Traps: Advanced Endpoint Protection

TRAPS:

Advanced Endpoint Protection should deliver on the following:

- Prevent all exploits, including those utilizing unknown Zero Day vulnerabilities.
- Prevent all malicious executables, without requiring any prior knowledge
- Provide detailed forensics against prevented attacks
- Highly scalable, lightweight and seamless with minimal to no disruption
- Integrate closely with network and cloud security

Palo Alto Networks® Traps™ provides Advanced Endpoint Protection that prevents sophisticated vulnerability exploits and unknown malware-driven attacks. Traps accomplishes this through a highly scalable, lightweight agent that uses an innovative new approach for defeating attacks without requiring any prior knowledge of the threat itself. By doing so, Traps provides organizations with a powerful tool for protecting endpoints from virtually every targeted attack.

Despite a plethora of endpoint security products on the market, endpoints are still being infected at an alarming rate. Traditional endpoint protection solutions use methods that simply cannot keep up with the rapidly evolving threat landscape. Instead of looking to identify the millions of individual attacks themselves, or detect malicious behavior that may be undetectable, Traps focuses on the core techniques that every attacker must link together in order to execute their attack. With this approach, Traps can thwart the attack before any malicious activity can successfully run.

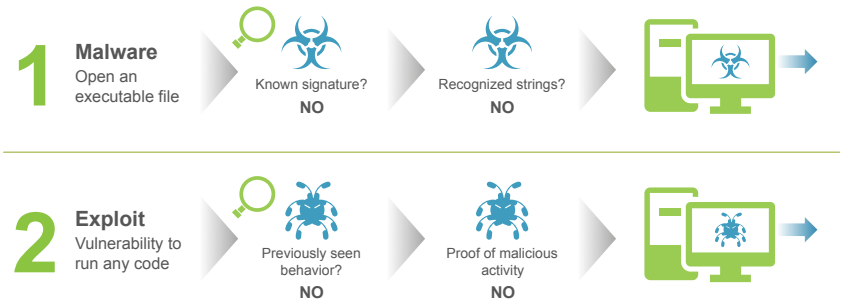

Figure 1: The failures of traditional security approaches

Multiple Types of Attack, Complete Protection

Attacks come in different forms and can arrive via multiple vectors including web, e-mail, and external storage. Most traditional endpoint security products protect endpoints from malicious executable files, which are the least sophisticated form. Some of the most advanced and targeted attacks arrive in the form of seemingly harmless data files that are opened by legitimate applications. For example, malicious code can be implanted in a Microsoft Word or PDF document- also known as an exploit. Traps protects endpoints by preventing malware in the form of executables and exploits in the form of data files or network-based attacks.

The most advanced threats these days leverage vulnerabilities in software that we use on a regular basis. They often come in the form of commonly used data files (pdf, rtf, doc, ppt, xls, etc.) or can be individually crafted to target proprietary software used in various industries.

paloalto networks

Once the file is opened, the malicious code takes advantage of a vulnerability in the legitimate application being used to view the file, allowing it to execute code and take full control of the endpoint.

How Exploit Prevention Works

Regardless of the attack or its complexity — in order for the attack to be successful the attacker must execute a series exploit techniques in sequence. Some attacks may involve more steps, some may involve less, in all cases at least two or three techniques must be used in order to exploit the targeted endpoint. Traps employs a series of exploit prevention modules aimed at mitigating and blocking the different exploit techniques available to attackers. Furthermore, each exploit needs to use a series of those techniques in order to be successful. Traps renders these techniques completely ineffective, which means the application is no longer vulnerable.

The Traps agent injects itself into each process as it is started. If the process attempts to execute any of the core attack techniques, the exploit attempt will fail because Traps had made the process impervious to those techniques. Traps will immediately block that technique, terminate the process, and notify both the user and the admin that an attack was prevented and report all of the details to the Endpoint Security Manager (ESM). Due to the chain-like nature of an exploit, preventing just one technique in the chain is all that is needed in order to block the entire attack.

By default, Traps policy is set to protect over 100 processes — each one with dozens of proprietary EPMs (Exploit Prevention Modules).

But unlike other products, Traps is not limited to protecting only those processes or applications.

By focusing on the exploit techniques and not the attack itself, Traps can prevent the attack without prior knowledge of the vulnerability, regardless of patches in place, and without signatures or software updates. It's important to note that Traps isn't scanning or monitoring for malicious activity, so there's a massive scalability benefit to this approach as very little CPU and memory are used.

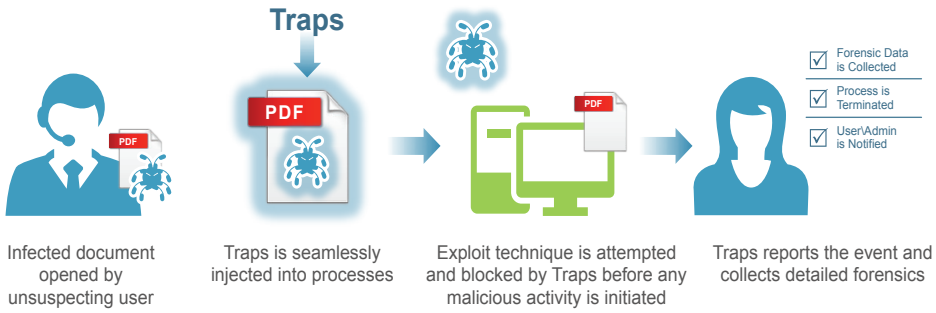

Figure 2: Exploit prevention – user experience

Preventing Malicious Executables

In addition to preventing exploits, Traps employs a multi-layered approach to the prevention of malicious executables by focusing on three key areas to ensure comprehensive protection. When combined, these methods offer unparalleled malware prevention and include:

1. **Policy-Based Restrictions:** Organizations can easily set up policies restricting specific execution scenarios. For example, you may want to prevent the execution of files from the Outlook tmp directory, or prevent execution of a particular file type directly from a USB drive.
2. **WildFire™ Inspection & analysis:** Traps queries the WildFire threat cloud with a hash and submits any unknown .exe files to assess their standing within the global threat community.
3. **Malware Techniques Mitigation:** Traps implements technique-based mitigations that prevent attacks by blocking techniques such as thread injection.

