TRAPS

Advanced Endpoint Protection

Palo Alto Networks® Traps™ advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. Traps minimizes endpoint infections by blocking malware, exploits and ransomware. Integration with your security platform delivers additional threat analysis, shared intelligence and automated containment.

Attackers must complete a certain sequence of events to successfully accomplish their objectives, whether stealing information or running ransomware. Nearly every attack relies on compromising an endpoint, and although most organizations have deployed endpoint protection, infections are still common.

By combining multiple methods of prevention, Traps stands apart in its ability to protect endpoints. Traps blocks security breaches and successful ransomware attacks that leverage malware and exploits, known or unknown, before they can compromise Windows®, macOS® or Linux endpoints, such as laptops, desktops, servers, virtual machines and cloud workloads.

Multi-Method Malware and Ransomware Prevention

Traps prevents the launching of malicious executable files, DLLs and Office files with multiple methods of prevention, reducing the attack surface and increasing the accuracy of malware prevention. This approach prevents known and unknown malware from infecting endpoints by combining:

- **WildFire threat intelligence:** Traps uses intelligence from Palo Alto Networks WildFire® cloud-based threat analysis service to prevent known malware. WildFire is the world's largest distributed sensor system focused on identifying and preventing unknown threats and converting to known threats, with more than 20,000 enterprise, government and service provider customers contributing to the collective immunity of all users across endpoints, networks and cloud applications.
- **Local analysis via machine learning:** This analysis method delivers instantaneous verdicts for any unknown executable files, DLLs or Office files before they are allowed to run. Traps examines hundreds of a file's characteristics in a fraction of a second without relying on prior knowledge of the threat.
- **WildFire inspection and analysis:** Traps also uses WildFire for deep inspection of unknown files beyond machine learning. When a new threat is detected, prevention controls are shared across the Next-Generation Security Platform, including all Traps customers, in as few as five minutes. WildFire combines the benefits of four independent techniques for high-fidelity and evasion-resistant discovery, including dynamic analysis, static analysis, machine learning and bare-metal analysis.
- **Granular child process protection:** Traps delivers fine-grained control over the launching of legitimate processes, such as script engines and command shells, that ransomware and other advanced threats commonly employ in a malicious fashion to bypass traditional security protections.

- **Behavior-based ransomware protection:** Traps monitors the system for ransomware behavior and, upon detection, immediately blocks the attack and prevents encryption of customer data.
- **Periodic scanning for dormant malware:** Traps performs scheduled or on-demand scans for dormant malicious executable files, DLLs and macros on an endpoint to remediate these without waiting for an attempt to run the malicious file.

Traps policies also enable organizations to whitelist and blacklist applications, restrict execution of applications, and quarantine malware.

Multi-Method Exploit Prevention

Rather than focusing on individual attacks, Traps blocks the exploit techniques the attacks use. By doing so at each step in an exploit attempt, Traps breaks the attack lifecycle and renders threats ineffective.

Traps delivers exploit prevention using multiple methods:

- **Pre-exploit protection:** Traps block vulnerability-profiling techniques before they launch exploitation attacks, effectively preventing the attacks.
- **Technique-based exploit prevention:** Traps prevents known and zero-day exploits by blocking the techniques attackers use to manipulate applications.
- **Kernel exploit prevention:** Traps prevents exploits that leverage vulnerabilities in the operating system kernel to create processes with escalated – that is, system-level – privileges. Traps also prevents injection techniques used to load and run malicious code from the kernel, such as those used in the WannaCry and NotPetya attacks.

Consistent Policies Across Operating Systems

Traps protects Windows, macOS and Linux endpoints with multiple methods of prevention. By doing so, Traps delivers consistent protection to all major operating systems to stop known and unknown malware and exploits before they can compromise a system. In contrast, native OS security features only protect their respective endpoints, which creates fragmented protection, leaves the endpoints vulnerable to attacks and slows down incident response.

Coordinated Enforcement With Network and Cloud

Traps and WildFire continuously share threat intelligence with each other, as does each component of Palo Alto Networks Next-Generation Security Platform, such as next-generation firewalls and cloud security services (see Figure 1). Traps customers receive access to this threat intelligence and the complete set of WildFire malware analysis capabilities.

The automatic conversion of this threat intelligence into prevention all but eliminates opportunities for attackers to use unknown and advanced malware to infect systems.

