Enterprise Strategy Group™ by TechTarget

SHOWCASE

FEBRUARY 2024

Strengthening Ransomware Prevention Through Hardware and Software Security Collaboration

Dave Gruber, Principal Analyst

Abstract: Malware is getting more advanced. Despite continuing investments in a variety of security solutions aimed at detecting and stopping attacks, ransomware is evading security controls. Earlier detection within the attack chain is needed. TechTarget's Enterprise Strategy Group believes that more active collaboration between security mechanisms is required to achieve earlier detection and prevention. Check Point and Intel are working together to combine software- and hardware-based threat detection to strengthen prevention capabilities.

Overview – The Problem

Ransomware attacks continue to be pervasive, disrupting organizations of every size, both operationally and financially. Three-quarters of organizations report experiencing an attempted ransomware attack within the past 12 months, with 27% indicating that attacks happened on a weekly basis or even more frequently.[1] Mitigating this persistent threat is challenging for most, as only one in six organizations (16%) that have been the victims of at least one successful ransomware attack reported that they were able to fully restore their data after the attack(s). It follows then that nearly two-thirds (65%) of survey respondents in this same research survey consider it one of the top three most serious threats to the viability of their organization.

The Ransomware Threat Persists

Despite continuing investments in a variety of security solutions aimed at detecting and stopping attacks, ransomware and other advanced attacks are successfully evading security controls.

As malware evolves and becomes more sophisticated, ransomware and other advanced attacks are successfully evading security controls. Security solutions must therefore detect these attacks sooner within the attack chain to protect against operational disruption.

While software-based endpoint security tools have set the standard for endpoint security solutions to date, TechTarget's Enterprise Strategy Group believes that more active collaboration is needed between security mechanisms to achieve earlier ransomware detection and prevention. Enterprise Strategy Group sees a specific opportunity for software-based security solutions to collaborate with hardware-based threat detection mechanisms to achieve faster ransomware detection.

Check Point and Intel are working together to combine software- and hardware-based threat detection to strengthen prevention capabilities. This paper explores the collaboration between Check Point and Intel and outlines how it is making a difference in detecting ransomware as well as other advanced threats.

[1] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.

This Enterprise Strategy Group Showcase was commissioned by Check Point Software and is distributed under license from TechTarget, Inc.

Security Is a Cat-and-Mouse Process

One of the ways in which malware is advancing is in its ability to avoid detection, motivating adversaries to understand and evade available endpoint security solutions. The thriving criminal cyber-economy goes to great lengths to acquire and understand the capabilities and limitations of each individual security solution available. This process helps them find techniques to evade controls, enabling the execution of malicious activities.

This cat-and-mouse process offers bad actors an avenue to fly under the radar while carrying out malicious activities. But despite these crafty techniques, malware is software and therefore *must* execute on the microarchitecture to succeed. So, while attackers have become adept at crafting malware that seeks to avoid detection, it still leaves a “fingerprint” on the hardware.

CPU Threat Detection

Malware is software and therefore *must* execute on the microarchitecture to succeed. So, while attackers have become adept at crafting malware that seeks to avoid detection, it still leaves a “fingerprint” on the hardware.

This creates an opportunity to detect the presence of malware from the hardware level, making detection very difficult to evade. It further creates an opportunity for defense mechanisms to gain an advantage, by monitoring the execution characteristics at the microarchitectural level of the silicon executing the malware payload instructions.

How Hardware-based Detections Work

Ransomware encryption, hashing used in cryptomining, and other advanced attacks have recognizable execution patterns at the microarchitecture level. This creates an opportunity to make use of unique capabilities within the hardware to craft malware detection within their solutions.

Enter Intel® Threat Detection Technology

Intel recognized this opportunity and created Intel Threat Detection Technology (Intel® TDT) to detect these patterns. Unique to the Intel platform, Intel TDT adds a hardware “eye” to malware monitoring, helping to boost detection efficacy. Applying machine learning (ML) models to runtime microarchitectural data from the chip, Intel TDT derives high-fidelity malware execution detections that are highly resistant to evasion.

Intel TDT Origins: Intel Performance Monitoring Unit

Previously available for many years, the Intel Performance Monitoring Unit (PMU) gathers low-level microarchitectural execution data as the CPU executes instructions from the software entities running on it.

First introduced in support of performance monitoring, debugging, and optimization, the PMU helped engineers profile and tune specific workloads. Intel recognized an opportunity to leverage the PMU to detect malicious activity, which resulted in the creation of Intel TDT.

