White Paper

Information Technology
Cybersecurity

Intel vPro® Security Overview

Introduction

This document covers hardware-based security features that work right out of the box as part of the Intel vPro® platform. Intel vPro® Security is comprised of three groups of security technologies. The three groups are: below-the-OS security, application and data protections, and advanced threat protections. Each section in this paper reviews all the technologies in one group, including both software and hardware security capabilities.

Why Intel vPro® Security?

Security matters more than ever as cyber-attacks continue to evolve to evade detection by software-only security methods. Threats are moving down the computing stack, using remote worker endpoint PCs as a direct vector into networks, cloud, and SaaS applications. Bad actors no longer just steal data, they can commandeer computing resources on a massive scale. Too often, the way in is a compromised PC that offers-up access identity, encryption keys, and passwords, in addition to sensitive data. Remote work has evolved from workers accessing assets via firewall or VPN protections to now accessing through SaaS and cloud hosted applications. These applications rely on Endpoint Detection and Response (EDR) security software to assess the health of the workers' devices (free from malware) to authenticate the user for every connection. This is the new zero trust security model, and this PC health assessment is critical for security operations to gauge risks. On top of all that, IT and information security professionals also face increasing regulatory compliance requirements for data localization and information privacy.

Many types of attacks target operating systems (OSs), browsers, applications, firmware and BIOS, in addition to system memory. According to CrowdStrike's 2024 global threat report [1], 75% of all attacks first execute as file-less Malware in memory while 90% of attacks originate at the endpoint.[2] In 2023, IBM reported that the global average cost of a data breach was $4.45M[3], while a leading cyber security company reported that crypto-jacking had increased by 659% from 2022 to 2023.[4]

Hackers continue to evolve their techniques, moving increasingly towards the hardware infrastructure. Organizations of all sizes need to invest in better technology to help protect their information security—from endpoint to network edge to cloud. That requires defense at each layer of infrastructure and applications, from hardware, BIOS/firmware, hypervisor, virtual machines (VMs), OS, network, cloud and applications. Intel aims to establish a robust foundation that ensures security against various threats. By enhancing security software and integrating protective features at every OS layer through hardware capabilities, Intel fulfills a dual role. It not only offers solutions to prevent direct hardware attacks but also provides essential hardware optimizations to support security software. Additionally, Intel is committed to collaborating with the software ecosystem to develop advanced security use cases.

Intel works with our partners to build security solutions that aim to help solve the toughest security problems. Security technologies available on Intel vPro® powered by Intel® Core™ Ultra Processors continue to raise the bar on platform security by helping stay ahead of bad actors. Hardware-based endpoint security helps reduce the attack surface to protect against physical hardware and software assets that run on the PC. The Intel vPro® platform provides built-in security features to help organizations protect, detect and recover from cyber-attacks in an increasingly challenging threat landscape.

While the AI PC landscape rapidly evolves, AI is increasingly being used as a force for both good and evil. AI is contributing to a rise in the frequency and complexity of cyberattacks, with a staggering 77% of organizations experiencing AI-related security breaches in 2023.[5] However, security for AI and AI for security are also marking a significant turning point in cybersecurity, bringing about innovative detection techniques. It's redefining the way endpoint security is implemented, using AI to strengthen defenses while minimizing disruption to the user experience. Intel vPro® offers the secure by design foundation for modern computing and AI with security capabilities built above and below the OS, delivering hardware-based protection for AI models and associated data at all stages of execution. Intel hardware-based security capabilities include encryption, threat detection, credential protection, kernel protection, and more to give organizations confidence and peace of mind using AI PCs.

Although no feature or set of features provides absolute security, the Intel vPro® platform powered by Intel® Core™ Ultra processors delivers a comprehensive suite of hardware-based security technologies for business. As security threats continue to adapt and attack lower levels within a system's resources, the security feature roadmap of the Intel vPro® platform continues to evolve. Continuing product improvement and investment is crucial to meeting customer needs. Intel technologies and products operate above and below-the-OS, putting Intel in a unique position to deliver hardware enhanced, built-in protection, helping to deny attackers access to modify or manipulate the hardware and firmware.

