WildFire™

WildFire identifies unknown malware, zero-day exploits, and 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 cyber attacks. Built on an enterprise security platform that 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 the 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 command-and-control traffic.

Advanced cyber attacks are employing stealthy, persistent methods to evade traditional security measures. Skilled adversaries demand that modern security teams re-evaluate their basic assumptions 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 on the industry's leading 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 Threat Prevention, providing baseline defenses against known exploits, malware, malicious URLs and command-and-control (C2) 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 cyber threats, that begins with positive security controls to reduce the attack surface; inspects all traffic, ports, and protocols to block all known threats; rapidly detects unknown threats by observing their actual behavior in a cloud-based virtual execution environment; then automatically employs new protections back to the front line to ensure previously unknown threats are known to all and blocked across the kill chain.

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 C2 activity by observing their actual behavior, rather then relying on pre-existing signatures. In addition to quickly turning unknown threats to known, WildFire generates protections that are shared globally in as little as 30 minutes. The security service tightly integrates with Palo Alto Networks® next-generation firewalls, allowing complete control over your network as cyber criminals attempt to deliver malware or communicate with infected systems.

Behavioral-based cyber threat discovery

To find unknown malware and exploits, WildFire executes suspicious content against Windows XP, Windows 7 and Android operating systems, with full visibility into common file types, including: EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, and Android APKs, including high risk embedded content such as Adobe Flash files, images, and Javascript.

paloalto networks

WildFire identifies over 130 potentially malicious behaviors to identify the true nature of malicious files based on their actions including:

- **Changes made to host:** observes all process 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:** 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.

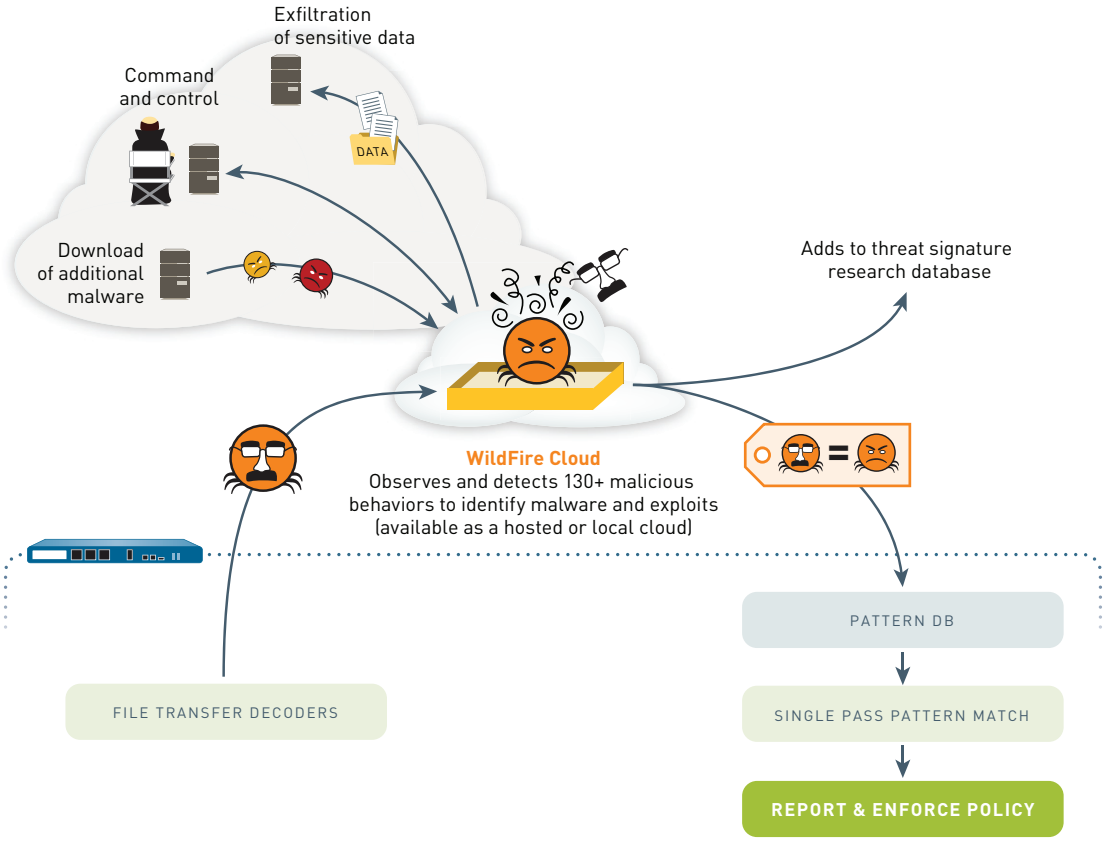
Extending the next-generation firewall platform that natively classifies all traffic across hundreds of applications, WildFire uniquely applies this behavioral analysis regardless of ports or encryption, including full visibility into web traffic, email protocols (SMTP, IMAP, POP) and FTP.

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-premises using the WF-500 appliance. In either case, WildFire provides the same best-in-class visibility and simple, cost effective deployment.

Threat prevention with global intelligence sharing

When an unknown threat is discovered, WildFire automatically generates protections to block it across the cyber kill-chain, sharing these updates with all subscribers across the globe in as little as 30 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 customer's global intelligence sharing helps put all of us one step closer to stopping cyber attackers.



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

In conjunction with protection from malicious and exploitive files, WildFire looks deeply into malicious outbound communication, disrupting command-control activity with anti-C2 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 protections 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 the management interface, Panorama, 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, 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 SEIM 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 APT kill chain.

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 datacenter 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+
- Enhanced file type support (PDF, Java, Office, APK, etc.) requires PAN-OS 6.0+

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 24-48 hours.

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

- Automatic WildFire signature updates every 30 minutes for all new malware detected anywhere in the world.
- Enhanced file type support, including: EXE, DLL, Adobe PDF, Microsoft Office Documents (.doc, .docx., .xls, .xlsx, .ppt, and .pptx), Java (.jar and class files), Android APKs. Includes analysis of commonly embedded objects such as Javascript, Flash, images, etc. Includes compressed (zip) and encrypted (SSL) content.
- WF-500 support.
- WildFire API for programmatic submission of up to 100 samples per day and up to 1,000 report queries by file hash 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
- 120GB SSD

Hardware Specifications

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

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

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

MAX POWER CONSUMPTION
- 510 Watts

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

MAX BTU/HR
- 1,740 BTU/hr

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

MAX CURRENT CONSUMPTION
- 11A@100VAC

SAFETY
- UL, CSA, 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 **www.paloaltonetworks.com/products**

paloalto networks
the enterprise security company™

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