Benefits

With inline ML powered by intelligence from our WildFire and URL Filtering services, the time from visibility to prevention of unknown network traffic becomes effectively zero. Your organization can:

- Stop new threats instantly, preventing initial infection and potential spread.
- Maintain the speed of business as you stop weaponized files, credential phishing, and malicious scripts without sacrificing the user experience.
- Leverage existing investments in Palo Alto Networks NGFWs, WildFire, and URL Filtering.
- Enjoy seamless, native integration between our NGFW and security subscriptions, eliminating the need for independent security tools while providing consistent protection and management.
- Future-proof your defenses to evolve with the latest attacks.

Why Seconds Matter

Preventing unknown threats with inline machine learning

Millions of new cyberthreats emerge every year, with organizations constantly racing to prevent them. Leveraging cloud-scale resources, automation, and other techniques, today's adversaries enjoy some inherent advantages: the ability to spread their attacks more quickly than ever, and the ability to deploy polymorphic malware and malicious content that evades detection by constantly changing its identifiable features.

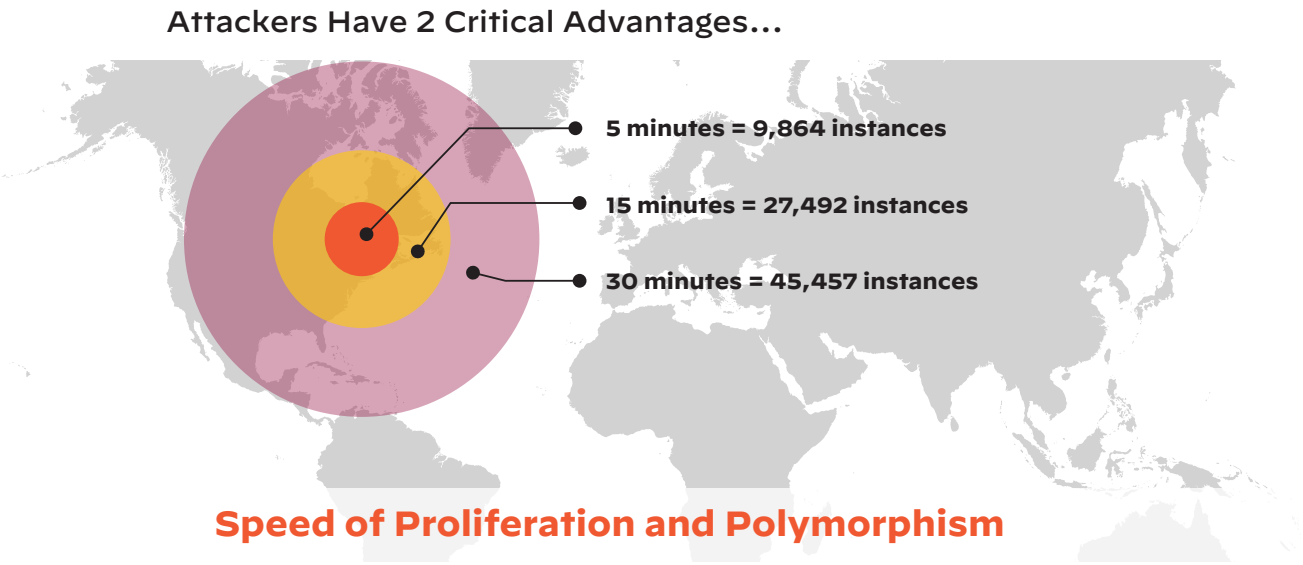

Figure 1: Palo Alto Networks Unit 42 data on the spread of malware

Adversaries are succeeding. In 2019, more than 140 million new malware samples were identified, and thousands of new malicious websites and domains were generated daily. New attacks are being launched far more quickly than traditional sandboxing, proxies, and independent signature technologies can deploy protections—they simply cannot keep pace. After an initial infection, modern malware can infect thousands more systems within seconds, well before protective measures can be developed and extended across organizations.

Industry Approaches to Stopping New Threats

Organizations have generally used four methods to try to prevent these net-new attacks.

Thor's Hammer

Using this strategy, an organization's policies refuse to allow files or web access into the organization at all, or else severely restrict the same. Of course, this is not realistic in most cases and is severely disruptive to the business.

Hold-and-Release

This approach involves stopping every file or website request for inspection and analysis until it is deemed benign. This method hasn't been very successful, either. Holding files hinders business productivity and causes a terrible user experience, but moreover, the approach simply doesn't scale. The more files sent for analysis, the more you hold, and the more business must slow down.

Content Disarm and Reconstruct

This method takes limited document-based file types and processes them to either remove code or convert the file format, in an attempt to disable potentially malicious content. This often destroys formatting or leads to corrupted files that never open, similar to issues end users can encounter when opening Office documents in "Safe Mode" or converting them to PDF. Due to the load on processing, this approach does not scale, and it negatively impacts business productivity and support follow-up. Lastly, while this approach does address file-based threats, it does not address web-based threats.