Intel vPro® Security: Below-the-OS Security

The Intel vPro® Security category of below-the-OS security is comprised of hardware-based technologies to help provide a secure and protected boot environment that can verify the integrity of firmware and the OS as it is loaded and to help protect the Unified Extensible Firmware Interface (UEFI) BIOS firmware and main memory starting at boot-up.

Intel® BIOS Guard

Intel BIOS Guard is a BIOS Flash update hardening technology that creates a very small trust boundary for BIOS image updates to Flash, eliminating the System Management Interrupt (SMI) handler and nearly all of the power-on self-test (POST) from the trust boundary. This small trust boundary helps reduce the risk of Flash based attacks in the Intel vPro platform, including permanent subversion and/ or denial of service attacks. Attacks on platform BIOS could result in security problems including BIOS-based Rootkit, denying bring-up of the system, and persistent platform denial of service.

Intel BIOS Guard uses the Model State Register (MSR) to generate the Flash open/close special cycles. This results in the Flash open/close only being writeable from BIOS Guard AC-RAM mode. Update authentication is also performed by the Intel BIOS Guard module. This yields a much smaller attack surface and a much more defensible environment from which to perform Flash operations. Furthermore, an Intel BIOS Guard-enabled system does not allow host Flash writes from any other environment.

Intel® Boot Guard

Intel Boot Guard provides a key element of hardware-based boot integrity that meets the Microsoft Windows requirements for UEFI Secure Boot to mitigate unauthorized BIOS boot block modifications.

Intel Boot Guard doesn't prevent access, or even write to the Initial Boot Block (IBB), rather it verifies the correctness of this code before the CPU comes out of reset to run the IBB. The related keys and policies reside in fuses. Intel Boot Guard only reads on the BIOS Boot Block. As a result, it fortifies the root and attacks on the root are thus stopped.

Intel Boot Guard becomes a hardware root of trust adding robustness to the chain of trust process where the UEFI boot process cryptographically verifies and/or measures each software module before executing it. The result of the Intel Boot Guard process is a reduction in the chance of malware exploiting hardware or software components on the platform.

Intel Firmware Update/Recovery

Intel Firmware Update/Recovery provides the ability to update the firmware on an end user's system and recover from a firmware failure. Firmware updates are signed by Intel, deployed by the PC manufacturer as a UEFI Capsule, and applied in a fault-tolerant manner on the end user system. In case of a power interruption failure during the update, the system automatically boots to a last known good state and restarts the firmware update process—all without user intervention.

Intel® Platform Trust Technology (Intel® PTT)

Intel® PTT is an integrated Trusted Platform Module (TPM) that offers the same capabilities of a discrete TPM, integrating secure storage for keys, passwords, and digital certificates into the Intel vPro platform. Intel PTT is a credential storage and key management solution to meet Windows OS hardware requirements. It is optimized for low power consumption in the S0iX environment. Intel PTT supports the Trusted Computing Group 2.0 standard and FIPS 140-2 certifications.

Intel® Runtime BIOS Resilience

Intel Runtime Bios Resilience is a unique feature that helps PC manufacturers enforce a below-the-OS policy. Its key value is to reduce the risk that malware can be injected into the System Management Mode (SMM) environment at runtime. It does so by setting up the page table with a policy that uses the security properties of paging and then locks the page table so it cannot be modified later during runtime. End users benefit because the platform is more secure against attacks launched from SMM.

If the platform implements a policy such that memory used by the OS is not mapped in the SMM page table along with Intel Runtime Bios Resilience, it will lock that policy. The entry point and all the code within SMM becomes locked down, along with the memory map and page properties. The OS memory then becomes inaccessible from SMM. This makes it challenging for an attacker at runtime to modify the page table and map memory that is used by the OS.

Prior to this technology, any code running in SMM could dynamically allocate memory as needed. This means if an attacker got into SMM, they could potentially allocate memory, gain visibility into the OS, and inject malware.

