

Defending Against Ransomware

Strengthening Ransomware Prevention Through
Hardware and Software Security Collaboration

Dave Gruber | Principal Analyst

ENTERPRISE STRATEGY GROUP

MARCH 2024

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

Introduction

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.

TABLE OF CONTENTS



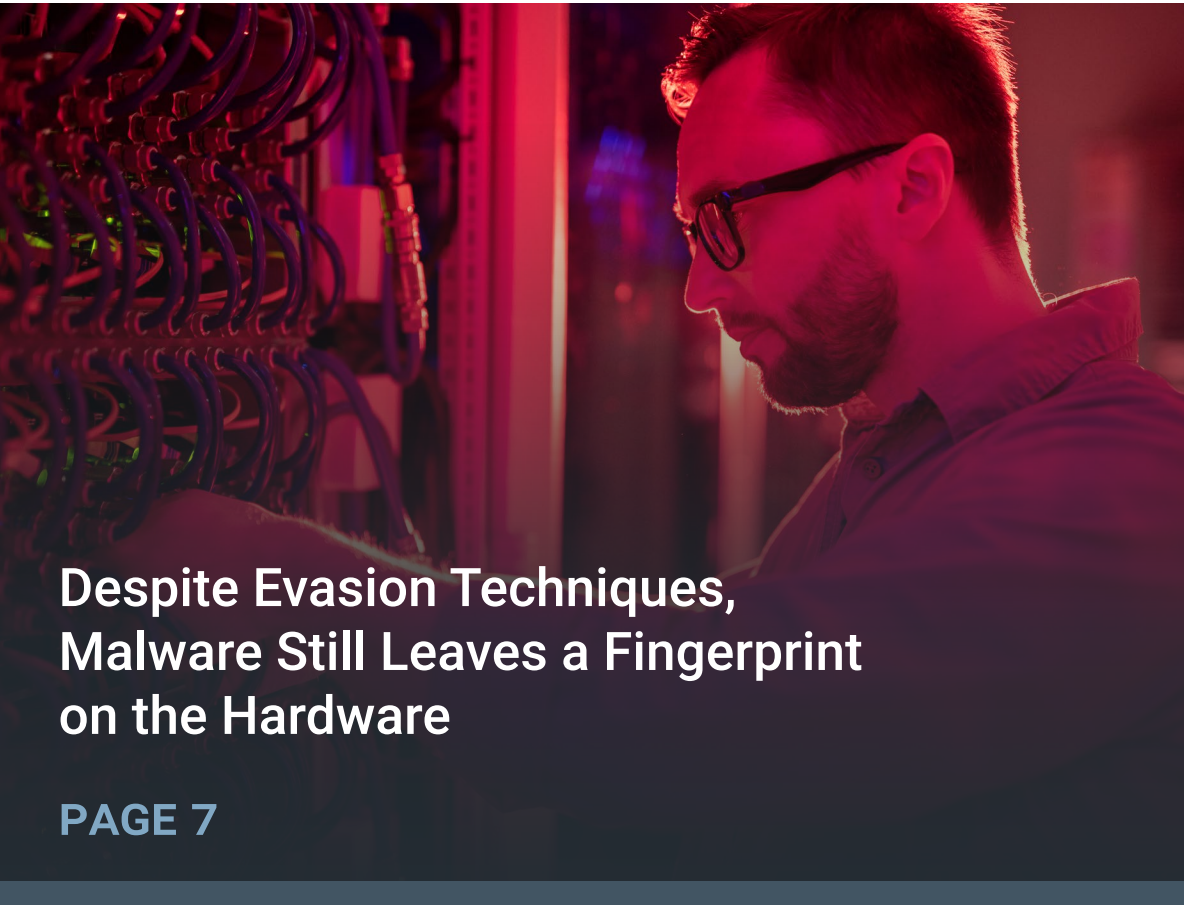
The Ransomware Threat Persists

PAGE 3



Ransomware Preparedness Is Woefully Lacking for Most

PAGE 5



Despite Evasion Techniques, Malware Still Leaves a Fingerprint on the Hardware

PAGE 7



Check Point Harmony and Intel Threat Detection Technology

PAGE 10



Conclusion

PAGE 13



Check Point Harmony: Complete Endpoint Security

PAGE 14



The Ransomware Threat Persists

The Ransomware Threat Persists

Despite continuing investment in security tools, 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 (see Figure 1).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 ransomware one of the top three most serious threats to the viability of their organization (see Figure 2).

