# NETWORK AND ENDPOINT SECURITY

**Working together to deliver greater visibility, protection and enforcement**

We've reached a tipping point: threats are evolving far too quickly for point products to keep up. Having multiple products operating and analyzing data in silos has led to a fragmented and incomplete understanding of what's happening in the enterprise security landscape. With more than 9 million new instances of malware each month, deploying disparate point products across endpoint, network and cloud is no longer enough.

This paper examines the changing threat landscape and highlights the growing importance of best-in-class endpoint protection working in lockstep with other security products to create coordinated and comprehensive enterprise security. We will demonstrate how Palo Alto Networks® Traps™ advanced endpoint protection provides superior endpoint threat prevention as well as bridges the gap between endpoint and perimeter security, improving upon the efficiency and effectiveness of next-generation firewalls to provide stronger defense with fewer resources.

### Today's Cybersecurity Challenge

We've witnessed a radical change in attacker behavior in recent years as attackers, primarily driven by money, have seen more favorable returns on their investments than in the past. The cost to create attacks is plummeting, partly due to the availability of commoditized, out-of-the-box attacks and attack services, as well as attackers' abilities to recycle or modify previously known threats, leverage known and open source security technology, and incorporate automation.

The ability to see a quick return has increased exponentially. Early and ongoing success of ransomware attacks has taught attackers that rewards can come quickly with minimal effort, and cryptocurrency makes the process even faster and more lucrative. Credential theft likewise increases the likelihood of gaining access to an organization's critical systems: attackers easily uncover personal information through social media, online databases and other sources, bypassing earlier stages of the attack lifecycle where attacks are commonly prevented and making their targeted attacks even more successful.

### Attacks Are Evolving Too

Attacks have grown in volume and sophistication. With attackers no longer working independently, taking advantage of technology in much the same way modern organizations do, more than 9 million new malware instances surface each month. With their increased adoption, the constant barrage of zero-day malicious files has moved beyond targeting Windows® systems to also include macOS®, Linux and Android®. Similarly, the explosive growth of cloud-hosted environments introduces yet more targets.

Perhaps most concerning is the huge increase in fileless attacks – estimated to make up 35 percent of attacks in 2018. These attacks include exploits, macros and other methods that don't depend on a user downloading a file to succeed. They succeed more often than file-based attacks because they largely bypass traditional endpoint security measures and leave few traces for forensic investigation.

A successful endpoint attack can cost an organization more than US$5 million on average due to productivity loss, system downtime and theft of information assets. It's a struggle for all groups responsible for preventing attacks – NetOps, Desktop Ops and SecOps – to keep up.

**Fileless Attacks**

Fileless attacks, also called in-memory or zero-footprint attacks, do not need a user to actively download a file to let in the attacker. Instead, they take advantage of vulnerabilities in applications already installed on a system. A common type of fileless attack uses an exploit kit to take advantage of a browser vulnerability, forcing the browser to run malicious code. Other fileless attacks use Microsoft® Word macros, PDF readers, the PowerShell® utility or JavaScript to carry out attacks in memory.

### Strong Perimeter Protection Is Not Enough

Next-generation firewalls focus on preventing attacks that target the network. Their visibility and prevention capabilities are limited by the location and configuration – the where and how – of these network enforcement points, and unfortunately, many things can circumvent a firewall:

- Offline and off-network users
- Encrypted traffic and attachments
- Misconfigured application control
- Exploits manipulating vulnerable applications
- Ransomware

Most attacks start by compromising an endpoint. Threats that evade firewall enforcement can be prevented by endpoint security products, many of which vary in degrees of effectiveness as they run in isolation from the rest of the security infrastructure and cannot quickly share valuable intelligence across the ecosystem.

### Strengthening Perimeter Protection

Organizations usually invest heavily in perimeter protection, but despite this, end users can unwittingly undercut these controls. When they operate outside the network, fall for phishing campaigns, or engage in other risky behavior due to normal human trust or curiosity, users open the door for attackers to circumvent hardened security measures, such as firewalls.

Additionally, many organizations deploy a variety of security tools in the hopes of protecting the organization against such attacks. However, this fragmented approach dramatically decreases operational efficiency, requiring manual configuration and integration while inevitably creating blind spots.

