# TRAPS TECHNOLOGY OVERVIEW

Palo Alto Networks Traps™ endpoint protection and response 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. Additionally, it enables organizations to automatically detect and respond to sophisticated attacks by using machine learning and artificial intelligence (AI) techniques from data collected on the endpoint, network, and cloud.

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.

Although attacks have become more sophisticated and complex, they still use basic building blocks to compromise endpoints. The primary attack methods continue to exploit known and unknown application vulnerabilities as well as deploy malicious files, including ransomware. These can be used individually or in various combinations, but they are fundamentally different in nature:

- Exploits are the results of techniques used against a system that are designed to gain access through vulnerabilities in the code of an operating system or application.
- Malware is a file or code that infects, explores, steals, or conducts virtually any behavior an attacker wants.
- Ransomware is a form of malware that holds valuable files, data, or information for ransom, often by encrypting data, with the attacker holding the decryption key.

Due to the fundamental differences between malware and exploits, effective prevention must protect against both. Traps combines multiple methods of prevention at critical phases within the attack lifecycle to halt the execution of malicious programs and stop the exploitation of legitimate applications, regardless of operating system, the endpoint's online or offline status, and whether it is connected to an organization's network or roaming (see Figure 1).

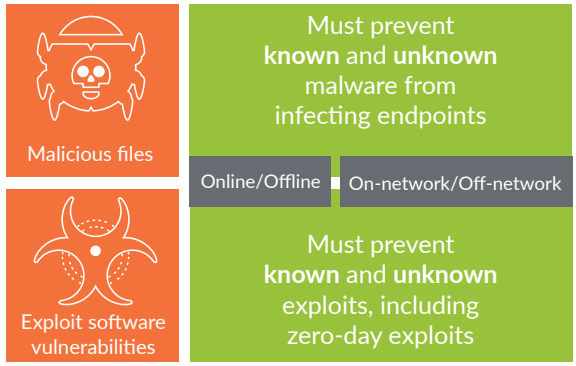


**Figure 1:** Malicious files vs. exploits

### Stop Malware and Ransomware

Traps prevents the execution of malicious files with an approach tailored to combating both traditional and modern attacks. Additionally, administrators can utilize periodic scanning to identify dormant threats, comply with regulatory requirements, and accelerate incident response with endpoint context. Known and unknown malware, including ransomware, is subject to multiple preventive technologies.

#### *WildFire Threat Intelligence*

In addition to third-party feeds, Traps uses the intelligence obtained from tens of thousands of WildFire® malware prevention service subscribers to continuously aggregate threat data and maintain the collective immunity of all users across endpoints, networks, and cloud applications.

1. Before a file runs, Traps queries WildFire with the hash of any Windows®, macOS®, or Linux executable file, as well as any DLL or Office macro, to assess its standing within the global threat community. WildFire returns a near-instantaneous verdict on whether a file is malicious or benign.
2. If a file is unknown, Traps proceeds with additional prevention techniques to determine whether it is a threat that should be blocked.
3. If a file is deemed malicious, Traps automatically terminates the process and optionally quarantines the file.

#### *Local Analysis via Machine Learning*

If a file remains unknown after the initial hash lookup and has not been identified by administrators, Traps uses local analysis via machine learning on the endpoint—trained by the rich threat intelligence of WildFire—to determine whether the file can run, even before it receives a verdict from deeper WildFire inspection. By examining hundreds of file characteristics in real time, local analysis can determine whether a file is likely malicious or benign without relying on signatures, scanning, or behavioral analysis.

#### *WildFire Inspection and Analysis*

In addition to local analysis, Traps can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware. WildFire brings together the benefits of independent detection techniques for high-fidelity and evasion-resistant discovery that goes beyond legacy approaches.

- **Static analysis** is a powerful form of analysis, based in the cloud, that detects known threats by analyzing the characteristics of samples prior to execution.

- **Dynamic analysis (sandboxing)** detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior.
- **Bare metal analysis** uses a hardware-based analysis environment specifically designed for advanced threats that exhibit highly evasive characteristics and can detect virtual analysis.

If WildFire determines a file to be a threat, it automatically creates and shares a new prevention control with Traps and other components of the Palo Alto Networks Security Operating Platform in minutes to ensure the threat is immediately classified as malicious and blocked if it is encountered again.

#### *Scanning for Dormant Malware*

Traps performs scheduled or on-demand scans for malicious Office files with macros, executable files, and DLLs to remediate these without the malicious files being opened.