As malware evolves and becomes more sophisticated, ransomware is 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, 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.

Figure 1. Ransomware Attacks Are Pervasive

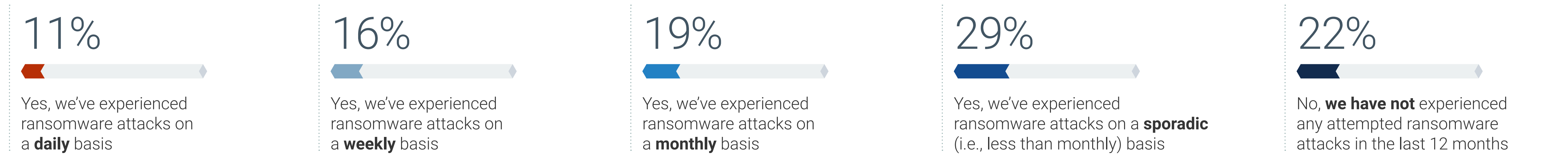
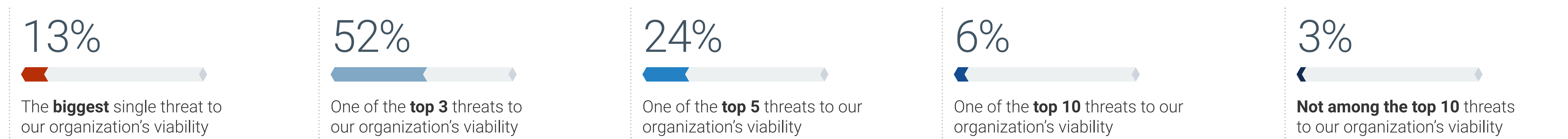


Figure 2. Ransomware Poses a Significant Threat to the Viability of Organizations



¹ Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023. All Enterprise Strategy Group research references are from this report.



Ransomware Preparedness Is Woefully Lacking for Most

Ransomware Preparedness Is Woefully Lacking for Most

Despite ransomware attacks posing significant threat to organizations, most organizations are not adequately prepared to deal with them. Enterprise Strategy Group research has shown a considerable gap between the average organization’s preparedness level and the relatively best-prepared ones.

This research revealed that only 12% of organizations were Leaders in ransomware preparedness activities, including readiness, prevention, response, recovery, and business continuity (see Figure 3).

Figure 3. Most Organizations Are Not Adequately Prepared to Defend and Respond to Ransomware Attacks

