WILDFIRE

Automatically Prevent Highly Evasive Zero-Day Exploits and Malware

Palo Alto Networks® WildFire™ cloud-based threat analysis 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 threat analysis and prevention service:

- 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 300 seconds of first discovery anywhere in the world, without requiring manual response.
- Builds collective immunity for unknown malware and exploits with shared real-time intelligence from more than 14,000 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 side-step legacy detection approaches. Now, even low-skill 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 become successful. Within the WildFire environment, threats are detonated, intelligence is extracted, and preventions are automatically orchestrated across the Palo Alto Networks Next-Generation Security Platform in 300 seconds of 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 malware and exploits using hundreds of behavioral characteristics.
- **Static analysis:** Highly effective detection of malware and exploits that attempt to evade dynamic analysis, as well as instant identification of variants of existing malware.
- **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:** Evasive threats are automatically sent to a real hardware environment for detonation, 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.

Automated Orchestration of Prevention

When zero-day exploits or malware are discovered by any WildFire user, the service automatically orchestrates enforcement of high-fidelity, evasion-resistant protections for all WildFire subscribers in 300 seconds of first discovery anywhere in the world. These protections are derived and shared across more than 14,000 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 Palo Alto Networks Next-Generation Security Platform, allowing the enforcement of new controls across:

- **Threat Prevention** to block malware, exploits, as well as command-and-control (anti-C2 and DNS-based callback) activity.
- **URL Filtering** with PAN-DB for the prevention of newly discovered malicious URLs.
- **AutoFocus™** contextual threat intelligence service, enabling the extraction, correlation and analytics 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 WildFire API.

The 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 in order 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 they are being examined in even the most advanced virtual environment and fail fully to detonate. To address this new class of attacks, WildFire has added 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, Android™ and macOS™ operating systems, with full visibility into commonly exploited file formats, including: EXE, DLL, ZIP, PDF, as well as Microsoft® Office documents, Java® files, Android APKs, Adobe® Flash® applets, and links within email messages. WildFire identifies hundreds of potentially malicious behaviors to uncover the true nature of malicious files based on their actions, including:

- **Complete malicious behavior visibility:** Identifies threats in all traffic across hundreds of applications, including web traffic, email protocols (SMTP, IMAP, POP) 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 (ransomware) or system destruction techniques.
- **Suspicious network traffic:** Performs analysis of all network activity produced by the suspicious file, including back door 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 correlate indicators of compromise (IoCs) and samples with human intelligence from the Unit 42 threat research team. Together, WildFire and AutoFocus provide a complete picture into unknown threats targeting your organization and industry, and increase your ability to quickly take action on intelligence, without 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. Customers can leverage the service as part of the Palo Alto Networks Next-Generation Security Platform without introducing a performance impact to the firewall. WildFire is available in multiple deployment modes, which can meet even the strictest local privacy or regulatory requirements, 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 Firewall, VM-Series, public cloud offerings, Aperture and Traps.
- **Private cloud delivery:** The WF-500, a local on-premise 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 cloud and private cloud by choosing to send sensitive files to the private cloud, while other content is analyzed by the global cloud.
- **European Union (EU) regional cloud delivery:** Files never leave our European data center, for organizations that need the benefit of WildFire but cannot send content beyond local borders due to regulation. Users still benefit from protections delivered from the global cloud.

Integrated Logging, Reporting and Forensics

WildFire users receive integrated logs, analysis and visibility into malicious events through the PAN-OS® security operating system 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-ID™ user identification technology, 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 (SIEM) systems.

Next-Generation Security Platform

WildFire is built on the Palo Alto Networks Next-Generation Security Platform, preventing known and unknown threats before they can cause harm, including:

- **Full visibility** into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard 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 Firewall, Threat Prevention, URL Filtering, Traps and Aperture, providing defenses against known exploits, malware, malicious URLs and command-and-control (C2) 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 and 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:

- PAN-OS 4.1+
- DF, Java, Office, and APK analysis require PAN-OS 6.0+
- Adobe Flash and webpage analysis require PAN-OS 6.1+

Licensing Information:

The WildFire global cloud subscription provides:

- Windows XP, Windows 7, macOS, and Android OS virtual analysis environments.
- Automated signature updates delivered every 300 seconds (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 (DNS) signatures, and URL signatures. URL signatures require a PAN-DB subscription.
- Supports PE files (EXE, DLL, and others), all Microsoft Office file types, PDF files, Flash files, and Java applets (JAR and CLASS), Android APKs, MacOS binaries (mach-O, DMG, PKG, and application bundles), and analysis of links within email messages. This includes support for compressed (zip) and encrypted (SSL) 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 Palo Alto Networks customer of Palo Alto Networks running PAN-OS 4.1 or greater, 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 (zip) and encrypted (SSL) content.
  - Automatic protections are delivered with regular threat prevention content updates (Threat Prevention license is required) every 24 hours.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com