WF-500 WILDFIRE APPLIANCE

Automatically detect and prevent zero-day exploits and malware with on-premise analysis that meets privacy and regulatory requirements.

The Palo Alto Networks® WF-500 private cloud appliance complements the WildFire® cloud-based threat analysis environment with on-premise analysis, detonation, and automated orchestration of prevention for zero-day exploits and malware. The appliance's private cloud architecture allows organizations to meet privacy and regulatory requirements while still benefiting from the shared threat intelligence and protections of more than 22,000 WildFire cloud subscribers.

Organizations in sensitive or regulated industries struggle to maintain data privacy while taking advantage of cloud-based malware analysis services that require sending content outside the organization. To provide the most advanced security with privacy, WildFire employs a unique hybrid approach, engaging a private cloud appliance for local detonation while leveraging shared intelligence and protections, including policy-based submissions of less sensitive content to the global cloud.

Turn the Unknown Into Known

As part of the shared WildFire architecture, the Palo Alto Networks WildFire appliance detects unknown threats through a combination of multiple complementary analysis techniques, including:

- **Static analysis** – inspects thousands of characteristics of a file to determine maliciousness quickly and effectively.
- **Local analysis** – conducts all threat analysis and generates protections on-premise, sending no content outside the bounds of your network unless configured to do so.

WF-500

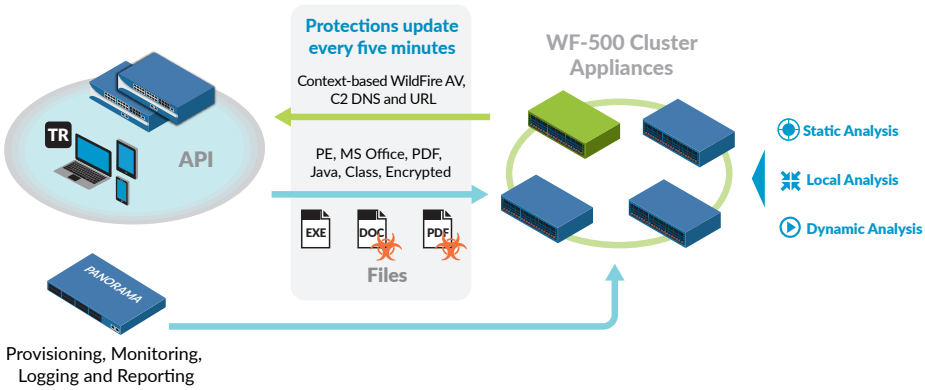
- **Dynamic analysis** – automatically detonates files in a virtual environment to uncover never-before-seen malware based on conclusive behavioral attributes.
- **Shared threat intelligence** – optionally leverages the shared threat intelligence and protections from more than 22,000 WildFire subscribers by anonymously querying the global WildFire cloud prior to local analysis.

The appliance executes suspicious content, with full visibility into commonly exploited file formats, including EXE, DLL, ZIP and PDF, as well as Microsoft® Office documents, Java® files, Adobe® Flash® applets and links within email messages.

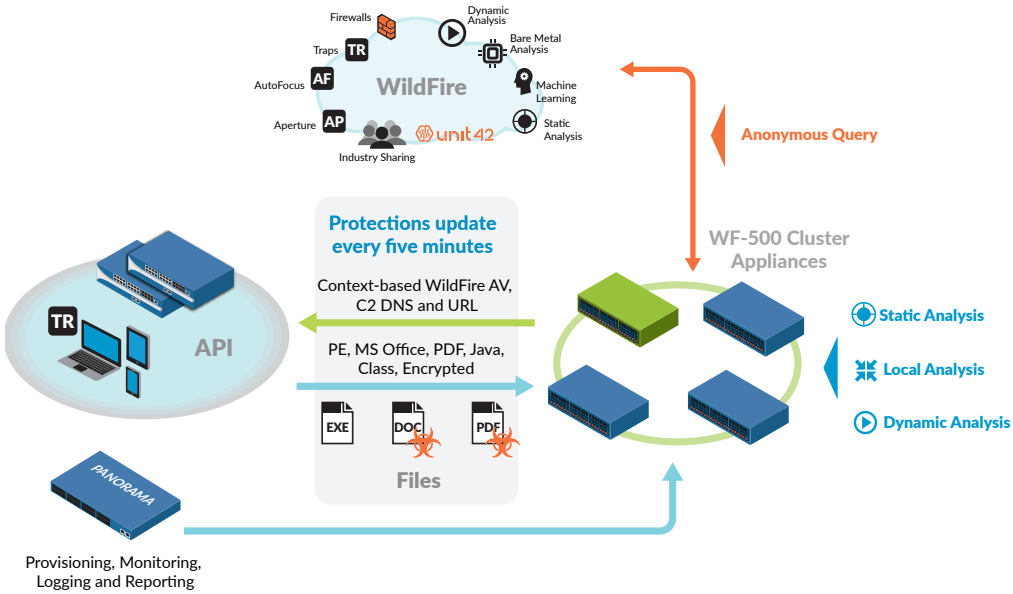
Local Analysis, Cloud Benefits

By default, the WildFire appliance conducts all threat analysis and generates protections on-premise; it does not send any content outside the bounds of your network. However, customers have policy-based options to leverage the collective threat intelligence from the entire WildFire ecosystem as appropriate, including:

