Advanced WildFire

Stop Highly Evasive Malware at Scale

Modern threat actors have two main advantages over organizations today: 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 greater opportunity 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, providing threat actors access to the tools they need to increase the volume, severity, and scope of attacks.

Modern malware has been shown to be highly evasive, using techniques such as packing, encryption, and fileless or memory-only presence to bypass traditional security defenses. These advanced evasion methods have added complexity in detecting new and sophisticated malware, rendering AV scanning and traditional sandboxing solutions useless.

Business Benefits

The Advanced WildFire security service enables you to:

- **Reduce the risk of patient zero.** Prevent 26% more highly evasive malware that bypasses traditional sandboxes, in addition to stopping over 99% of known and unknown malware.[1]
- **Take advantage of an "infinite" signature repository.** Access all known AV signatures, whether the threat was seen yesterday or 10 years ago, with real-time signature lookup provided on the NGFW.
- **Achieve comprehensive protection while meeting compliance requirements.** Join a global network of 85K+ customers with access to 10 regional clouds and 17 international certifications.
- **Eliminate dwell time risk.** Cut threat response time to seconds with automated delivery of coordinated protection across network, endpoint, and cloud, with 60x faster signature delivery than the nearest competitor.
- **Reduce actionable events and workload for the SOC.** Stop the initial threat, delivering fewer detection events to investigate and contain.
- **Avoid manual integrations.** Threat intel automatically flows into the Palo Alto Networks ecosystem, eliminating manual tooling or integration.

1. "Palo Alto Networks WildFire Detection Efficacy: Public Statement," AV-Test, June 2022.

The Pitfalls of Traditional Sandboxing Solutions

To mitigate risks associated with attacks using evasive attacks, organizations turn to network sandboxing solutions for malware analysis. Unfortunately, traditional sandboxing solutions can suffer from the following pitfalls that render them useless against advanced threats:

- **Traditional sandboxing solutions cannot stay hidden from malware**. Highly evasive malware checks for instrumentation or "hooks," which are used by sandboxes to log the activity of a sample when it is under analysis. Since analysis engines reside in the same environment as where the malware would execute, if malware observes the presence of these hooks, it will choose not to execute or, in cases of sophisticated malware, to evade the hooks. This tricks the sandbox into thinking the sample is benign.
- **Traditional sandboxing solutions may be tricked by latent behavior**. Some sandboxes can time out and miss a detection because of "sleeping" malware. Traditional sandboxes cannot simply reduce the timer to a low number because it might break the execution of other software.
- **Traditional sandboxing solutions cannot detect memory-resident malware**. Machine learning models trained on file structure alone are ineffective at detecting samples that employ evasion techniques such as obfuscation, packing, and execution of dynamically injected shellcode in process memory. Additionally, significant storage, compute, and infrastructure are required to look into memory samples, which most vendors do not invest in.
- **Traditional inline sandboxing solutions affect user productivity**. When a vendor chooses to hold files for analysis, they will, in turn, interrupt user workflows and productivity.
- **Traditional sandboxing solutions are slow to deliver verdicts**. Without a connected security ecosystem, signature updates can take anywhere from hours to days to provide updates.

Go Beyond Traditional Sandboxing

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 network, cloud, and endpoints. Advanced WildFire analyzes every unknown file for malicious intent and then distributes prevention in record time—60 times faster than the nearest competitor—to reduce the risk of patient zero.

