Advanced WildFire

Stop Highly Evasive Malware with Inline AI Protection

Today's modern threat actors have two main advantages over organizations: opportunity and accessibility. With the adoption of hybrid work, the shift to the cloud, and rapid growth in IoT and SaaS applications, the attack surface has expanded, providing significant opportunities for threat actors to find ways to infiltrate an organization. In addition, ransomware as a service and automation offerings have lowered the technical bar for deploying sophisticated malware campaigns, giving even lazy and less tech-savvy threat actors easy access to the tools they need to increase the volume, severity, and scope of attacks.

Go Beyond File Analysis with Cloud-Powered Inline ML and Inline Static Analysis

Palo Alto Networks Advanced WildFire® is the industry's largest cloud-based malware prevention engine that protects organizations from highly evasive threats using patented machine learning detection engines, enabling automated protections across networks, cloud, and customer application endpoints.

As a sample gets analyzed by Advanced WildFire, it will pass through a combination of the following analysis engines:

- **Lightweight inline machine learning** models on the Next-Generation Firewall provide real-time prevention of known malware and unknown variants.
- **Cloud-powered inline ML and static analysis** detect and prevent zero-day malware to safeguard against patient zero attacks.
- **Static analysis** looks at the characteristics of a file while leveraging dynamic unpacking to analyze threats attempting to evade detection through packing tool sets.
- **Cloud-based machine learning** models extract thousands of unique features, which is impossible without static or dynamic analysis.
- **Dynamic analysis** observes files as they detonate in a purpose-built, evasion-resistant virtual environment, enabling the detection of previously unknown malware.
- **Intelligent real-time memory analysis** captures snapshots of malicious activity in memory and conducts real-time analysis to identify malicious behavior, detecting highly evasive malware that would've otherwise gone undetected.

