TRAPS

Advanced Endpoint Protection

Palo Alto Networks Traps replaces traditional antivirus with multi-method prevention, a proprietary combination of purpose-built malware and exploit prevention methods that protect users and endpoints from known and unknown threats. Traps prevents security breaches, in contrast to breach detection and incident response after critical assets have already been compromised.

Traps Advanced Endpoint Protection:

- **Prevents cyber breaches** by preemptively blocking known and unknown malware, exploits and zero-day threats.
- **Protects and enables users** to conduct their daily activities and use web-based technologies without concern for known or unknown cyberthreats.
- **Automates prevention** by autonomously reprogramming itself using threat intelligence gained from WildFire.

Most organizations deploy a mixture of security solutions to protect their endpoint systems, including one or more traditional antivirus solutions. With the proliferation of free and low-cost tools, threat actors can now generate new and unique attacks that evade signature-based antivirus. Current endpoint security solutions and antivirus cannot protect users and systems against evasive, unknown or zero-day attacks.

Palo Alto Networks® Traps™ advanced endpoint protection, with its unique combination of the most effective, purpose-built, malware and exploit prevention methods, prevents known and unknown threats before they compromise an endpoint.

Traps Multi-Method Malware Prevention

Traps prevents malicious executables with a unique, multi-method prevention approach that maximizes the coverage against malware while simultaneously reducing the attack surface and increasing the accuracy of malware detection. This approach combines several prevention methods to instantaneously prevent known and unknown malware from infecting a system (Figure 1).

Admin Override Policies
Trusted Publisher
WF
WildFire Inspection and Analysis
Static Analysis via Machine Learning
Execution Restrictions

Figure 1: Traps Multi-Method Malware Prevention

1. **Static Analysis via Machine Learning:** This method delivers an instantaneous verdict for any unknown executable file before it is allowed to run. Traps examines hundreds of the file's characteristics in a fraction of a second, without reliance on signatures, scanning or behavioral analysis.
2. **WildFire Inspection and Analysis:** This method leverages the power of Palo Alto Networks WildFire™ cloud-based malware analysis environment to rapidly detect unknown malware and automatically reprogram Traps to prevent known malware. WildFire eliminates the threat of the unknown by transforming it into known in about 300 seconds.
3. **Trusted Publisher Execution Restrictions:** This method allows organizations to identify executable files that are among the "unknown good" because they are published and digitally signed by trusted publishers—entities that Palo Alto Networks recognizes as reputable software publishers.
4. **Policy-Based Execution Restrictions:** Organizations can easily define policies to restrict specific execution scenarios, thereby reducing the attack surface of any environment. For example, Traps can prevent the execution of files from the Outlook® "temp" directory or prevent the execution of a particular file type directly from a USB drive.
5. **Admin Override Policies:** This method allows organizations to define policies, based on the hash of an executable file, to control what is allowed to run in any environment and what is not. This fine-grained whitelisting (or blacklisting) capability controls the execution of any file, based on user-defined conditions that tie into any object that can be defined with Microsoft® Active Directory®.

Any executable file that is deemed to be malicious and prevented from running on the endpoint is quarantined in a protected repository accessible only to system administrators. Traps administrators can review quarantined files, delete them, or restore them to their original location on their respective endpoints, if necessary.

Traps Multi-Method Exploit Prevention

Traps uses an entirely new and unique approach to prevent exploits. Instead of focusing on the millions of individual attacks, or their underlying software vulnerabilities, Traps focuses on the core exploitation techniques used by all exploit-based attacks. Each exploit must use a series of these exploitation techniques to successfully subvert an application. Traps renders these techniques ineffective by blocking them the moment they are attempted. Organizations using Traps can run any application, including those developed in-house and those that no longer receive security support, without the imminent threat to their environment.

Traps implements a multi-method approach to exploit prevention, combining several layers of protection to block exploitation techniques (Figure 2):

Memory Corruption Prevention
Logic Flaw Prevention
Malicious Code Execution Prevention

Figure 2: Traps Multi-Method Malware Prevention

1. **Memory Corruption Prevention:** Traps prevents the exploitation techniques that manipulate the operating system's normal memory management mechanisms for the application that opens the weaponized data file containing the exploit.
2. **Logic Flaw Prevention:** Traps recognizes and blocks the exploitation techniques that allow an exploit to manipulate the operating system's normal application process and execution mechanisms.
3. **Malicious Code Execution Prevention:** In most cases, the end goal of exploitation is to execute the attacker's commands that are embedded in the exploit file. This prevention method recognizes the exploitation techniques that allow the attacker's malicious code to execute and blocks them before they succeed.

Next-Generation Security Platform

With the ever-decreasing cost of computing power, threat actors can launch increasingly numerous and sophisticated attacks with far greater ease than ever. Disjointed layers of security, and point solutions that rely on obsolete technologies or human response to alerts, are no longer sufficient or scalable. Only a platform that consolidates, automates and natively integrates multiple preventive technologies can ensure the prevention of advanced, targeted and evasive attacks.

The native integration of Traps with the Palo Alto Networks Next-Generation Security Platform enables organizations to continuously share the growing threat intelligence gained from thousands of enterprise customers across both networks and endpoints to coordinate prevention and response. The automatic reprogramming and conversion of threat intelligence into prevention all but eliminates the opportunity for an attacker to use unknown and advanced malware to infect a system. An attacker can use each piece of malware once, at most, anywhere in the world and only has seconds to carry out an attack before WildFire renders it entirely ineffective.

System Requirements and Platform Support

Traps protects unpatched systems and is supported across any platform that runs Windows®: desktops, servers, industrial control systems, virtual desktop infrastructure (VDI) components, virtual machines (VM), and embedded systems (Figure 3).

Operating Systems	
Windows XP (32-bit, SP3 or later)	
Windows Vista (32-bit, 64-bit, SP1 or later; FIPS mode)	
Windows 7 (32-bit, 64-bit, RTM and SP1; FIPS mode; all editions except Home)	
Windows Embedded 7 (Standard and POSReady)	
Windows 8 (32-bit, 64-bit)	
Windows 8.1 (32-bit, 64-bit; FIPS mode)	
Windows Embedded 8.1 Pro	
Windows 10 Pro (32-bit and 64-bit)	
Windows 10 Enterprise LTSB	
Windows Server 2003 (32-bit, SP2 or later)	
Windows Server 2003 R2 (32-bit, SP2 or later)	
Windows Server 2008 (32-bit, 64-bit; FIPS mode)	
Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode)	
Windows Server 2012 (all editions; FIPS mode)	
Windows Server 2012 R2 (all editions; FIPS mode)	
Virtual Environments	
VMware ESX	Oracle Virtualbox
Citrix XenServer	Microsoft Hyper-V
Virtual Desktop Infrastructure	
VMware Horizon View	Citrix XenDesktop
Physical Platforms	
SCADA	ATM
Windows Tablets	POS
Run-Time Footprint	
0.1% CPU Load	250 MB Disk Space
50 MB RAM	

Figure 3: Traps System Requirements and Platform Support

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com