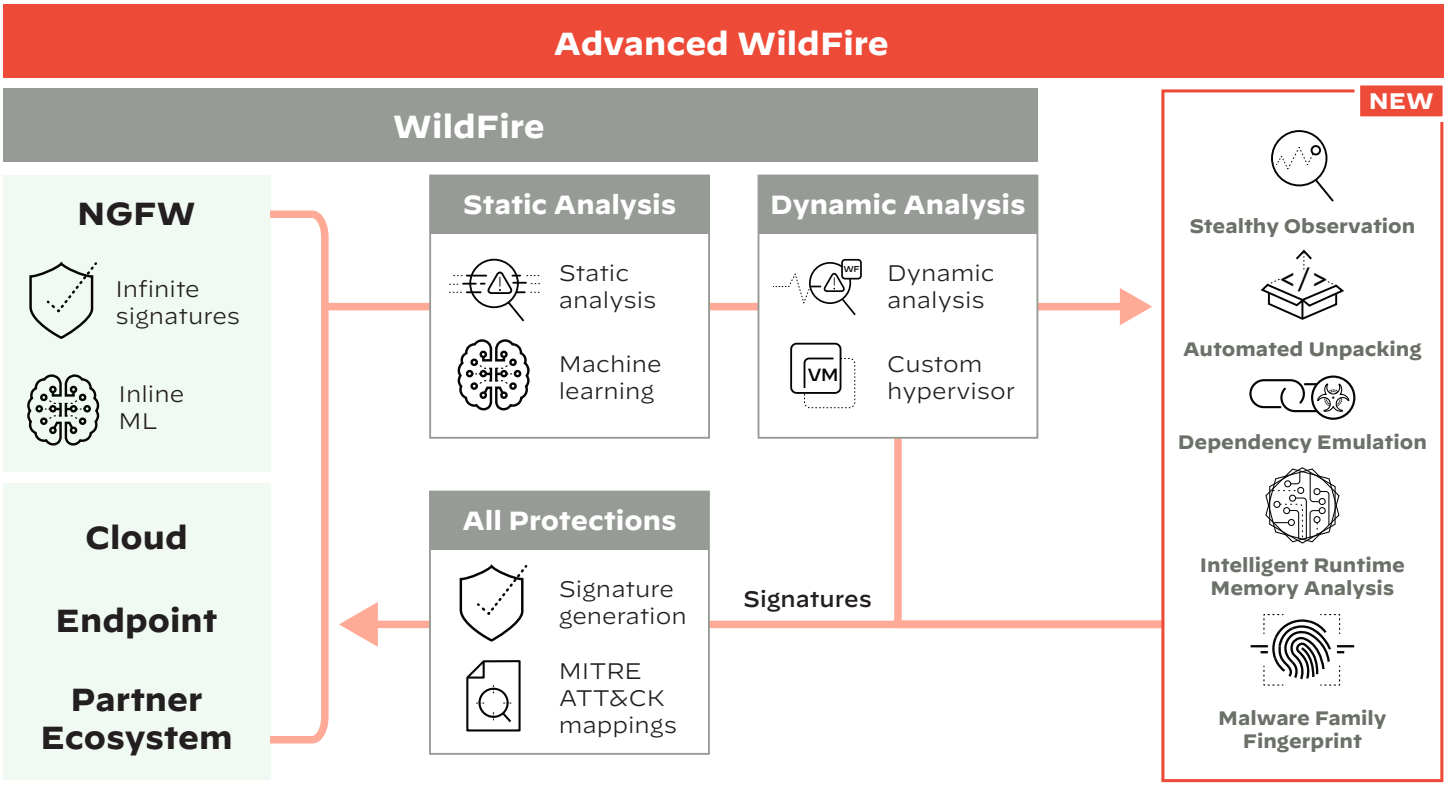

Figure 1: Advanced WildFire detection engines

Advanced WildFire is the industry's only malware prevention engine to defeat an additional 26% of highly evasive modern malware at scale with a brand-new infrastructure and patented analysis techniques, including intelligent runtime memory analysis, dependency emulation, malware family fingerprinting, and more. Unlike traditional solutions that depend solely on offline or delayed analysis of unknown malware, Advanced WildFire analysis and threat intelligence flow directly into machine learning models that act both locally at the firewall level and in the cloud—stopping over 99% of known and unknown malware.[2] After analysis, automated prevention is where Advanced WildFire shines: it applies rapid and consistent protection at the edge, in your data center, in the cloud, within software-as-a-service (SaaS) applications, and on endpoints.

