

# TRAPS 5.0

Palo Alto Networks® Traps™ advanced endpoint protection stops threats on the endpoint and coordinates enforcement with cloud and network security to prevent successful cyberattacks. Traps minimizes endpoint infections by blocking malware, exploits and ransomware. Integration with your security platform delivers additional threat analysis, shared intelligence and automated containment.

## Blocks Malware, Exploits and Ransomware

Attackers must complete a certain sequence of events, known as the attack lifecycle, to successfully accomplish their objectives, whether stealing information or running ransomware. To be successful, nearly every attack relies on compromising an endpoint, and although most organizations have deployed endpoint protection, infections are still common.

By combining multiple methods of prevention, Traps stands apart in its ability to protect endpoints. Traps blocks security breaches and successful ransomware attacks that leverage malware and exploits, known or unknown, before they can compromise endpoints.

As ransomware continues to plague organizations, 2017's WannaCry and NotPetya attacks have highlighted attackers blending two primary attack methods to compromise organizations: targeting application vulnerabilities through exploits, and deploying malicious files – including ransomware. These methods 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 operating system or application code.
- 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 requires an approach that protects 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).

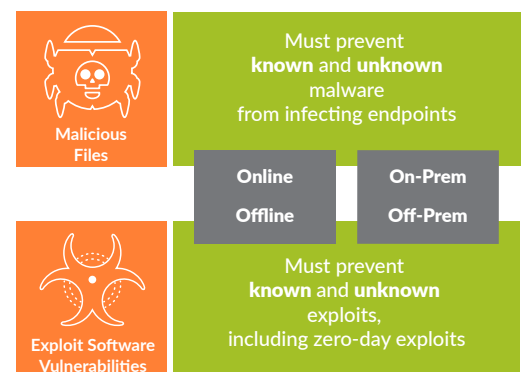
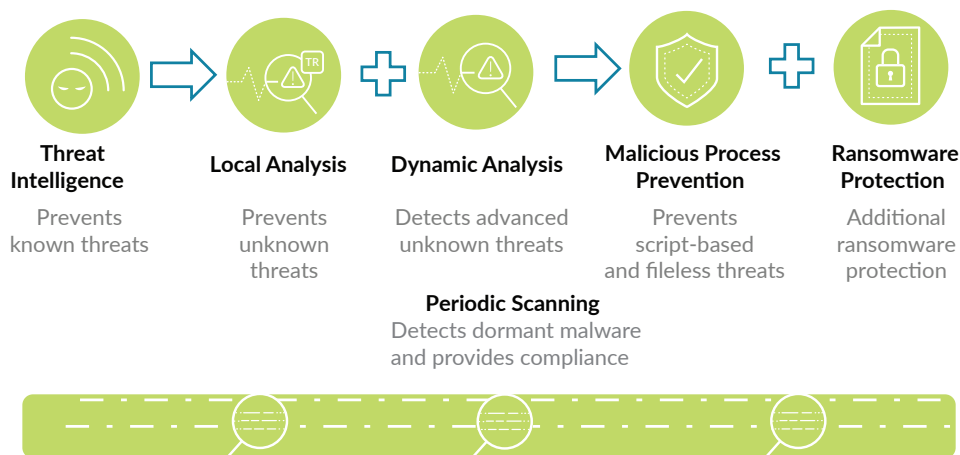


Figure 1: Malicious files vs. exploits



**Figure 2: Multi-method malware prevention**

## Multi-Method Malware Prevention

Traps prevents the execution of malicious files with an approach tailored to combating both traditional and modern attacks (see Figure 2). Additionally, administrators can utilize periodic scanning to identify dormant threats, comply with regulatory requirements and accelerate incident response with endpoint context.