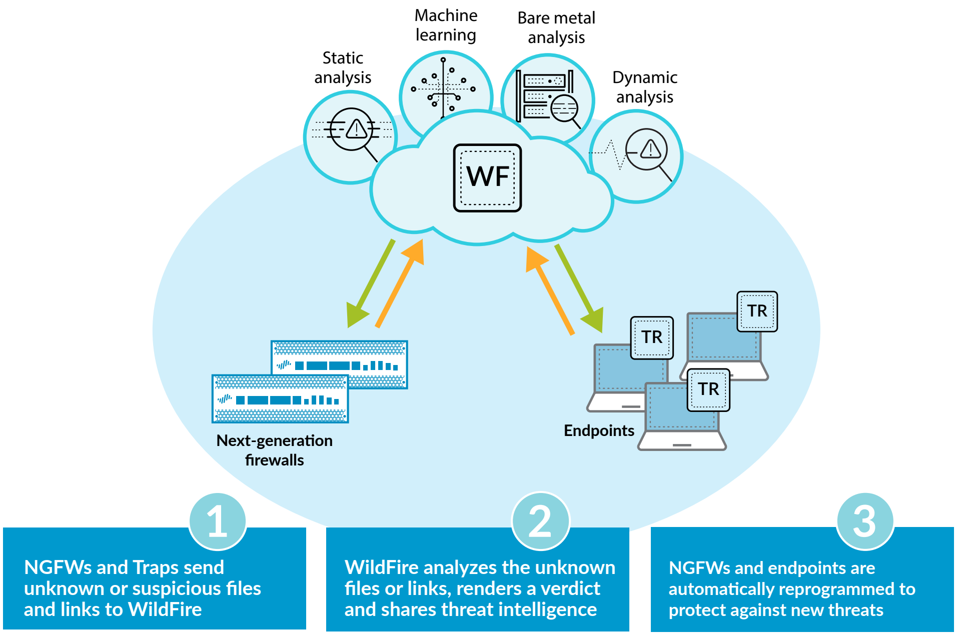
Machine learning
Bare metal analysis
Static analysis
Dynamic analysis
WF
TR
TR
TR
Next-generation firewalls
Endpoints
1
NGFWs and Traps send unknown or suspicious files and links to WildFire
2
WildFire analyzes the unknown files or links, renders a verdict and shares threat intelligence
3
NGFWs and endpoints are automatically reprogrammed to protect against new threats

Figure 1: Shared threat intelligence

Traps also shares logs with Panorama™ network security management, enabling security operations teams to view endpoint security logs in the same context as their firewall logs. This facilitates detection of threats that may have otherwise evaded detection.

Cloud-Based Management and a Lightweight Agent

Traps management service is cloud-delivered to save you the time and cost of building out your endpoint security infrastructure. The service is simple to deploy and requires no server licenses, databases or other infrastructure to get started. The intuitive, web-based interface makes it easy to manage policies and events, and accelerate incident response.

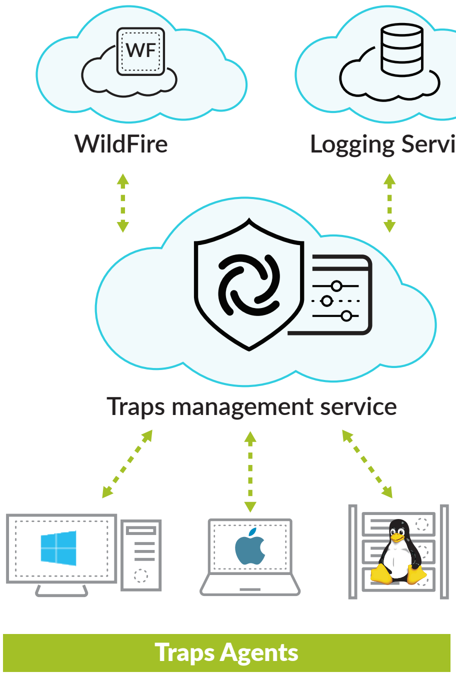

Figure 2: Traps technical architecture

System Requirements and Operating Systems Support

Traps supports multiple endpoints across Windows, macOS and Linux operating systems. For a complete list of system requirements and supported operating systems, please visit the Traps Compatibility Matrix webpage.

Industry-Recognized and Compliance-Ready

Traps has won multiple awards and received industry recognition, with recent accolades including:

- **"100 percent detection of real-world attacks":** Traps received the maximum performance rating in a commissioned evaluation by AV-TEST in December 2017.
- **"100 percent real-world protection test":** Traps received an "Approved" award from AV-Comparatives in its October 2017 "Comparison of Next-Generation Security Products."

Traps has also been validated to help meet compliance needs by Coalfire®, a global leader in cyber risk management and compliance services. In its reports, Coalfire states that any organization currently using legacy AV to comply with PCI DSS or HIPAA/HITECH requirements can confidently replace that solution with Traps and remain compliant.

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