TRAPS

Endpoint Protection and Response

Palo Alto Networks Traps™ stops threats and coordinates enforcement with network and cloud security to prevent successful cyberattacks. Traps blocks known and unknown malware, exploits, and ransomware by observing attack techniques and behaviors.

The threat landscape and adversary strategies have evolved from simple malware distribution to a broad set of automated, targeted, and sophisticated attacks that can bypass traditional endpoint protection. This has forced organizations to deploy multiple products from different vendors to protect against, detect, and respond to these threats. Traps brings powerful endpoint protection technology together with critical endpoint detection and response (EDR) capabilities in a single agent.

Stop Malware and Ransomware

Traps prevents the launching of malicious executable files, DLLs, and Office macros 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:

- **Local analysis via machine learning:** Traps examines hundreds of characteristics of a file without relying on prior knowledge of the threat and delivers instantaneous verdicts before threats are executed.
- **WildFire inspection and analysis:** Traps also uses WildFire® for deep inspection of unknown files. WildFire combines the benefits of multiple independent techniques—including static, dynamic, and bare metal analysis—for high-fidelity and evasion-resistant threat identification.
- **Scanning for dormant malware:** Traps performs scheduled or on-demand scans for malicious executable files, DLLs, and Office macros to remediate them without malicious files being opened.

Block Exploits and Fileless Attacks

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

Traps uses multiple methods to prevent exploits:

- **Pre-exploit protection** blocks reconnaissance and vulnerability-profiling techniques before they launch exploit attacks, effectively preventing attacks.
- **Technique-based exploit prevention** works to prevent known and zero-day exploits, without any prior knowledge of the threats, by blocking the techniques attackers use to manipulate legitimate applications.
- **Kernel exploit prevention** is able to prevent exploits that take advantage of 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 the WannaCry and NotPetya attacks.

Leverage Behavior-Based Protection

Sophisticated attacks that use multiple legitimate applications and processes for malicious operations have become more common, are hard to detect, and require visibility to correlate malicious behavior. For behavior-based protection to be effective, including identification of malicious activity occurring within legitimate processes, it's critical to understand everything happening on the endpoint. Traps enacts behavior-based protection in a few different ways:

- **Behavioral Threat Protection** detects and stops attack activity by monitoring for malicious sequences of events across processes and terminating attacks when detected.
- **Granular Child Process Protection** prevents script-based and fileless attacks used to deliver malware by blocking known processes from launching child processes commonly used to bypass traditional security.
- **Behavior-Based Ransomware Protection** safeguards you against encryption-based behavior associated with ransomware by analyzing and stopping ransomware activity before any data loss occurs.

Investigate and Respond to Attacks

To facilitate faster response and investigation, Traps has a number of actions admins or IR teams can use to further their investigation, collect necessary information, and take action to make any changes to the endpoint in question.

Following an alert or investigation, when remediation on the endpoint is needed, administrators have the option to:

- **Isolate endpoints** by halting all network access on compromised endpoints except for traffic to Traps management service, preventing them from communicating with and potentially infecting other endpoints.
- **Quarantine malicious files** and remove them from their working directories if Traps has not already quarantined the files.
- **File retrieval allows admins to pull** specific files from endpoints under investigation for further analysis.
- **Terminate processes** to stop any running malware from continuing to perform malicious activity on the endpoint.
- **Block additional executions** of a given file by blacklisting it in the policy.
- **Initiate live terminal connection** to the endpoint to navigate and manage files, explore the registry, run command line or Python commands, and review and manage active processes.

Protect Consistently Across Operating Systems

Traps uses multiple methods of prevention to consistently protect endpoints running all major operating systems—Windows®, macOS®, Linux, and Android®—by stopping known and unknown attacks before they compromise systems. 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.

Coordinate Enforcement with Network and Cloud

Traps tightly integrates with WildFire and the Next-Generation Firewall to broaden the perspective for endpoint attacks. This integration enables a continually improving security posture, including coordinated prevention from zero-day attacks. Whenever Traps, a firewall, or other product on the Palo Alto Networks Security Operating Platform® sees a new piece of malware or an endpoint user (unintentionally) execute a threat from an endpoint, the malware is sent to WildFire for analysis. If the suspect malware is deemed malicious, protections and awareness are automatically distributed in just minutes to all Next-Generation Firewalls and Traps-protected endpoints with no effort on the administrator's part, whether it happens at 1 a.m. or 3 p.m.

Quickly Detect, Investigate, and Respond to Threats

Traps uses Cortex™ Data Lake to store all event and incident data captured, allowing a clean handoff to Cortex XDR. Cortex XDR™ is the world's first detection and response app that natively integrates network, endpoint, and cloud data to stop sophisticated attacks.

Cortex XDR speeds alert triage and incident response by providing a complete picture of each threat and revealing the root cause automatically. By stitching different types of data together and simplifying investigations, Cortex XDR reduces the time and experience required at every stage of security operations, from triage to threat hunting. Tight integration with enforcement points lets you respond to threats quickly as well as apply the knowledge gained from investigations to detect similar attacks in the future.

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