WildFire

Eliminate Risks from Highly Evasive Malware

Today's adversaries have easy access to cloud scale, legitimate infrastructure, and machine learning to quickly distribute evasive malicious files to end users. Siloed security tools simply can't keep up with today's malware, which is proliferating at a rate of 1,000 new threats every five minutes, with up to 10,000 variants seen five minutes thereafter.

Business Benefits

- **Don't be the first victim of a new threat.** Inline prevention stops "patient zero" without affecting productivity.
- **Eliminate dwell time risk.** Cut threat response time to seconds with automated delivery of coordinated protection across network, endpoint, and cloud.
- **Reduce actionable events and workload for the SOC.** Stop the initial threat, delivering fewer detection events to investigate and contain.
- **Reduce TCO with cloud-based architecture.** Eliminate costs to deploy, manage, patch, and maintain appliance-based sandboxes.
- **Gain infinite analysis capacity with no incremental costs.** Subscription model delivers compute and scalability with no capacity-based charges.
- **Avoid manual integrations.** Threat intel automatically flows into the Palo Alto Networks ecosystem, eliminating manual tooling or integration.

Organizations suffering zero-day attacks or advanced persistent threats that cause data breaches can face:

- **Reputational risk**—highly visible media and press created by government and industry reporting requirements, compounded by the volume and type of information lost.
- **Regulatory risk**—sanctions imposed by governing bodies as well as increased compliance and assessment requirements, depending on information assets targeted (e.g., personally identifiable information [PII], account information, business or customer intellectual property).
- **Financial risk**—potential revenue loss associated with lower buyer confidence, ransomware, and increased regulations (e.g., downtime, reduced sales, increase in compliance requirements, cost of data retrieval).
- **Legal risk**—liability due to civil challenges and due diligence issues stemming from customer data loss and compliance with regulations (e.g., HIPAA, GDPR, US state legislation [CCPA, NYDFS Cybersecurity Regulation, etc.], Australian data privacy regulations).

To mitigate risks associated with evasive attacks, organizations turn to network sandboxing solutions for malware analysis. Unfortunately, all of these traditional solutions affect user productivity and are slow to deliver verdicts, interrupting workflows by holding files for analysis, trickling some content while samples are being scanned, or changing content and making many files unreadable. Moreover, these solutions have another fatal flaw: they can only protect against new threats after the first victim in an organization (a.k.a. patient zero) has already been identified or compromised.

Immediate Prevention Powered by Infinitely Scalable Cloud Analysis

Palo Alto Networks WildFire® malware prevention service eliminates the need to compromise security for performance and finally enables organizations to adopt a prevention-first posture. As the industry's most advanced cloud-based analysis and prevention engine for malware, WildFire analyzes every unknown file for malicious intent, and then distributes prevention in record time to reduce the risk of a first victim—and every threat thereafter.

Unlike traditional solutions that depend solely on offline or delayed analysis of unknown malware, WildFire analysis and intelligence flow directly into machine-learning models that act locally at the firewall level to stop up to 95% of new threats inline. For the rest, WildFire uses an innovative multi-technique approach to distribute signatures to every ML-Powered NGFW in seconds.

No other malware analysis engine can offer prevention without affecting productivity. WildFire combines dynamic and static analysis, innovative machine-learning techniques, recursive analysis, and a groundbreaking custom-built analysis environment to analyze, identify, and prevent even the most sophisticated and evasive threats. After analysis, automation is where WildFire shines: it applies rapid and consistent prevention at the edge, in your data center, from the cloud, within software-as-a-service (SaaS) applications, and on endpoints.

Key Capabilities

Prevent Unknown Threats at the Firewall Level with Inline Machine Learning

Powered by threat models continually honed in the cloud, WildFire includes an inline machine learning-based engine delivered within our hardware and virtual ML-Powered NGFWs. This innovative, signatureless capability prevents malicious content in common file types—such as portable executable files and fileless attacks stemming from PowerShell—completely inline, with no required cloud analysis, no damage to content, and no loss of user productivity. Whether an unknown file matches an existing signature or is classified by an ML-Powered NGFW, WildFire always performs full analysis, extracting valuable intelligence and data to provide context for security analysts, generate training updates for the machine-learning models, and share intelligence with other subscriptions to prevent other attack vectors.

Get Global Prevention Across the WildFire Ecosystem, Delivered in Seconds

For highly customized threats that its inline machine learning-powered prevention cannot stop, WildFire applies powerful cloud-based analysis to deliver prevention across networks, clouds, endpoints, or wherever WildFire-enabled sensors are deployed. Working in tandem with the new capabilities of PAN-OS®, WildFire generates and delivers prevention globally within seconds of initial analysis for most new threats. This innovative, cloud-scale delivery of evasion-resistant signatures closes the window for adversaries to successfully deploy malicious content.

