file	No
URL associated with the unknown file	No

Palo Alto Networks Subscription Services and WildFire Portal Through a Public API

Service	Type of File Transmitted	Session Data Transmitted (not configurable)
Traps	Unknown files	Filename
Prisma SaaS	Unknown executables MS Office	Filename
WildFire Portal	Files supported by WildFire	Filename
Prisma Access	Files supported by WildFire	Same as firewall

Partners can use the public API to upload files collected in connection with services they provided directly to customers.

Each new sample is passed through a series of analysis layers, including a) static analysis, which looks for known indicators, b) machine learning, which classifies files based on feature sets, and c) dynamic analysis, which observes how files behave, producing rich context-based signatures when zero-day malware is identified. After this process completes, an analysis report is produced for viewing by the administrator, and a verdict is delivered. In the case of a "malicious" verdict, WildFire produces a behavioral report and distributes protections, in the form of anti-malware signatures and anti-command-and-control signatures to all global WildFire subscribers, in as few as five minutes. These signatures can automatically prevent any active infection and halt further distribution of the newly detected threat. No manual action is required.

WildFire customers receive integrated logs, analysis, and visibility into WildFire events through the WildFire portal, firewall management interface, Panorama™ network security management, and AutoFocus™ contextual threat intelligence service, enabling teams to investigate and correlate events observed in their networks. Analysis results do not contain user IDs, IP addresses, or other data that could be considered personal data.

In addition to analysis reports and session data, WildFire customers have direct access to the original malware sample and a full packet capture of the dynamic analysis for internal use. Log data can be accessed via an API.

How WildFire Fits with EU Data Protection Laws

Processing personal data to ensure network and information security—for instance, through the WildFire service and Palo Alto Networks Security Operating Platform—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.*[1]

Files forwarded to the EU WildFire cloud will remain in the European Economic Area. As Palo Alto Networks in a multinational company, there may be a need in some cases to share files with our offices in other or other regions. We will do so only on the basis of EU Standard Contractual Clauses as approved by the European Commission[2] or other legal instruments for the transfer of personal data, provided for in EU data protection law.

We are transparent about data processing. We have notified the Dutch Data Protection Authority of the processing of personal data for inclusion in its public register.

Where a service provider like Palo Alto Networks processes personal data to ensure network and information security, this is a "legitimate interest" of the service provider and of its customers, providing a basis for the processing of personal data by Palo Alto Networks under EU data protection laws. This legitimate interest will generally also provide a basis for customers sharing data with the WildFire cloud, unless specific privacy or regulatory requirements prevent customers from sharing certain data. In such cases, customers can set privacy options when configuring their firewalls, as previously outlined, to limit data sharing.

WildFire: U.S. Government

WildFire: U.S. Government is FedRAMP authorized and keeps agency data private and available through security controls that meet stringent government requirements. It covers civilian and defense government security standards with a service that adheres to NIST 800-53 Revision 4 controls, delivered from two data centers within the continental United States.

How Palo Alto Networks Complies with Data Protection Rules

Palo Alto Networks is committed to protecting personal data processed in the global and regional WildFire clouds. We will not access the content of files in a way in which we could learn meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats.

File analysis is largely automated, and files determined to be benign are deleted shortly after analysis. Only malicious files are stored for further analysis as well as development and testing of new security products. We do not share such files with anyone else. Only threat signatures are shared with others, and such signatures do not contain personal data.

Files 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.

Customer Privacy Options

Our Next-Generation Firewalls allow customers to select which elements of session data and what types of files to share with Palo Alto Networks for analysis.

Customers have the option to restrict all sharing while still receiving firewall signatures and updates. However, we strongly encourage customers to share data with the network, because this enables the detection of emerging threats and the distribution of protective measures to all Palo Alto Networks customers as soon as possible.

Access and Disclosure

Access by Customers

The results of analyses performed on decrypted traffic are logged and viewable by the system administrator through the administrative interface. Data is divided into various categories to facilitate organization and provide context, and includes overall traffic, threat assessment, URL Filtering, WildFire analysis details, and data content filtering results. Administrators can access summaries and view log details, including WildFire sandbox analysis details, directly from a log viewing function in the interface, or they can download data as a PDF to share with others.

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.