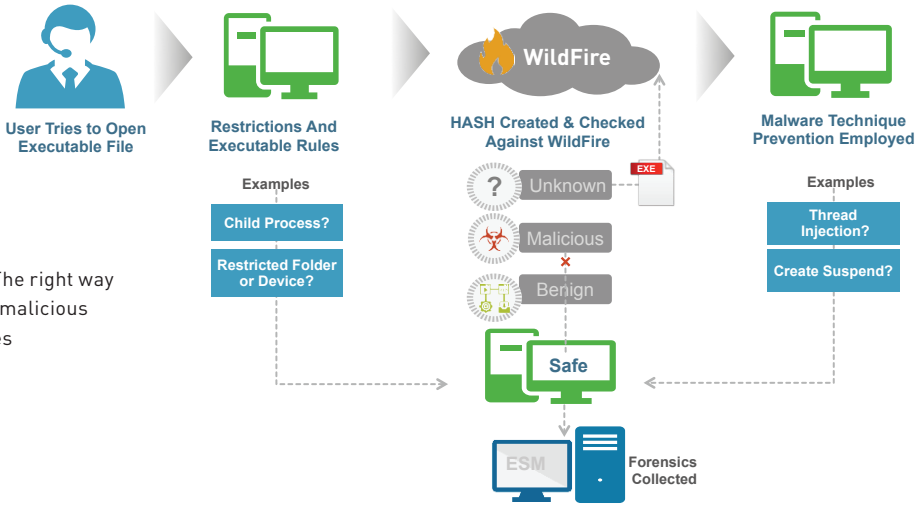

Figure 3: The right way to prevent malicious executables

Forensics

Forensic information available after an attack has been prevented is unavoidably less than the information available about an attack that has succeeded and done damage. Despite that, there is still a great amount of intelligence that can be gathered. By capturing all the forensics of the attempted attack, organizations can apply proactive defenses to other endpoints that may not be protected.

Extensive data is gathered from the Traps agent. The agent records details on an ongoing basis, about each process that was run and reports the logged information to the Endpoint Security Manager (ESM). The agent will also alert if there are any attempts to stop, remove, or otherwise tamper with Traps. When an attack is prevented, further detail can be gathered from the endpoint, including a full memory dump and information about the activities attempted by the malicious code.

Traps Deployment Architecture

Endpoint Security Manager – Console

The Traps infrastructure supports various architectural options to allow for scalability to large distributed environment. Installation of the ESM creates a database on a Microsoft SQL server and installs the administrative console within IIS. Microsoft SQL 2008 and 2012 are supported and the SQL server may be dedicated to ESM or a database can be created on an existing SQL server.

Endpoint Security Manager – Servers

ESM servers essentially act as proxies between Traps agents and the ESM database. Communications from Traps agents to ESM servers occur over HTTPS. ESM servers do not store data and therefore can be easily added and removed from the environment as needed to ensure adequate geographic coverage and redundancy.

Traps Agent

The Traps agent installer is a ~9 MB MSI package that can be deployed using your software deployment tool of choice. Subsequent updates to the agent can be deployed via the ESM. The agent consumes less than 25 MB on disk and less than 40 MB while running in memory. Observed CPU utilization is less than 0.1 percent. The agent employs various tamper proofing methods that prevent users and malicious code from disabling protection or tampering with agent configuration.

The lightweight structure allows for the Traps environment to scale horizontally and support large deployments of up to 50,000 agents per ESM while still maintaining a centralized configuration and database for policies. Traps can co-exist with most major endpoint security solutions, and the CPU utilization and I/O remains incredibly low. With such minimal disruption this makes Traps optimal for critical infrastructures, specialized systems, and VDI environments.

External Logging

The ESM can write logs to an external logging platform, such as SIEM, SOC or syslog, in addition to storing its logs internally. For an organization that deploys multiple ESMs, an external logging platform allows an aggregated view those log databases.

Coverage and Platform Support

Traps protects unpatched systems and is supported across any platform that runs Microsoft Window; desktops, servers, industrial control systems, terminals, VDI, VMs and embedded systems etc. Furthermore, Traps is extremely lightweight and is extensible to protect any application process, making it ideal for protection of specialized systems including ATM, POS, SCADA and many other industrial applications requiring non-intrusive protection of proprietary processes.

Traps currently supports the following Windows-based operating systems:

OPERATING SYSTEM:

- Windows XP (32-bit, SP3 or later)
- Windows 7 (32-bit, 64-bit, RTM and SP1; all editions except Home)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows Server 2003 (32-bit, SP2 or later)
- Windows Server 2003 R2 (32-bit, SP2 or later)
- Windows Server 2008 (32-bit, 64-bit)
- Windows Server 2012 (all editions)
- Windows Server 2012 R2 (all editions)
- Windows Vista (32-bit, 64-bit, and SP2)

VIRTUAL ENVIRONMENTS:

- VDI
- Citrix
- VM
- ESX
- VirtualBox/Parallels

PHYSICAL PLATFORMS:

- SCADA
- Windows Tablets

paloalto networks
the enterprise security company™

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