TOP FIVE REQUIREMENTS FOR EFFECTIVE ENDPOINT PROTECTION

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 succeed, 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, Palo Alto Networks Traps™ advanced endpoint protection stands apart in its ability to protect endpoints. Traps blocks security breaches and successful ransomware attacks that use 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: 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 or not it is connected to an organization's network.

This paper highlights the primary benefits our customers enjoy with Traps advanced endpoint protection.

1. FIGHTING THREATS WITH CLOUD-BASED MALWARE ANALYSIS

Today's complex threat landscape – combined with the diversity, volume and sophistication of threats in the modern enterprise environment – makes effective threat prevention challenging. This problem is compounded by the challenge of detecting never-before-seen malware and exploits in addition to identifying known malicious content.

To address these sophisticated, targeted and evasive threats, endpoint protection must integrate with shared threat intelligence to learn and evolve its defenses. In 2017, IDC Research reported that 39 percent of security professionals consider shared threat intelligence a high or extreme priority to improve security posture.[1] To that point, integrating cloud-based threat intelligence with endpoint protection enables deeper analysis to rapidly detect potentially unknown threats.

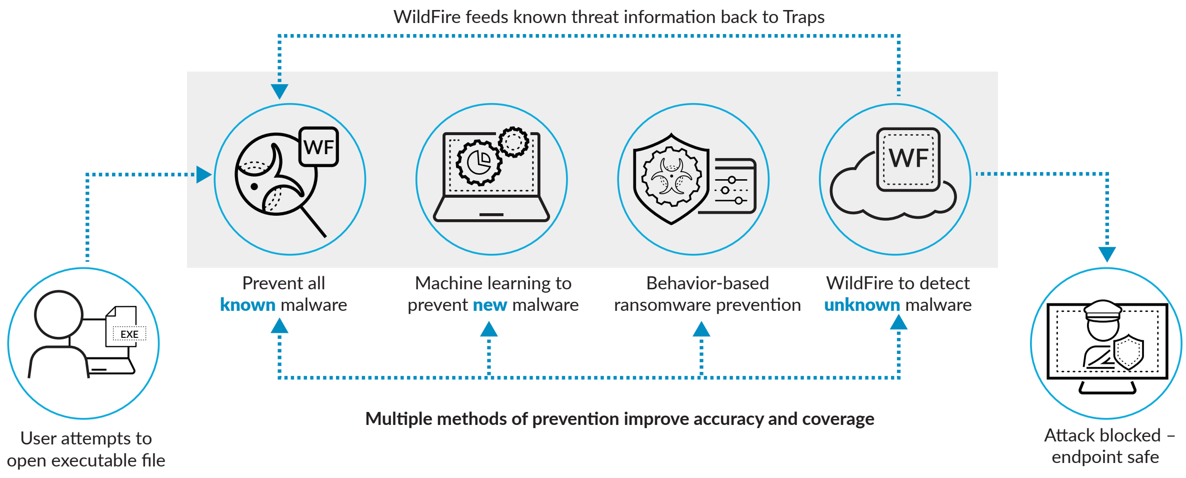
WildFire feeds known threat information back to Traps
WF
WF
EXE
User attempts to open executable file
Prevent all **known** malware
Machine learning to prevent **new** malware
Behavior-based ransomware prevention
WildFire to detect **unknown** malware
Multiple methods of prevention improve accuracy and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

Figure 1: Preventing known and unknown threats

Traps and WildFire

Traps prevents the execution of malicious files with an approach tailored to face traditional and modern attacks. To increase prevention accuracy and coverage, Traps takes advantage of multiple elements of WildFire® malware prevention service.

Threat Intelligence

Traps queries WildFire to quickly determine whether an instance of malware has been seen before, shortening the time to a verdict and immediately blocking known threats.

Machine Learning on the Endpoint

Traps uses machine learning to identify new threats. With more than 7 billion samples and 5 trillion artifacts collected and processed, WildFire has trained Traps to identify both bad and good files to provide more accurate verdicts as well as minimize false positives. This analysis looks at hundreds of a file's characteristics in a fraction of a second without relying on signatures, scanning or behavioral analysis. Any new threats Traps identifies are sent to WildFire for additional analysis, including dynamic analysis, static analysis, machine learning and bare metal analysis.