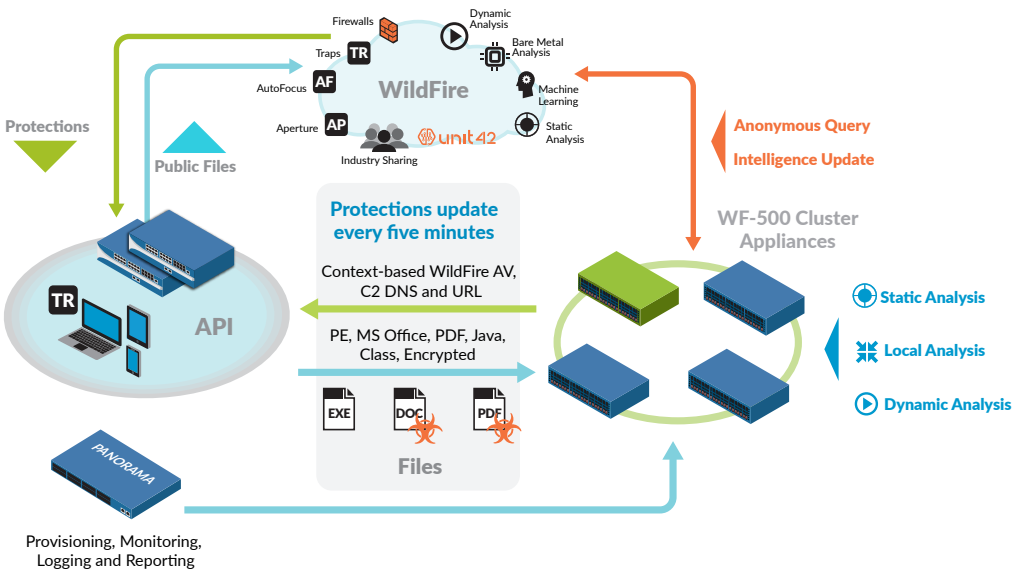
- **Stand-alone** – does not require any internet connectivity for detonation and protection generation. The appliance can be used in completely isolated environments and updated manually.



- **Cloud query** – can anonymously request verdicts from Palo Alto Networks cloud-based threat intelligence to improve accuracy and increase throughput without samples leaving the network.



- **Hybrid** – forwards files to either the WildFire appliance or global WildFire cloud with granular policies based on file type, application or the flow of network traffic (uploads and downloads).



Automated Orchestration of Prevention

Due to the WildFire appliance's unique cloud-based architecture, it forms the central orchestration point, responsible for the generation and dissemination of protections for all local Palo Alto Networks next-generation firewalls. Files are automatically sent to the appliance for detonation and intelligence extraction, creating new prevention controls in as few as five minutes from the first instance of a zero-day exploit or malware. The system covers multiple stages in the attack lifecycle, with anti-malware and DNS signatures, as well as updated URL categorization for PAN-DB.

Massive Analysis Scale and Reliability

The WildFire appliance supports powerful clustering capabilities, which provide increased reliability and analysis capacity for large networks. Threat information is shared with up to 20 clustered appliances to ensure a single, unified signature package is delivered to all firewalls. High availability, redundant storage and load balancing ensure analysis capabilities and data survive any hardware failures that may occur during the process of analyzing tens of thousands of files per day.

Threat Intelligence, Analytics and Correlation

In combination with the WildFire appliance and optional sample submission, organizations can use AutoFocus™ contextual threat intelligence service to hone in on the most targeted threats with high relevance and context. AutoFocus provides the ability to hunt across data extracted from the appliance, as well as correlate indicators of compromise and samples with human intelligence from the Unit 42 threat research team. Together, the WildFire appliance and AutoFocus provide a picture into unknown threats targeting your organization and industry, and increase your ability to quickly take action on intelligence, without adding specialized security staff.

Integrated Logging, Reporting and Forensics

WF-500 appliances are integrated into Panorama™ network security management, making it easier to centrally manage their health, policies and aggregated analysis statistics. WF-500 users receive integrated logs, analysis and visibility into malicious events through Panorama – the PAN-OS® security operating system's management interface – enabling teams to quickly investigate and correlate events observed in their networks.

Security Operating Platform

The WildFire appliance is natively engineered as part of the Palo Alto Networks Security Operating Platform, allowing the identification and automatic prevention of all threats, regardless of whether they come from the web, email or file servers – unlike single-function sandboxing appliances. As part of the platform, the WildFire appliance provides:

- 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™ advanced endpoint protection and Aperture™ SaaS security service, providing defenses against known exploits, malware, malicious URLs and command-and-control activity.
- Unknown threat detection and prevention with WildFire, including threat analytics with high relevance and context through the AutoFocus service.

WF-500 SYSTEM SPECIFICATIONS

Single Appliance
7,000 files/day
Clustered Appliances
120,000 + files/day (Up to 20 appliances per cluster)
OS Support
Windows XP or Windows 7
File Support
PE files (EXE, DLL and others), MS Office, PDF, Flash, Java applets (JAR and CLASS), analysis of links within email messages, compressed (ZIP) and encrypted (SSL) files.
Management
Panorama, API, CLI

WF-500 HARDWARE SPECIFICATIONS

Processor
Dual 6-Core Intel® Processor with Hyper-Threading Technology
Memory
128GB RA1
System Disk
120GB SSD
I/O Storage
4x10/100/1,000 DB9 Console serial port, USB HDD for 2TB of RAID storage
Capacity
2TB RAID1: 4x1TB RAID Certified
Power Supply
Dual 920W power supplies in hot swap, redundant configuration
Max Power Consumption
390 Watts
Rack Mountable (Dimensions)
2U, 19" standard rack (3.5"H x 21"D x 17.5"W)
Max Btu/hr
1,330 Btu/hr
Input Voltage (Input Frequency)
100–240VAC (50–60Hz)
Max Current Consumption
1aA @ 100VAC
Safety
UL, CSA, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Environment
Operating temperature: -4 to 158°F, -40 to 65°C Non-operating temperature: -4 to 158°F, -40 to 65°C

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

wf-500-wildfire-appliance-ds-043018