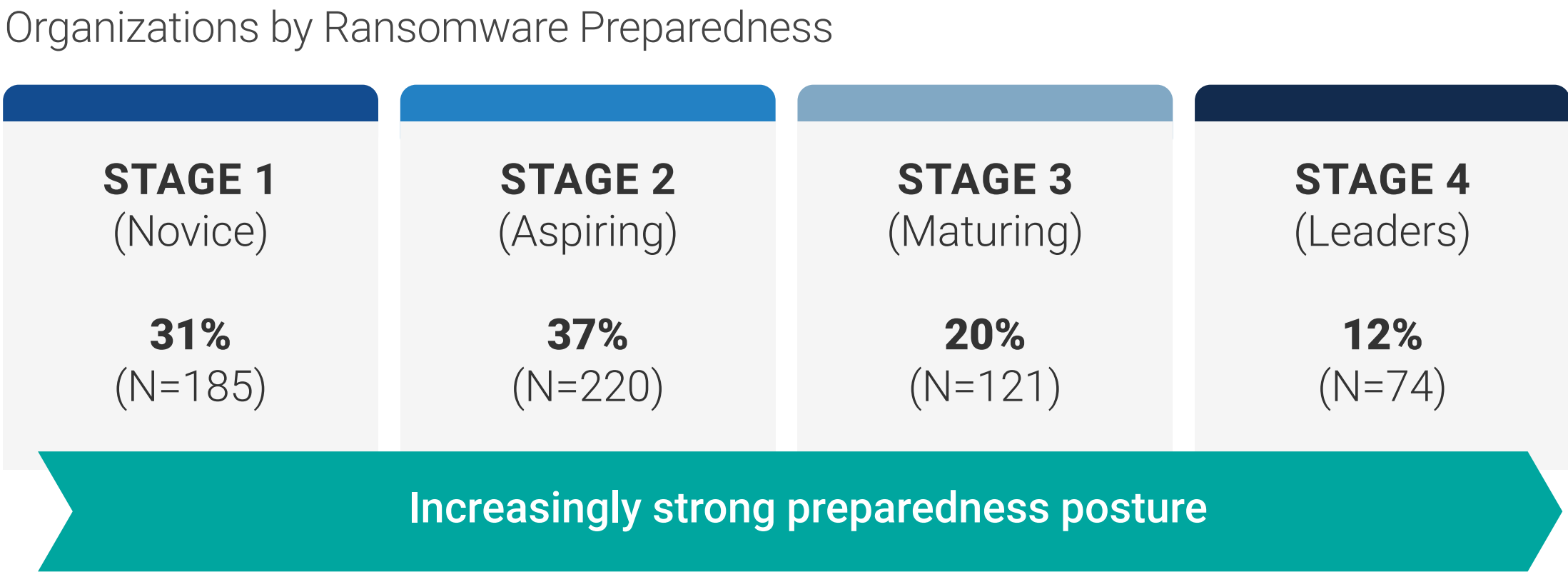
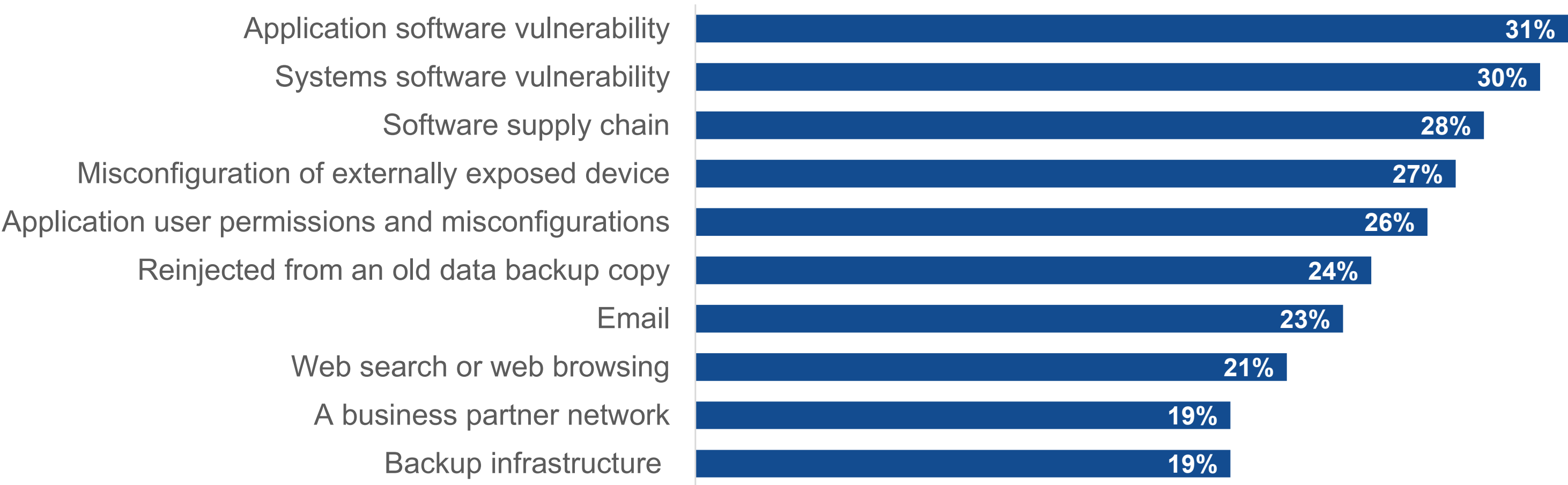


Figure 4. Software and Configuration Vulnerabilities Are a Big Initial Point of Compromise



Cybercriminals have become more sophisticated in their attacks over time and leverage many different methods to optimize their efforts. When respondents were asked to identify the initial point(s) of compromise associated with successful ransomware attacks, the results were interesting. While it has historically been perceived that ransomware attacks primarily emanate from email or unsafe web browsing, the current reality is different. Indeed, vulnerable application software and misconfigurations have been the most common points of entry for recent successful ransomware attacks (see Figure 4).