[1] Konstantin Rychkov and Duncan Brown, "Bridging Security Gaps with Network-to-Endpoint Integration," IDC Research, October 2018. https://www.paloaltonetworks.com/resources/whitepapers/bridging-security-gaps-with-network-to-endpoint-integration.

Malware Analysis

In the case of a never-before-seen file, WildFire performs static analysis to observe the file's behavior and render a verdict of malicious or benign. The file, if still unknown, is further subject to dynamic analysis by our custom hypervisor. Threats attempting to evade analysis are subject to bare metal analysis for full hardware execution to detect and prevent even the most evasive malware.

With Traps and WildFire working together, you get:

- The latest, most up-to-date detection technologies available at scale.
- Automated, proactive protection, accurate zero-day detection and prevention delivered in minutes for threats found across tens of thousands of customer networks around the globe.
- Extensibility with virtually unlimited scale to meet the analysis needs of even the largest organizations.
- Automatic distribution of up-to-the-minute threat intelligence, to and from firewalls, cloud and endpoints, to reprogram prevention and coordinate enforcement.
- Flexibility, with no additional hardware to purchase, deploy, configure, update or maintain.

As an integral part of the Palo Alto Networks Security Operating Platform, Traps continuously exchanges threat intelligence with WildFire. This two-way communication, which enables Traps to use intelligence from WildFire to automatically block newly identified malware, 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 Palo Alto Networks Logging Service are combined with logs from other sensors, enabling other Palo Alto Networks products, such as AutoFocus, Panorama™ network security management and Magnifier™ behavioral analytics, to aid in incident response.

2. PREVENT RANSOMWARE

Although ransomware is not new, major attacks like WannaCry, Petya/NotPetya and, more recently, TrickBot have shown that traditional prevention methods have become ineffective against advanced ransomware attacks. Attackers have evolved their approach and use of malware to become more sophisticated, automated, targeted and highly evasive.

WannaCry: Combining Malware and Exploits

When WannaCry first hit in May 2017, it was so effective that coverage of breaches attributed to it still appears in the news today. It remains effective due to a combination of malware and exploits. First, it exploits a vulnerability in the Microsoft Server Message Block protocol to gain kernel-level privileges through the use of a kernel asynchronous procedure call, or APC, attack. Kernel APC attacks use kernel privileges to carry out their objectives – making legitimate programs execute malicious code, in this case.

From the end user's point of view, ransomware like WannaCry locks up the screen on the endpoint, making it impossible to see other activities the ransomware is carrying out. At the same time, the malware spreads east-west, infecting as many vulnerable machines as it can, both internally and externally.

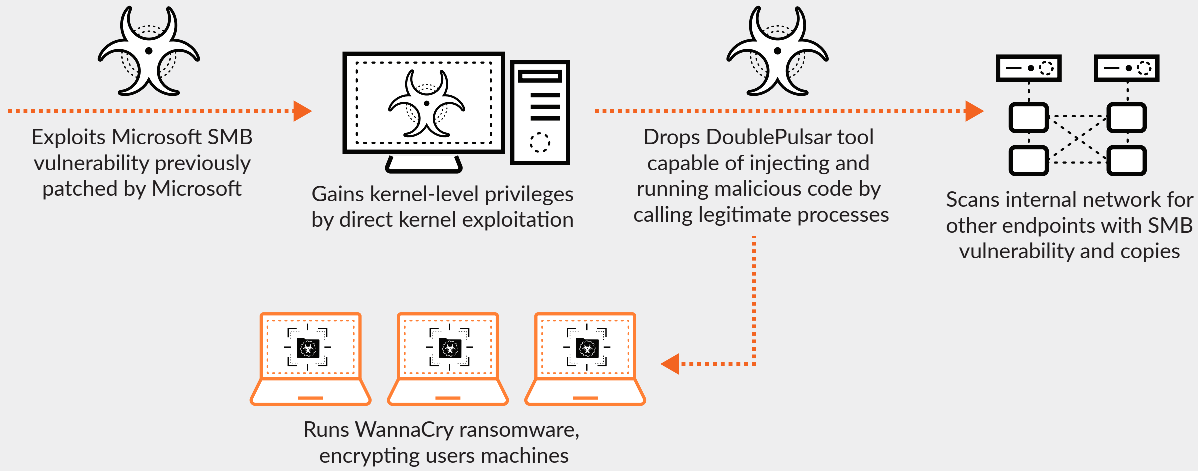
Exploits Microsoft SMB vulnerability previously patched by Microsoft
Gains kernel-level privileges by direct kernel exploitation
Drops DoublePulsar tool capable of injecting and running malicious code by calling legitimate processes
Scans internal network for other endpoints with SMB vulnerability and copies
Runs WannaCry ransomware, encrypting users machines

