On-Device Security in the AI PC Era

What does the AI PC with Intel vPro mean for users, and how does it work for them?

Executive Summary

As artificial intelligence (AI) finds its way into everything we do, so must better cybersecurity. The advent of increasingly complex and dangerous AI-accelerated attacks presents new protection challenges and opportunities for the industry. While the industry blazes forward with new endpoints, including new AI PCs, it needs new tools to protect endpoints and data by reducing the attack surface.

Today's security software solutions face crucial limitations because most AI processing occurs in the cloud rather than at the edge or on the PC itself. Due to privacy concerns and the large amounts of data being handled, it is not feasible to send all data to the cloud to identify attacks. Still, CISOs want to detect threats across all endpoints to gain a broader picture of active adversarial campaigns while protecting data and identities. This implies leveraging AI to locally identify the correct data to send upstream to take advantage of the endpoint detection and response (EDR) system's holistic extended detection and response (XDR) insights.

Similarly, for other security categories such as data loss prevention, it is challenging to perform the necessary AI computations on the endpoint to classify sensitive corporate data and protect against data exfiltration. With the advent of NPU- and GPU-accelerated AI, new security approaches are now possible at a larger scale using on-device computing. The security software ecosystem is also rapidly innovating new capabilities that will run on AI PCs.

As these features are implemented, AI-enabled PCs will offer significantly improved security capabilities for enterprises, replacing legacy solutions that were not performant or accurate. This re-architecting of endpoint security from cloud-centric to a blend of AI on the cloud and the endpoint is an inflection point. Data privacy, increased detection efficacy, lower costs, improved battery life, and the acceleration of features to ensure that the user experience is intact are all driving this innovation. More than that, having a complete solution that helps reduce the attack surface of the endpoints can lower the chances of an attack and minimize the impact on the individual and the enterprise.

Client-side security needs to address many different attack vectors simultaneously — in a way that ensures both users and enterprises feel safe when using their PCs. By leveraging local AI capabilities, organizations can bolster privacy and implement novel detection methods and security usage benefits. Vendors achieving this should have a long track record of success in deploying and managing enterprise-scale security.

Intel's Threat Detection Technology (Intel TDT) on Intel vPro-enabled systems combines CPU telemetry with AI workloads accelerated by the GPU to detect attacks. In partnership with PC OEMs and Microsoft, Intel vPro Security works at a silicon level to deliver enhanced security using virtualization and memory encryption. This virtualization helps isolate data and identities, helping to build a deep defense across many attack surfaces.

While no security platform can be entirely impenetrable, it is crucial for a security solution to minimize the attack surface and incorporate tools to swiftly identify and neutralize risks and threats and then recover effectively. This can only be achieved if the security ISV ecosystem embraces endpoint security solutions that leverage on-device compute and data enhanced by AI.

THE NEW CYBERSECURITY THREATS

Cybersecurity threats are becoming increasingly complex and dangerous, targeting multiple attack surfaces to find vulnerabilities. As such, protection at the OS level — and not only below it — is essential.

Ransomware can operate within a virtual machine, making it difficult for EDR software to detect. Fileless malware attacks that execute initially in memory also pose challenges for EDRs because scanning memory requires significant computing power and can disrupt the user experience. Identity and credential theft also require OS-level defense. Control-flow hijacking is an attack at the memory layer that attempts to redirect the flow of a program's execution in memory.

Additionally, below-the-OS firmware attacks target vulnerabilities in the motherboard's firmware, highlighting the need for comprehensive security across all layers. And the threats don't stop there. Supply chain corruption presents both a physical and virtual threat, as it can occur when either a hardware supplier is compromised or a software vendor is unknowingly breached. Phishing attacks are now enhanced by AI and take advantage of user vulnerabilities and data to better personalize the attacks. There are

even new attack vectors with the introduction of AI that involve injecting malicious code into an AI model itself, so protections are needed there as well.

Certain tools are essential to reduce the attack surface at the OS level and below, including BIOS/UEFI protections that prevent access to critical firmware-level settings. Secure Boot is a firmware feature designed to protect against boot attacks, which is currently standard for most Windows 11 PCs.