Regardless of the entry point, preventing ransomware damage requires earlier threat detection. New prevention strategies are needed.

A man with a beard and glasses is shown in profile, looking towards the left. He is wearing a dark shirt. The background is a data center with rows of server racks. The lighting is dim, with a strong red/pink hue. The text is overlaid on the lower left portion of the image.

**Despite Evasion Techniques,
Malware Still Leaves a Fingerprint
on the Hardware**

Despite Evasion Techniques, Malware Still Leaves a Fingerprint on the Hardware

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.

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 that is immune to many evasion techniques.

Enter Intel® Threat Detection Technology

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



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.**

Intel TDT Origins: Intel Performance Monitoring Unit

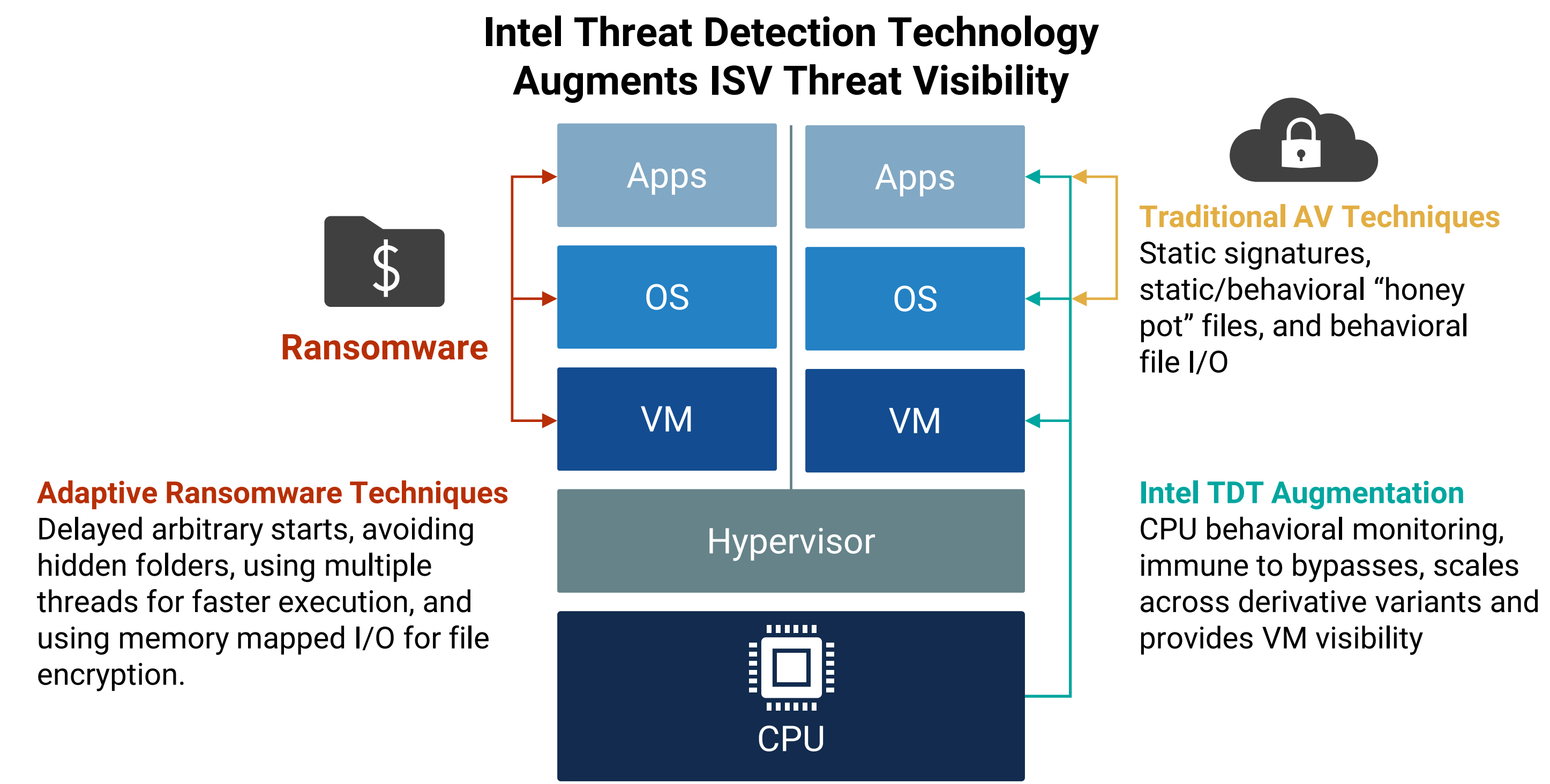
Previously available for many years, the Intel Performance Monitoring Unit (PMU) gathers low-level microarchitectural execution data as the CPU executes instructions from the software entities running on it.