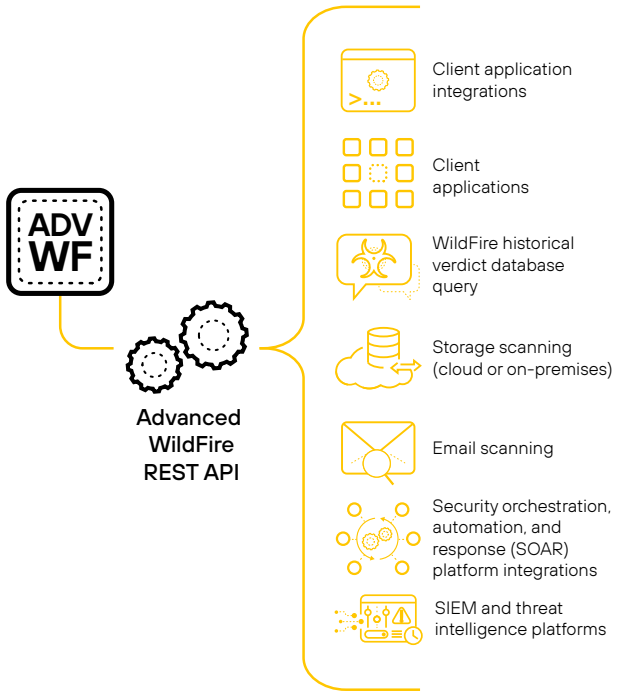


Figure 1: Advanced WildFire REST API

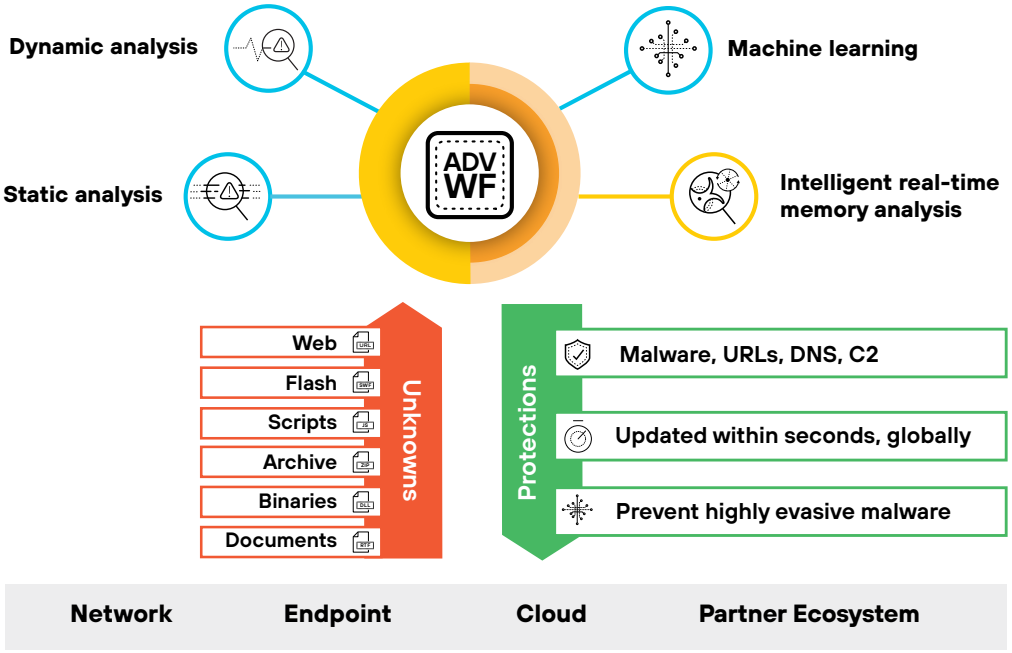
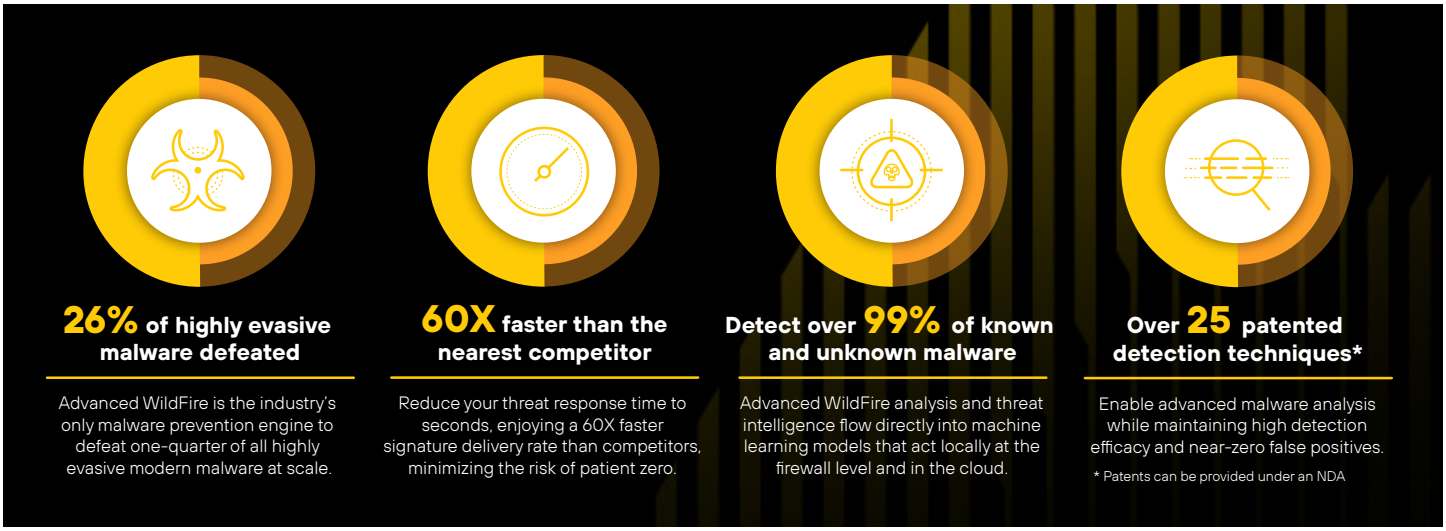


Figure 2: Integrated security for protection across your organization

Upon analysis, automated prevention is where Advanced WildFire excels. It applies rapid and consistent protection at the edge, in your data center, in the cloud, within software-as-a-service (SaaS) apps, and on endpoints. Advanced WildFire goes beyond traditional sandboxing methods to prevent unknown and highly evasive malware in the cloud.



Key Benefits

The Advanced WildFire solution enables you to:

- Take advantage of an "infinite" signature repository and access all known AV signatures.
- Achieve comprehensive protection while meeting compliance requirements.
- Reduce actionable events and workload for the SOC.
- Natively integrate with the Palo Alto Networks platform.
- Block malicious file types inline while leveraging an ML-based engine.