Use Signatures, Not Hashes

Because WildFire uses content signatures for prevention instead of hashes, it can identify more malware with a single signature. As a result, compared to the mostly hash-based systems that require 1:1 ratios, WildFire protects against more attacks with the same resources. A single WildFire signature can protect against up to millions of polymorphic variants of a single malware.

Root Out Malicious Behavior in All Traffic

WildFire identifies files with potential malicious behaviors and then delivers verdicts based on their actions by applying threat intelligence, analytics, and correlation alongside advanced capabilities:

- **Complete malicious behavior visibility** identifies threats in all traffic across hundreds of applications, including web traffic; email protocols like SMTP, IMAP, and POP; and file-sharing protocols like SMB and FTP, regardless of ports or encryption.
- **Suspicious network traffic analysis** monitors all network activity produced by a suspicious file, including backdoor creation, downloading of next-stage malware, visiting low-reputation domains, network reconnaissance, and much more.
- **Fileless attack/script detection** identifies when potentially malicious scripts, such as JScript and PowerShell, are traversing the network and forwards them to WildFire for analysis and execution.

The powerful discovery and analysis capabilities of WildFire are seamlessly integrated with numerous products across the Palo Alto Networks portfolio as well as within leading partner solutions across email and cloud platforms.

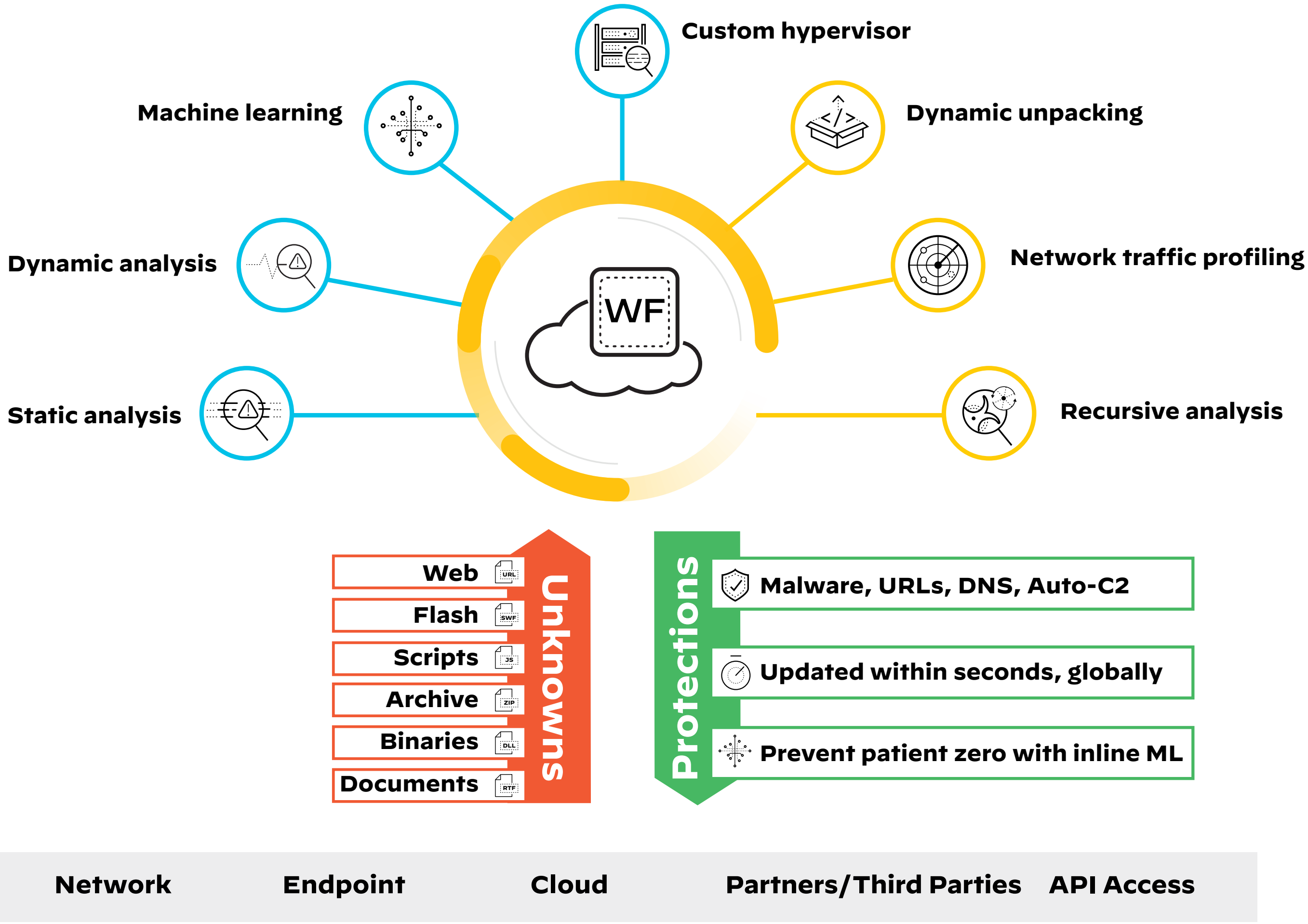

Figure 1: WildFire: the global nerve center for malware analysis

Uncover New Threats with a Multitechnique, Evasion-Resistant Approach

WildFire goes beyond traditional sandboxing approaches used to detect unknown threats in a cloud analysis environment, bringing together multiple techniques:

- **Dynamic analysis** observes files as they execute in a purpose-built, evasion-resistant virtual environment, enabling detection of previously unknown malware using hundreds of behavioral characteristics.
- **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.
- **Static analysis** complements dynamic analysis with effective detection of malware, providing instant identification of malware variants. Static analysis further leverages dynamic unpacking to analyze threats attempting to evade detection through the use of packing tool sets.
- **A custom-built hypervisor** prevents attacker evasion techniques with a robust, proprietary hypervisor that does not depend on open-source projects or proprietary software to which attackers have access.

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

Operational Benefits

- **Automate reprogramming of security controls to block unknown threats**: Shared real-time intelligence from more than 35,000 subscribers automatically updates and prevents threats across networks, endpoints, and clouds.
- **Gain detailed context on analyzed threats**: Get thorough reports of every malicious file sent to WildFire across multiple operating system environments and application versions.
- **Integrate seamlessly to enrich custom applications and existing security tools:** Leverage open API integration with SIEM, TIP, ticketing, SOAR, XDR tools, or custom use cases to process indicators of compromise (IoCs).