Stop Known Bad Inline, Inspect All Else in the Cloud

This approach, which we take at Palo Alto Networks, allows business to continue to operate but provides visibility into all network traffic while automatically updating protections when something malicious is found. We minimize the risk of infection while maximizing the user experience. It also scales with the offline approach to analyzing unknown traffic. Moreover, because the analysis capabilities live in the cloud, we're able to scale and continuously evolve, adding detection capabilities while minimizing operational impact to customers.

While this approach has proven tremendously effective for our customers, the Holy Grail has always been finding a way to prevent initial infections from never-before-seen threats as quickly as possible—hopefully reducing the time between visibility and prevention to zero. With the new capabilities in our WildFire® malware prevention and URL Filtering subscriptions, this is now a reality.

Prevent Unknown Threats with Inline Machine Learning

Palo Alto Networks has delivered the world's first ML-Powered Next-Generation Firewall (NGFW), providing inline machine learning (ML) to block unknown file- and web-based threats. Using a patented signatureless approach,

WildFire and URL Filtering proactively prevent weaponized files, credential phishing, and malicious scripts without compromising business productivity. Palo Alto Networks hardware and virtual NGFWs can apply new ML-based prevention capabilities:

- **WildFire inline ML** inspects files at line speed and blocks malware variants of portable executables as well as PowerShell® files, which account for a disproportionate share of malicious content.
- **URL Filtering inline ML** inspects unknown URLs at line speed. This feature can identify phishing pages and malicious JavaScript in milliseconds, stopping them inline so nobody in your network ever sees them.

Up to 95% of file- and web-based threats can be prevented inline without requiring analysis from the WildFire or URL Filtering clouds. For the rest, protections are delivered in seconds from the world's largest cloud native detection and prevention engines.

When it comes to addressing polymorphic malware variants and quickly mutating web-based threats, ML is a particularly powerful weapon to include in the arsenal. Able to ingest and process massive amounts of data quickly, an ML-based engine can make instant decisions and enable rapid response to prevent threats, rather than always waiting for a response from thorough static, dynamic, or other analysis processes. Another key advantage is that applications of ML models can capture changes in an executable file in a way that signature-based approaches cannot, which addresses the malware evasion techniques threat actors use to circumvent detection.

To effectively harness ML, we leverage the massive amounts of unbiased malicious samples, global telemetry, and analytics from our cloud-delivered WildFire and URL Filtering security subscriptions. With almost 10 years of analysis and threat intelligence from tens of thousands of customers and partners, these unique repositories directly inform and drive ML model creation that is small and efficient enough to be deployed inline and operate at line speed on our ML-Powered NGFWs.

While the deep intelligence and single source of truth remains in the cloud, enforcement and real-time decisions can be enacted at the control point on the NGFW, where speed matters the most. The continuously updated cloud repository and scaled processing allows new ML models to be created as needed, ensuring ML prevents the new unknowns as industry trends and new forms of threats take effect. The ML-based enforcement actions that operate inline address the vast majority of new file- and web-based threats, ongoing and proven cloud-based analysis with rapid prevention capabilities reduce the window of vulnerability for all other threats with zero delay.

How It Works: File-Based Attacks

Powered by threat models continually honed in the cloud, the WildFire subscription enables an inline ML-based engine, delivered within our hardware and virtual NGFWs. This capability prevents malicious file-based content, such as portable executable files and dangerous fileless attacks stemming from PowerShell, completely inline with no cloud analysis step. The ML models are updated daily for the most up-to-date detection capabilities.

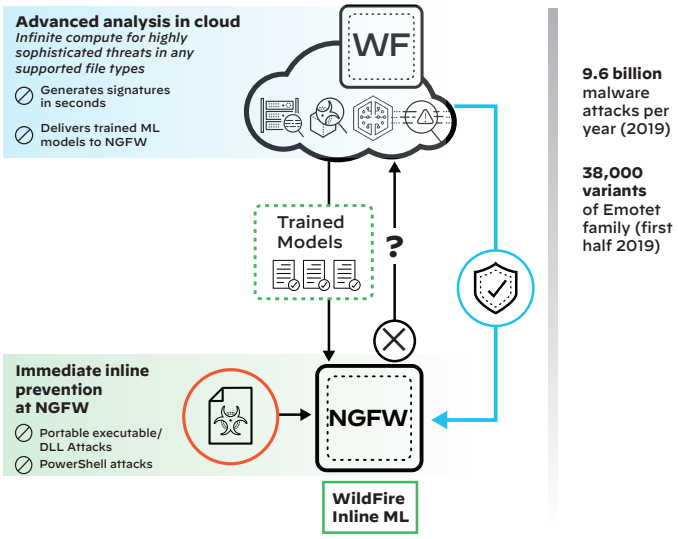

Figure 2: ML-based prevention of file-based attacks

While ML-based prevention is instant, scanned files are simultaneously routed to WildFire for analysis. This not only builds in a feedback loop for false positives, but also drives rapid prevention. Threats for which inline prevention would not have visibility (e.g., net-new threats delivered in different formats, such as PDFs or Office/Microsoft 365™ files; customized, highly evasive threats targeting a specific organization) are addressed with zero-delay signature updates. These innovative signatures are delivered continuously and in real time from the cloud to enable rapid prevention actions by cloud-based, near-real-time processes. Whether an unknown file matches an existing signature or is classified by ML models on the NGFW, WildFire always performs full analysis, extracting valuable intelligence and data to provide context for security analysts, training updates for the ML models, and intelligence sharing with other subscriptions to prevent other attack vectors.

