Zero Trust on the Endpoint

Extending the Zero Trust Model from Network to Endpoint with Advanced Endpoint Protection

March 2015

Executive Summary

The Forrester Zero Trust Model (Zero Trust) of information security advocates a "never trust, always verify" philosophy in protecting information resources. Though the model has traditionally been applied to network communications, it is clear that today's cyber threats warrant a new approach in which the Zero Trust model is extended to endpoints. Palo Alto Networks® Traps™ Advanced Endpoint Protection is an innovative endpoint protection technology that prevents exploits and malicious executables, both known and unknown. It has the proven capacity to act as the enforcer for Zero Trust and to serve as a vital component of an enterprise's security architecture and compliance suite on the endpoint.

What is the Zero Trust Concept?

The Zero Trust Model developed by Forrester Research seeks to change the paradigm by which many organizations think about defending the enterprise information infrastructure. Zero Trust is intended to remedy the deficiencies with perimeter-centric strategies and the legacy devices and technologies used to implement them. It does this by promoting "never trust, always verify" as its guiding principle.

In particular, with Zero Trust there is no default trust for any entity — including network segments, users, devices and applications. In addition, verifying that authorized entities are always doing only what they are allowed to do is a requirement.

The implications for these two changes are, respectively:

a) The enterprise must establish trust boundaries that effectively compartmentalize different segments of the internal computing environment. The general idea is to move security controls closer to the resources that require protection.

b) Trust boundaries must do more than just initial authorization and access-control enforcement.

To "always verify" also requires ongoing monitoring and inspection of associated communications traffic for subversive activities (i.e. threats).

The core Zero Trust principle and derivative implications are further reflected and refined in the three concepts that define the operational objectives of a Zero Trust implementation.

Concept #1: Ensure that all resources are accessed securely regardless of location. This suggests not only the need for multiple trust boundaries, but also increased use of secure access for communication to/from resources, even when sessions are confined to the "internal" network. It also means ensuring that only devices with the right status and settings (e.g., ones that are compliant with security policy) are allowed access to the network.

Concept #2: Adopt a least-privilege strategy and strictly enforce access control. The goal in this case is to absolutely minimize authorized access to resources in order to reduce the pathways available for malware and attackers to gain unauthorized access and subsequently spread laterally and/or exfiltrate sensitive data.

Concept #3: Inspect and log all traffic. This reiterates the need to "always verify" while also making it clear that adequate protection requires more than just strict enforcement of access control. Close and continuous attention must also be paid to exactly what is happening in "allowed" applications, and the only way to do this is to inspect the content for threats.

Zero Trust and the Endpoint

The Zero Trust network concepts outlined above are necessary but not sufficient to combat today's advanced cyber threats. The same rigor must be applied on the endpoint, on the OS, on connected devices, and in memory. This is particularly important, as most resources an attacker might be interested in — data and applications — will live on the endpoint. For the purposes of this paper, the endpoint is defined as: any computing device or platform potentially subject to attack.

Traps and Zero Trust

Palo Alto Networks Traps Advanced Endpoint Protection is designed to proactively block attacks targeting endpoints, including unknown malicious executables and zero-day exploits. Traps automatically detects and blocks a core set of techniques that every attacker must link together in order to execute any type of attack, regardless of its complexity. 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, allowing companies to stop malicious attempts before they can do any damage.

The Trap's agent injects itself into each process as it is started. This will automatically trigger and block advanced attacks that would otherwise evade detection.

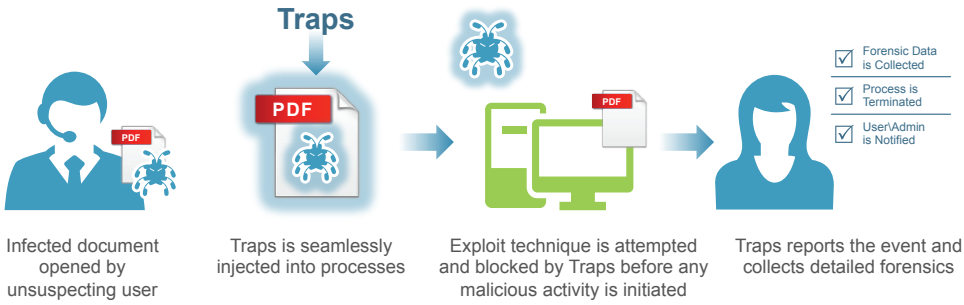

Figure 1: Traps blocks a core set of techniques to stop advanced attacks before they happen

If an exploit attempt is made using one of the attack techniques, Traps immediately blocks that technique, terminates the process, and notifies both the user and the admin that an attack was prevented. Throughout each event, Traps collects detailed forensics and reports this information to the Endpoint Security Manager (ESM), resulting in better visibility and an understanding of attacks that were prevented. With Traps, endpoints are always protected, regardless of patch, signature or software-update levels; plus, it requires no prior knowledge of an attack in order to prevent it.