*"We were looking for the widest range of protection we could get, including preventing an employee from launching an executable that locks up their computer with ransomware. With Traps running in conjunction with our next-generation firewalls, if an end user does something foolish on their computer, on or off our network, we apply policy to it and prevent the threat from detonating."*

– David Shanker, vice president of Information Technology, JBG Smith

As powerful as next-generation firewalls are, there are several things they cannot do to prevent an attack. Understanding the location and configuration of your next-generation firewall allows endpoint security to cover potential gaps, including:

- **Offline and off-network users:** Endpoints are regularly removed from network boundaries, exposing the devices to networks with limited or no ability to prevent malicious activity.
- **Exploits manipulating vulnerable operating systems and applications:** With multiple methods of exploit delivery, such as website ads and email, endpoints are vulnerable to application manipulation, allowing a high chance of malware delivery and limiting threat prevention to only the latter stages of the attack lifecycle.
- **Ransomware:** Preventing unknown ransomware on the network requires finely tuned security controls with no allowed margin of error. If a threat is not detected in delivery, the lack of endpoint and east-west traffic visibility will vastly increase potential damage.
- **Encrypted traffic and attachments:** With more than half of internet traffic now encrypted, attackers can easily circumvent basic network prevention capabilities using SSL and SSH, exposing the endpoint via encrypted websites and email.
- **Misconfigured application control:** The ability to apply policies controlling access to unwanted software as a service – SaaS – or web applications is sometimes misconfigured, set to alert only, or disabled, exposing the endpoint to malicious activity.

Rather than operate in a silo, endpoint protection must share what it sees and prevents with both the network and the cloud – coordinating analysis, response and prevention to strengthen overall security posture – to free up teams to tackle other priorities. Effective security calls for tight coordination and communication between the endpoint, network and cloud.

### 3 Requirements for Endpoint Security That Enhances Perimeter Protection

A successful attack on an endpoint creates a beachhead into a network that a next-generation firewall, even with correct configuration and policy implementation, cannot block or prevent. This underscores the importance of ensuring endpoint protection is truly effective, able to:

1. **Prevent Successful Attacks:** The two principal methods of compromising endpoints are via malware and exploits. Malware encompasses executable files, often self-contained, designed to perform malicious activities on a system. Exploits take advantage of software flaws or bugs in legitimate applications to provide attackers with remote code-execution capabilities and can be used to remotely execute malware. Effective endpoint protection will prevent, not just detect, attacks of both types. Further, as attackers learn and their methods evolve, an effective endpoint protection offering will protect against known threats as well as never-before-seen attacks.

> *"The types of threats today are so immediate and difficult to detect, the old signature-based virus protection is not valid whatsoever anymore. We've had such success with the next-generation firewalls, and Traps is so tightly integrated with the rest of the Palo Alto Networks platform – it just makes sense."*
>
> – Bret Lopeman, IT security engineer, Ada County

2. **Coordinate Analysis and Response:** Many organizations deploy a variety of endpoint agents and tools simultaneously in hopes of providing the security the organization needs. However, a fragmented approach with numerous tools and products requires security teams to either manually configure proper information exchanges or set up third-party tools to facilitate visibility, inevitably creating blind spots. Rather than operate in a silo, endpoint protection must share what it sees and prevents with both the network and the cloud. Coordinated analysis and response – spanning the endpoint, cloud and network – will strengthen the overall security posture, freeing up teams to tackle other priorities.
3. **Shorten Time to Action:** The time between when an infection happens and when it is discovered can span days or months. A 2017 study showed that the mean time to identify an attack was 191 days.[1] The longer an attack takes to identify, the more severe its impact – and the worse for organizations with IT staff who are already overburdened. Endpoint security products need to automatically halt threats, stopping their spread without any additional user or IT action.

> *"We can clearly see the effectiveness in a real environment of the next-generation firewall using threat intelligence from WildFire, based on information Traps was picking up. That gives us a good sense of security, knowing that intelligence is shared across the enterprise."*
>
> – Joel Pfeifer, principal security analyst, HealthPartners

### Putting the Pieces Together

Few organizations can say both their firewalls and endpoint security are strong, let alone natively integrated. Palo Alto Networks Traps advanced endpoint protection extends the protection of the firewall to create a network of sensors and enforcement points, enhancing security across an entire organization.