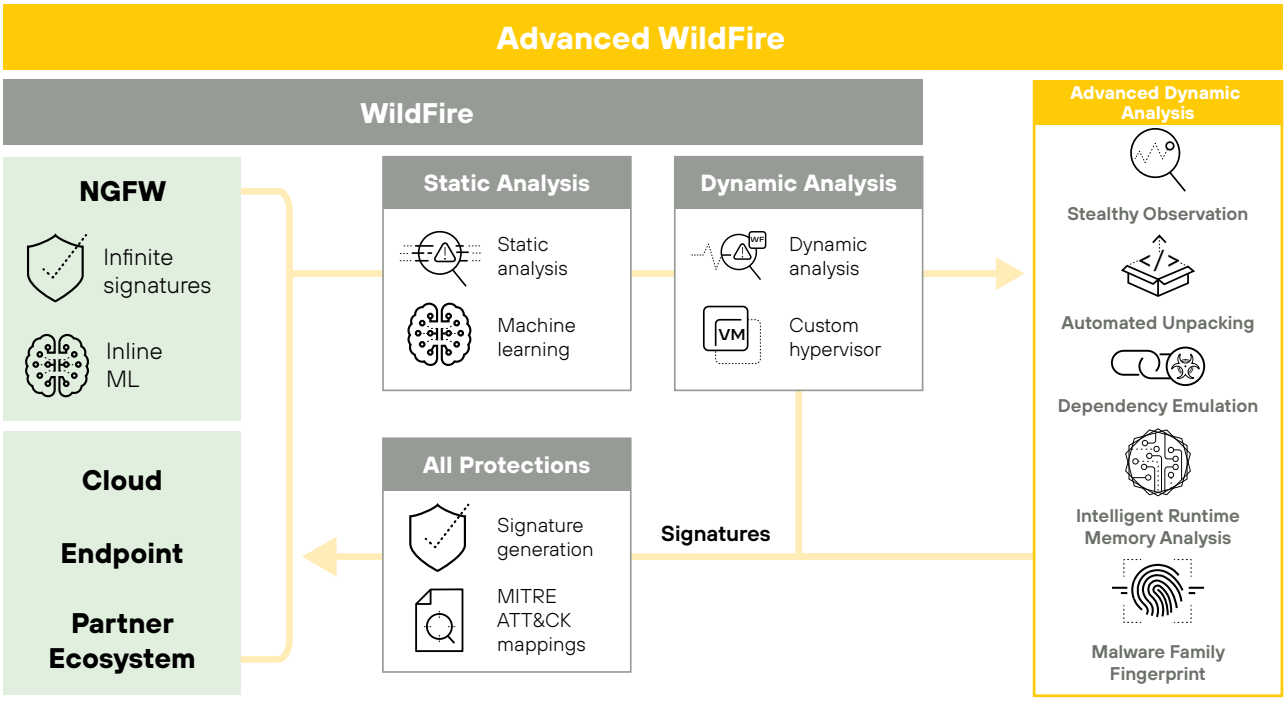


Figure 3: Advanced WildFire detection engines

Product Capabilities

Detect Malicious Behavior

Advanced WildFire identifies files with potential malicious behaviors and delivers a verdict based on their actions by applying threat intelligence, analytics, and correlation alongside advanced capabilities, which include:

- **Complete malicious behavior visibility** to identify threats in all traffic across hundreds of applications, including web traffic and email protocols such as SMTP, IMAP, and POP.
- **Suspicious network traffic analysis** evaluates all network activity caused by a suspicious file, such as backdoor creation, download of next-stage malware, and much more.
- **Fileless attack/script detection** to identify when potentially malicious scripts, such as JScript and PowerShell, traverse the network and forward them to Advanced WildFire for analysis and execution.

Stop Threats at the Firewall Level with Inline Machine Learning

Advanced WildFire is powered by continuously trained threat models in the cloud and features an inline machine learning-based engine deployed within our hardware and virtual ML-Powered NGFWs. This novel, signatureless feature detects dangerous content in common file types—such as Portable Executable files and fileless attacks originating from PowerShell—completely inline, with no need for cloud analysis, content damage, or loss of user productivity.

Prevent Highly Evasive Malware

Defeat modern malware evasion techniques using the following key features:

- **Stealthy observation**: Malware conducts environmental checks and withholds detonation if it believes it's in a sandbox environment. It uses a custom-hardened hypervisor where analysis components exist outside the guest virtual machine (VM).
- **Automated unpacking**: Advanced WildFire gains complete visibility into file contents during analysis and generates signatures on packed payloads.
- **Dependency emulation**: Using the new dependency emulation capabilities, the sandbox environment will satisfy all external dependencies required for malware to execute, allowing analysis engines to observe malicious behavior.
- **Intelligent runtime memory analysis**: Detection infrastructure to support intelligent runtime memory analysis enables a snapshot to be taken at critical points in memory when malicious behavior is observed.
- **Malware family fingerprinting**: Employs patented malware family fingerprinting detection to correlate new threats to known malware families, generating preventions for evasive malware at scale.

