TRAPS

Advanced Endpoint Protection

Palo Alto Networks Traps replaces traditional antivirus with a multi-method prevention approach that secures endpoints against known and unknown malware and exploits before they can compromise a system. Traps prevents security breaches and successful ransomware attacks, in contrast to detection and response after critical assets have been compromised.

Traps advanced endpoint protection:

- **Prevents cyber breaches and successful ransomware attacks** by preemptively blocking known and unknown malware, exploits and zero-day threats
- **Protects and enables users** to conduct their daily activities and use web-based technologies without concerns for known or unknown cyberthreats
- **Automates prevention** by autonomously reprogramming itself using threat intelligence gained from WildFire

Despite the continuous investments in traditional antivirus solutions and "next-gen" AV products, organizations continue to experience cyber breaches and successful ransomware attacks with increasing frequency. The security industry as a whole, and traditional antivirus solutions in particular, have struggled – and more often failed – to prevent successful security breaches stemming 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 cyber breaches.

Palo Alto Networks® Traps™ advanced endpoint protection secures endpoints with its unique multi-method prevention, blocking cyber 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.

Traps Multi-Method Malware Prevention

Traps prevents malicious executables rapidly and accurately with a unique, multi-method prevention approach that maximizes coverage against malware while simultaneously reducing the attack surface and increasing the accuracy of malware detection. This approach combines several prevention methods to instantaneously prevent known and unknown malware from infecting a system:

1. **WildFire Threat Intelligence:** Traps prevents previously seen malware using intelligence from Palo Alto Networks WildFire™ threat analysis service. WildFire is the world's largest distributed sensor system focused on identifying and preventing unknown threats, with more than 15,500 enterprise, government and service provider customers contributing to the collective immunity of all other users.
2. **Local Analysis via Machine Learning:** This method delivers an instantaneous verdict for any unknown executable 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:** Traps uses the WildFire cloud-based malware analysis environment to rapidly detect unknown malware. When a new malware threat is found, WildFire automatically creates and shares a new prevention control with Traps (as well as other components of the Palo Alto Networks Next-Generation Security Platform) in as few as five minutes, without human intervention. WildFire goes beyond legacy approaches used to detect unknown threats, bringing together 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. **Malicious Process Control:** 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.

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.

Traps Multi-Method Exploit Prevention

Traps uses an entirely unique approach to preventing exploits. Instead of focusing on the millions of individual attacks or their underlying software vulnerabilities, Traps focuses on the exploitation techniques used by all exploit-based attacks. Each exploit must use a series of these exploitation techniques to successfully manipulate an application. Traps renders these techniques ineffective by blocking them the moment they are attempted.

Traps delivers comprehensive exploit prevention using multiple methods:

1. **Pre-Exploitation Protection:** Traps prevents vulnerability-profiling techniques used by exploit kits prior to launching an exploitation attack. 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 Exploitation Protection:** Traps prevents exploits that leverage vulnerabilities in the operating system kernel to create processes with escalated (system-level) privileges. This enables Traps to block advanced attacks that target 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 cyber breaches by blocking both malware and exploits, leaving the endpoint exposed to attacks.

Next-Generation Security Platform

As an integral component of the Palo Alto Networks Next-Generation Security Platform, Traps both 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 to 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.

Award-Winning, Industry-Recognized and Compliance-Ready

Traps has won multiple awards and received industry recognition as a significant endpoint security offering. Some of the most recent accolades include:

- **“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.”
- **“Visionary”** – Gartner named Traps a “Visionary” in its “2017 Magic Quadrant for Endpoint Protection Platforms.”

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 Payment Card Industry (PCI) Data Security Standard (DSS) and 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 traditional 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/OS X® operating systems. For a complete list of system requirements and supported operating systems, please visit the Traps Compatibility Matrix webpage.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com