### 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 deeper 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*

Endpoint attacks often comprise multiple events that occur in the system. By itself, each event appears benign as attackers leverage legitimate applications and operating system functions to achieve their goal. Strung together, however, they may represent a malicious event flow. With Behavioral Threat Protection, Traps can detect and act on malicious chains of events that target multiple operations on an endpoint, such as network, process, file, and registry activity. When Traps detects a match, Traps executes a policy-based action, such as block or alert. In addition, Traps reports the behavior of the entire event chain up to the console and identifies the actor that caused the activity chain. Traps can also quarantine files that were involved in malicious flows. Behavioral Threat Protection is ideal for protecting against script-based and fileless attacks.

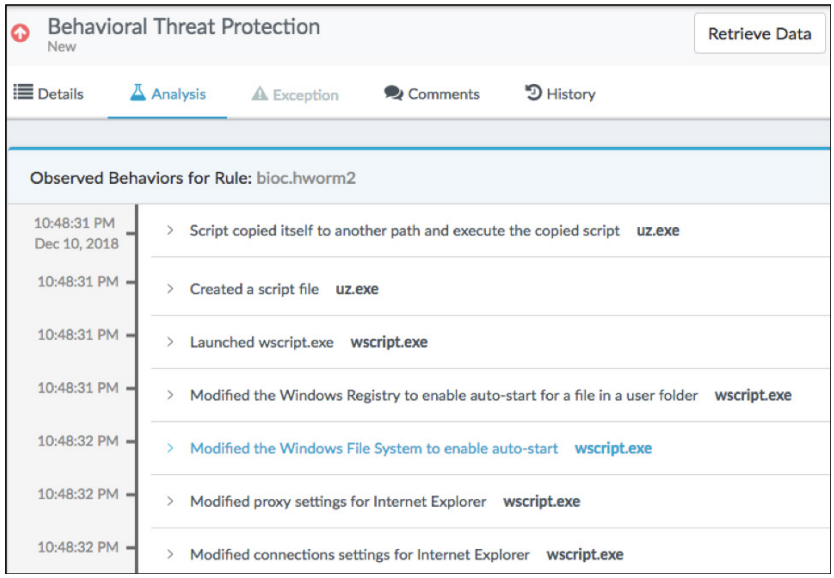


**Figure 2:** Behavioral Threat Protection timeline

#### *Granular Child Process Protection*

This module prevents script-based attacks used to deliver malware by blocking known targeted processes from launching child processes that are commonly used to bypass traditional security approaches. Traps prevents script-based and fileless 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 controls through regular content updates. Administrators have additional flexibility and control with the ability to whitelist or blacklist child processes, along with command-line comparisons, to increase detection without negatively affecting process performance or shutting processes down.

### *Behavior-Based Ransomware Protection*

This module protects against encryption-based behavior associated with ransomware by analyzing and stopping ransomware activity before any data loss occurs. To combat these attacks, Traps employs decoy files to attract the ransomware. When the ransomware attempts to write to, rename, move, delete, or encrypt the decoy files, Traps analyzes the behavior and prevents the ransomware from encrypting and holding files hostage. When configured to operate in Prevention Mode, Traps blocks the process attempting to manipulate the decoy files. When you configure this module in Notification Mode, Traps logs a security event.