Global Prevention Across the Advanced WildFire Ecosystem in Seconds

Advanced WildFire applies a robust cloud-based analysis to deliver prevention across networks, clouds, and endpoints for highly customized threats that inline machine learning-powered prevention can't stop. In addition, Advanced WildFire-enabled sensors are deployed to provide global prevention within seconds of initial analysis for most new threats.

Use Signatures, Not Hashes

Advanced WildFire uses content signatures for prevention instead of hashes to identify more malware with a single signature, protecting against up to millions of polymorphic variants of a single malware.

Deploy in a Compliant and Secure Cloud-Based Architecture

Files are submitted to the Advanced WildFire global cloud, delivering speed and scale. Customers can turn on the service, which includes users of hardware and virtual ML-powered NGFWs, public cloud offerings, Next-Generation CASB, and Cortex XDR® agents. In addition, Palo Alto Networks directly manages the Advanced WildFire infrastructure, following industry-standard best practices for security and confidentiality, with regular SOC 2 compliance audits. See the Advanced WildFire privacy datasheet and certifications webpage for more information.

Integrate Seamlessly with Existing Security Tools and Custom Applications

The rapid move to the cloud and digital transformation efforts are surfacing security challenges requiring rapid, effective, and on-demand malware analysis outside of the next-generation firewall or traditional control points. Customers can leverage the industry-leading malware analysis capabilities of Advanced WildFire to integrate with existing SOAR tools to secure custom applications (such as business-to-consumer web portals), scan file share and storage locations for malicious content before cloud migration, and more. Furthermore, an Advanced WildFire subscription on NGFW unlocks API access for a fixed number of submissions and queries.

Standalone WildFire API

A Standalone WildFire API subscription allows you to query the WildFire cloud threat database for information about potentially malicious content and submit files for analysis using the advanced threat analysis capabilities of WildFire based on your organization's specific requirements.

Integrated Logging, Reporting, and Forensics

Advanced WildFire users receive integrated logs, analysis, and visibility into malicious events through the PAN-OS® management interface, Panorama® network security management, Strata™ Cloud Manager, Cortex XDR, or Cortex XSOAR®, enabling teams to investigate quickly and correlate events observed in their networks.

Table 1: Features and Licensing Summary

	Capabilities Activated with the Advanced WildFire Subscription Attached to NGFW
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, and HTTPS. An encrypted version additionally supports the previously mentioned protocols.
File Analysis per Day	80 million + unique files analyzed per day.
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), the United Kingdom, United States (Global Cloud and US Government Cloud). Regional Clouds.
WildFire API Key	The Advanced WildFire subscription on the NGFW includes access to the Advanced WildFire API, enabling integrating Advanced WildFire into other applications. This API has daily limits for file submissions and hash queries.
Integrations	• With Palo Alto Networks, including all cloud-delivered security subscriptions, Cortex XDR, Cortex XSOAR, Prisma Access, Prisma Cloud, and SaaS Security. • With technology partners for verdict determination on third-party services with the Advanced WildFire API.
Management and Reporting	Palo Alto Networks Panorama and WebUI, API, and AIOps.

Table 1: Features and Licensing Summary (continued)		
	Capabilities Activated with the Advanced WildFire Subscription Attached to NGFW	
Forensics	• Detailed analysis of every malicious file sent to Advanced 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.	
	Advanced WildFire Feature	**PAN-OS Requirement**
Requirements†	WildFire cloud-based file analysis	Any supported PAN-OS
	Advanced WildFire cloud-based file analysis	Any supported PAN-OS
	NGFW inline machine learning (PE, ELF, PS1, PS2, Office)	10.1+
	Advanced WildFire real-time signature delivery	10.1+
	Advanced WildFire inline patient zero protection	11.1
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 10.1.

† Customers can purchase Advanced WildFire with any PAN-OS version and will receive additional features upon upgrade. To use the features of the Palo Alto Networks Advanced WildFire subscription, you'll need to meet the PAN-OS requirements shown here.

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

strata_ds_advanced-wildfire_032624