AT A GLANCE
WILDFIRE

Palo Alto Networks® WildFire™ cloud-based threat analysis service is the industry's most advanced automated 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.

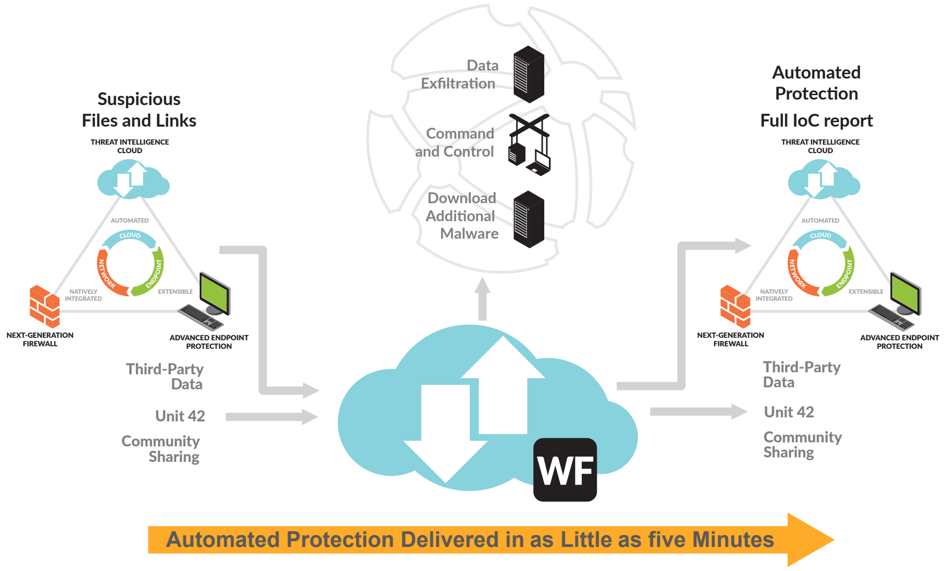
Automatically Prevent Highly Evasive Zero-Day Exploits and Malware

WildFire turns 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 within 300 seconds of first discovery anywhere in the world. 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.

WildFire Highlights

- 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



AT A GLANCE
WILDFIRE

YOU NEED	WE OFFER
Automated detection and prevention for zero-day exploits and malware	WildFire identifies previously unknown threats across the network, endpoint and cloud, generating new prevention controls that are automatically enforced within 300 seconds of first discovery anywhere in the world.
The ability to identify and prevent the most evasive threats	The service is built on the most advanced analysis environment in the industry, including a custom-built hypervisor and industry-first bare metal analysis, enabling conclusive identification of even the most evasive threats.
Simple, pervasive deployment and management	Any Palo Alto Networks Next-Generation Security Platform can become a sensor and enforcement point for unknown threats by turning on the WildFire subscription, without any additional hardware or performance impact. The service is managed centrally through policy as part of PAN-OS® security operating system or Panorama™ network security management.
Shared protections from a global community of users	WildFire gains leverage from a global community of more than 14,000 users, forming the industry's largest distributed sensor network focused on detecting and preventing unknown threats.
A cloud-based system that meets privacy and regulatory requirements	WildFire is available through multiple delivery modes that meet your privacy and regulatory requirements, from fully public cloud deployments to an on-premise private cloud appliance, as well as regional clouds based in the European Union, Japan and Singapore.
Threat intelligence with high relevance and context	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 Unit 42, Palo Alto Networks threat research team.

> ***"WHEN [WILDFIRE] FINDS SOMETHING CORRUPTED OR A POTENTIAL THREAT, IT'S QUICKLY IDENTIFIED AND ALL OUR SYSTEMS ARE INSTANTLY PROTECTED. OUR PAST SECURITY SYSTEM INSPECTED EMAIL ATTACHMENTS THAT PASSED THROUGH OUR CENTRALIZED EMAIL EXCHANGE SERVER. IN MANY CASES, THREATS WERE INVISIBLE TO IT AND ENTERED OUR NETWORKS. WILDFIRE SOLVES THIS PROBLEM AND GIVES US THE SAME LEVEL OF REAL-TIME INSPECTION OF TRAFFIC PASSING FROM THE PUBLIC TO PRIVATE NETWORK. ONCE WE SAW HOW EFFECTIVE WILDFIRE IS, WE EXPANDED IT TO ALL DEVICES AND BRANCHES."***

Massimiliano Tesser | *CAME Group*