NETWORK AND ENDPOINT SECURITY

Working together to deliver greater visibility, protection, and enforcement

The enterprise security landscape is littered with the remains of security point products that promised to prevent successful cyberattacks but failed to deliver. Multiple products operating and analyzing data in silos lead to a fragmented and incomplete understanding of what's ultimately needed: an automated system that aggregates threat information from multiple vectors and responds accordingly. Although technology has enabled our organizations and users, it has also introduced gaps in security and fragmented policies that have enabled attackers to circumvent controls and pinpoint vulnerabilities.

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.

Attackers Evolve

We've seen a sea change in attacker behavior in recent years as the attackers, primarily driven by money, see much more favorable returns on their investments than in the past. The costs to create attacks are plummeting for many reasons, including 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 more prone to being prevented and making their targeted attacks even more successful.

Attacks Evolve Too

Attacks have grown in volume and sophistication. Thanks to attackers no longer working individually and instead taking advantage of technology in much the same way modern organizations do, more than 9 million new instances of malware are seen each month.[1] The constant barrage of zero-day malicious files has moved beyond targeting Windows® systems to also include macOS®, Linux and Android® – with their increased adoption, they have become attractive targets. Similarly, the explosive growth in 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.[2] 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[3] 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 leverage 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.

How Endpoint Protection Can Help the Entire Organization

The endpoint is a critical component of an effective, comprehensive security architecture. However, unlike every other security mechanism an organization can control, when it comes to endpoint devices, it's the users – busy, distracted and occasionally less security-savvy – who are in control.

Attackers perform reconnaissance on users to trick them into opening risky files or visiting compromised websites. For instance, someone in HR would not think twice about opening a résumé that looks entirely authentic but is, in fact, designed to exploit a vulnerability in the operating system. A bank customer might open a seemingly legitimate monthly statement and bring malware into the network. Almost all attacks start by compromising an endpoint, so when something malicious occurs on the endpoint, the firewall needs to know. Firewalls can and should benefit from critical knowledge gained from endpoint attacks, and endpoint security should benefit from knowledge gained from events that happen on the firewall. Effective security calls for tight coordination and communication between the endpoint, network and cloud (see Figure 1).

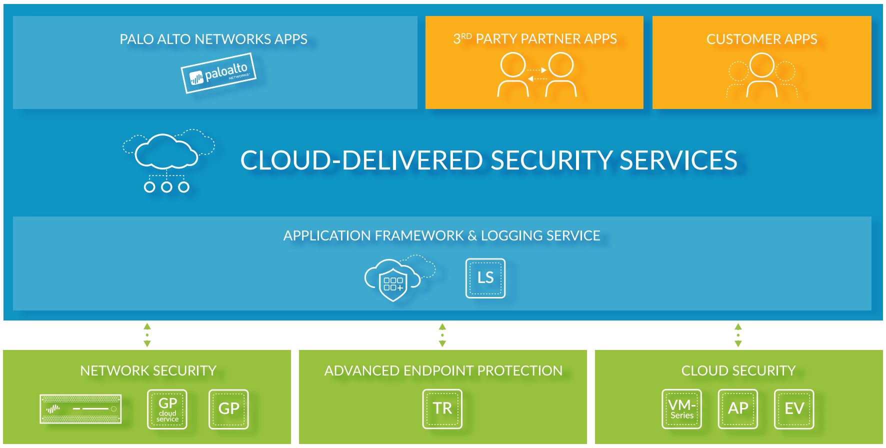

Figure 1: Palo Alto Networks Security Operating Platform

[1] AV-TEST Malware Statistics. AV-TEST, March 2018. https://www.av-test.org/en/statistics/malware/

[2] The State of Endpoint Security. Ponemon, 2017. Retrieved from https://www.ponemon.org/blog/the-2017-state-of-endpoint-security-risk-report

[3] Ibid.

Strong Perimeter Protection Is Not Enough

Next-generation firewalls focus on preventing attacks that target the network. Their visibility and prevention capabilities are limited to what occurs on the network, though – and unfortunately, many things can circumvent a firewall:

- Offline and off-network users
- Encrypted traffic and attachments
- Exploits manipulating vulnerable applications

A good endpoint security product should enhance network security and help prevent attacks in any of these circumstances. Many endpoint security point products protect against these attacks with varying degrees of effectiveness because they run in isolation from the rest of the security stack and cannot quickly share valuable intelligence across the ecosystem.

> *"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

3 Requirements for Effective Endpoint 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 by:

Preventing 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. Truly 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.