Figure 2: Simplified WannaCry attack sequence

Traps combines multiple methods of prevention against known and unknown malware, ransomware, and exploits to stop the execution of malicious programs before an endpoint can be compromised. With protection at critical stages of the attack lifecycle, Traps can prevent successful ransomware attacks regardless of operating system and whether an endpoint is online or offline, connected to the corporate network or not.

Leading up to the WannaCry outbreak, endpoints protected by Traps detected and shut down the ransomware in multiple stages of the attack lifecycle. First, Traps would have detected the exploit technique attempting to escalate kernel privileges to the user level. As soon as Traps had detected that action, it would have shut down the attack. If that were not successful, the malicious process protection module would have detected and stopped the parent process from spawning a child process. If previous modules had not detected the threats, the agent would have detected the attack and stopped it by identifying it as a known threat through one of multiple means, including local analysis, the ransomware protection module or a detailed analysis by WildFire.

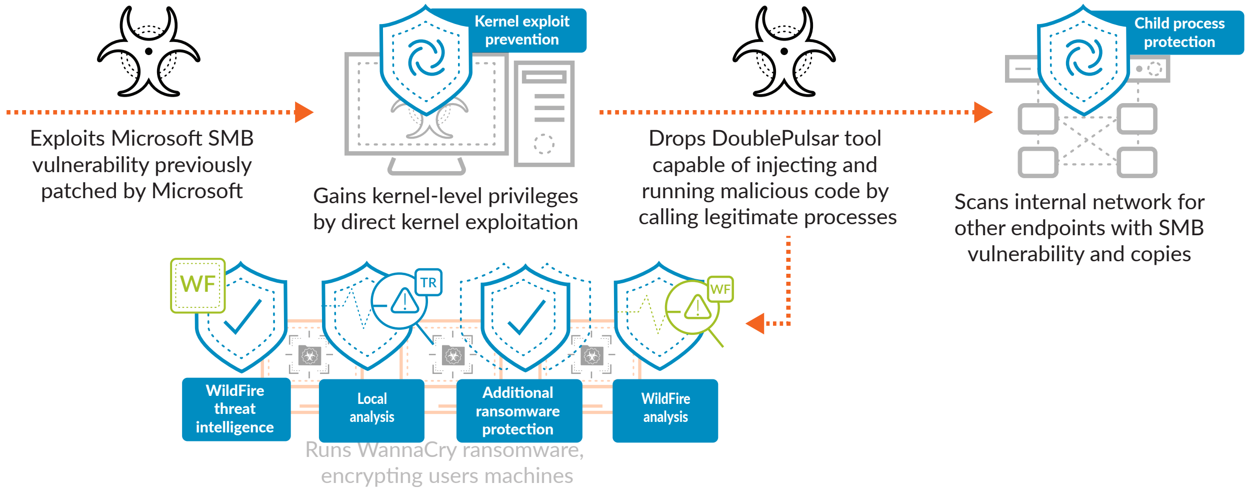
Exploits Microsoft SMB vulnerability previously patched by Microsoft
Kernel exploit prevention
Gains kernel-level privileges by direct kernel exploitation
Drops DoublePulsar tool capable of injecting and running malicious code by calling legitimate processes
Child process protection
Scans internal network for other endpoints with SMB vulnerability and copies
WF
TR
WF
WildFire threat intelligence
Local analysis
Additional ransomware protection
WildFire analysis
Runs WannaCry ransomware, encrypting users machines

Figure 3: Traps vs. WannaCry

During and after the outbreak, there were no known Palo Alto Networks customers infected by WannaCry as the threat had been submitted to WildFire almost a month before the May 12, 2017, attack on the U.K.'s National Health Service. When we look into AutoFocus™ contextual threat intelligence service, we see WannaCry was first discovered on April 16, 2017, at which time protections were created and distributed to all Palo Alto Networks devices and services.

To finish the job, an attacker must succeed at every stage of the attack lifecycle, whereas Traps only has to succeed in one stage to shut down the attack.

