WILDFIRE

Protection from Targeted and Unknown Attacks

WildFire™ cloud-based malware-analysis environment is an advanced threat intelligence service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. Once deployed, WildFire automatically disseminates updated protections in near-real time to immediately halt threats from spreading – without manual intervention. This closed-loop, automated process gives organizations the assurance that their networks, endpoints and cloud are armed with the absolute latest threat intelligence at all times.

Benefits

- Our Next-Generation Security Platform provides up-to-date protection throughout your organization to reduce the attack surface across multiple attack vectors.
- WildFire identifies unknown malware and zero-day exploits using advanced static and dynamic analysis techniques against multiple OS and application versions.
- WildFire automatically generates malware, URL and DNS signatures and distributes them within minutes to all global, WildFire-subscribed Palo Alto Networks platforms.
- Information about indicators of compromise (IOCs) from WildFire analysis reports is used by our Next- Generation Security Platform and our technology partners to identify infected hosts and prevent secondary downloads.

Advanced cyberattacks are employing stealthy and persistent methods to evade traditional security measures. Skilled adversaries demand that modern security teams re-evaluate their prevention tactics to better address the volume and sophistication of today's attacks. Purpose-built for high fidelity hardware emulation, WildFire analyzes suspicious samples as they execute. When new threats emerge, Palo Alto Networks® Next-Generation Security Platform automatically routes suspicious files and URLs to WildFire for deep analysis.

WildFire inspects millions of samples per week from its global network of customers and threat intelligence partners looking for new forms of previously unknown malware, exploits, malicious domains and outbound command-and-control activity. The cloud-based service creates new protections that are capable of blocking targeted and unknown malware, exploits, and outbound C2 activity by observing their actual "behavior," rather than relying on pre-existing signatures. The protections are shared globally in minutes.

Next-Generation Security Platform

WildFire is built on our industry-leading Next-Generation Security Platform, benefiting from full visibility into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard ports or SSL encryption. Known threats are proactively blocked with our Next-Generation Firewall, Threat Prevention, URL Filtering, Traps and Aperture, providing baseline defenses against known exploits, malware, malicious URLs and command-and-control (C2) activity. Unknown files, and email links are forwarded and analyzed by WildFire in a scalable sandbox environment, where new threats are identified and protections are automatically developed and delivered to the security elements in your organization in the form of signatures and verdict updates. The result is a unique, closed-loop approach to preventing cyberthreats that includes: positive security controls to reduce the attack surface; inspection of all traffic, ports and protocols to block all known threats; rapid detection of unknown threats by observing the actions of malware in a cloud-based execution environment; and automatic deployment of new protections back to the frontline to ensure threats are known to all and blocked across the attack lifecycle.

Behavior-Based Cyberthreat Discovery

To find unknown malware and exploits, WildFire executes suspicious content in the Windows® XP, Windows 7, Android® and Mac® OS X® operating systems, with full visibility into common file types, including: EXE, DLL, ZIP, PDF, as well as Microsoft® Office documents, Java® files, Android APKs, Adobe® Flash® applets, and webpages, including high-risk, embedded content, such as Java and Adobe Flash files and images.

WildFire identifies hundreds of potentially malicious behaviors to uncover the true nature of malicious files based on their actions, including:

- **Changes made to host:** WildFire observes all processes for modifications to the host, including file and registry activity, code injection, memory heap spray (exploit) detection, addition of auto-run programs, mutexes, Windows services, and other suspicious activities.
- **Suspicious network traffic:** WildFire performs analysis of all network activity produced by the suspicious file, including backdoor creation, downloading of next-stage malware, visiting low-reputation domains, network reconnaissance, and much more.
- **Anti-analysis detection:** WildFire monitors techniques used by advanced malware that is designed to avoid VM-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, disabling of host-based security features, and more.

Natively integrated with our Next-Generation Security Platform, which is capable of classifying all traffic across hundreds of applications, WildFire uniquely applies this behavioral analysis to web traffic, email protocols (SMTP, IMAP, POP) and FTP, regardless of ports or encryption.

WildFire Architecture

To support static and dynamic malware analysis at scale, across the organization, WildFire is built on a cloud-based architecture that can be leveraged by your existing Palo Alto Networks Next-Generation Security Platform with no additional hardware. Where regulatory or privacy requirements prevent the use of a cloud infrastructure, a local hardware solution can be deployed on premises using the WF-500 appliance. You can leverage both the cloud and local versions of WildFire within the same environment. This hybrid solution enables you to define which files types are sent to the cloud and which are sent to the local appliance, based on data sensitivity. Analysis results in the form of new protections that are shared globally.