1. Ponemon Institute. 2017 Cost of a Data Breach Study, June 2017.

Adding Traps to the security ecosystem creates a closed-loop system: as threats emerge, suspicious files and URLs are routed to Palo Alto Networks WildFire® malware prevention service for deep analysis, shared intelligence and automated containment, whether they came from the firewall or the endpoint. Panorama™ network security management ingests logs from next-generation firewalls and Traps, enabling security operations teams to view endpoint security logs in the same context as their firewall logs.

As part of the Security Operating Platform, automated integration and intelligence sharing ensure all parts of the security infrastructure understand newly identified threats and can automatically update preventions, without human intervention, in as few as five minutes. Eliminating the well-known silos and communication barriers between network and endpoint teams as well as disparate products enables open communication and visibility between the products. With gaps and fragmentation reduced, overall protection and security effectiveness increase.

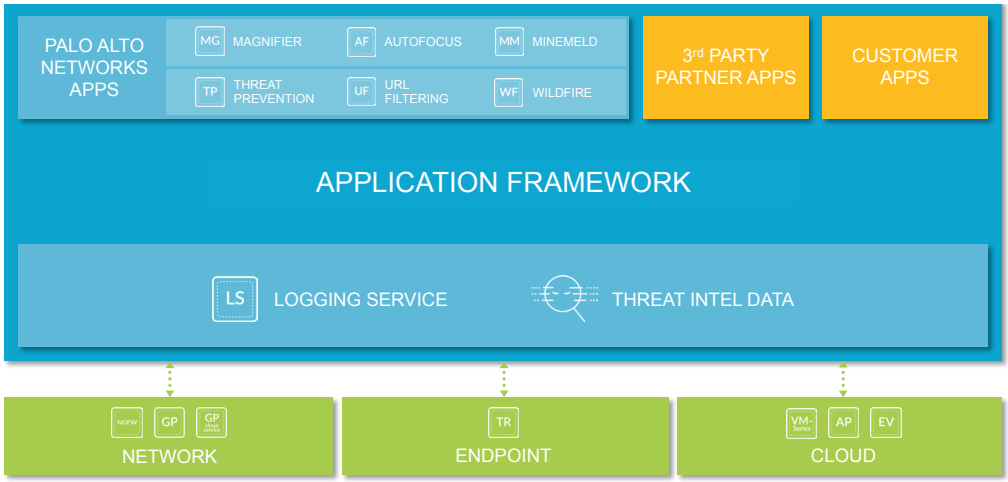


**Figure 1:** Palo Alto Networks Security Operating Platform

Traps can improve the prevention capabilities of your next-generation firewall and reduce operational overhead in several ways, allowing you to:

- **Detect and prevent known and unknown threats,** including evasive threats, as well as share threat intel across network, endpoints and cloud with WildFire, minimizing the number of alerts administrators must address.
- **Gain visibility** into known and unknown threats across all traffic, files and applications with context to drive proactive response.
- **Deliver persistent protection** for endpoints, online or offline, on- or off-network.
- **Coordinate enforcement** and automatically reprogram defenses across networks, clouds and endpoints to protect against new threats.
- **Automate response** using Traps and firewall policies to isolate and quarantine suspicious endpoints, minimizing the potential impact of an attack.
- **Enhance overall security** by helping security teams correlate discrete activities observed on the network and endpoints for a unified picture of security events across the environment. In conjunction with automated policies, reduce the attack surface across endpoints, firewalls, clouds and SaaS applications.