3. HIT PAUSE ON "PATCH TUESDAY"

Thousands of new software vulnerabilities and exploits are discovered each year, requiring diligent software patch distribution by software vendors on top of patch management by system and security administrators in every organization. This regular flow of patches and updates often lands on "Patch Tuesday," the monthly or semimonthly day when Microsoft releases security patches for its software.

Patching is a critical part of a sound endpoint protection strategy. However, patch management only protects an organization's endpoints after vulnerabilities are discovered and patched. Delays of days, weeks or longer are inevitable as patches for newly discovered vulnerabilities must be developed, distributed, tested and deployed. Although patch management is an important aspect of any information security program, much like signature-based anti-malware detection, it is an endless race against time that offers no protection against zero-day exploits. Vulnerability exploits, however, constitute the primary reason patches are applied.

A great deal of attention has been paid to malware since the earliest days of computing, and although malware prevention is critical to endpoint protection, it is only one part of a comprehensive endpoint security strategy. Exploit prevention is equally important but less understood.

Understanding Exploit Techniques

Many advanced threats work by placing malicious code in seemingly innocuous data files. When these files are opened, the malicious code leverages unpatched vulnerabilities in the native application used to view the file, and the code executes. Because the application being exploited is allowed by IT security policy, this type of attack bypasses application whitelisting controls.

Although there are many thousands of exploits, they all rely on a small set of core techniques that change infrequently. Regardless of the exploit or its complexity, for an attack to succeed, the attacker must execute a series of these core exploit techniques in sequence, like navigating a maze to reach the goal.

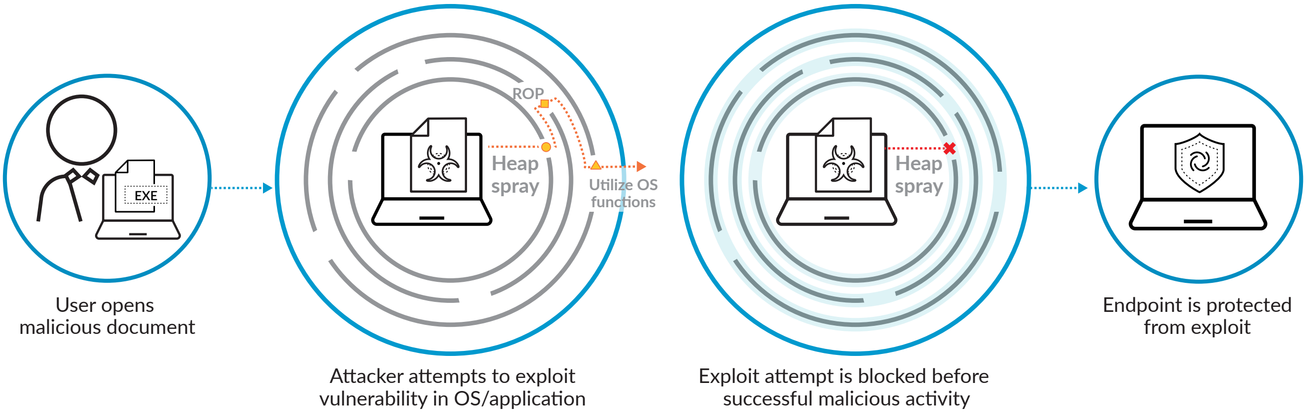
EXE
User opens malicious document
ROP
Heap spray
Utilize OS functions
Attacker attempts to exploit vulnerability in OS/application
Heap spray
Exploit attempt is blocked before successful malicious activity
Endpoint is protected from exploit

Figure 4: Focus on exploit techniques, not exploits themselves

Traps focuses on the core techniques all exploits use and, by rendering those techniques ineffective, negates application vulnerabilities whether they are patched or not.

Naturally, it's still best to keep up with the latest security patches. However, Traps gives you the option, and confidence, to hit "pause" on Patch Tuesday, knowing that Traps will continue protecting vulnerable applications. The Traps agent injects itself into individual processes as they start up. If a process attempts to execute any core attack technique, the corresponding exploit prevention module, or EPM, prevents that exploit, kills the process and reports details to Traps management service.

