AT A GLANCE
WILDFIRE

Attacks are increasing in number and evasiveness. This requires better-detailed detection that can keep up with the rapid threat innovation of cybercriminals and provide the tools needed for quick prevention and protection with easy mitigation. Palo Alto Networks® WildFire™ cloud-based threat analysis service offers a completely new approach to cybersecurity with an automated, closed-loop detection feature to prevent against advanced, never-before-seen threats.

Automated Detection and Prevention

Our natively integrated Next-Generation Security Platform brings network, cloud and endpoint security into a common architecture – with complete visibility and control – ensuring your organization can detect and prevent attacks. As new threats emerge, the platform automatically routes suspicious files and URLs to WildFire for deep analysis.

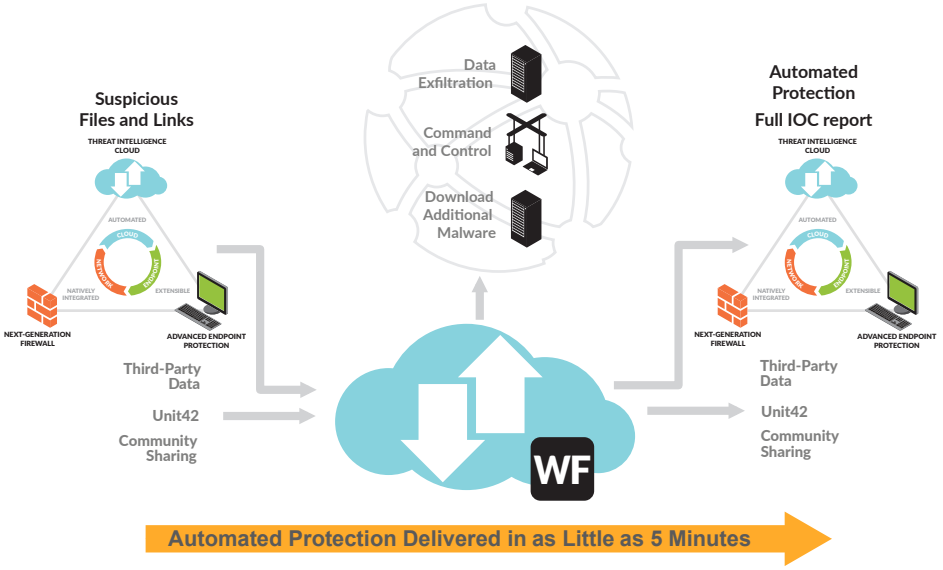
WildFire inspects millions of samples daily from its global network of customers and threat intelligence partners, looking for new forms of previously unknown malware, exploits, malicious domains, and outbound command-and-control activity. WildFire matches any forwarded samples against its database of known files and designates never-before-seen items for further investigation, which covers static and dynamic analysis against multiple operating systems and application versions. WildFire produces a verdict and behavioral report for unknown samples that are analyzed. If a sample is categorized as malware WildFire will automatically generates malware, URL and DNS signatures and distributes them to all global WildFire-subscribed Palo Alto Networks security platforms within minutes. This immediately halts threats from spreading without any additional manual action required.

Our security platform facilitates easy mitigation through correlated forensics and shared protections between our other security services: Threat Prevention, URL Filtering, GlobalProtect™ network security client for endpoints, Aperture™ SaaS security service, and Traps™ advanced endpoint protection. Information about indicators of compromise (IOCs) from WildFire analysis reports is used by the NGFW and technology partners to identify infected hosts and prevent secondary downloads.

This closed-loop, automated process gives organizations the assurance that their networks, endpoint and cloud are armed with the absolute latest threat intelligence at all times. Our platform streamlines day-to-day operations and boosts security efficacy, while the one-of-a-kind, multilayered defense model prevents threats at each stage of the attack lifecycle.

WildFire Highlights

- Granular and coordinated threat analysis across all traffic and attack vectors
- Static and dynamic analysis against different operating systems and file types commonly used in targeted attacks, including: Microsoft® Office®, PDF, Portable Executable and Java®
- Automatically creates protections against new threats and delivers them back to all global WildFire-subscribed Palo Alto Networks security platforms within minutes
- Detailed forensics to easily prioritize and execute follow-on security actions
- Full control over your data



AT A GLANCE
WILDFIRE

YOU NEED	WE OFFER
A cloud-based global solution that doesn't require additional hardware	WildFire employs a unique cloud-based architecture, which allows organizations to scale granular detection and protection seamlessly across the entire network, even in sensitive industries where all analysis must be done on premises. This means you get automatic prevention without the headache of having to implement and manage separate devices for web and email at every ingress/egress point within your network.
Comprehensive, real-time analysis	WildFire analyzes exploitive documents that can uniquely target specific versions of client applications, like Adobe® Reader®, across several versions of that application simultaneously within a single VM. WildFire provides granular detection and quick protection in as little as five minutes.
Pervasive detection and prevention throughout your organization	WildFire can be easily and flexibly deployed from any existing Palo Alto Networks Next-Generation Security Platform deployment, enabling granular malware detection and up-to-date security for all data, applications and users, both inside and outside the corporate network, endpoint and cloud.
Actionable IOC reports	WildFire provides granular behavior analysis and indicators of compromise reports, made available to our platform technologies and used by elements like the dynamic correlation objects on our NGFW as well as our technology partners for automated, fast and accurate mitigation.
Full control over your data	WildFire hybrid architecture provides granular controls over what data will be submitted for analysis. Elements like file type and session as well as choosing the data path and the regional cloud where the analysis and data storage will take place, are all configurable.

"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 | *CIO, CAME Group*