Multiple ways to securely store keys, along with passwords and certifications, have been implemented by Microsoft at the OS layer, leveraging zero-trust secure enclaves that have been built into the hardware to create additional layers of protection. There are also tools designed to prevent unauthorized rogue firmware updates that can circumvent countermeasures that might exist at higher layers. There are also new tools designed to protect against attack vectors that seek to compromise the AI models people use inside their applications.

THE INTEL VPRO PLATFORM AND AI PCS

Intel vPro Security offers a robust and comprehensive approach to addressing a wide range of challenges, from the application level to the OS layer and down to the silicon hardware level. The Intel vPro platform has been an industry standard for security since 2006, with improvements and new features consistently added in the intervening years. Intel vPro has added support for operating systems beyond Windows, including OSX, Linux, and even ChromeOS.

Intel has been focused on security since long before the introduction of Intel vPro and continues to evolve and advance its security efforts. Its approach to security is comprehensive not just in scope but also in its proactive nature, addressing most vulnerabilities well before they become problems.

In fact, Intel found that its proactive product security assurance efforts accounted for 96% of vulnerabilities disclosed in 2024, and 100% of the Intel processor vulnerabilities addressed were discovered through internal security research.[1] Intel also found that its closest competitor reported 4.4x more firmware vulnerabilities in its own hardware root-of-trust in the same year.

Intel attributes much of its progress in proactively addressing vulnerabilities to its product security assurance efforts. It is working to ingrain the security-first mindset of its

[1] 2024 Intel Product Security Report

product security assurance program into the company culture. This program also includes the continuous efforts of Intel's Product Security Incident Response Team, which is responsible for managing vulnerabilities across the company, and a bug-bounty initiative that accounted for 53% of the vulnerabilities addressed in 2024.[2]

Intel vPro Security has the pieces necessary to address many of the attack surfaces that concern most CIOs and CISOs. Intel TDT has been in development for the last seven years and uses the compute engines inside the company's latest Intel Core Ultra family of processors to enhance detection while freeing up as much performance as possible for critical business applications. The CPU telemetry and AI functionality provide unique detection assistance for EDRs offloaded to the GPU. Intel has been shipping Intel TDT since its 6th Gen Intel Core processors were introduced, which means that more than a billion installed devices can take advantage of this hardware-based threat detection.

When the system boot is ready to set up the runtime operating system environment, Intel Trusted Execution Technology (Intel TXT) uses a Measured Launch Environment (MLE) to prevent attempts to interfere with a system's bootup sequence. This is accomplished by using the trusted platform module (TPM) to provision known good values for both the BIOS and hypervisor to ensure that enterprise PCs are launching into a trusted known state every time.

Intel Boot Guard Technology provides the hardware-based security required for secure system boot integrity. This is designed to mitigate unauthorized BIOS boot block modifications. Intel Boot Guard authentication begins with the Intel processor hardware and extends this trust with the help of microcode, the Boot Guard Authenticated Code Module (ACM) and BIOS Initial Boot Block (IBB) extending all the way to the operating system. This way, Intel Boot Guard is designed to authenticate firmware integrity and meet Microsoft's requirements for UEFI Secure Boot.

Additionally, Intel System Resource Defense and Intel Systems Security Report capabilities continue to provide the required protection at runtime against System Management Mode-based firewall attacks, and Intel Runtime BIOS Resilience helps perform secure updates to the BIOS image on the flash.

Once in a runtime environment, the Intel CPU AES-NI provides the power- and performance-optimized crypto instruction set that can be utilized for protection-at-rest

[2] Ibid.

capabilities (e.g., BitLocker Disk Encryption). Meanwhile, technologies such as Intel Total Memory Encryption provide the necessary memory protection capabilities for applications and AI assets during execution, and Intel Virtualization Technologies VT-x and VT-d help create a runtime isolation environment for Windows Virtualization-based security. The Intel Total Memory Encryption - Multi-Key (TME-MK) is the only hardware technology running on Windows 11 that provides VM hardware-based memory encryption. In addition to VM isolation and encryption, Windows Hypervisor-enforced Paging Translation (HVPT) is available only with Intel Core (Ultra Series 2, 200) with Intel vPro through Intel Virtualization Redirect Protection (VT-rp) technology. At the same time, Intel VT-x and VT-d, along with VT-rp, help create the required runtime isolation and sandboxing to run AI usages securely.