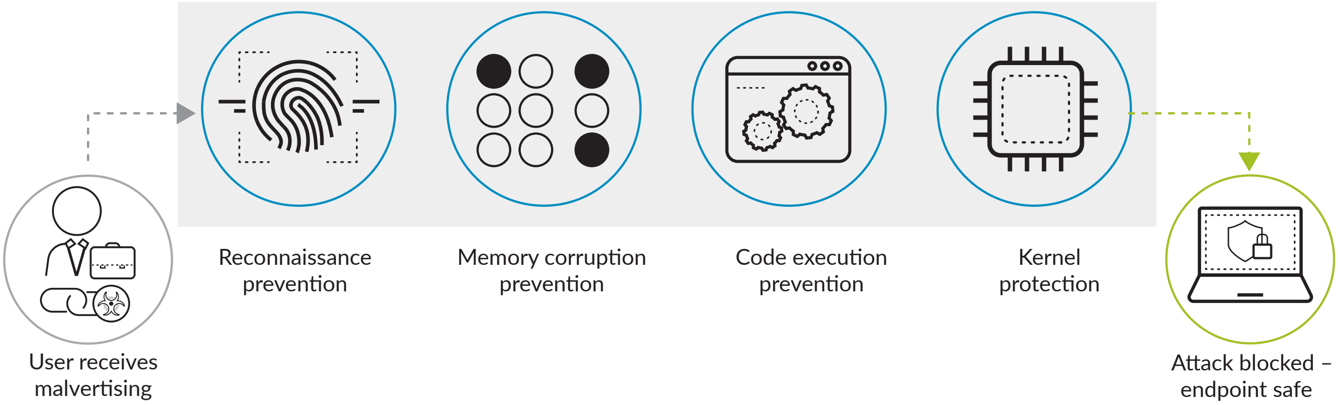
Reconnaissance prevention
Memory corruption prevention
Code execution prevention
Kernel protection
User receives malvertising
Attack blocked – endpoint safe

Figure 5: Multiple methods of exploit prevention

By default, Traps policies are configured to protect more than 100 processes, each with dozens of proprietary EPMs. Beyond the defaults, you can protect all manner of processes and applications by simply adding them to the policy configuration. Processes that have run on the endpoint automatically show up in the management console, making it easy to protect them with the click of a button. This is especially useful for organizations running industry-specific applications, such as point-of-sale systems, ATMs and SCADA systems.

A prevention-based endpoint protection strategy intercepts and blocks attacks before malicious activity occurs on endpoints. This means preventing an exploit from running or preventing malware from being executed. Such a proactive approach proves an ounce of prevention is worth a pound of cure.

4. PROTECT RESOURCE-SENSITIVE ENVIRONMENTS

Virtual endpoints and servers, whether in virtual desktop infrastructure, aka VDI, environments or cloud workloads, encounter the same security challenges as their physical counterparts. This has led to a slew of new challenges for the professionals tasked with securing them.

The frequent antivirus signature updates, application patches and operating system updates required to secure endpoints against known vulnerabilities are particularly challenging in virtual environments, where "golden images" are used to provision virtual endpoints. Many traditional physical endpoint products can create unforeseen complications when applied to virtual environments. Furthermore, purpose-built, virtual security products often leave gaps in the overall security architecture if they are not part of a cohesive security infrastructure.

A new approach is needed to protect virtual and cloud environments from the ground up – one that offers continuous protection without the need for signatures, patches or updates; integrates seamlessly into any virtual environment; and is part of an end-to-end security platform that encompasses physical, virtual and cloud computing environments.

No Patching or Signature Updates Required

To secure VDI and cloud workloads against known vulnerabilities, traditional security procedures require the most recent antivirus signatures, application patches and operating system updates after the initial boot from a golden image. This presents several technical and operational challenges.

For instance, the required updates increase network traffic, straining available bandwidth and system resources. Where immediate updates are not performed, administrators must schedule updates during off-peak hours, which is often challenging in organizations with 24/7 uptime requirements. After the initial boot up from a golden image, these endpoints and workloads remain vulnerable until all necessary security updates have been completed.

Traps prevents known and unknown exploits, as well as malicious executable files that target operating system and application vulnerabilities, without the need for signatures, patches or updates. It protects endpoints and servers – physical, virtual or in the cloud – from the moment they become available, making urgent patches to the golden image or live systems relics of the past.

