TRAPS

Advanced Endpoint Protection

Palo Alto Networks® Traps™ advanced endpoint protection replaces legacy antivirus with multi-method prevention built into a single, lightweight agent that secures endpoints from known and unknown malware and exploits. On its own, or as part of the Palo Alto Networks Next-Generation Security Platform, Traps stops targeted, sophisticated threats like ransomware without reliance on signatures.

Despite continuous investments in legacy antivirus solutions and "next-gen" AV products, organizations continue to suffer security breaches and successful ransomware attacks with increasing frequency. The security industry as a whole, and legacy antivirus solutions in particular, have struggled – and more often failed – to prevent successful security breaches originating from endpoints.

Attempts at improving the effectiveness and efficiency of antivirus solutions, as well as the security industry's collective focus on detection and response, have only resulted in incremental improvements in endpoint protection while exposing additional flaws that limit their effectiveness in preventing security breaches.

Traps secures endpoints with its unique multi-method prevention, blocking security breaches and successful ransomware attacks that leverage malware and exploits, known or unknown, before they can compromise macOS® or Windows® endpoints, such as laptops, desktops and servers.

Multi-Method Malware Prevention

Traps prevents the launching of malicious executables, DLLs and Office files with a unique, multi-method prevention approach that reduces the attack surface and increases the accuracy of malware prevention. This approach combines several methods to prevent known and unknown malware from infecting endpoints:

1. **WildFire threat intelligence:** Traps prevents known malware using intelligence from Palo Alto Networks WildFire™ cloud-based threat analysis service. WildFire is the world's largest distributed sensor system focused on identifying and preventing unknown threats and converting to known threats, with more than 17,000 enterprise, government and service provider customers contributing to the collective immunity of all other users across endpoints, networks and cloud applications.
2. **Local analysis via machine learning:** This method delivers an instantaneous verdict for any unknown executable, DLL or Office file before it is allowed to run. Traps examines hundreds of the file's characteristics in a fraction of a second, without reliance on signatures, scanning or behavioral analysis.
3. **WildFire inspection and analysis:** In addition to local analysis, Traps uses WildFire for deep inspection of unknown files beyond just machine learning. Should a new threat be detected, prevention controls are shared across the Palo Alto Networks Next-Generation Security Platform, including all Traps customers, in as few as five minutes, without human intervention. 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.
4. **Granular child process protection:** Traps delivers fine-grained control over the launching of legitimate processes, such as script engines and command shells, that can be used for malicious purposes. This technique is commonly used by ransomware and other advanced threats to bypass traditional security protections.
5. **Behavior-based ransomware protection:** In addition to existing multi-method preventions including exploit prevention, local analysis and WildFire, Traps monitors the system for ransomware behavior and, upon detection, immediately blocks the attack and prevents encryption of customer data.

In addition, Traps enables organizations to whitelist and blacklist applications, define policies to restrict execution of applications, and quarantine malware to prevent its unintended dissemination.

Multi-Method Exploit Prevention

Each exploit must use a series of exploitation techniques to successfully manipulate an application. Instead of focusing on the millions of individual attacks, Traps focuses on key exploit techniques typically used by all exploit-based attacks. By preventing one, Traps breaks the attack lifecycle and renders the threat ineffective.

Traps delivers exploit prevention using multiple methods:

1. **Pre-exploit protection:** Traps prevents vulnerability-profiling techniques exploit kits use before they launch exploitation attacks. By blocking these techniques, Traps prevents attackers from targeting vulnerable endpoints and applications, in effect preventing the attacks before they begin.
2. **Technique-based exploit prevention:** Traps prevents both known and zero-day exploits by blocking the exploitation techniques attackers use to manipulate applications. Although there are thousands of exploits, they all rely on a small set of exploitation techniques that change infrequently. Traps blocks these techniques, thereby preventing exploitation attempts before they can compromise endpoints.
3. **Kernel exploit prevention:** Traps prevents exploits that leverage vulnerabilities in the operating system kernel to create processes with escalated (system-level) privileges. Traps also prevents injection techniques used to load and run malicious code from the kernel, such as those used in WannaCry and NotPetya attacks. These enable Traps to block advanced attacks that target or stem from the operating system itself.

True Prevention for Mac

Traps secures macOS systems and replaces legacy AV with a multi-method prevention approach that secures endpoints against known and unknown malware and exploits before they can compromise a system. This is in contrast to existing signature-based AV and "next-gen" security solutions for macOS that cannot prevent security breaches by blocking both malware and exploits, leaving the endpoint exposed to attacks.

Next-Generation Security Platform

As an integral component of the Next-Generation Security Platform, Traps shares and receives threat intelligence from WildFire. Each component of the platform (such as next-generation firewalls and Traps) that is deployed among the global community of Palo Alto Networks customers continuously shares threat intelligence with WildFire. Traps customers receive access to this threat intelligence as well as the complete set of WildFire malware analysis capabilities.

The automatic reprogramming and conversion of this threat intelligence into prevention all but eliminates opportunities for attackers to use unknown and advanced malware to infect a system. An attacker can use a given piece of malware at most once in an environment where Traps is deployed, and only has seconds to carry out an attack before WildFire renders it entirely ineffective.

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 correlation of discrete activities observed on the network and endpoints for a unified picture of security events across the environment, and thus detection of threats that may have otherwise evaded detection.

Award-Winning, 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 detected 100 percent of real-world attacks and received a maximum performance rating in a commissioned evaluation by AV-Test Q3, 2017
- **"Visionary"** – Gartner named Traps a "Visionary" in its "2017 Magic Quadrant for Endpoint Protection Platforms."
- **"Overall Winner and 2016 Product of the Year"** – Traps was granted CRN's coveted "Product of the Year" award among all endpoint security offerings evaluated for the competition.
- **"Approved Business Product"** – AV-Comparatives, the independent organization that tests and assesses antivirus software, presented Traps with its award in its first-ever "Comparison of Next-Generation Security Products."
- **"Strong Performer"** – Forrester® Research named Traps (v3.3) a "Strong Performer" in its report, "The Forrester Wave™: Endpoint Security Suites, Q4 2016."

Traps has also been validated to help our customers meet their compliance needs as they replace their antivirus. Coalfire®, a global leader in cyber risk management and compliance services, conducted an independent evaluation of Traps with respect to the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, as well as the requirements of the Breach Notification Rule as formalized by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Rule of 2013.

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.

System Requirements and Operating Systems Support

Traps supports endpoints (desktops, servers, industrial control systems, virtual desktop infrastructure components, virtual machines and embedded systems) across Windows and macOS/Mac® OS X® operating systems. For a complete list of system requirements and supported operating systems, please visit the Traps Compatibility Matrix webpage.

paloalto NETWORKS®

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

traps-ds-091217