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 sequences enables Intel TDT to recognize these attacks (see Figure 5). 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.

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

Figure 5. Intel Threat Detection Technology Augments Software-based Security Threat Visibility





Check Point Harmony and Intel Threat Detection Technology

Check Point Harmony and Intel TDT

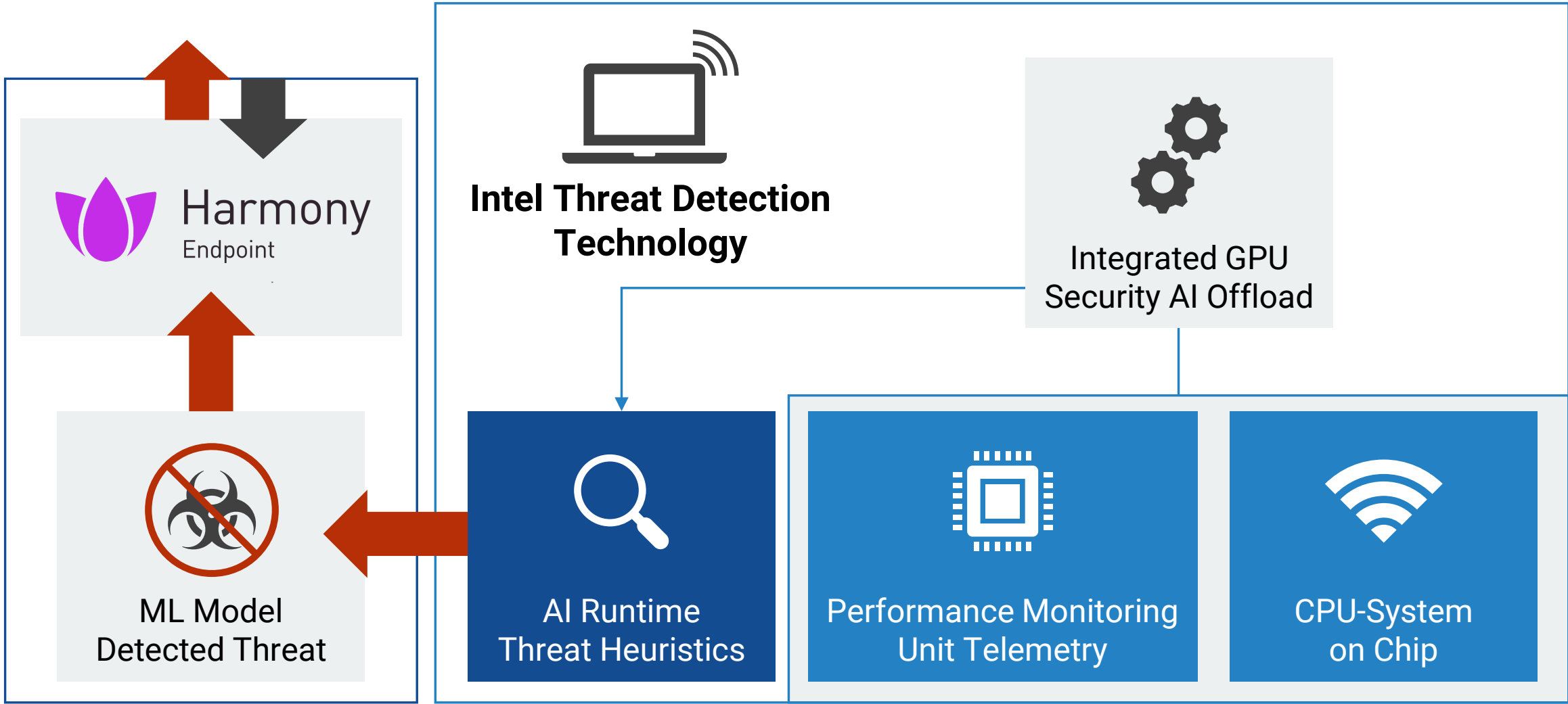
As ransomware moves faster and spreads wider within organizations, faster detection and response times are critical to cyber-readiness strategies. Integrated with Check Point Harmony, Intel TDT on Intel vPro provides a hardware-assisted, multilayered threat detection solution that can identify malicious activity within microseconds, resulting in earlier detection and faster defensive actions combatting ransomware and other advanced threats (see Figure 6).