Intel® System Resources Defense

Intel® System Resources Defense is a feature of Intel Runtime BIOS Protection that extends the ability to enforce resources access policies for SMI handler firmware beyond memory resources. It is a mechanism that can enforce policy on what system resources can be accessed by firmware SMI handlers from within SMM by establishing a ring 0 and ring 3 privilege separation with regard to hardware access from SMI handlers. When Intel SRD is implemented with policy that reduces SMI handlers' access to hardware resources such as policy with minimal required access to keep the platform running, it can help to harden the platform by reducing the attack surface in SMM. When Intel System Resources Defense and Intel Runtime BIOS Resilience are implemented with a policy that does not allow SMI handlers to access resources that could potentially affect OS secrets, then the security of the OS is improved by isolating the trusted compute base of the OS from the SMI handlers. In simpler terms, this means that it reduces the risk that a bug or vulnerability in the SMI handler could be used to launch an attack on the OS.

Intel® Trusted Execution Technology (Intel® TXT)

Intel TXT is the technology that the OS or hypervisor can use to initiate a measured and controlled launch of system software called the Measured Launch Environment (MLE). The MLE is a protected environment. Generally, the OS or hypervisor uses Intel TXT to establish the MLE at OS boot time.

Intel TXT measures key components executed during launch the MLE and allows the OS to check the consistency in behaviors and launch-time configurations against a "known good" sequence. Using this verified benchmark, the system can quickly assess whether any attempts have been made to alter or tamper with the launch time environment.

Intel TXT can work with a discrete Intel TPM or with Intel PTT (an integrated TPM 2.0 solution). In addition, using Intel TXT with a TPM enables attestation of the authenticity of the UEFI firmware and the OS.

Intel® System Security Report

Using Intel TXT to launch the OS and a hypervisor on an Intel vPro platform enables the OS to use Intel System Security Report, a patented, trusted hardware-to-software channel to gain below-the-OS security visibility. In coordination with Intel TXT, Intel System Security Report communicates policies to the OS in a trusted manner at runtime. Intel System Security Report provides a one-time report at the time of the Intel TXT launches. This typically happens towards the beginning of the OS boot. Intel System Security Report works with Intel TXT to provide this information in a trusted manner. Without this capability, neither the OS's hypervisor nor MLE would have any visibility into what system hardware or resources may be accessible from firmware SMI handlers.

Intel® Partner Security Engine

Powered by the latest Intel® Core™ Ultra processors, Intel® Partner Security Engine is a dedicated and isolated security engine designed to run third party (OEM/OSV) signed firmware securely on Intel silicon. This allows OEMs and OSVs to execute custom security usages securely on Intel silicon. Using this technology, sensitive data such as encryption keys can be stored securely, isolated from the rest of the system, thus preventing emerging attack techniques such as speculative execution from accessing key material.

Intel vPro® Security: Application & Data Protections

Application and data protections use hardware-accelerated virtualization, encryption and memory protection to help eliminate an entire class of attacks that evade current software solutions.

Intel® Virtualization Technology (Intel® VT-x)

Hardware virtualization technology provides enhanced security by isolating different workspaces and reducing attack surfaces. Intel VT-x creates and isolates a secure region of memory. On client machines, virtualization provides a mechanism to isolate secure workloads from the main OS and thus create a secure firewall between malware running in the OS and secure workloads running inside a secure VM.

Intel VT-x can help protect data and virtualized containers with hardware-enforced isolation and encryption. It is designed to protect the confidentiality of memory content from physical attacks while providing the performance needed to run virtualization-based workloads without impacting the user experience. An isolated execution environment provides security by protecting secrets such as authenticated user credentials.

In addition to isolation and encryption, Intel VT-x can help compromised client systems recover faster. Independently isolated workspaces can help reduce the time and cost to quickly resolve matters without impacting other workloads on the same system.

Intel® Virtualization Technology for Directed I/O (Intel® VT-d)

Intel VT-d allows multiple VMs and containers to directly access I/O devices, while providing isolation and with low virtualization overhead. Intel VT-d enables an OS to protect itself from faulty device Direct Memory Access (DMA) and interrupts. On client machines, Intel VT-d is used to protect secure workloads from unauthorized device DMA initiated from the main OS. It maintains a secure firewall between malware running in the main OS and secure workloads running inside a secure VM.