How It Works: Web-Based Attacks

The URL Filtering subscription enables ML directly on the NGFW, stopping never-before-seen phishing and JavaScript attacks inline before they're unleashed on your organization. Malicious URLs are identified in milliseconds and blocked instantly. If a URL is not deemed malicious, it is passed on to the URL Filtering cloud for detailed analysis to determine its proper categorization and deliver a verdict within minutes.

Our ML models, powered by training sets straight out of our URL Filtering service, are updated daily for the most up-to-date detection capabilities. ML-based prevention of web-based attacks immediately stops new malicious URLs in their tracks before they can infect users, and detailed cloud analysis provides broader categorization capabilities that can be built into your web security policy.

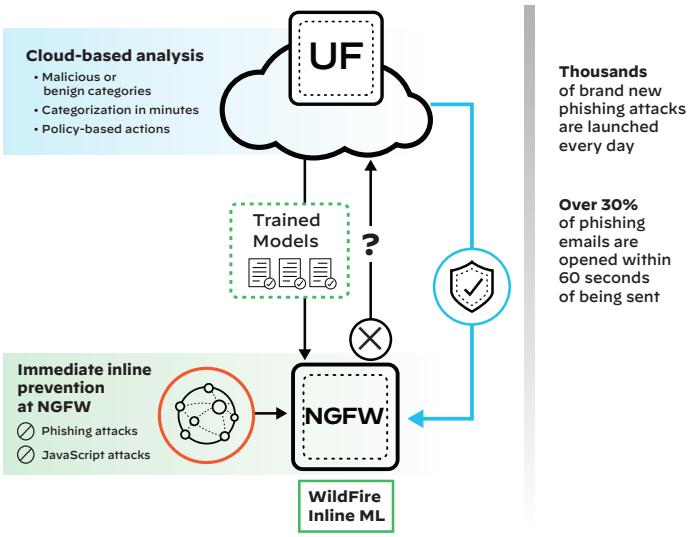

Figure 3: ML-based prevention of web-based attacks

Why Palo Alto Networks?

Predictive Models Powered by Our Cloud Analysis

We are uniquely capable of building and enhancing an extremely rich source of files to train our predictive ML classifiers. Data sources include:

- **WildFire**, one of the world's largest globally available, multi-region, massively scalable, elastically consumable malware analysis clouds.
- **URL Filtering**, a cloud-based service that uses global threat intelligence to accurately categorize and block URLs used for malware delivery, command and control, and evasive phishing.

Trillions of files and URLs—both benign and malicious—have been analyzed thanks to a distributed sensor system that pulls data from more than 52,000 enterprise, government, and service provider customers as well as more than 40 partners. This unique threat data set empowers Palo Alto Networks researchers and data scientists to create accurate and efficient ML models that are consistently updated and automatically delivered to the NGFW for protection that is always up to date.

Additional Resources

- URL Filtering datasheet
- WildFire datasheet
- Overview: Artificial Intelligence and Machine Learning in the Security Operation Center

Table 1: Security Subscriptions
Requirements
To use the inline ML-based prevention capabilities, you need:
• VM-Series or PA-Series ML-Powered Next-Generation Firewalls with PAN-OS® 10.0
• Active WildFire, URL Filtering subscriptions
• Firewalls configured to connect to the internet
Recommendation
• Configure the firewalls to submit files to the WildFire cloud or URL Filtering for model optimization and false positive management.

The Power of Palo Alto Networks Security Subscriptions

Today, cyberattacks have increased in volume and sophistication, using advanced techniques to bypass network security devices and tools. This challenges organizations to protect their networks without increasing workloads for security teams or hindering business productivity. Seamlessly integrated with our industry-leading ML-Powered NGFW platform, our cloud-delivered security subscriptions coordinate intelligence and provide protections across all attack vectors, providing best-in-class functionality while eliminating the coverage gaps disparate network security tools create. Take advantage of market-leading capabilities with the consistent experience of a platform, and secure your organization against even the most advanced and evasive threats. Benefit from any of our security subscriptions:

- **Threat Prevention:** Go beyond traditional intrusion prevention system (IPS) solutions to automatically prevent all known threats across all traffic in a single pass.
- **WildFire:** Ensure files are safe by automatically detecting and preventing unknown malware with industry-leading cloud-based analysis.
- **URL Filtering:** Enable the safe use of the internet by preventing access to known and new malicious websites before your users can access them.
- **DNS Security:** Disrupts attacks that use DNS for command and control and data theft without requiring any changes to your infrastructure.
- **IoT Security:** Protect internet-of-things (IoT) and OT devices across your organization with the industry's first turnkey IoT security solution.
- **GlobalProtect™** network security for endpoints: Extend ML-Powered NGFW capabilities to your remote users to provide consistent security everywhere in your environment.

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