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

Automatic attack investigation.	Automatic restoration of damaged user data from proactively created anti-ransomware backups.
Automatic attack remediation, sanitizing the entire kill chain.	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 as well as the amount of operational disruption.

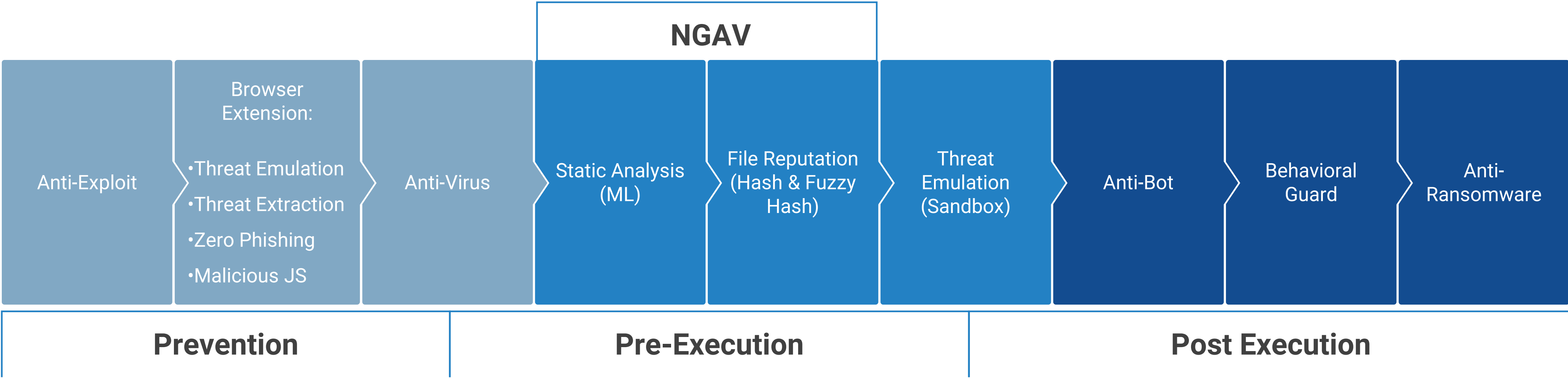
Figure 6. Intel Threat Detection Technology Collaborates With Check Point Harmony Endpoint



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 7).

Figure 7.
Check Point Harmony Endpoint: Defense in Depth





Conclusion

The devastating impacts of repeated, frequent, and often successful ransomware attacks have become the new normal. Ransomware remains a formidable threat to many organizations' viability, with most respondents recognizing that it supersedes all other potential threats. More than ever, this technology threat is a business-level issue that mobilizes executive and IT teams to ensure crucial data loss is mitigated. Once successfully attacked, few organizations can restore all of their data, and minimal progress has been made in the past 18 months on this front.

This is mainly due to the wide-ranging business impacts of ransomware, which go far beyond data-related woes (such as data exposure and data loss) to fundamentally affect business processes and operations with significant compliance exposure ramifications and the specter of financial and reputational loss. Cybercriminals are constantly adapting and targeting valuable or regulated data as well as the infrastructure to optimize their chance at extortion.

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/ML 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.

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 honeypot-based detections.
- Volume encryption detection and protection.
- Intel TDT on Intel vPro for detections at hardware speed.

LEARN MORE



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

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

© 2024 TechTarget, Inc. All Rights Reserved.