- **WildFire threat intelligence:** In addition to third-party feeds, Traps leverages the intelligence obtained from tens of thousands of subscribers to the WildFire® cloud-based threat analysis service to continuously aggregate threat data and maintain the collective immunity of all users across endpoints, networks and cloud applications.
  - Traps queries WildFire with the hash of any Windows® or macOS® executable file, DLL, or Office file before the file runs to assess its standing within the global threat community. WildFire returns a near-instantaneous verdict on whether the file is malicious or benign. If the file is unknown, Traps proceeds with additional prevention techniques to determine whether it is a threat that should be terminated.
  - If the file is deemed malicious, Traps automatically terminates the process and optionally quarantines it.
- **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 receiving a verdict from the 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 sends unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware. WildFire brings together the benefits of independent techniques for high-fidelity and evasion-resistant discovery that go beyond legacy approaches. These techniques include:
  - **Static analysis via machine learning** – a more powerful version of local analysis, based in the cloud, that detects known threats by analyzing the characteristics of samples prior to execution.
  - **Dynamic analysis** – a custom-built, evasion-resistant virtual environment in which previously unknown submissions are detonated to determine real-world effects and behavior.
  - **Bare metal analysis** – 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 Palo Alto Networks Next-Generation Security Platform in as few as five minutes, ensuring the threat is immediately classified as malicious and prevented, should it be encountered again.

Additional prevention capabilities include:

- **Granular child process protection:** 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 directly from the Palo Alto Networks threat research team, Unit 42. 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 impacting process performance or shutting them down.
- **Behavior-based ransomware protection:** In addition to existing multi-method prevention measures, including exploit prevention, local analysis and WildFire, Traps monitors the system for ransomware behavior. Upon detection, it immediately blocks attacks and prevents encryption of customer data.

- **Scanning:** Administrators can scan endpoints and attached removable drives for dormant malware, with an option to automatically quarantine it for remediation when found. Periodic or on-demand scanning can be configured as part of a security profile on one or more endpoints.
- **Admin override policies:** Traps enables organizations to define policies based on the hash of an executable file to control what is or isn't allowed to run in their environments. This not only reduces the attack surface but eliminates negative impact on homegrown or heavily customized applications.
- **Malware quarantine:** 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, Traps immediately quarantines malicious executable files, DLLs and Office files to prevent propagation or execution attempts of infected files.
- **Grayware classification:** Traps enables organizations to identify non-malicious but otherwise undesirable software, such as adware, and prevent it from running in their environments.
- **Execution restrictions:** Traps enables organizations to easily define policies to restrict specific execution scenarios to reduce 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.

### Multi-Method Exploit Prevention

Rather than relying on signatures or behavior-based detection to identify exploit-based attacks, Traps takes the unique approach of targeting the limited number of techniques – the tools, if you will – any exploit-based attack must use to manipulate a software vulnerability. By preventing the techniques instead of identifying each individual attack, Traps is able to protect unpatched systems, unsupported legacy systems, applications IT is unaware of, and never-before-seen exploits – also called 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. 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 (i.e., system-level) privileges. Traps also protects against new exploit techniques used to execute malicious payloads, such as those seen in 2017's WannaCry and NotPetya attacks. By blocking processes from accessing the injected malicious code from the kernel, Traps can prevent the 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 all exploit-based attacks, Traps provides customers three important benefits:

- **Protects unpatchable applications and shadow IT:** Providing a positive work experience is critical to the productivity of any organization, but running unsupported legacy applications or granting users the flexibility to download and run programs as they please introduces risk. Traps enables organizations to run any applications, including those developed in-house, no longer receiving updates or security support, or running in their environment without IT's awareness, without opening the network to the threat of exploit-based attacks.
- **Eliminates the urgency to patch applications as soon as possible:** Organizations using Traps can apply security patches when it is appropriate 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.
- **Prevents zero-day exploits from succeeding:** Because Traps blocks the limited set of exploitation techniques zero-day exploits typically use, Traps protects organizations against attacks that utilize zero-day exploits.

### 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 require the ability not only to apply security rules across a mixed environment from a single screen but to protect against a wide variety of threats, from basic to advanced.

Through the Traps management service, organizations can control default, as well as granular, security policies across Windows, macOS and Linux consoles with confidence that multiple methods of protection are keeping their systems safe from attacks.

