TRAPS ADVANCED ENDPOINT PROTECTION

Technology Overview

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. Alone or as part of the Palo Alto Networks Next-Generation Security Platform, Traps stops targeted, sophisticated threats like ransomware without reliance on signatures.

Multi-Method Prevention

Threat actors rely primarily on two attack vectors to compromise endpoints: malicious executables (malware) and the exploitation of vulnerabilities. These attack vectors are used individually or in various combinations, but fundamentally different in nature:

- Malware is a malicious executable, often self-contained, designed to perform nefarious activities on a system.
- Exploits are weaponized data files or content designed to leverage software flaws or bugs in legitimate applications to provide attackers with remote code-execution capabilities.

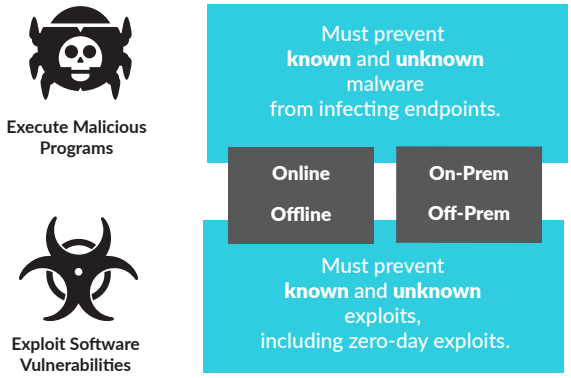

Figure 1: Effective endpoint security must prevent both malware and exploits

Preventing attackers from compromising endpoints and servers requires an advanced endpoint protection product that prevents both known and unknown variants of malware and exploits, and delivers this prevention whether a machine is online or offline, on-premise or off-premise, connected to the organization's network or not (Figure 1). In fact, effective breach prevention cannot be achieved unless all these requirements are met simultaneously.

Due to the fundamental differences between malware and exploits, meeting these requirements necessitates an approach that combines multiple threat prevention methods optimized to prevent either the execution of malicious programs or the subversion of legitimate applications by vulnerability exploits.

Traps multi-method prevention blocks malware and exploits, known and unknown, before they compromise endpoints such as laptops, desktops, servers and Windows® tablets.

Traps Multi-Method Malware Prevention

Traps prevents malicious executables, DLLs and Office files rapidly and accurately with a unique, multi-method prevention approach that maximizes coverage against malware while reducing the attack surface and increasing the accuracy of malware prevention. This approach combines several prevention methods to instantly block known and unknown malware from compromising a system:

- **Granular child process protection:** Traps prevents script-based attacks by default with out-of-the-box, fine-grained controls over the launching of legitimate applications (such as script engines and command shells) and continues to grow these through regular content updates. Administrators get additional flexibility and control with the ability to whitelist or blacklist child processes, along with command line comparisons to increase detection without impacting legitimate processes.
- **Execution restrictions:** Traps enables organizations to easily define policies to restrict specific execution scenarios, thereby reducing the attack surface of any environment. For example, Traps can prevent the execution of files from the Outlook® "temp" directory, or a particular file type from a USB drive.
- **Gatekeeper enhancements:** Traps prevents attackers from bypassing the macOS® operating system's digital signature verification mechanism. The macOS Gatekeeper allows or blocks the execution of applications based on their digital signatures, which are ranked in three "signature levels": Apple® System, Mac® App Store® and Developers. Traps extends the Gatekeeper functionality to enable customers to specify whether to block all child processes or allow only those with signature levels that match (or exceed) that of their parent process.
- **WildFire threat intelligence:** In addition to third-party feeds, Traps leverages the intelligence obtained from over 17,000 WildFire customers, continuously aggregating data from endpoints, networks and SaaS applications to prevent known threats.

  1. Traps queries WildFire with the hash of any Windows or macOS executable, DLL, or Office file (Windows only) before the file can run to assess its standing within the global threat community, and only proceeds with additional prevention techniques if the file is unknown.
  2. If the file is deemed malicious, Traps automatically terminates and optionally quarantines it.

