WILDFIRE

Automatically Prevent Highly Evasive Zero-Day Exploits and Malware

Palo Alto Networks WildFire® malware prevention service is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware. The service employs a unique multi-technique approach, combining dynamic and static analysis, innovative machine learning techniques, and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats.

WildFire

- Detects evasive zero-day exploits and malware with a unique combination of dynamic and static analysis, novel machine learning techniques, and an industry-first bare metal analysis environment.
- Orchestrates automated prevention for unknown threats in as few as five minutes from first discovery anywhere in the world, without requiring manual response.
- Builds collective immunity for unknown malware and exploits with shared real-time intelligence from approximately 26,000 subscribers.
- Provides highly relevant threat analysis and context with AutoFocus contextual threat intelligence service.

Today, organizations must contend with an entire marketplace of malware and exploit developers selling or renting out their malicious tools, making them available to all classes of attackers. At the same time, advanced evasion techniques have been commoditized, allowing attacks to sidestep legacy detection approaches. Now, even low-skilled adversaries can launch unique attacks capable of evading traditional threat identification and prevention approaches, requiring human intervention that cannot scale against the volume of unknown threats seen today.

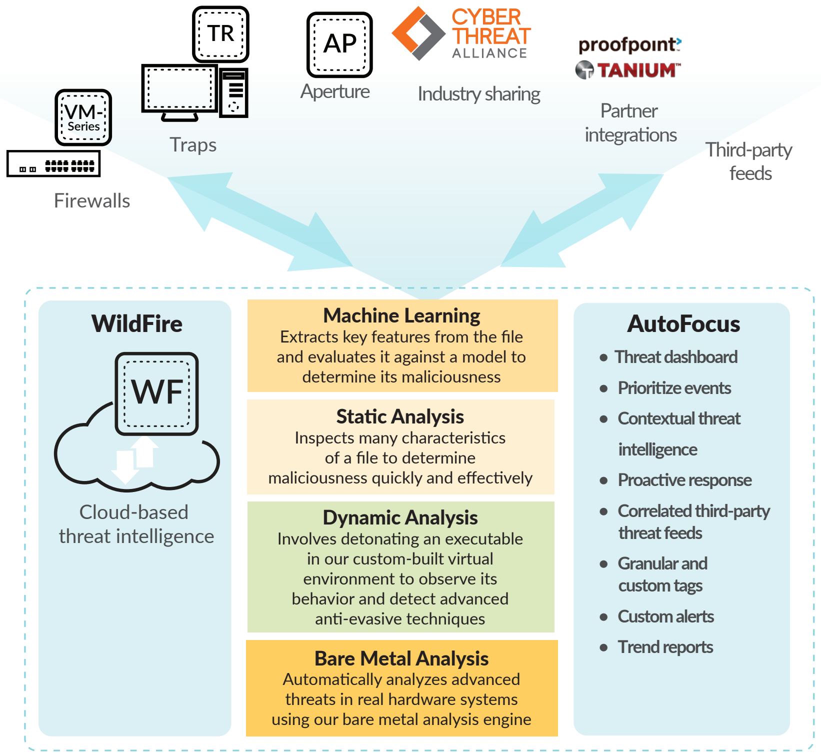
WildFire changes the equation for adversaries, turning every Palo Alto Networks platform deployment into a distributed sensor and enforcement point to stop zero-day malware and exploits before they can spread and succeed. Within the WildFire environment, threats are detonated, intelligence is extracted, and prevention is automatically orchestrated across the Palo Alto Networks Security Operating Platform in as few as five minutes after first discovery anywhere in the world.

Find the Unknown With a Unique Multi-Technique Approach

WildFire goes beyond traditional approaches used to detect unknown threats, bringing together the benefits of four independent techniques for high-fidelity and evasion-resistant discovery, including:

- **Dynamic analysis** – observes files as they detonate in a purpose-built, evasion-resistant virtual environment, enabling detection of zero-day exploits and malware using hundreds of behavioral characteristics.
- **Static analysis** – complements dynamic analysis with effective detection of malware and exploits, as well as providing instant identification of malware variants. Static analysis further leverages dynamic unpacking to analyze threats attempting to evade detection using packer tools.
- **Machine learning** – extracts thousands of unique features from each file, training a predictive machine learning model to identify new malware, which is not possible with static or dynamic analysis alone.
- **Bare metal analysis** – detonates evasive threats in a real hardware environment, entirely removing an adversary's ability to deploy anti-VM analysis techniques.

Together, these four unique techniques allow WildFire to discover and prevent unknown malware and exploits with high efficacy and near-zero false positives.