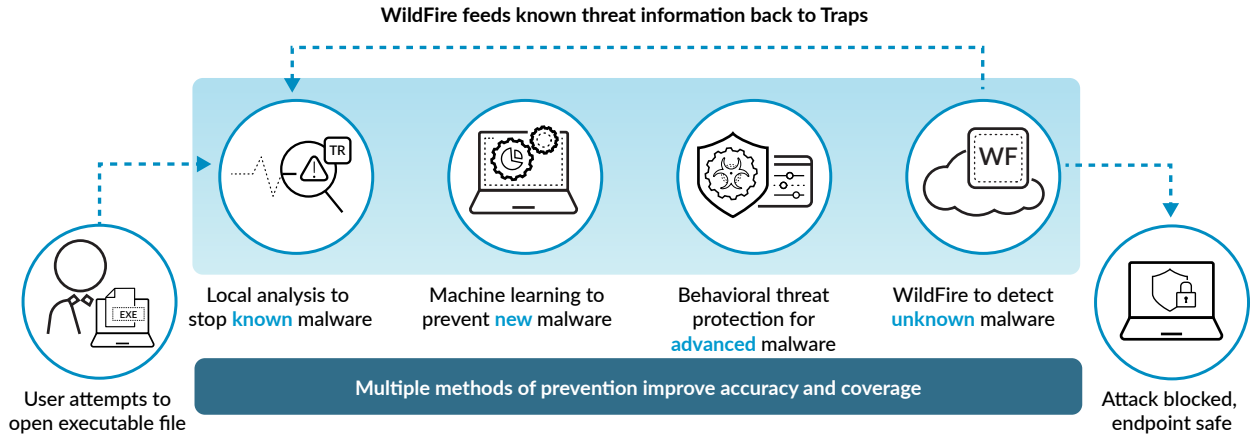


**Figure 3:** Multi-method prevention

## Block Exploits and Fileless Threats

Rather than relying on signatures or behavior-based detection to identify exploit-based attacks, Traps takes the unique approach of targeting the limited set of techniques, or tools, any exploit-based attack must use to manipulate a software vulnerability. By preventing the use of these techniques instead of identifying each individual attack, Traps can protect unpatched systems, unsupported legacy systems, and shadow IT—that is, applications IT is unaware of—as well as prevent zero-day exploits. Traps delivers exploit prevention using multiple methods.

### *Pre-Exploit Protection*

Traps prevents the vulnerability-profiling techniques exploit kits use prior to launching attacks. By blocking these techniques, Traps prevents attackers from targeting vulnerable endpoints and applications, effectively preventing the attacks before they begin.

### *Technique-Based Exploit Prevention*

Traps prevents known, zero-day, and unpatched vulnerabilities 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. By blocking these, Traps prevents exploitation attempts before endpoints can be compromised.

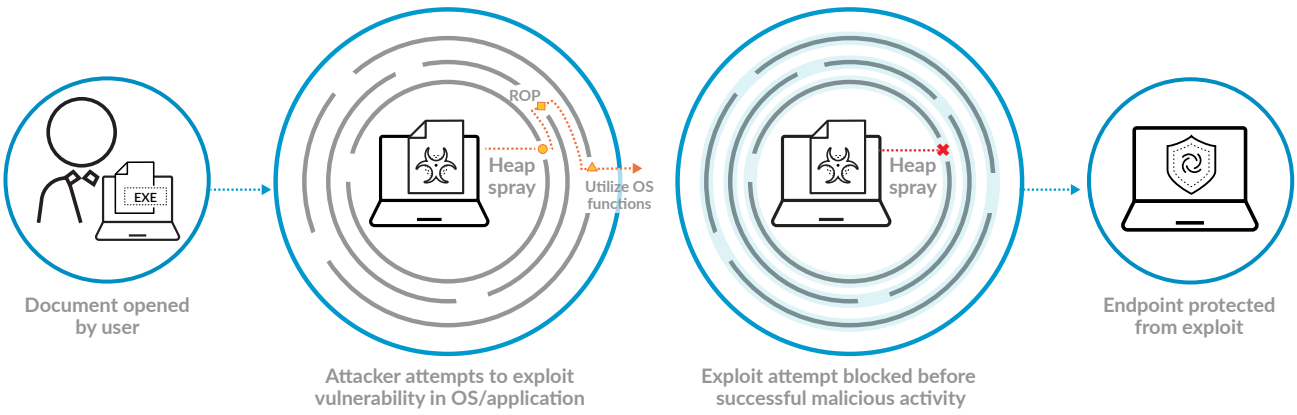


**Figure 4:** Focus on exploit techniques rather than the exploits themselves

*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 2017 WannaCry and NotPetya attacks. By blocking processes from accessing the injected malicious code from the kernel, Traps can stop an attack early in the attack lifecycle without affecting legitimate processes. This enables Traps to block advanced attacks that target or stem from the operating system itself.

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

- **Protects unpatchable applications and shadow IT:** A positive work experience is critical to the productivity of any organization, but running unsupported legacy applications or letting users download and run programs as they please introduces risk. Traps enables organizations to run any applications—including those that were developed in-house, are no longer receiving updates or security support, or are running in the environment without IT's awareness—without opening the network to the threat of exploit-based attacks.
- **Prevents successful zero-day exploits:** Because Traps blocks the limited set of exploitation techniques zero-day exploits typically use, it protects organizations against attacks that utilize zero-day exploits.
- **Eliminates the need to urgently patch applications:** Organizations using Traps can apply security patches when it is best for the business and after sufficient testing. Traps prevents the exploitation of application vulnerabilities regardless of when an organization applies security patches issued by application vendors.