With Intel VT-d, I/O device assignment can extend the protection and isolation properties of VMs for I/O operations. This technology also increases client system reliability by recording and reporting to system software any DMA or interrupt errors that may otherwise corrupt memory or impact VM isolation.

Kernel DMA Protection

DMA-capable devices can read and write to system memory without having to engage the system processor. Once, these devices existed only inside the PC, but today, hot plug PCIe ports such as Thunderbolt™ technology give modern PCs greater extensibility – but at the risk of "drive-by" DMA attacks.

To address that, Intel VT-d provides the foundation for solutions such as Kernel DMA Protection on Microsoft Windows 10 (1803 and above). In addition, VT-d based security has been supported on Mac OS since version 10.8.2 and on Linux since Kernel version 4.21. All these solutions block peripheral devices from unauthorized access to system memory.

Mode-Based Execution (MBEC) Control

MBEC virtualization provides an extra layer of protection from malware attacks in a virtualized environment. It enables hypervisors to more reliably verify and enforce the integrity of kernel level code.

MBEC provides finer-grain control on execute permissions to help protect the integrity of system code from malicious changes. It provides additional refinement within the Extended Page Tables by turning the Execute Enable (X) permission bit into two options: XU for user pages, and XS for supervisor pages. The CPU selects one or the other based on permission of the guest page and maintains an invariant for every page that does not allow it to be both writable and supervisor-executable at the same time. A benefit of this feature is that a hypervisor can more reliably verify and enforce the integrity of kernel-level code. The value of the XU/XS bits is delivered through the hypervisor, so hypervisor support is necessary.

Intel® Total Memory Encryption (Intel® TME)

Hardware-based security features delivered by the Intel vPro platform complement virtualization security with memory encryption for more system security. Protecting data requires hardware-based security capabilities at every layer, including the encryption of data in endpoint system memory.

Intel TME on Intel vPro platforms encrypts all system memory and enables confidentiality of DRAM/NVRAM that is outside the system processor package. Intel TME helps protect against data exposure via physical attack on memory confidentiality. This protection helps to prevent data exposure via "cold boot"/physical memory/DIMM removal attacks in the event of a stolen system—in which an attacker dumps memory by performing a hard reset of the target machine. This protection can extend to help protect against memory bus probing, as well. Intel TME encrypts data as it leaves the system processor, which can help protect against relocation or splicing memory attacks. If a system is stolen, Intel TME provides protection such that keys are not accessible by software or by using external interfaces to the system processor.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

Intel AES-NI improves on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in the modern Intel® processors for business clients and servers. Comprised of seven new instructions, Intel AES-NI makes pervasive encryption feasible in areas where previously it was not—that gives IT environments fast, more affordable data protection, and more security. For example, Intel AESNI is used by full disk encryption (FDE) solutions, including Microsoft BitLocker and Google Chrome disk encryption, to protect data at rest, allowing VMs to individually encrypt storage volumes.

Advanced Programmable Interrupt Controller (APIC) Virtualization

Virtual machine monitors (VMMs) emulate most guest accesses to interrupts and the APIC in a virtual environment. VMMs also virtualize all guest interrupts—this feature is called virtualized APIC (APICv).

All virtualized activities relating to interrupts and APIC, to and from the guest OS, go through the VMM in systems without APICv; however, in systems with APICv, they are executed more securely in hardware, not in the VMM. Each virtual processor has a local APICv instance. The APICv provides a simple inter-partition communication mechanism. This helps protect the system because all activities can stay inside the VM, thus eliminating the need to issue the "VM exit" command. In addition to inter-partition protection, the APICv results in reduced interrupt overhead in guests and increased I/O throughput.

Intel® VT-Redirect Protections (Intel® VT-rp)

Intel VT-rp is defense-in-depth hardware-assistance for kernel page protections, designed to protect against kernel memory corruption and page table attacks. Intel® VT-rp paging structures provide a low-overhead root-of-page walkthrough HW provided paging structures (Hypervisor based Linear Address Translation) to prevent alias and page remapping attacks and maintain legacy compatibility for fall back. As a result, the OS kernel and page table are protected from malicious attacks that could threaten important applications and data with minimal performance impact.