To prevent the execution of malicious executables on the endpoint, Traps focuses 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 the execution of a particular file type directly from a USB drive.

2. **WildFire™ inspection and analysis:** Traps queries the WildFire threat intelligence 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.

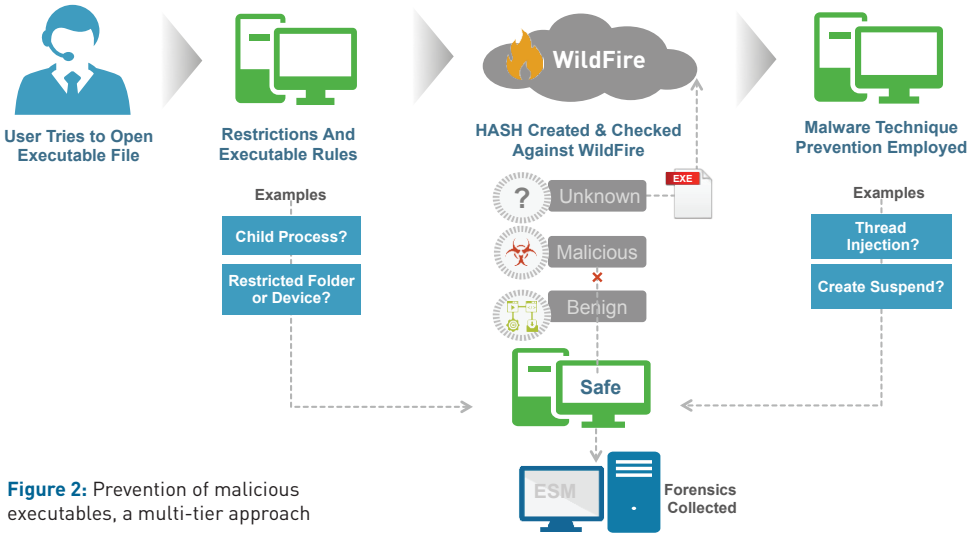

Figure 2: Prevention of malicious executables, a multi-tier approach

Traps fits into the Zero Trust model by operating deep within the operating system and persistently enforcing the Zero Trust concept. No application or attached device should be trusted on the endpoint. Many endpoint security approaches begin by trusting everything and monitoring for known patterns or malicious behaviors, while others attempt to whitelist trusted applications and block all others. Both of these methodologies fall short of implementing Zero Trust on the endpoint, which must be done on multiple levels:

- **Do not trust unknown applications:** Executables that have never been seen on the endpoint before should not be trusted. This concept can be applied in two ways:
  - **Static Whitelisting:** The administrator can establish a static list of approved applications or digital signers that are allowed to run on the endpoint.
  - **Dynamic Analysis:** The endpoint agent integrates with a dynamic analysis engine that analyzes new executables to determine if they are malicious or not. By leveraging the dynamic-analysis capabilities of WildFire, organizations gain the advantages of the massive scale of this cloud-based threat intelligence service without the need to manage static whitelisting.
- **Do not trust known applications:** Whitelisting is not enough. Trusted applications have vulnerabilities that can be exploited by attackers. In order to have Zero Trust on the endpoint, exploitation of trusted applications must be prevented. This involves multiple methods including:
  - **Exploit Prevention:** The exploit prevention in Traps can be applied to any application, including proprietary, legacy, and industry-specific applications.
  - **Child Process Blocking:** Some applications should not be allowed to create child processes. This can be enforced by Traps.
- **Do not trust external media:**
  - Prevent execution from removable media.

The Palo Alto Networks Enterprise Security Platform, which includes Traps Advanced Endpoint Protection, the next-generation firewall, and the WildFire threat-intelligence cloud, enables full implementation of Zero Trust from network to endpoint.

Conclusion

In a dynamic and constantly evolving threat environment, it is clear that the enterprise can no longer rely on static defenses. A tight perimeter is no longer an option. Zero-day attacks easily bypass signature-based defenses, and social engineering can readily trick users into executing malware using "trusted" credentials. Leveraging the Zero Trust model as part of a comprehensive security architecture provides enterprise architects and administrators with a better way to organize and connect their defenses. Palo Alto Networks Traps Advanced Endpoint Protection enables Zero Trust by preventing the execution of malicious executables and exploits, without depending on pre-existing signatures or assuming that a user or application is trusted.

For more information regarding the Palo Alto Networks Enterprise Security Platform and its component technologies, please visit **www.paloaltonetworks.com**.

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