Advanced WildFire goes beyond traditional sandboxing approaches to prevent unknown and highly evasive malware in a cloud environment. Over 25 patented detection techniques enable advanced malware analysis while maintaining high detection efficacy and near-zero false positives. 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.
- **Static analysis** looks at the characteristics of a file while leveraging dynamic unpacking to analyze threats attempting to evade detection through the use of packing tool sets.
- **Cloud-based machine learning** models extract thousands of unique features from each file which is not possible with static or dynamic analysis alone. Information gathered is then used to further train the predictive machine learning models to identify new malware.
- **Dynamic analysis** observes files as they execute in a purpose-built, evasion-resistant virtual environment, enabling the detection of previously unknown malware using hundreds of behavioral characteristics.
- **Intelligent runtime memory analysis** captures snapshots of malicious activity in memory and conducts real-time analysis to identify malicious behavior, detecting highly evasive malware that would not have otherwise gone undetected.

Key Capabilities

Root Out Malicious Behavior in All Traffic

Advanced 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, traverse the network and forwards them to Advanced WildFire for analysis and execution.

The powerful discovery and analysis capabilities of Advanced 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.

Stop Unknown Threats at the Firewall Level with Inline Machine Learning

Powered by threat models continually homed in the cloud, Advanced 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, Advanced 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.

2. "Palo Alto Networks WildFire Detection Efficacy: Public Statement," AV-Test, June 2022.

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 is in a sandbox environment. By using a custom hardened hypervisor where analysis components exist entirely outside of the guest VM, Advanced WildFire conducts stealthy observation to uncover malicious behavior during malware execution, including actions performed in memory, remaining completely invisible to the program under analysis.

Automated Unpacking

It is common for malicious actors to obfuscate their payloads using tools like encoding, encryption, and packing. Packing inhibits static or dynamic data from being useful for accurate detection. With automated unpacking, Advanced WildFire gains full visibility into file contents during analysis. Advanced WildFire also now generates signatures on packed payloads.

Dependency Emulation

One of the most malicious file types, portable executables, often require external dependencies to be satisfied to execute. With new dependency emulation capabilities, the sandbox environment will satisfy all external dependencies required for malware to execute, allowing the analysis engines to observe malicious behavior.

Intelligent Runtime Memory Analysis

Advanced WildFire introduces a brand-new detection infrastructure to support intelligent runtime memory analysis, enabling snapshots to be taken at critical points in memory when malicious behavior is observed. This not only provides the most relevant information for post-execution analysis but also efficiently allocates storage and compute resources.

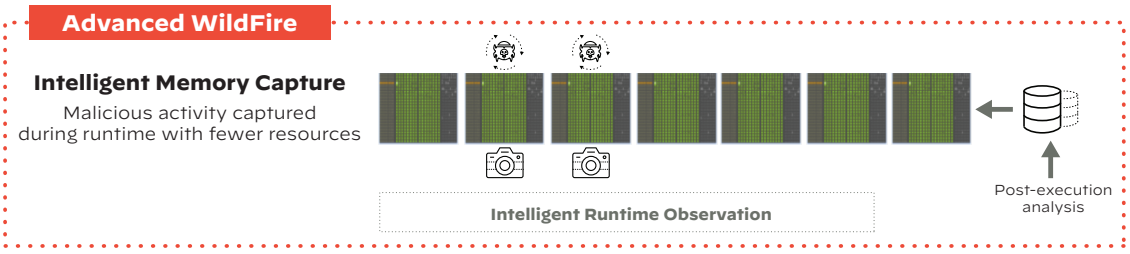

Figure 2: Intelligent runtime memory analysis

Malware Family Fingerprinting

Advanced WildFire extracts packed executables, commonly used to evade static signatures and generic pattern matching, and uses patented malware family fingerprinting detection to correlate new threats to known malware families, generating preventions for evasive malware at scale.

Get Global Prevention Across the Advanced WildFire Ecosystem, Delivered in Seconds

For highly customized threats that inline machine learning-powered prevention cannot stop, Advanced WildFire applies powerful cloud-based analysis to deliver prevention across networks, clouds, endpoints, or wherever Advanced WildFire-enabled sensors are deployed. Working in tandem with the capabilities of PAN-OS, Advanced 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.