Intel® Linear Address Space Separation (Intel® LASS)

Modern computing systems use different types of memory addresses (physical memory, virtual address, and logical address) to retrieve critical data needed to maintain system operations. Attackers can gain mapping of all addresses where system-critical data is stored or accessed if the linear address space is compromised. Intel LASS is an instruction set architecture (ISA) extension introduced alongside the latest Intel® Core™ Ultra processors, which allows the processor to separate privilege levels based on linear addresses and prevent unnecessary page walks. Intel LASS provides defense-in-depth hardening to prevent attackers from using a variety of techniques to expose the layout of the kernel address space and gain memory address mapping. Thus, protecting against targeted kernel exploitation such as meltdown-style side channel attacks and helping to ensure that critical data and credentials are protected.

Intel vPro® Security:
Advanced Threat Protections

Advanced threat protections are a group of technologies implemented by security ISVs that can find hard-to-detect attacks and help reduce false positives, while having minimal impact to system performance. Advanced threat protections help find ransomware and cryptomining attacks, and they deliver less performance impact by offloading specific compute-intensive tasks to the Intel graphics engine.

Intel® Threat Detection Technology (Intel® TDT)

Intel TDT is a set of technologies that harness silicon-level telemetry and acceleration capabilities to help identify threats and detect anomalous activity. Leveraging AI, Intel TDT profiles or fingerprints malware executing on the CPU microarchitecture to help identify file-less malware, ransomware, and cryptojacking attacks – in real time, and with minimal end user impact.

Malware is evading today's traditional antivirus (AV) signature and Endpoint Detection and Response (EDR) behavioral approaches, using techniques that make it increasingly difficult for security software to find them. Common malware techniques include cloaking in virtual machines (VMs), obfuscation, or even hiding in memory as a valid system process. Malware must execute on the CPU microarchitecture, and the right hardware and CPU telemetry with AI is able to identify its final execution making the malware visible for security ISVs who remediate. This increases detection efficacy with Intel's hardware augmentation and increases overall security workload performance.

Intel TDT is integrated into leading security vendors' software to improve security efficacy and performance, resulting in increased threat detection efficacy on Intel vPro platforms. Intel TDT helps software threat detection agents take full advantage of the advanced telemetry capabilities rooted in Intel silicon. Security vendor's solutions can utilize Intel TDT to improve detection of persistent attacks such as cryptomining and ransomware. Intel TDT enhances system protection by delivering two powerful and innovative capabilities. These two capabilities will grow with new detectors over time. The two capabilities are: Accelerated Memory Scanning for searching malware signature patterns in memory and Advanced Platform Telemetry for detection of evolving cyber threats and exploits.

Intel® Threat Detection Technology – Accelerated Memory Scanning

CrowdStrike's 2024 Threat Landscape report shows that 75% of all attack types use file-less malware techniques like execution in memory to evade Endpoint Detection and Response (EDR) defenses.[1] These Living off the Land techniques make it hard to distinguish malware from benign system processes. It is compute intensive to scan memory and Intel Threat Detection Technology – Accelerated Memory Scanning (AMS) delivers an API for ISVs to offload and parallelize scanning to the integrated GPU. This method improves memory scanning efficiency while lowering performance overhead, which ultimately expands detection coverage for malware hiding in system memory. ISVs can typically gain 4 to 7 times the ability to scan more and detect more threats.[6] Additionally, some ISVs have tied AMS to trigger when they see early indicators of an attack. This allows a more detailed complete snapshot at the suspect memory region vs arbitrary time-based memory scanning.

Intel® Threat Detection Technology – Advanced Platform Telemetry

Advanced telemetry built-in to the Intel vPro platform uses targeted detection, which combines machine learning with hardware telemetry to profile exploits and detect their behavior. This adds a new detection assist capability that does not increase the ISVs sub 1% performance envelope on the endpoint. Intel TDT AI is offloaded to the GPU so that it does not introduce performance impacts, making it a highly effective, low-overhead tool that does not require intrusive scanning techniques or signature databases—leading to improved malware detection. According to testing by SE labs, Intel TDT has been shown to increase overall EDR ransomware protection efficacy by 24% over software alone.[7] This feature is especially useful against threats that do not have a signature to detect, such as malware hiding from disk scanners and zero-day attacks.

