WildFire

WildFire™ threat intelligence service identifies unknown advanced persistent threats (APTs) through dynamic analysis in a scalable, cloud-based virtual environment. WildFire automatically disseminates protections in near real-time to help security teams meet the challenge of advanced cyberattacks. WildFire is built into the Palo Alto Networks® Enterprise Security Platform, which natively classifies all traffic, inclusive of threats and the applications that carry them — regardless of port or SSL encryption.

- Identifies unknown malware and zero-day exploits using advanced static and dynamic analysis techniques.
- Combines complete visibility and control over known threats and applications with cloud-based dynamic analysis of unknown threats to ensure accurate, safe and scalable malware analysis.
- True in-line blocking of exploitive and malicious files, as well as malware delivery websites and command-and-control traffic.

Advanced cyberattacks are employing stealthy, persistent methods to evade traditional security measures. Skilled adversaries demand that modern security teams re-evaluate their basic assumption that traditional intrusion prevention systems, antivirus and single-purpose sandbox appliances are up to the task of defeating APTs.

Enterprise Security Platform

WildFire is built into our industry-leading Enterprise Security Platform, with full visibility into all network traffic, including stealthy attempts to evade detection, such as non-standard ports or SSL encryption. Known threats are proactively blocked with our Threat Prevention and URL Filtering services, providing baseline defenses against known exploits, malware, malicious URLs and command-and-control (CnC) activity. Unknown files are analyzed by WildFire in a scalable, virtual sandbox environment where new threats are identified and protections are automatically developed and delivered to you in the form of an update. The result is a unique, closed-loop approach to controlling cyberthreats that begins with positive security controls to reduce the attack surface; inspects all traffic, ports, and protocols to block known threats; rapidly detects unknown threats by observing their actual behavior in a cloud-based virtual execution environment; and then automatically deploys new protections back to the front line to ensure previously unknown threats are known to all and blocked across the attack lifecycle.

WildFire

WildFire is an advanced, virtual malware analysis environment, purpose-built for high fidelity hardware emulation, analyzing suspicious samples as they execute. The cloud-based service detects and blocks targeted and unknown malware, exploits, and outbound CnC activity by observing their actual behavior, rather than relying on pre-existing signatures. In addition to quickly turning unknown threats into known, WildFire generates protections that are shared globally in about 15 minutes. The security service is natively built to run on Palo Alto Networks next-generation firewalls, allowing complete threat prevention and control over your network as cyber criminals attempt to deliver malware or communicate with infected systems.

Behavior-based cyberthreat discovery

To find unknown malware and exploits, WildFire executes suspicious content in the Windows® XP, Windows 7 and Android™ operating systems with full visibility into common file types, such as EXEs, DLLs, ZIP files, PDF documents, Office® Documents, Java®, Android APKs, Adobe® Flash® applets, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files, images, and within multiple versions of an application simultaneously.

paloalto NETWORKS®

WildFire identifies more than 250 potentially malicious behaviors to identify the true nature of malicious files based on their actions, including:

- Changes made to host: observes all processes for modifications to the host, including file and registry activity, code injection, heap spray (exploit) detection, the addition of auto-run programs, mutexes, Windows services, and other suspicious activities.
- Suspicious network traffic: 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: monitors for techniques used by advanced malware to avoid VM-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, disabling of host-based security features, and more.