AI-Enhanced Security Capabilities

New AI PCs enable new types of AI-enhanced security. Intel is already working with some of the world's leading cybersecurity ISVs to harness new AI security capabilities while also taking advantage of the three different processor engines in the latest Intel Core Ultra family of products. Previously, Intel's choice for running security workloads was a combination of CPU and GPU technologies, but with the addition of the NPU, there are more opportunities to balance workloads and algorithms on the cores that deliver the best performance and experience.

Intel has already demonstrated a few AI-enabled tools with top security ISVs. BUFFERZONE, for example, has worked with Intel to accelerate its NoCloud anti-phishing solution using Intel's OpenVINO framework. This solution runs locally on the Core Ultra NPU and uses clickstream and page analysis to determine the authenticity of URLs and ensure that they do not lead to phishing websites. Since the entire application runs locally, none of the user's or enterprise's information is sent to the cloud. BUFFERZONE also reported that running on Intel Core Ultra Series 2 using the NPU translated to a 91% reduction in anti-phishing cost.[3]

CrowdStrike collaborated with Intel to improve AI endpoint security by leveraging the NPU to reduce CPU usage spikes when enabling endpoint clustering and processing feature vectors. This reduced CPU consumption from 35% to less than 1% by using the

[3] BUFFERZONE and Intel AI Anti-Phishing Solution Presented at MWC 2024, BUFFERZONE, February 2024

NPU to accelerate a neural network approach to clustering assessment.[4] Several advanced POCs with Intel have shown that on-client AI can provide significant benefits.

To make Intel vPro even easier for enterprises to use, the company announced Intel vPro Fleet Services, which offers a cloud-based deployment model rather than an on-premises server. This one-to-many remediation capability should help to fix fleetwide issues like July 2024's Blue Friday, when some 8.5 million Windows devices crashed because of a faulty update. This was one of the many lessons learned from that event, which Intel detailed in its CES 2025 blog post.[5]

Intel, in partnership with Microsoft and CrowdStrike, established a new MITRE Center for Threat-Informed Defense (CTID) project leveraging the work the three companies have done together using Intel vPro. This Security Stack Mappings project[6] took vPro features and mapped them to more than 150 MITRE ATT&CK framework attack techniques. This shows the significance of Intel's hardware-based security across Windows 11 and as integrated into leading security tools such as CrowdStrike and Microsoft Defender.[7]

Call to Action

The endpoint security landscape is always evolving, and the latest threats are becoming increasingly complex. Because of this, approaches to endpoint security must evolve along with the new attack vectors. Companies must do everything possible to reduce attack surfaces. This is especially true in this new era of AI, which enables both AI-enhanced cyberattacks and AI-enhanced protection capabilities with AI PCs.

Intel's trusted and constantly evolving approach uses AI to enhance security, whether on the CPU and GPU or by leveraging the NPU for enhanced on-device methods. Intel vPro also leverages foundational hardware features to protect key attack surfaces within AI itself while it executes on the client compute cores.

IT professionals looking for endpoint security for their incoming AI PCs should consider Intel's complete approach to protection, which incorporates its well-regarded and trusted Intel vPro platform and expansive relationships with the world's leading security ISVs using the latest AI capabilities.

[4] CrowdStrike, Intel, and Dell: Clustering and Similarity Assessment for AI, CrowdStrike, April 2024
[5] CES 2025: Intel to Power Large PC Refresh with New Silicon-Based Security, Intel, January 2025
[6] Security Stack Mappings Project, MITRE, April 2024
[7] Center for Threat Informed Defense, Mapping Frameworks, Intel vPro, January 2025

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTORS
Anshel Sag, Vice President and Principal Analyst, AR/VR/XR, 5G Mobility, PCs, Smartphones, Graphics

PUBLISHER
Patrick Moorhead, CEO, Founder and Chief Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy." Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
Intel commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.