Intel® Control-flow Enforcement Technology (Intel® CET)

Intel CET is designed to protect against the misuse of legitimate code through control-flow hijacking attacks. Return/Jump oriented programming (ROP/JOP) are popular attack techniques used in subversion of control-flow. ROP or JOP attacks can be particularly hard to detect or prevent because the attacker uses existing code running from executable memory to change program behavior.

Intel CET provides protection in hardware to defend against control flow subversion techniques. The significance of Intel CET is that it is built into the microarchitecture of the CPU core.

Intel CET is an instruction set extension to implement control flow integrity. It offers two key capabilities to help defend against control-flow hijacking: indirect branch tracking and shadow stack. Indirect branch tracking helps to defend against jump/call-oriented programming (JOP/COP) attack methods. Shadow stack delivers return address protection to help defend against ROP attack methods.

AI PC Enabling: AI for Security & Security for AI

The rapid growth of the AI PCs in the market is poised to make end-point security stronger for consumers and enterprises by introducing revolutionary new security capabilities. Conversely, AI is also speeding up the rate of attacks, including the volume and sophistication of said attacks. As such, AI for security and security for AI are now more critical focus areas for security than ever. AI for security primarily leverages the NPU to enable or enhance security use cases with the goal to provide more privacy, reduced latency, more data for novel detections, and lowered SaaS costs. Security for AI is intended to help protect AI models, thus giving users peace of mind that their AI PC applications are better protected. As hundreds of ISVs are delivering AI based features to run on client xPUs, it's critical that the models and data inputs to these models have enterprise security controls applied.

The Intel vPro® platform provides a more secure computing foundation for AI apps and data with a robust set of security features that PC manufacturers must design into every PC bearing the Intel vPro® badge. In addition, Intel works with the broadest ISV ecosystem in the PC industry to enhance end point security by leveraging and protecting AI solutions running on the client.

AI for Security

Intel is working hand in hand with the ISV security ecosystem to identify and understand new use cases on client security that are now possible by leveraging the GPU and the Neural Processing Unit (NPU). Innovative new AI for security usages include autonomously classifying malware, anti-phishing, deep fake protection, data loss prevention, and more. The industry is truly at an inflection point where cybersecurity as applied on endpoints is being completely reengineered with AI. Alongside these innovations, the ecosystem is being reengineered to enable quicker remediation decisions, lower costs to the ISV, and reduce latency, enabling novel use cases by shifting AI closer to the source with a full set of end point data.

Security for AI

On the other hand, Intel is also working with ISVs to engineer security for AI solutions to protect AI that is running on the client. Intel's existing hardware security capabilities help provide foundational protections for AI models and data at rest or at run time. For example, runtime attacks can target AI applications and user data. Intel is also working with specialized security for AI ISVs that have holistic security controls to protect many types of attacks to AI. These ISVs can provide model scanning to detect the presence of malware, LLM guard railing to prevent model data poisoning attacks, AI firewalling to ensure that internal or external data calls are secure, or that data used for model inference is PII protected. Intel is also one of the driving members for MITRE ATLAS which is an industry information repository of known attack methods to AI. With these ecosystem engagements and security capabilities, Intel is striving to help protect AI models and ensure confidence in adopting AI PC applications knowing that they are better protected.

Intel vPro® Security Summary

As sophisticated attacks continue to evade conventional detection tools and processes, security teams must adopt new technologies and use them to deploy new detection, hunt, and response capabilities. Security teams looking to improve threat intelligence, hunting, analysis, and rapid response capabilities should evaluate hardware-based security solutions.