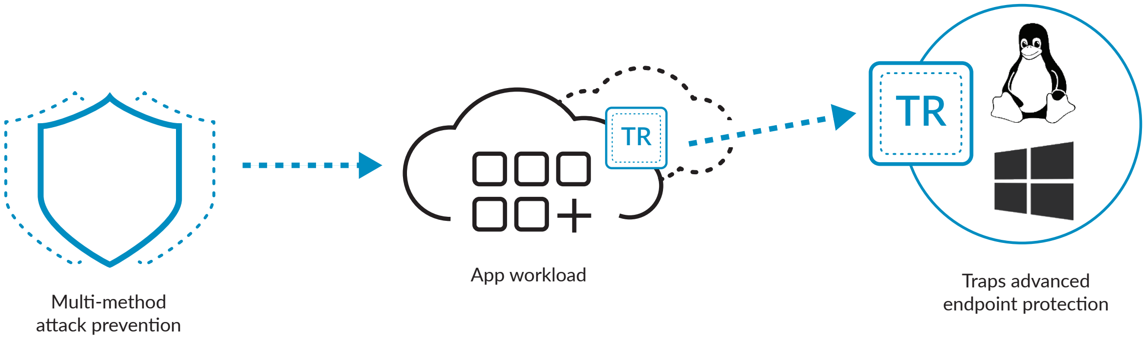

Figure 6: Cloud workload protection

Traditional security products, ill-suited for deployment in VDI and cloud environments, often create unforeseen technical and operational challenges. Presenting a new approach that eliminates many of these, Traps:

- Does not use signatures or require system patches/updates
- Protects VDI endpoints and servers from the moment they are initialized
- Features license elasticity and scalability, built into its architecture
- Performs no system scans and thus does not affect shared storage or end-user productivity
- Is fully integrated with the Security Operating Platform

Optimized for Virtual and Cloud Environments

Deploying security built for physical endpoints to protect virtual environments often introduces logistical and architectural challenges, such as requiring organizations to develop mechanisms to track and apply software and licenses as virtual instances are spun up or down.

Security must be able scale to accommodate thousands of simultaneous virtual sessions. In VDI environments where storage is shared among virtual sessions, organizations must mitigate the performance impact of system scans that are often at the core of "detective" security measures.

Traps is designed to work seamlessly in these environments, with license elasticity and the ability to scale to tens of thousands of endpoints built into its architecture.

5. PROTECT ENDPOINTS FROM DAY ONE

Deploying and managing endpoint protection shouldn't be difficult. However, customers of traditional endpoint protection products complain about day-to-day management, database maintenance, agent updates and constant tuning to eliminate false positives and keep resource utilization in check. Worst, even with all this work, endpoints still get compromised.

A customer who was evaluating Traps put it into "listen mode" to see if it would catch anything the customer's existing endpoint protection product could not. Within minutes of deploying agents, a domain controller lit up the Traps management service console with alerts. When the incident response team pulled up the console, they immediately identified a piece of targeted malware that had been running on that server for some time. This was an eye-opener, and the customer immediately realized the simplicity and power Traps offers, even from day one.

Traps Management Service

As new malware variants pop up around the globe, and as new software bugs and vulnerabilities are discovered, it can be challenging to ensure your endpoints remain secure. With the cloud-based Traps management service, you save the time and cost of building out your own global endpoint security infrastructure. Its simplified deployment requires no server licenses, databases or other infrastructure to get started, enabling you to start protecting your endpoints from day one.

Palo Alto Networks deploys and manages the Traps management service security infrastructure globally to manage the endpoint security policy for local and remote endpoints, ensuring the service is secure, resilient, up to date and available when you need it. This allows you to focus on defining the polices to meet your corporate usage guidelines instead of deploying and managing the infrastructure.

Traps management service comprises the following components:

- Traps management service web interface is a cloud-based security infrastructure service designed to minimize the operational challenges of protecting your endpoints. From the Traps management service, you can manage your endpoint security policy, review security events as they occur and perform additional analysis of associated logs.
- Traps agents protect each local or remote endpoint. The agent enforces your security policy on the endpoint and reports when it detects a threat. Agents communicate securely with Traps management service using Transport Layer Security 1.2.
- Logging Service is a cloud-based logging infrastructure that allows you to centralize the collection and storage of Traps agent logs, regardless of location. Traps agents and Traps management service forward all logs to the Logging Service. You can view these logs in Traps management service, and with the Log Forwarding app, you can forward logs to an external syslog receiver.