TR
AP
CYBER THREAT ALLIANCE
proofpoint
TANIUM
VM-Series
Traps
Aperture
Industry sharing
Partner integrations
Third-party feeds
Firewalls
WildFire
WF
Cloud-based threat intelligence
Machine Learning
Extracts key features from the file and evaluates it against a model to determine its maliciousness
Static Analysis
Inspects many characteristics of a file to determine maliciousness quickly and effectively
Dynamic Analysis
Involves detonating an executable in our custom-built virtual environment to observe its behavior and detect advanced anti-evasive techniques
Bare Metal Analysis
Automatically analyzes advanced threats in real hardware systems using our bare metal analysis engine
AutoFocus
Threat dashboard
Prioritize events
Contextual threat intelligence
Proactive response
Correlated third-party threat feeds
Granular and custom tags
Custom alerts
Trend reports

Figure 1: Evasion-resistant discovery

Automated Orchestration of Prevention

When zero-day exploits or malware are discovered by any WildFire subscriber, the service automatically orchestrates enforcement of high-fidelity, evasion-resistant protections for all WildFire subscribers in as few as five minutes from first discovery anywhere in the world. These protections are derived and shared across more than 26,000 WildFire users, forming the industry's largest distributed sensor network focused on detecting and preventing unknown threats. WildFire also forms the central prevention orchestration point for the Security Operating Platform, allowing the enforcement of new controls through:

- **Threat Prevention** to block malware, exploits, and command-and-control activity.
- **URL Filtering** with PAN-DB for the prevention of newly discovered malicious URLs.
- **AutoFocus™ c**ontextual threat intelligence service, enabling the extraction, correlation and analysis of threat intelligence with high relevance and context.
- **Traps™** advanced endpoint protection and Aperture™ SaaS security service for real-time verdict determination and threat prevention.
- **Integration** with our technology partners for verdict determination on third-party services with the WildFire API.

Most Advanced Malware Analysis Environment

WildFire brings forth years of groundbreaking innovation to provide the most advanced analysis environment in the industry, enabling the most accurate and evasion-resistant detection of unknown threats available today. The WildFire engine is based on two primary components:

- **Custom-built hypervisor:** Built from the ground up to avoid use of commonly used, open source emulation software that has become trivial to evade, the WildFire hypervisor is immune to commoditized anti-VM analysis techniques used to evade detection in traditional malware analysis environments. The custom hypervisor also provides a flexible framework to continue building advanced detection and evasion-resistant capability into WildFire in the future.
- **Bare metal analysis:** The most sophisticated threats can potentially observe that they are being examined in an advanced virtual environment and fail to fully detonate. To address this class of advanced attacks, WildFire has the ability to automatically analyze advanced threats in real hardware systems using our bare metal analysis engine. Now, even the most evasive threats can be conclusively identified and prevented.

Within the malware analysis environment, WildFire executes suspicious content in the Windows® XP, Windows 7, Windows 10, Android® and macOS® operating systems, with full visibility into commonly exploited file formats, such as EXE, DLL, ZIP, 7ZIP, RAR Archive, Mach-O, Mach-OSX DMG, ELF (Linux) and PDF, as well as Microsoft Office documents, Java files, Android APKs, Adobe Flash® applets and links within email messages. WildFire identifies files with potential malicious behaviors and delivers verdicts based on their actions, through:

- **Complete malicious behavior visibility** – identifies threats in all traffic across hundreds of applications, including web traffic, email protocols like SMTP, IMAP and POP, as well as file sharing protocols like SMB and FTP, regardless of ports or encryption.
- **Changes made to host** – observes all processes for modifications to the host, including evidence of exploitation, persistence mechanisms, data encryption or system destruction techniques.
- **Suspicious network traffic** – 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** – monitors techniques used by advanced malware that are designed to avoid VM-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, disabling of host-based security features and much more.
- **Threat intelligence, analytics and correlation.**

In combination with WildFire, organizations can use AutoFocus to hone in on the most targeted threats with high relevance and context. AutoFocus provides the ability to hunt across all data extracted from WildFire, as well as third-party threat feeds, using MineMeld™ threat intelligence syndication engine. It allows users to correlate indicators of compromise and samples with human intelligence from the Unit 42 threat research team in the form of tags. Together, WildFire and AutoFocus provide a complete picture of unknown threats targeting your organization and industry, increasing your ability to quickly take action by:

- Automatically updating External Dynamic Lists on Palo Alto Networks next-generation firewalls.
- Automatically exporting indicators of compromise to third-party tools via STIX™, TAXII™ and APIs.

These actions require no human intervention and reduce the cost of adding specialized security staff.

Safe, Scalable Cloud-Based Architecture

The unique cloud-based architecture of WildFire supports unknown threat detection and prevention at massive scale across the network, endpoint and cloud. You can take advantage of the service as part of the Security Operating Platform without introducing a performance impact to the firewall. To meet even the strictest local privacy or regulatory requirements, WildFire is available in multiple deployment modes, including:

- **Global cloud delivery:** Files are submitted to the WildFire global cloud, delivering scale and speed, and enabling any customer of Palo Alto Networks to quickly turn on the service, including next-generation firewalls, VM-Series, public cloud offerings, Aperture and Traps.
- **Private cloud delivery:** The WildFire appliance, a local on-premises device, conducts all threat detonation, intelligence extraction and protection generation, but it maintains the ability to receive updates from the global cloud for customers with privacy or regulatory requirements.
- **Hybrid cloud delivery:** You can combine the benefits of the global and private clouds by choosing to send sensitive files to the private cloud while other content is analyzed by the global cloud.
- **Global cloud infrastructure:** Users benefit from automated protections delivered through the global cloud without the need to send content beyond their borders, allowing them to maintain privacy and compliance at scale.