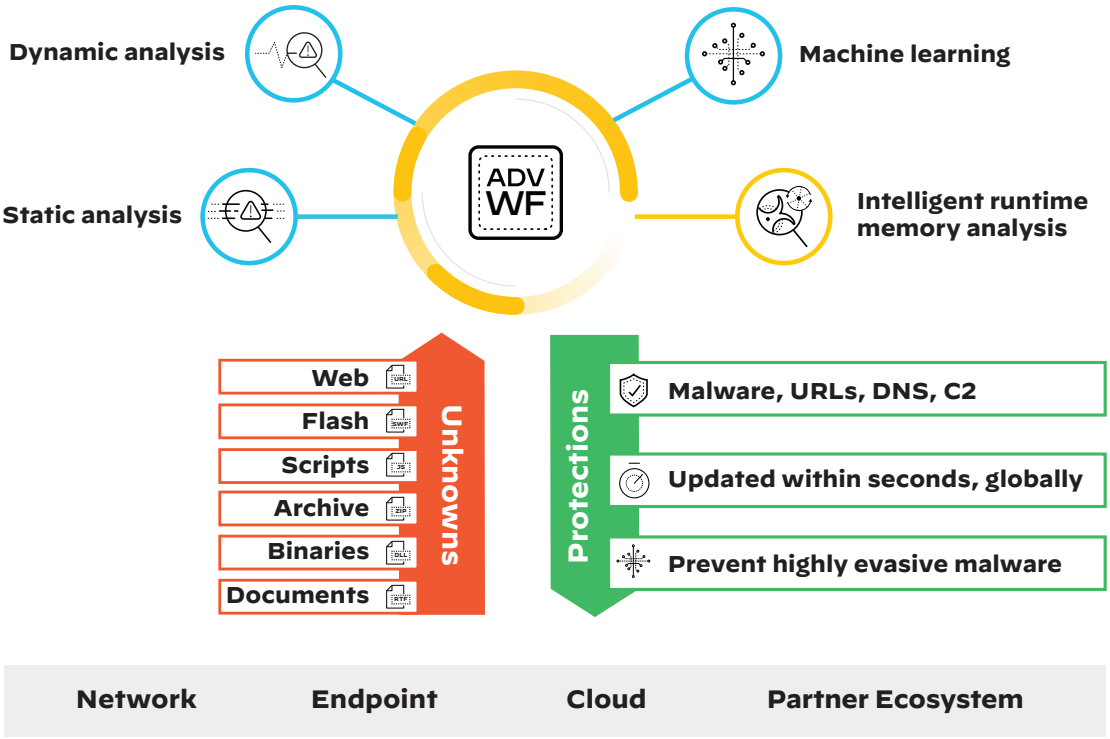

Figure 3: Integrated security for protection across your organization

How Advanced Threat Prevention and Advanced WildFire Work Together

The primary function of Advanced WildFire is to determine whether a given file is malware, greyware, or benign. When Advanced WildFire determines a file is malicious, that file is sent through the AV pipeline to have a signature generated. This new signature is then distributed to Advanced WildFire customers in the next five-minute update and to Advanced Threat Prevention customers in the next daily AV content package.

When a file passes through the firewall, there are several mechanisms used to block malware. The following describes the process for a firewall that has both the Advanced WildFire and Advanced Threat Prevention subscriptions and is configured according to best practices:

1. There are file-type-specific machine learning models that run on the data plane of the firewall. These models provide a measure of protection against zero-day malware.
2. The firewall checks against the signatures in its local cache to see if there is a match for the file. The local cache on the firewall is primarily populated by the AV content package provided by Advanced Threat Prevention and the Advanced WildFire five-minute signature update. The AV content package contains ~1.2 million signatures, and the five-minute update will contain new malware that Advanced WildFire has detected.
3. If there is no match in the local cache, the firewall will query the real-time signature service provided by Advanced WildFire to search the complete database of historical signatures to see if there is a match. With PAN-OS Nova, you can hold the transfer of the file while this query is taking place. If there is a match, a signature is:
    a. Installed into the local cache of the firewall.
    b. Included in the next five-minute update to all Advanced WildFire customers.
    c. Re-included in the Advanced Threat Prevention AV content package for the next day.
4. If there is no match from the real-time signature service and Advanced WildFire has not seen the file before, it will be sent to the Advanced WildFire cloud for analysis.