Coordinating 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 requiring security teams to either manually configure proper information exchanges or set up third-party tools to facilitate visibility, inevitably creates 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 – strengthens the overall security posture, freeing up teams to tackle other priorities.

Shortening Time to Action

It can take days or months from the time an infection happens until it is discovered. A recent study showed that the mean time to identify an attack was 191 days.[4] The longer an attack takes to identify, the more severe its impact – and the worse for organizations with already overburdened IT staff. Endpoint security products need to automatically halt threats, stopping their spread without any additional user or IT action.

Traps: Putting Prevention First

Traps advanced endpoint protection meets these requirements: it prevents successful attacks, coordinates analysis and response, and shortens the time to action.

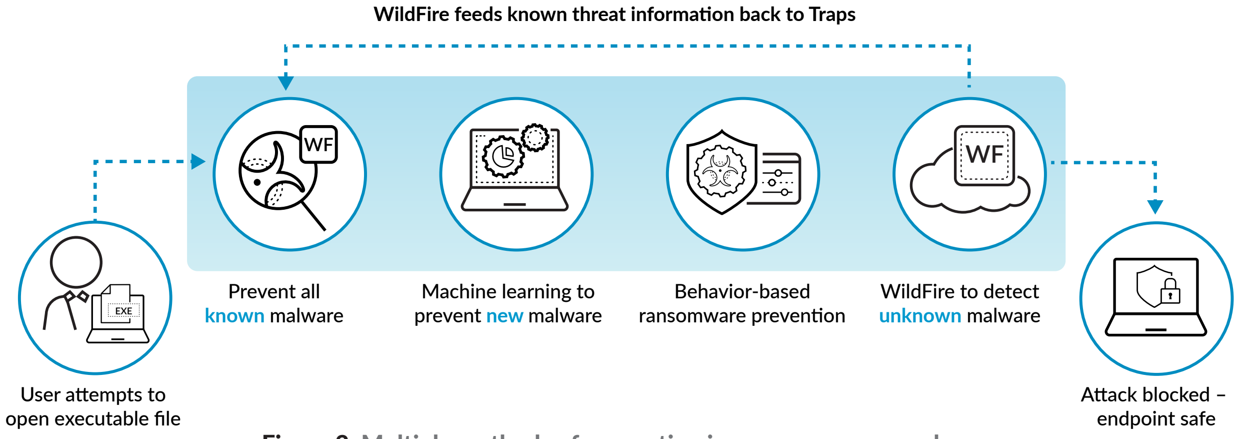
WildFire feeds known threat information back to Traps
WF
WF
EXE
User attempts to open executable file
Prevent all known malware
Machine learning to prevent new malware
Behavior-based ransomware prevention
WildFire to detect unknown malware
Attack blocked – endpoint safe

Figure 2: Multiple methods of prevention improve accuracy and coverage

[4] 2017 Cost of Data Breach Study. Ponemon, June 2017. Retrieved from https://www.ibm.com/security/data-breach

By combining multiple methods of prevention in a single, lightweight agent, Traps stands apart in its ability to protect endpoints online and offline. Traps uses intelligence from Palo Alto Networks WildFire® cloud-based threat analysis service to prevent known malware and provide deep inspection of unknown files, including dynamic analysis, static analysis, machine learning and bare metal analysis. Traps blocks security breaches and ransomware attacks that leverage malware and exploits – known or unknown – before they can compromise endpoints. 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.

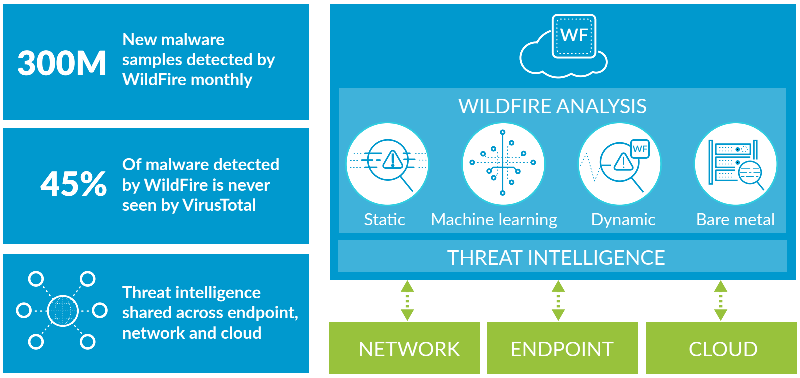
300M
New malware samples detected by WildFire monthly
45%
Of malware detected by WildFire is never seen by VirusTotal
Threat intelligence shared across endpoint, network and cloud
WF
WILDFIRE ANALYSIS
Static
Machine learning
Dynamic
Bare metal
THREAT INTELLIGENCE
NETWORK
ENDPOINT
CLOUD