- **Leverage actionable threat intelligence**: Together with AutoFocus contextual threat intelligence, you can understand adversaries and their intent as well as track campaigns to ensure your next move is the right one.

Stop Complex, Multistage Attacks

Threat actors continue to evolve malware to evade existing analysis techniques by breaking attacks into distinct components and stages, using multiple concurrent delivery vectors, and exploiting reputable cloud services to avoid detection. These strategies render traditional single-stage, single-vector malware analysis ineffective.

By combining the cloud scale of WildFire with advanced file analysis and URL crawling, Multi-Vector Recursive Analysis (MVRA) delivers a unique and comprehensive solution to prevent threat actors' sophisticated multistage, multihop attacks. Unlike other solutions, WildFire can follow multiple stages of attack from a file analysis standpoint even if execution fails in a given stage. This workflow unifies analysis across both web and file attack vectors, enabling a unique, holistic view of a campaign over multiple stages. Attackers can no longer hide malicious content behind multiple stages of benign URLs or reputable document sharing sites.

Deploy in a Safe, Scalable Cloud-Based Architecture

The cloud-based architecture of WildFire supports unknown threat analysis and prevention at massive scale across networks, endpoints, and clouds. Files are submitted to the WildFire global cloud, delivering scale and speed, and any Palo Alto Networks customer can quickly turn on the service—including users of hardware and Virtual ML-Powered NGFWs, public cloud offerings, Prisma® SaaS, and Cortex® XDR™ agents. Palo Alto Networks manages the WildFire infrastructure directly, following industry-standard best practices for security and confidentiality, with regular SOC 2 compliance audits. See the WildFire Privacy datasheet for more information.

To enable you to better address data sovereignty and privacy concerns, we maintain distributed regional WildFire clouds that give you more control over the location of your data. Providing the same detection and prevention capabilities as the WildFire public cloud, these clouds allow you to adjust submissions to address localized data privacy concerns.

Integrate Seamlessly with Existing Security Tools and Custom Applications

The rapid move to the cloud and digital transformation efforts are surfacing security challenges that require rapid, effective, and on-demand malware analysis performed outside of the next-generation firewall or traditional control points. The WildFire API enables customers to make queries to WildFire for information about potentially malicious content and submit files for analysis using the advanced threat analysis capabilities of WildFire. Using this RESTful API, customers can leverage the industry-leading malware analysis capabilities of WildFire to integrate with existing SOAR tools, secure custom applications (such as business-to-consumer web portals), scan file share and storage locations for malicious content prior to cloud migration, and more. A standard WildFire subscription unlocks API access for a fixed number of submissions and queries. A separate standalone WildFire subscription, which does not require the purchase of a next-generation firewall, enables customers to purchase flexible submission and query volumes to access WildFire malware analysis via an API wherever it is needed.