Hardware-based security delivered as part of the Intel vPro platform, is the bedrock of any security solution. Security solutions rooted in hardware offer a greater opportunity to provide security assurance against current and future threats. Intel hardware, and the added assurance and security innovation it brings, help to harden the layers of the stack that depend on it. In addition, as the PC landscape evolves, Intel is delivering a more secure foundation for AI with industry leading security capabilities in combination with a history of collaboration with the security ecosystem to enable and enhance security use cases while instilling confidence and peace of mind using AI PC applications.

Below-the-OS security is enabled with BIOS and boot flow protection technology. This helps identify unauthorized changes to hardware and firmware by providing visibility into how the OS and BIOS are using hardware protection.
These technologies help to minimize the risk of malicious code injection by locking down memory in the BIOS and help prevent compromising the operating system. Intel PTT acts as a TMP, and stores keys, passwords, and digital certificates. Intel Firmware Update/Recovery focuses on firmware failures and BIOS updates, helping to make end user systems more secure with resilient updates from Day One. With added visibility into firmware security measures, businesses can more accurately assess the security of their systems.

Application and data protections are achieved through Intel virtualization and encryption technologies. This helps prevent memory corruption and tampering attacks. In addition, these technologies help to protect data and virtualized containers with hardware-enforced isolation and encryption. MBEC provides finer grain control on execute permissions to help protect the integrity of the system code from malicious changes. Finally, Intel TME helps prevent cold boot attacks in the event of a stolen system.

Advanced Threat Protections help detect attacks sooner. Using the GPU for active memory scanning, it leaves the CPU available for users to get work done. Hardware telemetry is used to helps identify threats and detect anomalous activity without compromising end user performance. Intel CET helps protect against ROP/JOP attacks. Lastly, Intel TDT not only provides advanced threat detection against ransomware and crypto mining without compromising performance but is also the only AI-based silicon security supported across a billion PCs.[8]

As cyber-attacks continue to evolve, security solutions that help to prevent and solve even the most sophisticated attacks are critical to keeping your business protected. The Intel vPro® platform powered by Intel® Core™ Ultra processors provides comprehensive IT security for your business in the age of AI.

Security starts with Intel. Learn more.

Additional Resources

Intel vPro® Platform

Intel.com/vPro

Intel.com/TDT

Intel vPro Platform Support

Intel.com/support

Intel AI Solutions

Intel.com/AI

Notices & Disclaimers

[1] CrowdStrike, 2024 Global threat report

[2] Verizon, Business 2023 Mobile Security Index

[3] IBM, Cost of a Data Breach Report 2023

[4] 2024 SonicWall cyber threat report

[5] FBI, FBI releases internet crime report

[6] CrowdStrike, CrowdStrike Falcon® Enhances Fileless Attack Detection with Intel Accelerated Memory Scanning Feature

[7] Based on SE Labs – Enterprise Advanced Security (Ransomware) – Intel Threat Detection Technology study published March 2023 (commissioned by Intel), which compared ransomware detection capabilities of an Intel vPro system powered by Intel Core processor against systems powered by AMD Ryzen Pro processors on Windows OS. EDR refers to endpoint detection and response vendor. SE Labs tested Intel's hardware approach to ransomware detection, using a wide range of ransomware attacks similar to those used against victims in recent months. Systems tested included Intel® Core™ i7-1185G7, AMD Ryzen Pro 5675U, AMD Ryzen Pro 5875U, AMD Ryzen Pro 6650U, and AMD Ryzen Pro 6850U. Visit www.intel.com/tdt to learn more.

[8] Intel® TDT provides the only silicon-enabled AI threat detection to help stop ransomware and cryptojacking attacks for Windows-based systems. Details at www.intel.com/performance-vpro. Results may vary

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. No product or component can be absolutely secure.

AI features may require software purchase, subscription or enablement by a software or platform provider, or may have specific configuration or compatibility requirements. Details at www.intel.com/PerformanceIndex. Results may vary.

Intel® technologies may require enabled hardware, software or service activation.

Built into the hardware, Intel® Thread Director is provided only in performance hybrid architecture configurations of 12th Gen or newer Intel® Core™ processors; OS enablement is required. Available features and functionality vary by OS.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps. Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

All versions of the Intel vPro® platform require 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 www.Intel.com/PerformanceIndex/performance-vPro for details.

Nov2024/HM