### Respond to Sophisticated Attacks with Cortex XDR

Traps continuously collects and monitors endpoint data and activity. In the event of a security incident, Traps quickly correlates suspicious activity and event patterns on one or more endpoints. If Traps prevents an attack, no further administrator action is required.

Cortex XDR™ is a cloud-based detection and response app that empowers SecOps to stop sophisticated attacks and adapt defenses in real time. By combining rich network, endpoint, and cloud data with analytics, Cortex XDR detects highly evasive attacks. Cortex XDR speeds alert triage and incident response by providing a complete picture of each threat and its root cause automatically, reducing the time and experience required at every stage of security operations, from triage to threat hunting. For response, tight integration with enforcement points empowers SecOps to respond to threats quickly and apply the knowledge gained to adapt defenses and prevent future threats, making the next response even faster. Following an investigation, when remediation on the endpoint is needed, administrators have the option to:

- **Terminate processes** to stop any running malware from continuing to perform malicious activity on the endpoint.
- **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.
- **Block additional executions** of the same file by blacklisting it in the policy.

### Tight Integration with Cortex Data Lake

Traps uses Cortex Data Lake to store all event and incident data it captures, allowing a clean handoff to Cortex XDR for further investigation and incident response. Cortex XDR is the world's first detection and response app that breaks silos by integrating endpoint, cloud, network apps. It speeds alert triage and incident response by providing a complete picture of an attack, including root cause, and stitching together the sequence of events. Through tight integration with enforcement points like Traps, Cortex XDR detects and contains threats quickly, and applies the knowledge gained to continually improve your security.

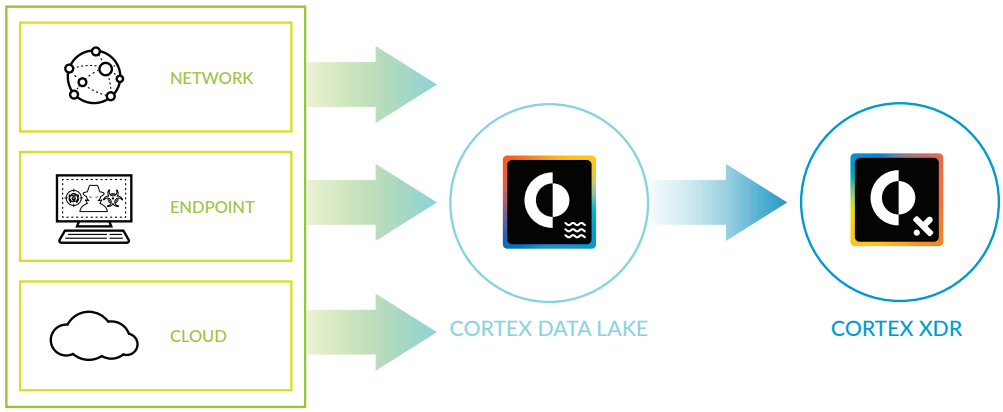


**Figure 5:** Integration of endpoint, cloud, and network data with Cortex XDR

## Extending Traps Prevention Beyond Windows Environments

Although native security has grown among major operating system vendors, such security remains focused on its own OS, creating fragmented protection, policies, enforcement, and visibility. Organizations need to be able to apply security rules across a mixed environment from a single screen as well as protect against a range of threats, from basic to advanced.

Through Traps management service, organizations can control default and custom security policies across Windows, macOS, Linux, and Android® endpoints with confidence that multiple methods of protection are keeping their systems safe from attack.

### *Traps on Mac*

Traps secures macOS systems against malware and exploits with more than just "checkbox" security. Traps malware prevention includes multiple methods, such as local analysis, WildFire inspection and analysis, Gatekeeper enhancements, trusted publisher identification, and administrator override policies. The methods of exploit prevention available include kernel privilege escalation protection and technique-based exploitation mitigation, which includes JIT and ROP mitigation as well as dylib hijacking protection.

Traps prevents attackers from bypassing the macOS digital signature verification mechanism, Gatekeeper. This mechanism 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 Gatekeeper functionality to enable customers to specify whether to block all child processes or allow only those with signature levels that match or exceed those of their parent processes.