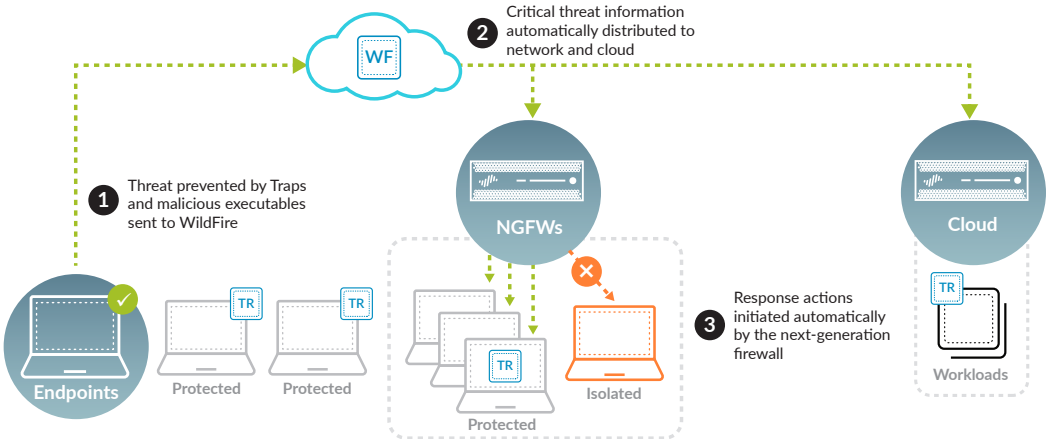


**Figure 2:** Traps coordinated enforcement

### How Traps Improves Endpoint Security and Productivity

Traps addresses the weakest links in a heavily managed and monitored security ecosystem: the endpoints. Traps protects users from increasingly sophisticated adversaries who have become adept at disguising their intent and taking advantage of human nature. It allows users to enjoy a seamless experience without the friction often caused by traditional security methods, such as signatures, scanning or restarts from patch updates.

With its multi-method approach to prevention, Traps prevents known, unknown and highly evasive threats while minimizing the number of alerts an administrator must address. Traps uses intelligence from WildFire to prevent known malware and provide deep inspection of unknown files, including dynamic analysis, static analysis, machine learning and bare metal analysis. It goes beyond merely blocking exploits and fileless attacks: it terminates the process, informs the user and administrator, and collects detailed forensics other parts of the security ecosystem can use.

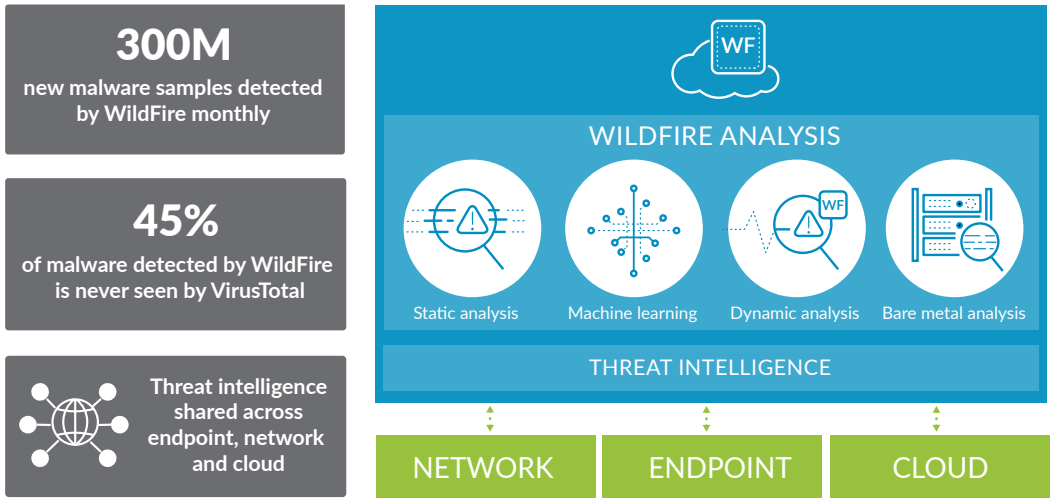


**Figure 3:** Threat intelligence and sharing

Minimizing the potential for exposure from an attack, Traps automatically inserts itself into critical phases of the attack lifecycle to halt the execution of malicious programs and stop the exploitation of legitimate applications. It does this regardless of operating system, an endpoint's online or offline status, and whether it is connected to the organization's network or roaming. Additional scanning capabilities in Traps detect dormant, non-executed malware and can quarantine it to ensure it does not detonate, thus disrupting potential attacks before they can infect the endpoint and other parts of the network.