Today, Intel CPUs support hundreds of such performance monitoring events, allowing for highly tuned fine-grained runtime profiling of malware execution. Monitoring for specific execution sequence enables Intel TDT to recognize these attacks. Examples of telemetry made available by the PMU that can be used to profile malware execution include number of instructions executed; branches executed; and execution data related to cache, memory access, etc.

The Intel TDT ML function is offloaded to the integrated GPU for both overhead reduction and efficiency gains. Because in most enterprise applications the GPU is not heavily loaded, there is GPU bandwidth available. Ongoing advancements in Intel’s iGPUs further improve the efficacy and efficiency of Intel TDT’s models over time.

Check Point Harmony and Intel TDT

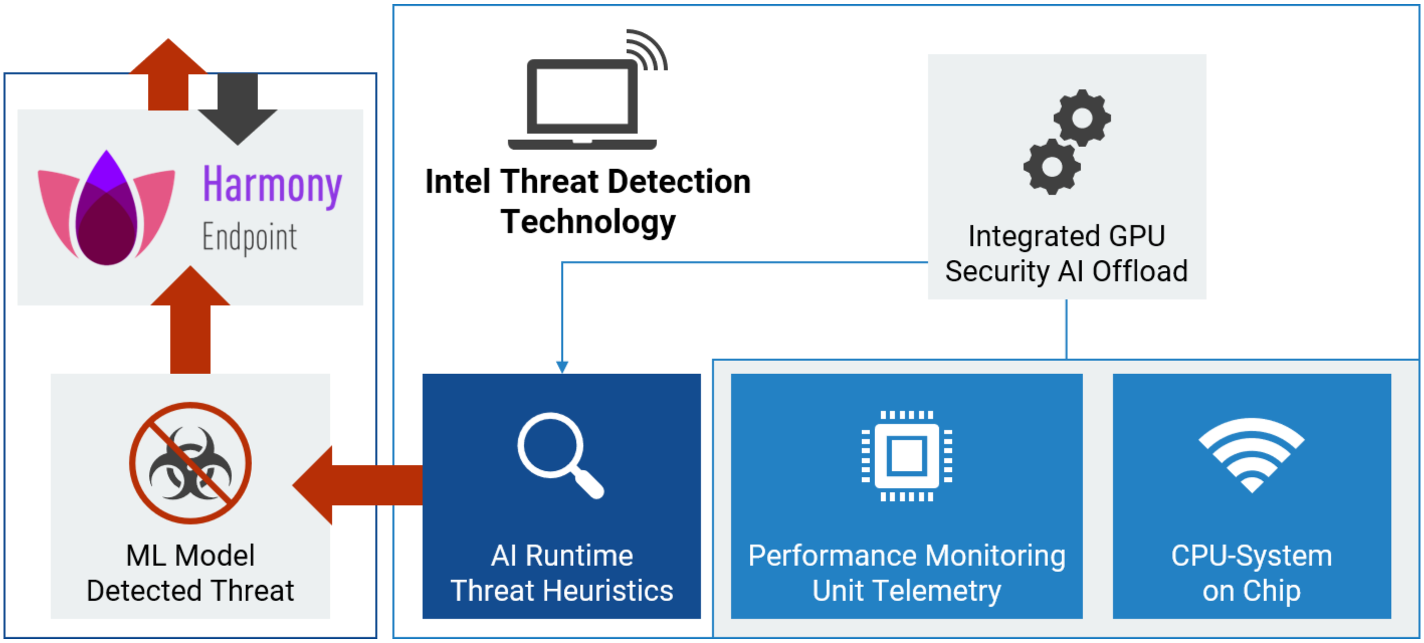
As ransomware moves faster and spreads wider within organizations, faster detection and response times are critical to cyber-readiness strategies. Integrated with Check Point Harmony, Intel TDT provides a hardware-assisted, multilayered threat detection solution that can identify malicious activity within microseconds, resulting in earlier detection and faster defensive actions combatting ransomware and other advanced threats (see Figure 1).

The Intel TDT architecture allows Check Point Harmony Endpoint to enable, harvest, and analyze Intel TDT signals to monitor and detect exploit behaviors in real time, including ransomware. Once detected, Check Point Harmony provides automated support for the full investigation and response actions, including:

- Automatic attack investigation.
- Automatic attack remediation, sanitizing the entire kill chain.
- Automatic restoration of damaged user data from proactively created anti-ransomware backups.
- Generation of a complete forensic report.