Without Advanced WildFire, customers have no way of determining if a new, never-before-seen file is malicious or not. In addition to being limited to the 1.2 million malware signatures in the AV package, customers will miss out on real-time signature lookup and the five-minute update post-Advanced WildFire cloud analysis. In practice, this means that they will not get coverage for new malware until the next day, as opposed to within five minutes of discovery.

Use Signatures, Not Hashes

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

Operational Benefits

- **Automate reprogramming of security controls to block unknown threats.** Shared real-time intelligence from a network of over 85,000 customers automatically updates and prevents threats across networks, endpoints, and clouds.
- **Gain detailed context on analyzed threats.** Get thorough visualization of every malicious file sent to Advanced WildFire across multiple operating system environments and application versions with AIOps.
- **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).

Deploy in a Complaint and Secure Cloud-Based Architecture

Files are submitted to the Advanced WildFire global cloud, delivering speed and scale, 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 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.

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

Figure 4: Advanced WildFire regional clouds

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 Advanced WildFire API enables customers to make queries to Advanced WildFire for information about potentially malicious content and submit files for analysis using the advanced threat analysis capabilities of Advanced WildFire. Using this RESTful API, 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 prior to cloud migration, and more. An Advanced WildFire subscription unlocks API access for a fixed number of submissions and queries. A separate stand-alone Advanced WildFire subscription, which does not require the purchase of a next-generation firewall, enables customers to purchase flexible submission and query volumes to access Advanced WildFire malware analysis via an API wherever needed.

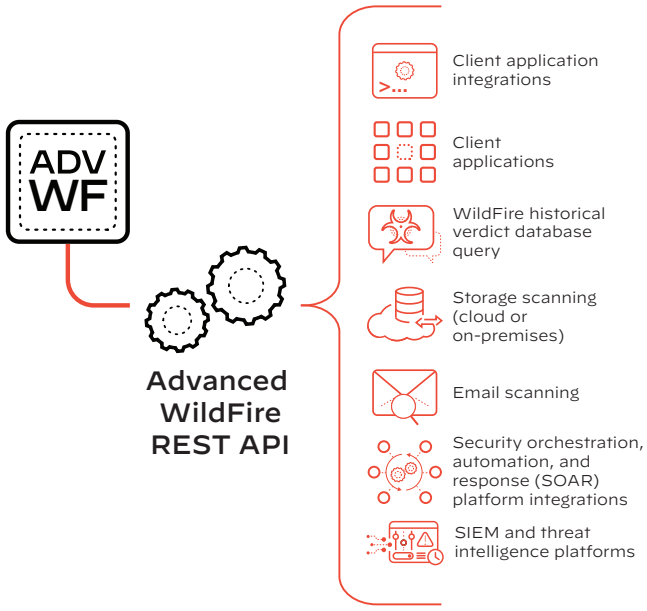

Figure 5: Advanced WildFire API

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, Cortex XDR, or Cortex XSOAR, 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 threat actors benefit from the ever-growing opportunities to take advantage of insecure networks while leveraging sophisticated cloud-based tool sets to deploy threat campaigns. 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 over 85,000 customers to instantly coordinate intelligence and protect against 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:

- **Advanced Threat Prevention**: Stop known exploits, malware, spyware, and command-and-control (C2) threats while utilizing industry-first prevention of zero-day attacks. Prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire malware prevention**: Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60x faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering**: Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security**: Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.
- **Enterprise DLP**: Minimize the risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise, with 2x greater coverage of any cloud-delivered enterprise DLP.

- **SaaS Security**: The industry's only Next-Generation CASB natively integrated into Palo Alto Networks SASE offers proactive SaaS visibility, comprehensive protection against misconfigurations, real-time data protection, and best-in-class security.
- **IoT Security**: Safeguard every "thing" and implement Zero Trust device security 20x faster with the industry's smartest security for smart devices.
- **AIOps**: AIOps for NGFW redefines firewall operational experience by empowering security teams to proactively strengthen security posture and resolve firewall disruptions.