- **Admin override policies:** Traps enables organizations to define policies based on the hash of an executable file to control what is allowed and not allowed to run in their environments.
- **Local analysis via machine learning:** If the file remains unknown after the initial hash lookup, Traps uses local analysis via machine learning – trained by WildFire on the endpoint – as one of its prevention techniques to determine whether the file can run, even before receiving a verdict from WildFire. By examining hundreds of file characteristics in real time, local analysis can determine whether a file is likely to be malicious or benign without reliance on signatures, scanning or behavioral analysis.
- **WildFire inspection and analysis:** In addition to local analysis, Traps sends unknown executables, DLLs and Office files to WildFire for discovery and analysis to rapidly detect unknown malware and automatically reprogram itself. WildFire goes beyond legacy approaches used to detect unknown threats, bringing together the benefits of independent techniques for high-fidelity and evasion-resistant discovery, including dynamic analysis, static analysis, machine learning and bare metal analysis for highly evasive malware. Once a file is known, 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.
- **Malware quarantine:** Traps immediately quarantines malicious executables, DLLs and Office files to prevent propagation or execution attempts of infected files. Although essential in most environments, this capability is particularly useful in preventing the inadvertent dissemination of malware in organizations where network- or cloud-based data storage and SaaS applications automatically sync files across multiple users and systems.
- **Grayware classification:** Traps enables organizations to identify non-malicious but otherwise undesirable software and prevent it from running in their environments.
- **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.

> WildFire is the world's largest distributed sensor system focused on identifying and preventing unknown threats, with more than 17,000 enterprise, government and service provider customers contributing to the collective immunity of all other users.

Traps 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 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:

- **Pre-exploit 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.
- **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 typically rely on a small set of exploitation techniques that change infrequently. Traps blocks these techniques, thereby preventing exploitation attempts before they can compromise endpoints.
- **Kernel exploit prevention:** Traps prevents exploits that leverage vulnerabilities in the operating system kernel to create processes with escalated (system-level) privileges. Traps also protects against new exploit techniques used to execute malicious payloads, such as those seen in the recent WannaCry and NotPetya attacks. By blocking processes from accessing the injected malicious code from the kernel, Traps is able to prevent the attack early in the attack lifecycle without impacting legitimate processes. This enables Traps to block advanced attacks that target or stem from the operating system itself.

By blocking the techniques common to all exploit-based attacks, Traps provides customers three important benefits:

1. **Traps protects unpatchable applications.** Organizations can run any application, including those developed in-house and those that no longer receive updates or security support, without the threat of exploit-based attacks on their environment.
2. **Traps eliminates the urgency to patch applications as soon as possible.** Organizations using Traps can apply security patches whenever most convenient. Traps will prevent the exploitation of application vulnerabilities regardless of when the organization applies the security patches issued by the application vendor.

3. **Traps eliminates the threat of zero-day exploits.** Because zero-day exploits typically use a limited set of exploitation techniques that Traps blocks, organizations are protected against attacks that utilize zero-day exploits.

Traps Multi-Method Prevention for Mac

Traps secures macOS (and Mac OS X®) systems and replaces legacy AV with a multi-method approach to prevention that blocks both malware and exploits, known or unknown, before they can compromise a Mac endpoint. This contrasts with 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.

Traps secures Mac systems against malware without the use of outdated AV technologies or signature-scanning techniques. Traps prevents known and unknown malware on Mac systems through multiple methods, including local analysis, WildFire inspection and analysis, Gatekeeper Enhancements, Trusted Publisher Identification, and Admin Override Policies.

Traps prevents exploitation of Mac systems without the error-prone heuristic or signature-based approaches common to legacy AV solutions. It prevents known and unknown exploits using multiple methods, including technique-based exploitation mitigation (e.g., JIT and ROP Mitigation, Dylib-Hijacking Protection) and Kernel Privilege Escalation Protection.

Next-Generation Security Platform

As an integral component of the Palo Alto Networks Next-Generation Security Platform, Traps continuously exchanges threat intelligence with WildFire, as does each component of the platform deployed among the global community of Palo Alto Networks customers. Traps customers receive access to this intelligence and WildFire's complete set of malware analysis capabilities included with their Traps subscription. Traps uses the intelligence to automatically reprogram itself to prevent malware on the endpoint, no matter where it is discovered.