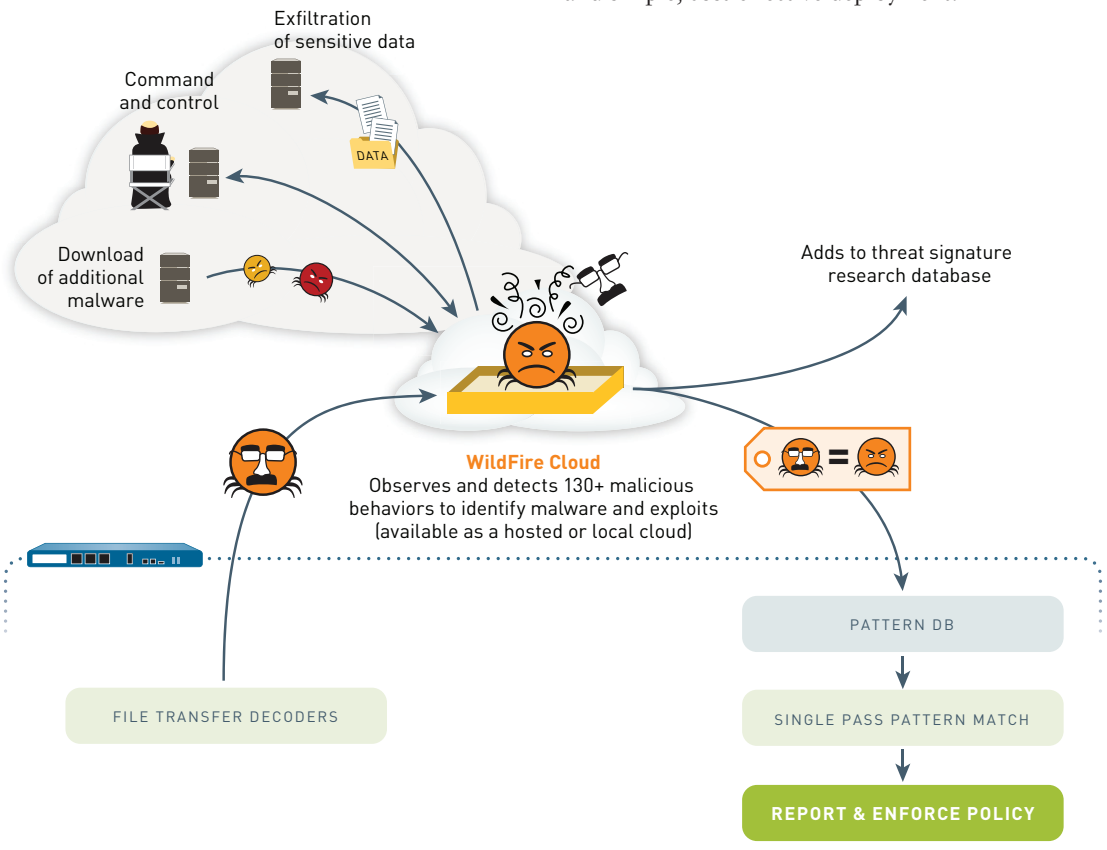
Extending the next-generation firewall platform that natively classifies all traffic across hundreds of applications, WildFire uniquely applies this behavioral analysis, regardless of ports or encryption, including full visibility into Web traffic, email protocols (i.e. SMTP, IMAP, POP) and FTP.

Cloud-based detection architecture

To support dynamic malware analysis across the network at scale, WildFire is built on a cloud-based architecture that can be leveraged by your existing Palo Alto Networks next-generation firewall, with no additional hardware. Where regulatory or privacy requirements prevent the use of public cloud infrastructure, a private cloud solution can be built on premise using the WF-500 appliance.

In addition to either public or private cloud deployments, leveraging both within the same environment is also an option. Our hybrid cloud capabilities allow users more file analysis flexibility, as they are able to define which file types are sent to the WildFire public cloud versus the on-premise WF-500, or private cloud. The WildFire hybrid cloud capability enables customers to alleviate privacy or regulatory concerns, by utilizing both the WF-500 for file types containing sensitive data, and benefit from the comprehensive analysis and global threat intelligence services of the WildFire public cloud for all others.

In each case, WildFire provides the same best-in-class visibility and simple, cost-effective deployment.



How WildFire Works: WildFire provides a logical combination of next-generation firewall hardware and scalable cloud-based malware analysis.