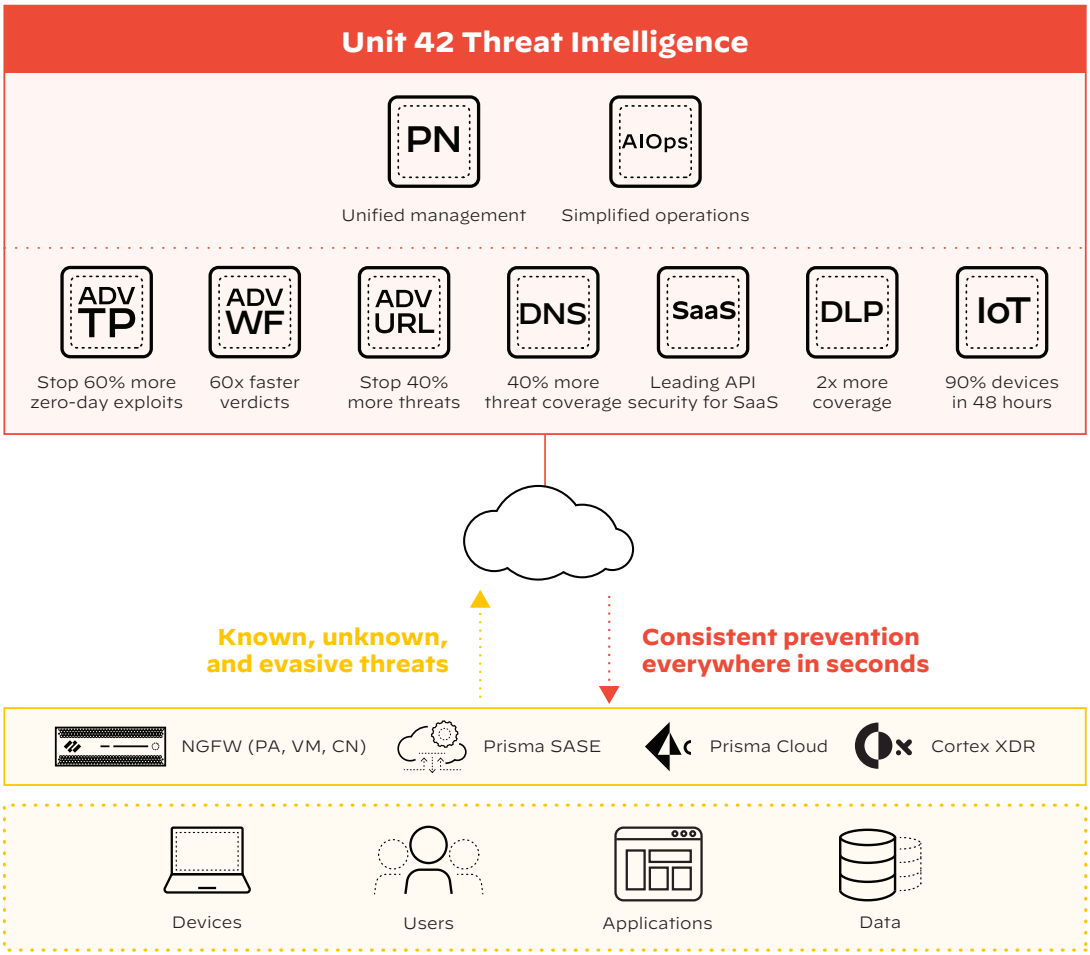

Figure 6: Palo Alto Networks Cloud-Delivered Security Services

Table 1: Features and Licensing Summary	
Capabilities Activated with the Advanced WildFire Subscription Attached to NGFW	
Advanced Analysis, Prevention, and Anti-Evasion Techniques	**Static analysis** combines static 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 hardened hypervisor, behavioral scoring, network profiling, and multistage recursive analysis. **Intelligent runtime memory analysis** captures snapshots of malicious activity in memory and conducts runtime analysis to identify malicious behavior.
OS Support	macOS, Android, Windows 7/10, and Linux

Table 1: Features and Licensing Summary (continued)	
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
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), United Kingdom, United States (Global Cloud and US Government Cloud)
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
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.
Requirements†	To use the features of the Palo Alto Networks Advanced WildFire subscription, you will need to meet the following PAN-OS requirements:

Feature	PAN-OS Requirement
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+

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.

† Customers can purchase Advanced WildFire with any PAN-OS version and will receive additional features upon upgrade.

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