The automatic conversion of threat intelligence into prevention all but eliminates the opportunity for an attacker to use unknown and advanced malware to infect a system. An attacker can use a given piece of malware at most once, anywhere, and only has seconds to carry out an attack before WildFire renders it entirely ineffective.

The Palo Alto Networks Next-Generation Security Platform benefits Traps customers even if Traps is deployed in environments that do not include any other component of the platform. In these deployment scenarios, Traps maintains access to the malware analysis capabilities and threat intelligence of WildFire. Traps uses this intelligence to automatically block malware that is first encountered elsewhere, including on other customers' firewalls, SaaS applications and endpoints. This effectively enables Traps customers to leverage the investments other customers have made in their network, cloud and endpoint security products from Palo Alto Networks.

When deployed in environments that include other components of the Next-Generation Security Platform (such as next-generation firewalls), Traps delivers significant additional advantages not available to customers in Traps-only deployments.

- **Single-pane-of-glass visibility into security events:** Traps can share its 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. Security teams can thus detect threats that may have otherwise evaded detection and, in conjunction with automated policies, eliminate attack surfaces across their entire environment, from endpoints to firewalls to cloud and SaaS applications.
- **Network security enhanced by endpoint protection:** Traps bolsters the prevention capabilities of our next-generation firewalls by sharing malware discovered on endpoints with WildFire, which automatically creates and shares new prevention controls with Traps and our next-generation firewalls in as few as five minutes, without human intervention. This enhances network security by preventing unknown malware that may have otherwise passed through perimeter defenses to infect unprotected endpoints.

Traps Technical Architecture

The technical architecture of Traps is optimized for maximum availability, flexibility and scalability. At a high level, the architecture consists of Traps endpoint agents managed through a central Endpoint Security Manager (Figure 2). The ESM implements a three-tiered architecture that consists of an ESM Console, central ESM Database and any number of ESM Servers.

Endpoint Security Manager Console

The ESM Console is the administrative interface for Traps. Running on Internet Information Services for Windows, the ESM Console provides access to the central Policy Database of Traps. Organizations can deploy multiple ESM Consoles, each of which can reside in physical, virtual or cloud environments.

ESM Database

The Traps Policy Database is the central repository of all information necessary to configure, maintain and operate the Traps advanced endpoint protection environment, such as prevention policies and settings, activity and forensic logs, ESM and agent configurations, and WildFire interface configurations.

Endpoint Security Manager Servers

ESM Servers act as proxies between Traps agents and the ESM Database. ESM Servers do not store data and can therefore be readily added and removed from the environment as needed to ensure adequate geographical coverage and redundancy. ESM Servers can be installed on Windows Server® deployments in physical, virtual or cloud environments.

Traps Endpoint Agent

The Traps endpoint agent consists of various drivers and services, yet requires minimal memory and CPU usage (200MB disk space, 50MB RAM). Following its deployment onto the endpoints, system administrators have complete control over all Traps agents in the environment through the ESM Console.

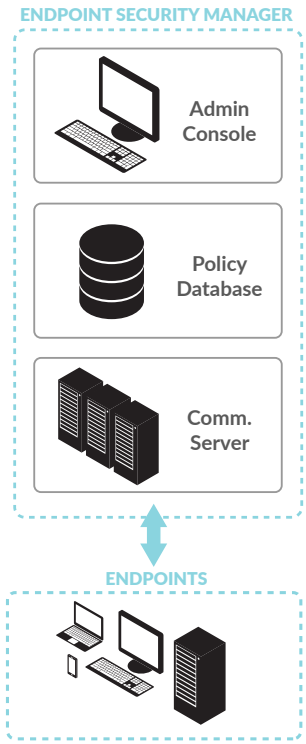

Figure 3: Technical architecture of Traps

System Requirements and Platform 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.

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 the 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 traditional AV to comply with PCI DSS or HIPAA/HITECH requirements can confidently replace that solution with Traps and remain compliant.

Conclusion

To learn more about Traps, attend an Ultimate Test Drive event and experience its prevention capabilities firsthand. Alternatively, contact your sales representative to schedule an in-house evaluation for your organization.

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-wp-091517