### *Traps on Android*

Traps prevents known malware and unknown APK files from running on Android endpoints. The Traps app enforces your organization's security policy as defined in the Traps management service. The security policy determines whether to block known malware and unknown files, upload unknown files for in-depth inspection and analysis, treat malware as grayware, or perform local analysis to determine the likelihood that unknown files are malware. You can also whitelist trusted signers to enable unknown, signed apps to run before Traps receives an official verdict for the app.

### *Traps on Linux*

Traps protects Linux servers by preventing attackers from executing malicious ELF files or exploiting known or unknown Linux vulnerabilities to compromise endpoints. The agent also extends protection to processes that run in Linux containers. Traps enforces your organization's security policy as defined in the Traps management service. When a security event occurs on your Linux server, Traps collects forensic information you can use to analyze the incident further. Traps on Linux operates transparently in the background as a system process. When you install it on a Linux server, Traps automatically protects any new or existing containerized processes regardless of how the container is deployed and managed.

## Simple Endpoint Security Management

With a modern user interface, Traps aims to help your administrators quickly coordinate and protect your organization with out-of-the-box, day-one capabilities, without sacrificing your complex environment's need for control and customization.

### *Cloud-Based Management*

The multi-region, cloud-based Traps management service saves you from investing in building out your own global security infrastructure and ties in to Palo Alto Networks Security Operating Platform for additional integration and value. The service is simple to deploy and requires no server licenses, databases, or other infrastructure to get started, enabling your organization to protect hundreds or millions of endpoints without incurring additional operating costs.

### *Intuitive Interface*

Traps was designed to address security teams' growing responsibilities with an interface that makes it easy to manage policies and events as well as accelerate incident response. Elements include:

- **Multiple grouping methods,** such as partial hostname, domain or workgroup, IP address, range, or subnet.
- **Security profiles and simplified, rule-based policies** to protect endpoints out of the box while enabling granular customization for sensitive departments or individuals and easy reuse of settings across different endpoint groups.
- **Event workflows** to help identify high-priority events and enable teams to communicate on status, progress, and other useful information. Integrated WildFire analysis displays information such as hash values, targeted users, applications, processes, and URLs involved in delivery or phone-home activities for incident response.

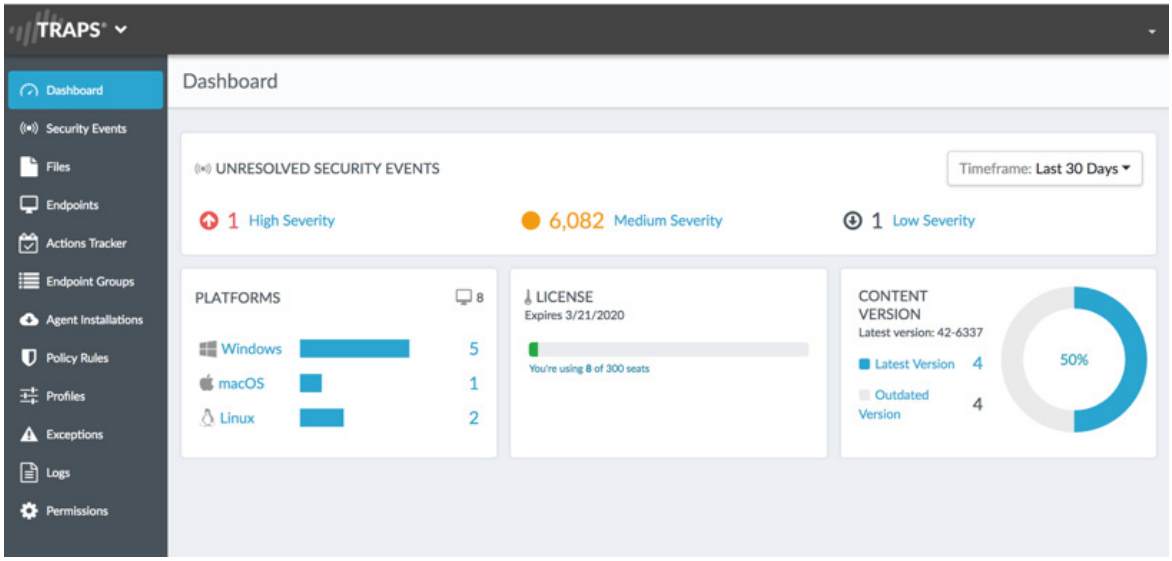


**Figure 6:** Traps management service dashboard

### Benefits of a Connected Platform

As an integral part of the Security Operating Platform, Traps continuously exchanges data with WildFire, and endpoint logs with Cortex Data Lake, to help your organization coordinate and automate enforcement across your entire security ecosystem—including endpoints, networks, and clouds.