Integrated with Traps, WildFire malware prevention service identifies previously unknown malware and generates signatures that Palo Alto Networks next-generation firewalls and the Traps management service can use to detect and block the malware. When a Traps agent detects an unknown sample, Traps management service can automatically forward it to WildFire for analysis. Based on the properties, behaviors and activities the sample displays when analyzed and executed in the WildFire sandbox, WildFire delivers a verdict: benign, grayware, phishing or malicious. WildFire then generates signatures to recognize any newly discovered malware and makes the signatures globally available in as few as five minutes.

Traps management service provides out-of-the-box protection for all registered endpoints, with a default security policy for each type of platform.

Traps Security Profiles

Out of the box, Traps management service provides default security profiles you can use to begin protecting your endpoints from threats immediately. Although security rules enable you to block or allow execution of files on your endpoints, security profiles help you customize and reuse settings across different groups of endpoints. When Traps detects a behavior that matches a rule defined in your security policy, it applies the security profile attached to the rule for further inspection. You can enjoy immediate protection with multiple security profiles:

- **Exploit profiles** block attempts to exploit system flaws in browsers and operating systems. These help protect against exploit kits, illegal code execution, and other attempts to exploit process and system vulnerabilities.
- **Malware profiles** protect against the execution of malware, including Trojans, viruses, worms and grayware. Malware profiles serve to define how to treat behavior common with malware, such as ransomware or script-based attacks, and how to treat known malware and unknown files.
- **Restrictions profiles** limit where executable files can run on an endpoint. For example, you can restrict files from running from removable media or specific, local folders.
- **Agent settings profiles** let you customize settings that apply to the Traps application, such as the disk space quota for log retention. For Mac® and Windows® platforms, you can also customize user interface options for the Traps console, such as accessibility and notifications.

Conclusion

Security built solely to protect virtual endpoints often lacks the broader contextual intelligence critical to effective enterprise security architecture. Integrated threat intelligence, including data on the tactics, techniques and procedures of new and previously seen cyberattacks, is often critical to successfully defend systems and networks.

As an integral part of the Palo Alto Networks Security Operating Platform, Traps prevents cyberattacks automatically and in real time, regardless of the nature of the endpoints and the systems you have deployed. In concert with WildFire, Traps and the entire Security Operating Platform benefit from increased contextual visibility into – and protection against – correlated threat actors and campaigns, wherever they may try to attack.

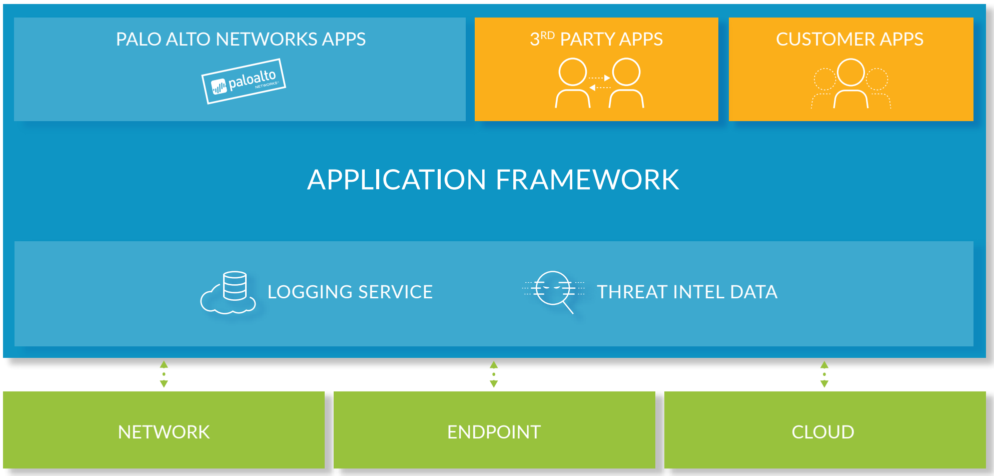

Figure 7: Palo Alto Networks Security Operating Platform

Customers depend on Traps to ensure endpoints are protected, whether online or off, on-site or remote. IT teams must be able to confidently apply policies that control access to critical resources, and you need confidence in the integrity and configuration of the devices being used to connect to your network, whenever and wherever that may be. Protection cannot depend on full-time network access – it should just work, out of the box, from day one.

For more information about Traps, please visit www.paloaltonetworks.com/traps.

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