#### Traps on Mac

Traps secures macOS systems against malware and exploits, and it does so 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 admin override policies. The multiple methods of exploit prevention available include kernel privilege escalation protection as well as technique-based exploitation mitigation, including JIT and ROP mitigation as well as dylib-hijacking protection.

## Gatekeeper Enhancements

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 Linux

The Traps Linux agent is designed to protect Linux servers and operates transparently in the background as a system process. The Traps Linux agent is focused on protecting exposed server processes tailored for Linux-based servers. The exploit prevention modules protect against Linux exploit techniques, such as ROP, local privilege escalation, brute force and others. The lightweight, non-disruptive agent uses minimal CPU resources – about 0.1 percent – and has small memory and disk footprints – 512MB and 200MB, respectively – making it ideal for protecting virtual machines and cloud workloads. The Traps Linux agent provides immediate protection out of the box and does not require a restart upon installation.

## Simplified Endpoint Security Management

With a modern user interface (see Figure 3), Traps aims to help administrators quickly coordinate and protect their organizations with out-of-the-box capabilities from day one without sacrificing the need for control and customization required in complex environments.

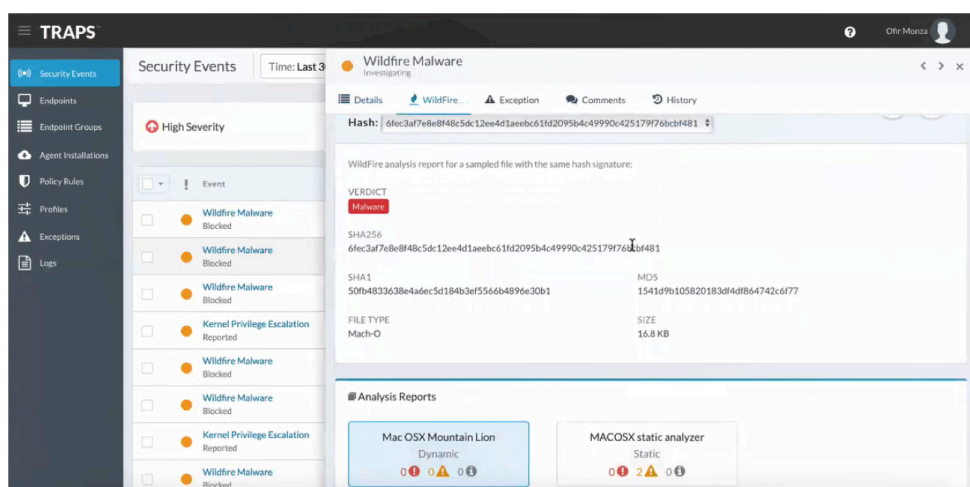


Figure 3: Traps management server

## Cloud-Based Management

The multi-region, cloud-based Traps management service saves organizations from having to invest in building out their own global security infrastructures and ties into Palo Alto Networks Next-Generation Security 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 organizations to protect hundreds to 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, with elements including:

- **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 and processes, and URLs involved in delivery or phone-home activities for incident response.

## Benefits of a Connected Platform

As an integral part of the Next-Generation Security Platform, Traps continuously exchanges data with WildFire and endpoint logs with our Logging Service to help organizations coordinate and automate enforcement across their entire security ecosystems, including endpoints, networks and clouds.

## Coordinated Enforcement

Traps shares unknown files with WildFire to rapidly dissect potentially unknown malware and disseminate critical threat information across the Next-Generation Security Platform. This bidirectional threat intelligence sharing ensures all Palo Alto Networks components are automatically reconfigured with new prevention controls in as few as five minutes, no matter where threats are first encountered, eliminating the need for manual updates or third-party tools. This automated communication reduces gaps in security and simplifies workloads, ensuring critical network and endpoint vectors work together to prevent unknown attacks that may have evaded perimeter defenses.

## Centralized Logging Across the Platform

To surface evasive threats and prevent attacks, organizations 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.

Palo Alto Networks Logging Service is a cloud-based storage offering for the 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 the Logging Service allows customers to collect ever-expanding volumes of data without needing to plan for local compute and storage.