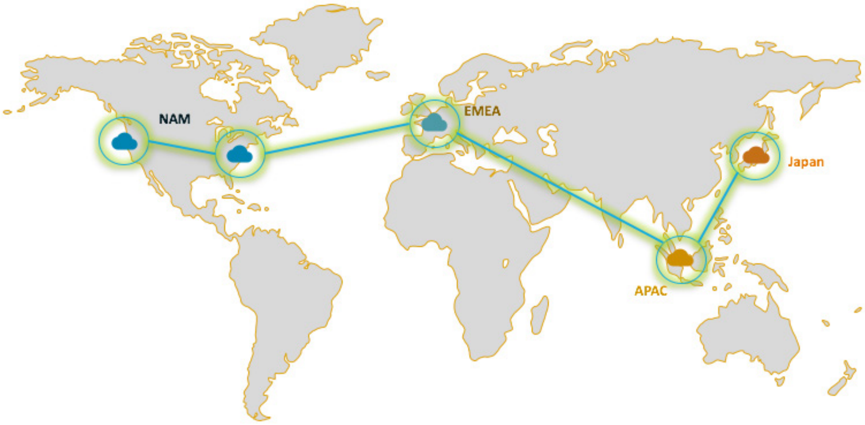


Figure 2: Global cloud infrastructure

Integrated Logging, Reporting and Forensics

WildFire users receive integrated logs, analysis and visibility into malicious events through the PAN-OS® management interface, Panorama™ network security management, AutoFocus or the WildFire portal, enabling teams to quickly investigate and correlate events observed in their networks. This allows security staff to rapidly locate and take action on the data needed for timely investigations and incident response, including:

- Detailed analysis of every malicious file sent to WildFire across multiple operating system environments, including both host- and network-based activity.
- Session data associated with the delivery of the malicious file, including source, destination, application, user, URL and other attributes.
- Access to the original malware sample for reverse engineering, with full PCAPs of dynamic analysis sessions.
- An open API for integration with third-party security tools, such as security information and event management systems, or SIEMs.

Security Operating Platform

Built on the Security Operating Platform, WildFire blocks known and unknown threats before they can cause harm, taking advantage of:

- **Full visibility into all network traffic,** including stealthy attempts to evade detection, such as the use of nonstandard ports or SSL encryption.
- **Attack surface reduction** with positive security controls to proactively take away infection vectors.
- **Automatic known threat prevention** with our next-generation firewalls, Threat Prevention, URL Filtering, Traps and Aperture, providing defenses against known exploits, malware, malicious URLs, and command-and-control activity.
- **Unknown threat detection and prevention** with WildFire, including threat analytics with high relevance and context through the AutoFocus service.

The result is a unique, closed-loop approach to preventing cyberthreats, ensuring they are known to all and blocked across the attack lifecycle.

Maintaining the Privacy of Your Files

The security and privacy of customer data is our top-priority. The WildFire infrastructure is managed directly by Palo Alto Networks, leverages industry-standard best practices for security and confidentiality, and is regularly audited for SOC 2 compliance. You can find further information in the WildFire Privacy datasheet.

WildFire Requirements

WildFire analysis of certain file types requires the following version, or a newer version, of PAN-OS:

- Baseline WildFire functionality requires PAN-OS 4.1+
- DF, Java, Office and APK analysis requires PAN-OS 6.0+
- Adobe Flash and webpage analysis requires PAN-OS 6.1+

Licensing Information

The WildFire global cloud subscription provides:

- Windows XP, Windows 7, Windows 10, macOS and Android OS virtual analysis environments.
- Automated signature updates delivered every five minutes for zero-day malware and exploits discovered by any WildFire subscriber submitting samples to the WildFire global cloud. Signatures include file-based antivirus signatures, Domain Name System signatures and URL signatures. URL signatures require a PAN-DB subscription.
- Support for PE files, such as EXE, DLL and others; all Microsoft Office file types, PDFs; Flash files; Java applets, including JAR and CLASS; RAR and 7ZIP archive files; Linux ELFs; Android APKs; macOS binaries, such as Mach-O, DMG, PKG and application bundles; scripts, including JScript, VBScript, PowerShell and Shell script; and analysis of links within email messages. This includes support for compressed and encrypted content.
- Analysis of select samples in a bare metal analysis environment, as determined by the WildFire system.
- Basic WildFire functionality is available as a standard feature on all Security Operating Platform deployments running PAN-OS 4.1 or later, enabling a restricted set of WildFire features, including:
  - Windows XP and Windows 7 virtual analysis environments.
  - Automated submission of only EXE and DLL file types, including compressed and encrypted content.
  - Automatic protections delivered with regular Threat Prevention content updates every 24 hours, given an active Threat Prevention subscription.

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