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™, Cortex XDR, Cortex XSOAR, or the WildFire Portal, enabling teams to quickly investigate and correlate events observed in their networks. With this information, security teams can rapidly locate and take action on the data needed for timely investigations and incident response, regardless of the application they use.

The Power of Palo Alto Networks Security Subscriptions

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats.

- **Threat Prevention:** Goes beyond traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance.
- **Advanced URL Filtering**: Provides best-in-class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protections.
- **WildFire:** Ensures files are safe with automatic detection and prevention of unknown malware powered by industry-leading, cloud-based analysis and crowd-sourced intelligence from over 42,000 customers.
- **DNS Security:** Harnesses the power of machine learning to detect and prevent threats over DNS in real time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
- **IoT Security:** Provides the industry's most comprehensive IoT security solution delivering ML-powered visibility, prevention, and enforcement in a single platform.
- **Enterprise DLP**: The industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users.
- **SaaS Security:** Delivers integrated SaaS security that lets you see and secure new SaaS applications, protect data, and prevent zero-day threats at the lowest TCO.

Table 1: Features and Licensing Summary

Capabilities Activated with WildFire Subscription Attached to NGFW	
Advanced Analysis, Prevention, and Anti-Evasion Techniques	**Static analysis**—combines memory analysis, machine learning, and analysis of file anomalies, malicious patterns, and known malicious code. **Inline ML-based prevention (on firewall)**—blocks unknown malicious executables and PowerShell attacks. **Dynamic analysis**—includes custom hypervisor, behavioral scoring, network profiling, and multiversion analysis. **MVRA**—combines advanced file analysis with URL crawling to prevent multistage, multihop attacks.
OS Support	macOS, Android, Windows XP/7/10, Linux
File Support	PE files (EXE, DLL, and others), all Microsoft Office file types, Mac OS X files, Linux (ELF) files, Android Package Kit (APK) files, Adobe Flash and PDF files, archive (RAR and 7-Zip) files, script (BAT, JS, VBS, PS1, Shell script, and HTA) files, analysis of links within email messages, and encrypted (TLS/SSL) files.
Protocol Support	SMTP, POP3, SMB, FTP, IMAP, HTTP, HTTPS

Table 1: Features and Licensing Summary (continued)	
Capabilities Activated with WildFire Subscription Attached to NGFW	
File Analysis per Day	Elastic
Signature Type	• Based on new/zero-day malware discovered in web traffic (HTTP/HTTPS), email protocols (SMTP, IMAP, and POP), and FTP traffic. • Generated on the malware payload of the sample and tested for accuracy and safety.
Protection Updates for Unknown Malware	• Seconds, with zero-delay signatures to connected NGFW.*
Regional Cloud Locations	• Australia, Canada, Germany, India, Japan, The Netherlands (EU Regional Cloud), Singapore (APAC Regional Cloud), United Kingdom, United States (Global Cloud and US Government Cloud)
WildFire API Key	The WildFire subscription on the NGFW includes access to the WildFire API key, enabling integrating WildFire into other applications. This key has daily limits.
Integrations	• With Palo Alto Networks, including all cloud-delivered security subscriptions, Cortex XDR, Cortex XSOAR, Prisma Access, Prisma Cloud, Enterprise DLP, SaaS Security.
	• With technology partners for verdict determination on third-party services with the WildFire API.
Management and Reporting	Palo Alto Networks Panorama and WebUI, API
Forensics	• Detailed analysis of every malicious file sent to WildFire across multiple operating system environments, including both host- and network-based activity. • Access to the original malware sample for reverse engineering, with full PCAPs of dynamic analysis sessions. • Open API for integration with third-party security tools, such as security information and event management (SIEM) systems.
Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our privacy datasheets.
Requirements	To use the Palo Alto Networks WildFire subscription, you will need: • Palo Alto Networks Next-Generation Firewalls running PAN-OS • Palo Alto Networks Threat Prevention license
Recommended Environment	Palo Alto Networks Next-Generation Firewalls deployed in any location, as both internal and external sources, may introduce file-based threats into the network.

* Requires PAN-OS 10.0 and above.

paloalto® NETWORKS

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