The net result is less operational disruption because the time between detection and blocking is reduced, thereby reducing attack progression and propagation and the amount of operational disruption.

Figure 1. Intel Threat Detection Technology Collaborates with Check Point Harmony Endpoint

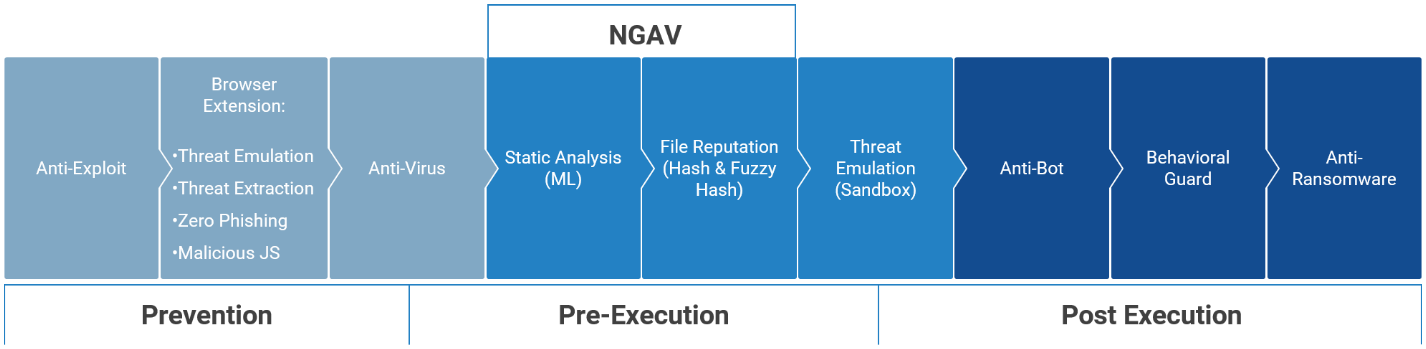


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Defense in Depth: More Than Antivirus, More Than Next-gen Antivirus

Combining proactive, active, and reactive mechanisms, Check Point Harmony Endpoint offers comprehensive endpoint security that combines attack surface reduction, prevention, and runtime protection (see Figure 2).

Figure 2. Check Point Harmony Endpoint: Defense in Depth



Source: Check Point Software.

Check Point Harmony: Complete Endpoint Security

Check Point Harmony Endpoint provides broad 360° endpoint security capabilities across a broad range of platforms. This set of capabilities provides protections related to the many aspects of ransomware attacks.

Protection Against Most Common Infiltration Vectors

- Web protection including AI-powered anti-phishing capabilities to prevent credential stealing.
- Extensive vulnerability and patch management capabilities to reduce the possibility of exploiting known vulnerabilities.
- File emulation to detect malicious content.
- Encryption for removable media and hard disks to reduce data exfiltration in multiphase ransomware attacks.
- Port protection to prevent infiltration using USB and similar devices.

Detection of Abnormal Behaviors and Lateral Movement

- Signature-driven behavioral protections.
- Anti-bot detections on network traffic.

Ransomware and Recovery

- Algorithmic and honey-pot-based detections.
- Volume encryption detection and protection.
- Intel TDT for detections at hardware speed.

Conclusion

Ransomware and other advanced attacks continue to evade modern security controls. Enterprise Strategy Group believes that hardware and software security solutions must collaborate more effectively to keep up with ransomware and the rapidly advancing threat landscape. A more robust, collaborative security architecture capable of employing AI at both the hardware and software level is needed.

Hardware and software security solutions must seamlessly and transparently work together to identify and thwart attacks faster, before they progress and cause damage and disruption. This will require a more advanced security architecture, combining attack-surface reduction, analysis of suspicious activities pre-execution, and the rapid detection of malicious activity post-execution, all wrapped in active containment and mitigation response actions.

Check Point and Intel are leading examples of companies that understand these principles. Enterprise Strategy Group recommends that IT and security leaders responsible for endpoint security solutions explore how the combination of Check Point Harmony Endpoint with Intel vPro-based PCs can strengthen security posture and reduce operational disruption.

DISCLAIMER: Intel technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. Your costs and results may vary. All versions of the Intel vPro® platform requires an eligible Intel processor, a supported operating system, Intel® LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance, and stability that define the platform. See intel.com/performance-vpro for details.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com