Traps uses the Logging Service 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, Panorama™ network security management and Magnifier behavioral analytics, for further investigation and incident response with endpoint context. Additionally, Traps customers receive 100GB of Logging Service storage free with their Traps subscription and may add more if needed.

## Single-Pane Visibility Into Security Events

Panorama provides centralized management for static rules and dynamic security updates in an ever-changing threat landscape. Panorama ingests logs from both next-generation firewalls and Traps, 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 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, clouds and SaaS applications.

## Traps Technical Architecture

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

### Traps Endpoint Agent

The Traps endpoint agent consists of various drivers and services, but it requires only minimal memory and CPU usage – 512MB RAM and 200MB disk space – to ensure a non-disruptive experience for users. Following its deployment onto the endpoints, system administrators have complete control over all Traps agents in the 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 the 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 Service

The Traps management service sends unknown malware to WildFire. Based on the properties, behaviors and activities the sample displays when it is analyzed and executed in the WildFire sandbox, WildFire determines a verdict for the sample: benign, grayware, phishing or malicious. WildFire then generates signatures that allow other Palo Alto Networks products to recognize the newly discovered malware and makes these globally available every five minutes.

### Logging Service

As previously described, the Logging Service 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 the Logging Service allows customers to collect ever-expanding volumes of data without needing to plan for local compute and storage.

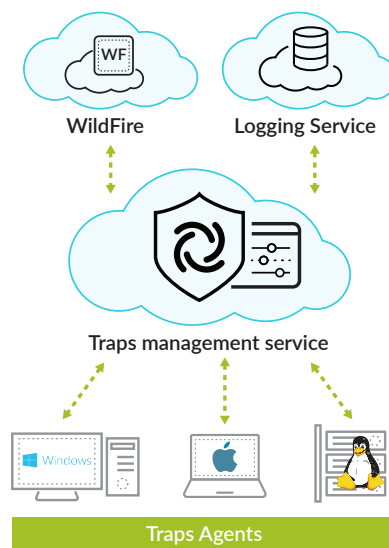


Figure 4: Traps technical architecture

---

## 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.

## System Requirements and Platform Support

Traps supports multiple endpoints 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-premise deployment, [click here](#).

## Summary of Traps Benefits

- **Proven effective in stopping real-world threats:** In multiple third-party tests, including AV-TEST, AV-Comparatives 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 Next-Generation Security Platform, Traps stops targeted, sophisticated threats like ransomware without relying on prior threat knowledge. By minimizing endpoint infections, teams can significantly reduce the amount of 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 at endpoints. Because Traps does not depend on signatures, it's capable of preventing newly morphed malware and unknown exploits through its 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 organizations 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.
- **Eliminates silos by connecting endpoints to a security platform:** As an integral part of Palo Alto Networks Next-Generation Security Platform, Traps continuously exchanges threat intelligence with WildFire threat analysis service. This two-way communication enables Traps to use intelligence from WildFire to automatically block newly identified malware and turns all your endpoints into a network of sensors and enforcement points that can strengthen security across your entire environment. Additionally, endpoint logs stored in the Logging Service are combined with logs from other sensors, enabling products such as AutoFocus, Panorama and Magnifier to assist in incident response.
- **Reduces infrastructure costs and operational complexity:** The Traps management service is a cloud-based deployment that provides security parameters for administrators on startup, protecting their organizations 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.
- **Meets compliance needs:** Coalfire®, a global leader in cyber risk management and compliance services, has independently evaluated Traps with respect to PCI DSS and HIPAA compliance requirements as well as those of the Breach Notification Rule 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 can confidently replace its existing solution with Traps and remain compliant. Traps also helps organizations fulfill the needs of the Global Data Protection Regulation, or GDPR, by ensuring strong protection for endpoints, assuring risk and compliance officers that adequate security measures are in place.

## 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 and 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 and 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](http://www.paloaltonetworks.com)

© 2018 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. traps-5.0-ds-030818



Work smarter.

At Insight, we'll help you solve challenges and improve performance with Intelligent Technology Solutions™.

Learn more