Threat Prevention with Global Intelligence Sharing

When an unknown threat is discovered, WildFire automatically generates protections to block it across the cyberattack lifecycle, sharing these updates with all global subscribers in as little as five minutes. These quick updates are able to stop rapidly spreading malware; since these updates are payload based, they can block proliferation of future variants without any additional action or analysis.

In addition to protecting organizations from malicious and exploitive files and links, WildFire looks deeply into malicious outbound communication, disrupting command-and-control activity with anti-C2 signatures and DNS-based callback signatures. The information is also fed into URL Filtering with PAN-DB, where newly discovered malicious URLs are automatically blocked. This correlation of threat data and automated protections are key to identifying and blocking ongoing intrusion attempts and future attacks on your organization.

Integrated Logging, Reporting and Forensics

WildFire users receive integrated logs, analysis and visibility into WildFire events through the management interface, Panorama™, AutoFocus™ or the WildFire portal, enabling teams to quickly investigate and correlate events observed in their networks. This allows security staff to rapidly locate the data needed for timely investigations and incident response. Host-based and network-based indicators of compromise become actionable through log analysis and custom signatures.

To aid security and IR staff in discovering infected hosts, WildFire also provides:

- Detailed analysis of every malicious file sent to WildFire across multiple operating system environments, including both host-based and network-based activity.
- Session data associated with the delivery of the malicious file, including source, destination, application, User-ID™, URL, etc.
- Access to the original malware sample for reverse-engineering and full PCAPs of dynamic analysis sessions.
- An open API for integration with best-in-class SIEM tools, such as the Palo Alto Networks application for Splunk, and leading endpoint agents. This analysis provides a wealth of indicators of compromise (IOCs) that can be applied across the attack lifecycle.
- Native integration with Traps™ advanced endpoint protection and Aperture; advanced SaaS protection.
- Access to the actionable intelligence and global context provided by Palo Alto Networks AutoFocus threat intelligence service.
- Natively integrated with the correlation engine in our next- generation firewalls.

Maintaining the Privacy of Your Files

WildFire leverages a public cloud environment managed directly by Palo Alto Networks. All suspicious files are securely transferred between the Next-Generation Security Platform and the WildFire data center over encrypted connections, signed on both sides by Palo Alto Networks. Any files that are found to be benign are destroyed, while malware files are archived for further analysis.

WildFire Requirements:

- PAN-OS® 4.1+
- DF, Java, Office, and APK analysis require PAN-OS 6.0+
- Adobe Flash and webpage analysis require PAN-OS 6.1+

Licensing Information:

Basic WildFire functionality is available as a standard feature on all platforms running PAN-OS 4.1 or greater:

- Windows XP and Windows 7 image analysis
- EXE and DLL file types, including compressed (zip) and encrypted (SSL) content
- Automatic submission of suspicious files
- Automatic protections are delivered with regular threat prevention content updates (Threat Prevention license is required) every 24-48 hours

The WildFire subscription adds near-real time protection from advanced threats, including these additional features:

- Automatic WildFire signature updates every 15 minutes for all new malware detected anywhere in the world
- Enhanced file-type support, including: PE files (EXE, DLL, and others), all Microsoft Office file types, PDF files, and Java applets (JAR and CLASS)

WF-500

The WF-500 is an optional hardware appliance to support customers who choose to deploy WildFire as a private cloud for additional data privacy. The WF-500 is sized to accommodate most mid-range to large-scale networks, with the option of deploying additional appliances as traffic volumes increase or for networks that require geographic distribution.

The WF-500 can be deployed in a hybrid mode with the global WildFire services.

WF-500 Specifications

Processor	Memory	System Disk
Dual 6-Core Intel® Processor with Hyper -Threading Technology	128 GB RA 1	20GB SSD

Hardware Specifications

I/O Storage	Capacity	Power Supply
4x10/100/1,000 DB9 Console serial port, USB HDD for 2 TB of RAID storage	2TB RAID1: 4 x 1TB RAID Certified	Dual 920W power supplies in hot swap, redundant configuration
Max Power Consumption	**Rack Mountable (Dimensions)**	
390 Watts	2U, 19” standard rack (3.5”H x 21”D x 17.5”W)	
Max Btu/Hr	**Input Voltage (Input Frequency)**	
1300 BTU/hr	100-240VAC (50-60Hz)	
Max Current Consumption	**Safety**	
3.2A@120VAC	UL, CUL, CB	
EMI	**Environment**	
FCC Class A, CE Class A, VCCI Class A	Operating Temperature: 32 to 95 F, 5 to 35 C Non-operating Temperature: -4 to 158 F, -40 to 65 C	

To view additional information about the WF-500 security features and associated capacities, please visit www.paloaltonetworks.com/products.

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

pan-ds-wildfire-060216