INFO & INSIGHTS

# SCANNING SHOULDN'T BE FIRST IN YOUR ENDPOINT ARTILLERY

**Antivirus has undoubtedly been the default solution for protecting endpoints for decades.** Most antivirus solutions will scan the endpoint, cross-referencing files against a signature database of known threats. While adequate for identifying known threats, scanning technology cannot keep up with the advanced threats targeting endpoints today. Below are the four primary reasons why scanning shouldn't be your first line of defense when securing endpoints.

1. **Reliance on Signature Database**

   In the current threat landscape, malware can change at breakneck speed, meaning signature databases need continuous updates of the most recent signatures to avoid becoming outdated. Like scanning, these updates can reduce system performance. Antivirus solutions often allow users to schedule updates for more convenient times, but this can leave databases outdated for extended periods, during which threats can easily bypass and evade detection by scanners.

2. **Identifies Only Known Threats**

   Scanners are limited to what is already known about a sample. Anything unknown – such as zero-day threats or polymorphic malware – goes undetected. Attackers often make slight modifications to existing threats that let them bypass detection from scanning engines, resulting in polymorphic malware, or variants. These variants require entirely new signatures in order to be detected, rendering scanners useless. Creating new signatures is labor-intensive, and cannot keep pace with the rate at which attackers can modify threats.

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

3. **Performance Impact**

   Antivirus solutions periodically scan for malicious files or threats, regardless of system activity at the time. This consumes significant resources, eating into disk space and slowing down devices. To minimize impact, users often bypass or reschedule scans, change scanning frequency, or deactivate antivirus entirely. While any of these actions can temporarily avoid performance degradation, they leave systems vulnerable to malware that previous scans may not have detected. Additionally, periodic scanning increases the risk of missing malware introduced to the system between scans.

4. **Files at Rest Not Seen as Threats**

   Malicious files pose no actual threat to a system until they are executed. Antivirus solutions scan for potentially malicious files, greatly impacting performance searching for things that are not threatening the system.

Palo Alto Networks® Traps™ advanced endpoint protection uses a multi-method approach to malware prevention, protecting against the evolving threat landscape and addressing the concerns antivirus scanners present, all without relying on signatures. Traps integrates with WildFire™ cloud-based threat analysis service to prevent known, unknown and zero-day threats, focusing on malware as it becomes active, rather than consuming system resources for dormant activity.

When a piece of malware is identified anywhere in the WildFire community, WildFire automatically creates and shares preventive measures to all Traps-protected endpoints. This ensures Traps prevents known or newly identified malware without requiring periodic updates. If a file has never been seen before, Traps uses static analysis to determine if the file contains malicious characteristics and delivers a verdict within a fraction of a second. WildFire is also the industry's most advanced anti-evasion malware sandbox, with a bare metal analysis environment for full hardware execution. Traps, integrated with WildFire, can identify and prevent even the most evasive threats.

To learn more about Traps and its multi-method malware prevention as an alternative to scanning, visit https://www.paloaltonetworks.com/products/secure-the-endpoint/traps.

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.