#### *Coordinated Enforcement*

The integrated Security Operating Platform delivers greater security value than isolated components. Whenever a next-generation firewall sees a new piece of malware, or whenever an endpoint sees a new threat, protections are made available in minutes to all other next-generation firewalls and endpoints running Traps, requiring no administrative effort, whether it happens at 1 a.m. or 3 p.m. Tight integration between your network, endpoints, and clouds enables a continually improving security posture and provides coordinated enforcement to protect you from zero-day attacks.

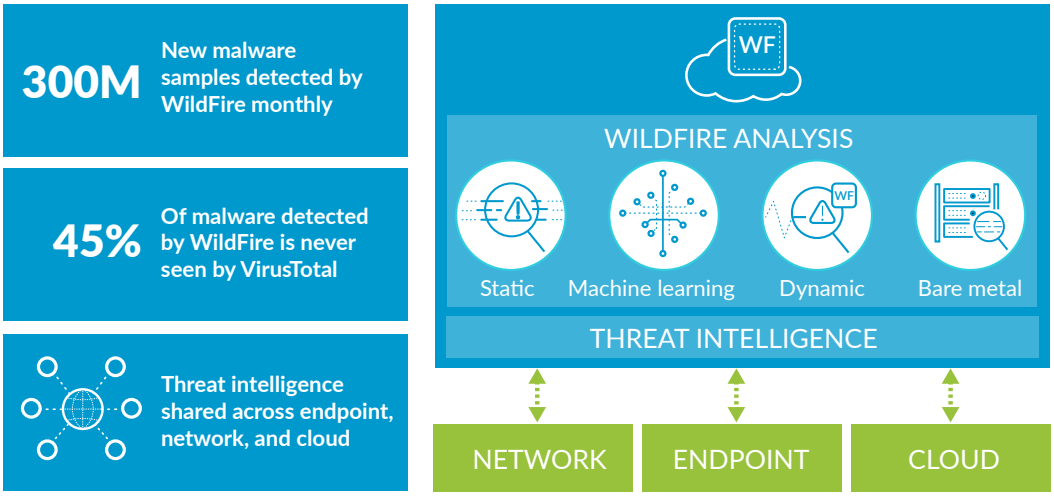


**Figure 7:** Threat intelligence gathering and sharing

#### *Centralized Logging Across the Platform*

To surface evasive threats and prevent attacks, your organization must be able to perform advanced analytics as well as detection and response on all available data. Security applications that perform such analytics need access to scalable storage capacity and processing power.

Cortex Data Lake is a cloud-based storage offering for the context-rich, enhanced network and endpoint logs Palo Alto Networks security products generate, including those of our next-generation firewalls, GlobalProtect™ cloud service, and Traps. The cloud-based nature of Cortex Data Lake allows you to collect ever-expanding volumes of data without needing to plan for local compute and storage.

Traps uses Cortex Data Lake to store all event and incident data it captures, ensuring a clean handoff to other Palo Alto Networks products and services, such as AutoFocus™ contextual threat intelligence and Cortex XDR, for further investigation and incident response with endpoint context.

## Traps Technical Architecture

The architecture of Traps is optimized for maximum availability, flexibility, and scalability to manage millions of endpoints. It comprises the components that follow.

### *Traps Endpoint Agent*

The endpoint agent consists of various drivers and services, but it requires only minimal memory and CPU usage—512 MB RAM and 200 MB disk space—to ensure a non-disruptive user experience. Once it's deployed on your endpoints, your administrators have complete control over all Traps agents in your environment through the Traps management service.

### *Traps Management Service Web Interface*

This is a cloud-based security infrastructure service designed to minimize the operational challenges associated with protecting your endpoints. From Traps management service, you can manage endpoint security policy, review security events as they occur, identify threat information, and perform additional analysis of associated logs.

### *WildFire Malware Analysis Service*

Traps management service can send unknown malware to WildFire. Based on the properties, behaviors, and activities the sample displays during analysis and execution in the WildFire sandbox, WildFire determines a verdict for the sample: benign, grayware, or malicious. WildFire then generates signatures and makes these globally available every five minutes, allowing other Palo Alto Networks products to recognize the newly discovered malware.