Figure 3: **Threat intelligence gathering and sharing**

Traps coordinates endpoint protection with network and cloud security to provide additional threat analysis, shared intelligence and automated containment. A cloud-delivered management service simplifies implementation and reduces costs while intuitive, built-in workflows reduce the time needed to create and execute policies as well as accelerate incident response across the organization. Event and incident data Traps captures is stored in Palo Alto Networks Logging Service, ensuring a clean handoff to other components of the Security Operating Platform, such as AutoFocus™ contextual threat analysis service, Panorama™ network security management and Magnifier™ behavioral analytics, for further investigation and incident response with endpoint context. Traps is integrated throughout the platform, facilitating discovery, detection, containment and, ultimately, broader automated prevention across the entire security architecture.

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.

Traps minimizes the potential of exposure from an attack by automatically inserting itself into critical phases of the attack lifecycle to halt the execution of malicious programs and stop the exploitation of legitimate applications (see Figure 4). 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.

Putting the Pieces Together

Deploying Traps on endpoints extends the protection of the firewall to create a network of sensors and enforcement points, enhancing security across the entire organization. As part of Palo Alto Networks Security Operating Platform, automated integration and intelligence sharing ensures all parts of the security ecosystem understand newly identified threats and automatically update preventions, without human intervention, in as few as five minutes. By eliminating the well-known

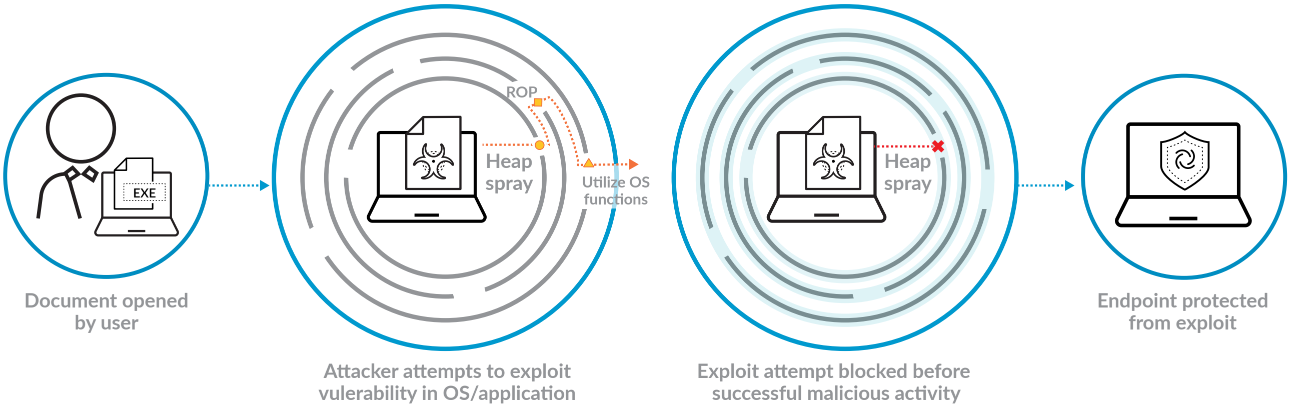
EXE
Document opened by user
ROP
Heap spray
Utilize OS functions
Attacker attempts to exploit vulerability in OS/application
Heap spray
Exploit attempt blocked before successful malicious activity
Endpoint protected from exploit

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

silos and communication barriers that have existed between network and endpoint teams and disparate products, organizations enable open communication and visibility between their security products. Gaps and fragmentation are also reduced, increasing overall protection.

How Traps Improves Endpoint Security and Productivity

Traps addresses the weakest link in a heavily managed and monitored security ecosystem: the endpoint. Traps protects users from increasingly sophisticated adversaries who have become adept at masquerading 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 and unknown as well as highly evasive threats while minimizing the number of alerts an administrator must deal with. 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.

> *"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

How Traps Enhances the Firewall

Organizations 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. Traps not only reduces security teams' workloads by deflecting attacks before they can cause harm but also feeds timely threat intelligence into firewalls automatically. This coordination increases the effectiveness, efficiency and overall value of firewall investments while delivering the end-to-end visibility many organizations struggle to obtain.

How Traps Enhances Overall Security

Few organizations can say both their firewalls and endpoint security are strong, let alone natively integrated. Adding Traps to the security ecosystem creates a closed-loop system: as threats emerge, suspicious files and URLs are routed to WildFire for deep analysis, 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. This helps them correlate 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.

> *"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

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 parts 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 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