Threat prevention with global intelligence sharing

When an unknown threat is discovered, WildFire automatically generates protections to block it across the attack lifecycle, sharing these updates with all subscribers across the globe in as little as 15 minutes. These quick updates are able to stop rapidly spreading malware, as well as identify and block the proliferation of all future variants without any additional action or analysis. Palo Alto Networks customers' global intelligence sharing helps put all of us one step closer to stopping cyberattackers.

In conjunction with protection from malicious and exploitive files, WildFire looks deeply into malicious outbound communication, disrupting command-and-control activity with anti-CnC signatures and DNS-based callback signatures. The information is also fed into PAN-DB, where newly discovered malicious URLs are automatically blocked. This correlation of data and in-line protection are key to identifying and blocking ongoing intrusions as well as future attacks on a network.

Integrated logging, reporting and forensics

WildFire users receive integrated logs, analysis, and visibility into WildFire events in Panorama management interface, or the WildFire portal, enabling teams to quickly investigate and correlate events observed in their networks. This allows security staff to quickly 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 and application versions, including both host-based and network-based activity.
- "Grayware" verdicts for programs like adware or trackware that do not pose a direct security threat, but display otherwise suspicious behavior and can affect network performance, allowing for more accurate incident prioritization, granular content visibility and control.
- 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.
- Native integration with Traps™ Advanced Endpoint Protection to perform hash checks and receive unknown EXE files for further analysis.
- An open API for integration with best-in-class SIEM tools, such as the Palo Alto Networks application for Splunk®. This analysis provides a wealth of indicators of compromise (IOCs) that can be applied across the APT attack lifecycle.
- Access to the actionable intelligence and global context provided by Palo Alto Networks new AutoFocus™ service.

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 firewall 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:

- Use of WildFire requires PAN-OS® 4.1+
- Java, Office, APK, and multi-version PDF analysis requires PAN-OS 6.0+
- Adobe Flash and Web page analysis requires PAN-OS 6.1+
- Grayware verdicts and hybrid cloud capabilities require PAN-OS 7.0+

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 analysis images.
- EXE and DLL file types, including compressed (zip) and encrypted (SSL) content.
- Automatically submit suspicious files to WildFire.
- Automatic protections are delivered with regular Threat Prevention content updates (threat prevention license is required) every 24 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, Portable Document Format (PDF) files, Java® applets (JAR and CLASS), Android® application packages (APK), Adobe® Flash® applets (SWF and SWC), and Web pages.
- WF-500 support.
- WildFire API for programmatic submission of up to 1,000 samples per day and up to 10,000 report and verdict queries per day.

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.

WF-500 Specifications

PROCESSOR
- Dual 6-Core Intel Processor with Hyper-Threading

MEMORY
- 128 GB RAM

SYSTEM DISK
- 120 GB SSD

Hardware Specifications

I/O
- 4x10/100/1,000
- DB9 Console serial port, USB

STORAGE CAPACITY
- 2 TB RAID1: 4 x 1TB RAID Certified HDD for 2 TB of RAID Storage

POWER SUPPLY
- Dual 920 W power supplies in hot swap redundant configuration

MAX POWER CONSUMPTION
- 390 watts

RACK MOUNTABLE (DIMENSIONS)
- 2U, 19" standard rack (3.5" H x 21" D x 17.5" W)

MAX BTU/HR
- 1,300 BTU/hr

INPUT VOLTAGE (INPUT FREQUENCY)
- 100-240 VAC (50-60 Hz)

MAX CURRENT CONSUMPTION
- 3.2A@120 VAC

SAFETY
- UL, CUL, CB

EMI
- FCC Class A, CE Class A, VCCI Class A

ENVIRONMENT
- 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 on the WF-500 security features and associated capacities, please visit: **http://www.paloaltonetworks.com/products/platforms/wildfire/wf-500/overview.html.**

paloalto NETWORKS®

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