### *Cortex Data Lake*

As previously described, Cortex Data Lake is a cloud-based storage offering for context-rich enhanced network and endpoint logs generated by Palo Alto Networks security products, including those of our next-generation firewalls, GlobalProtect cloud service, and Traps. The cloud-based nature of Cortex Data Lake allows you to collect ever-expanding volumes of data without needing to plan for local compute and storage.

### *Cross-Environment Detection and Response*

Cortex XDR speeds alert triage and incident response by providing a complete picture of each attack, including the root cause and sequence of events. By stitching endpoint, network, and cloud data together as well as simplifying investigations, Cortex XDR reduces the time and experience required for every stage of security operations. Tight integration with Traps lets you contain threats quickly and apply knowledge gained to continually improve your security.

## Security and Hardening

The cloud-based Traps service supports strong communication protocol encryption—SSL/TLS 1.2 or higher—between Traps agents, Traps management service, and WildFire. Traps management service has also received SOC 2 Type 1 Plus certification.

## System Requirements and Platform Support

Traps supports multiple endpoint types—desktops, servers, industrial control systems, virtual desktop infrastructure components, virtual machines, and cloud workloads—across Windows, macOS, Linux, and Android operating systems. For a complete list of system requirements and supported operating systems, please visit the Traps Compatibility Matrix webpage.

For more information on Traps on-premises deployment, click here.

## Summary of Traps Benefits

- **Proven effective in stopping real-world threats:** In multiple third-party tests, including AV-TEST and NSS Labs evaluations, Traps detected 100 percent of real-world attacks and received the maximum Performance rating. On its own or as part of the Security Operating Platform, Traps stops targeted, sophisticated threats like ransomware without relying on prior threat knowledge. By minimizing endpoint infections, security teams can significantly reduce the time they spend analyzing potential infections and reimaging endpoints.
- **Protects at critical phases of the attack lifecycle:** IDC Research estimates 70 percent of attacks originate on endpoints. Because Traps does not depend on signatures, it can prevent newly morphed malware and unknown exploits through a combination of powerful offline and online prevention methods from the kernel level on up, rather than trying to stop an attack by focusing on individual, specific threats. Proactive scanning lets you discover and remove latent threats before they run. By preventing attacks early in the attack lifecycle, security teams reduce endpoint infections and minimize the likelihood of attacks moving into the data center and throughout the organization.

- **Reduces infrastructure costs and operational complexity:** Traps management service is a cloud-based deployment that provides security parameters for administrators on startup, protecting your organization from day one by default. The Traps agent employs various tamper-proofing methods to prevent users and malicious code from disabling protection or manipulating agent configurations. The agent has an observed CPU utilization of less than 0.1 percent, and its lightweight structure as well as incredibly low CPU utilization and I/O ensure minimal disruption, making Traps ideal for mobile workforces, critical infrastructures, virtual desktop infrastructure, and cloud environments.
- **Eliminates security silos by connecting endpoints to a security platform:** The integrated Security Operating Platform delivers greater security value than isolated components. Whenever a next-generation firewall sees a new piece of malware, or whenever an endpoint sees a new threat, protections are automatically made available in minutes to all other next-generation firewalls and endpoints running Traps. Tight integration between your network, endpoints, and clouds continually improves your security posture and provides coordinated enforcement to protect you from zero-day attacks.
- **Employs rapid detection and response:** Traps uses Cortex Data Lake to store all event and incident data it captures, allowing a clean handoff to Cortex XDR for further investigation and incident response. Cortex XDR speeds alert triage and incident response by providing a complete picture of an attack, including root cause, and stitching together the sequence of events. Through tight integration with enforcement points like Traps, Cortex XDR detects and contains threats quickly, and applies the knowledge gained to continually improve your security.

## Learn More About Traps

### Participate in a Traps Live Demo

Live demos let you stay at your desk and interact with Palo Alto Networks engineers as they quickly run through the components that make up the multiple methods of prevention employed by Traps to show you how each stops various attacks throughout the attack lifecycle.

### Get Hands-On with Traps in a Virtual Ultimate Test Drive

Ready to go deeper? Try out Traps yourself, from your office, without the risk of running malware in your environment. Certified Palo Alto Networks instructors will teach you as well as answer your questions about the ins and outs of the product.

### Chat with the Team

Take the discussion to the next level and set up a meeting with our Endpoint Sales team.

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-technology-overview-wp-022519