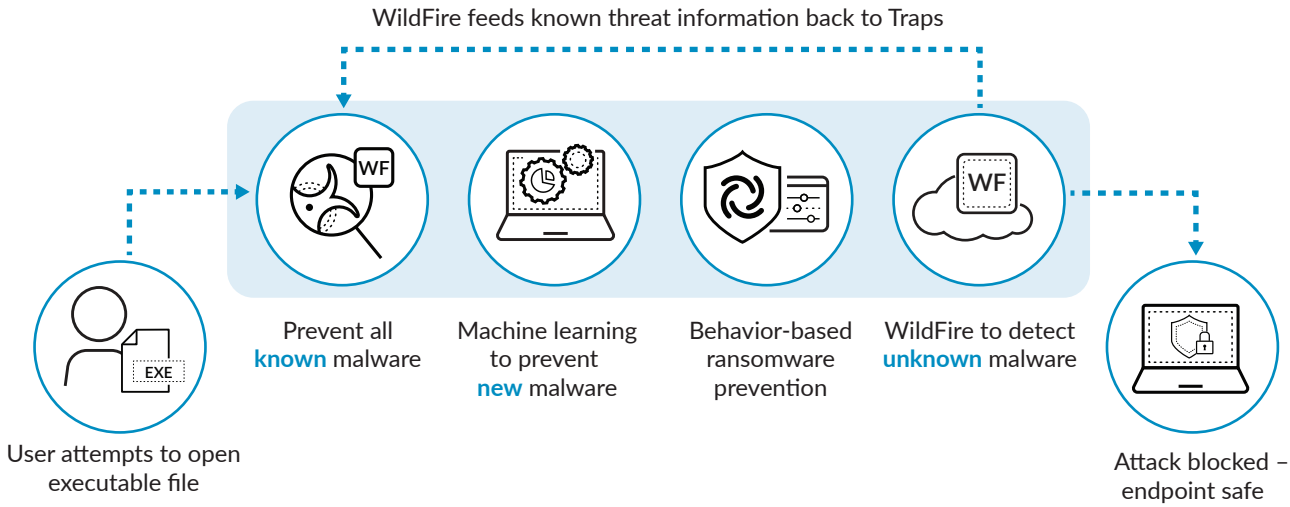


**Figure 4:** Multiple methods of prevention for accuracy and coverage

Even the smallest teams can effectively manage high-density endpoint implementations, including virtual desktop infrastructure or cloud-hosted environments across platforms, thanks to the cloud-based infrastructure of Traps, further reducing overhead and maintenance.

Traps combines multiple methods of prevention to meet the toughest of endpoint protection requirements and then some, allowing you to:

1. **Prevent successful attacks:** Traps blocks security breaches and ransomware attacks that use malware and exploits – known or unknown – utilizing intelligence from WildFire to prevent known threats and provide deep inspection of unknown files.
2. **Coordinate analysis and response:** Traps is integrated throughout the Palo Alto Networks Security Operating Platform, facilitating discovery, detection, containment and broader automated prevention across the endpoint, network and cloud.
3. **Shorten time to action:** The cloud-delivered Traps management service simplifies implementation and reduces cost while intuitive, built-in workflows reduce the time needed to create and execute policies, accelerating incident response across your organization.

**Jungfrau Railway Company,** operating the highest-elevated railway station in Europe, could not afford prolonged outages as its infrastructure handled an ever-growing share of customer business. The company struggled to prevent malware from entering its network, so when it fell victim to the WannaCry ransomware, Jungfrau turned to Palo Alto Networks. During the implementation, Jungfrau used Traps and WildFire to identify threats on its servers and endpoints. Today, the company estimates Traps has reduced its team's remedial work by 10 to 20 days annually.

## Conclusion

Until now, the missing piece of the security puzzle has been the inability to seamlessly integrate endpoints into a security ecosystem. Attempts to use a hodgepodge of third-party applications, hardware and custom integration to address sophisticated, endpoint-targeted attacks have failed in exploit prevention or early detection of malware. Palo Alto Networks addresses this gap by integrating firewalls and endpoint security in a way that provides unmatched, comprehensive protection. Bringing together all pieces of the puzzle – firewalls, clouds and endpoints – and aggregating all knowledge in one place results in contextual awareness previously only attainable through time-consuming, manual effort. Traps provides complete attack prevention for the endpoint as an integral part of the Palo Alto Networks Security Operating Platform, complementing and enhancing your next-generation firewalls and other security tools. With Traps, your security is much greater than the sum of its parts.

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


network-and-endpoint-security-wp-100418