2. http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

Access by Palo Alto Networks

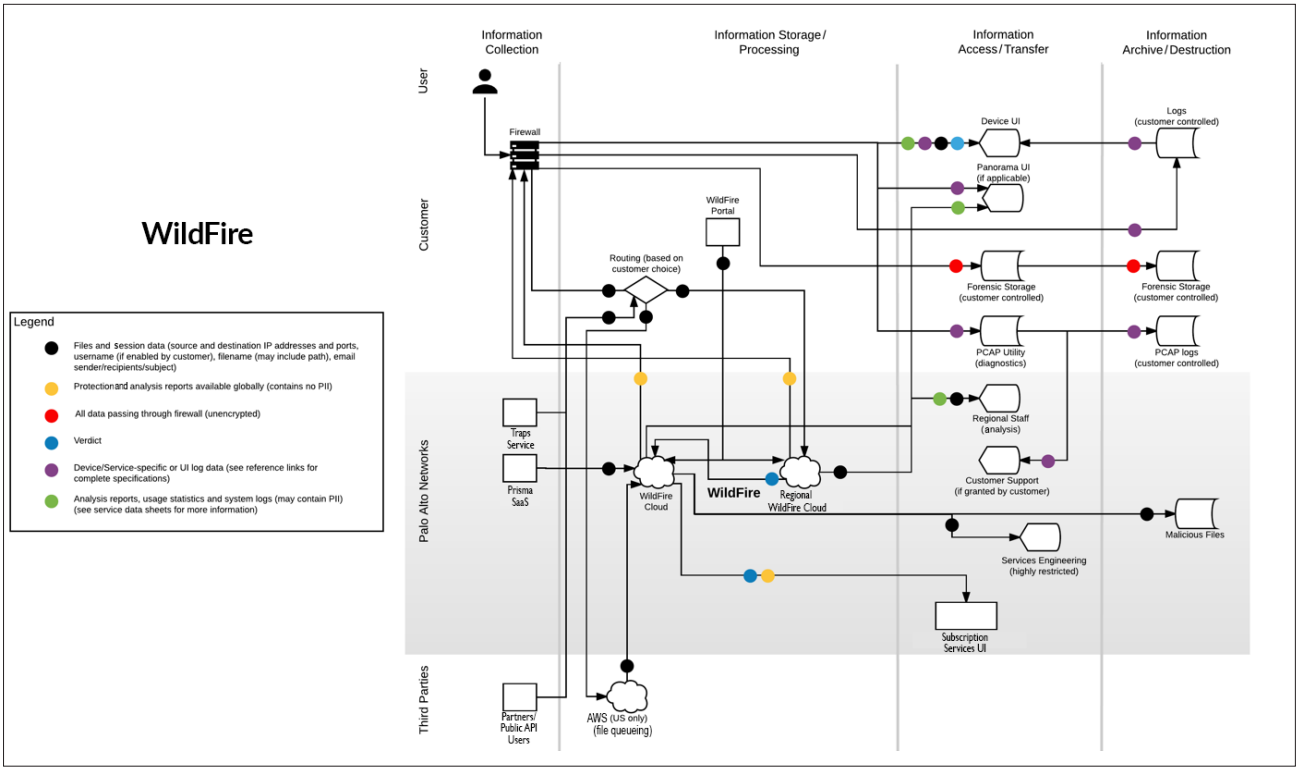
Within Palo Alto Networks, access to the WildFire production system is restricted to the teams that analyze samples, generate reports and signatures, and test signatures for efficacy. This may include team members from WildFire threat research and engineering. All access privileges are managed by engineering leadership and audited for privilege access violations.

Retention

Customers have complete control over the duration of storage for logs on the firewall. Files sent to the WildFire cloud for processing and analysis are retained until processing takes place. Once analyzed, files categorized as benign are retained for 14 days in case the analysis decision is reversed. Files determined to be malicious are retained for 10 years. Signatures and sample reports for corresponding files, which do not include personal information, are stored indefinitely.

Security of Data in WildFire

Session data sent from Next-Generation Firewalls to the WildFire cloud is encrypted in transit. All data in the cloud is encrypted while at rest. Palo Alto Networks has also achieved SOC 2 Type II certification for its US- and EU-based WildFire data centers to demonstrate its strong security policies and internal controls environment.



Sub-Processors

WildFire is hosted in data centers managed by Palo Alto Networks, Amazon Web Services, and Google Cloud.

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. The discovery process relied upon the good faith accuracy of the information provided; TrustArc 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 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.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

wildfire-privacy-overview-ds-081419