intel

Modern AI PCs Need Advanced Security

Get robust, intelligent, and multilayered protection with Intel® Core™ Ultra processors and Intel vPro®.

Are your endpoints secured for the new AI era?

AI has opened a new era of opportunities and challenges for enterprises across all industries. In early 2024, 65 percent of survey respondents said their organizations were regularly using generative AI (GenAI)—almost double the percentage reported just 10 months earlier.[1] Organizations are exploring today's AI-everywhere era across a wide spectrum of AI PC usages—from GenAI assistants that unleash new worker productivity to AI-enabled business applications that unleash new experiences and AI developer tools that can infuse AI into corporate apps. All these usages require implementing enterprise-class security before AI is adopted and scaled across the organization.

Many organizations are exploring the benefits of adopting AI beyond the core and across the enterprise. Secure client-to-cloud model training and inference can be run on AI-enabled desktops, laptops, workstations, and other endpoint devices. While AI PCs offer a huge potential for improving end user productivity, they also exponentially increase the surface area for hackers to exploit. AI being run locally on a PC uses sensitive datasets that present an attractively large attack target. Remote workers using AI-enabled client applications present new attack surfaces that are not as protected as they would be inside traditional corporate firewalls.

Should an organization experience a breach, the consequences can be catastrophic. The aftermath could cost millions of dollars in fines and operational downtime, in addition to potentially causing irreparable loss of customer trust and long-term damage to your brand reputation.

45 percent

of organizations say data privacy concerns are major barriers to AI adoption,[2] while 34 percent hesitate over security.[3]

Are your endpoints secured for the new AI era? (cont.)

$4.88 million

One IBM study estimates the average cost of a data breach is 4.88 million US dollars (USD) in 2024, up 10 percent from 2023.[4]

If the above statistic gives you cause for concern, it should. Threats have become more sophisticated, and they continue to evolve. These threats run the gamut from kernel exploits to email phishing, and they target different PC attack surfaces above and below the operating system (OS). AI is being deployed as a weapon against itself, as bad actors can use it to make their attacks harder to detect, more destructive, or both.

Along with safeguarding against active threats, you might also be tasked with meeting internal intellectual property guidelines or regulatory compliance. The Health Insurance Portability and Accountability Act (HIPAA), Telecommunications Act, Family Educational Rights and Privacy Act (FERPA), and Gramm-Leach-Bliley Act (GLBA) are just a few of the many regulations mandating how confidential information is stored, accessed, and used. Does the AI PC help address these data concerns or introduce new requirements with its ability to self-contain data used for AI on client?

Fortunately, there is a comprehensive approach to security that involves hardware and software working together to protect your AI PCs (and help you sleep better at night). This eBook outlines how AI PCs with Intel Core Ultra processors and the Intel vPro platform help strengthen your defenses against modern cyberthreats.

Securely run AI on PCs

As explained previously, today's AI-enabled PCs need advanced data protection that addresses sophisticated threats, system vulnerabilities, and security requirements and that is easily integrated into your currently installed security software. AI PCs powered by Intel Core Ultra processors and built on the Intel vPro platform offer proactive, responsive, and restorative capabilities across multiple layers of hardware, OS, and software.

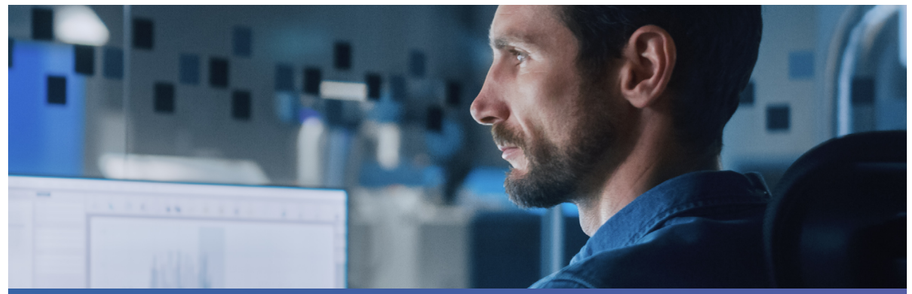
The key to boosting AI security is enhanced visibility into both anomalous behavior and malware activity. Intel vPro foundational protections are now mapped to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) cyberthreats framework and Adversarial Threat Landscape for AI Systems (ATLAS) AI-threats framework, which give you insights into the hardware features that can mitigate real-world attack techniques. These globally accessible knowledge bases help organizations understand the tactics and techniques adversaries use to target AI systems, enabling them to better prepare for and respond to potential threats.

By aligning with ATT&CK and ATLAS, Intel vPro gives AI PCs hardware-enabled, proactive security mechanisms that effectively identify attack behaviors and mitigate potential damage. If your AI PCs are running on Windows 11, then you're in luck. The OS is also aligned with the ATT&CK and ATLAS frameworks. This OS alignment adds another critical layer of security on top of the hardware.

Improve inferencing performance and security

In the new AI era, the humble business PC makes a huge evolutionary leap and becomes today's AI PC. These modern PCs take center stage as a means for driving digital transformation and end-user productivity. They can run inference and other AI applications on-device using data localized to a private, closed environment. They reduce the risk of exposing confidential information and intellectual property (IP) in transit or stored in the cloud.

AI PCs with Intel Core Ultra processors and Intel vPro protect their sensitive data with hardware- and AI-enabled security mechanisms.



Intel vPro hardware-enabled security can reduce the administrative time spent on detecting and resolving security breaches by 35 percent.[5]

The benefits of local inferencing

- **Compliance:** For industries with strict regulatory requirements, local inferencing helps ensure compliance with data protection laws by keeping data within the confines of the device.
- **Control:** Organizations have greater control over their data and models, allowing them to implement custom security measures tailored to their specific needs.
- **Resilience:** Local inferencing can continue to function even if a cloud service is disrupted, ensuring continuous operation and access to critical functionalities.

Add protection below the OS

Users and system-critical software are protected during boot up thanks to hardware-based authentication and security.

Hardware-enabled security using Intel vPro can help reduce material security breaches by up to 23 percent.[5]

Below-the-OS mechanisms include:

Secure boot

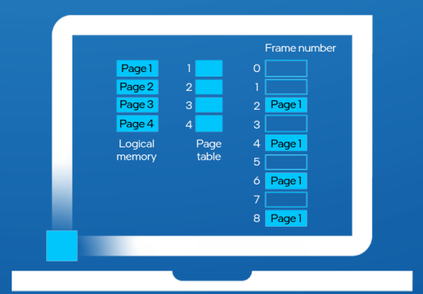
Intel® Boot Guard is below-the-OS security designed to prevent firmware and software attacks that penetrate through the BIOS.

Resilient BIOS

Intel® Runtime BIOS Resilience helps extend security against malicious code injection in Unified Extensible Firmware Interface (UEFI) memory.

Silicon-enabled security

Intel® Partner Security Engine enables system-on-chip (SOC) security mechanisms that can be isolated from other security engines. It uses a dedicated crypto system to offload services such as secure boot, attestation, key storage, and other cryptography.



Prevent kernel exploits and other memory attacks

95 percent of IT leaders surveyed report that cyber-attacks are more sophisticated than ever, and many IT leaders feel unprepared for these new threat vectors.[6] A kernel exploit is an example of a sophisticated attack that compromises the OS kernel.

To mitigate runtime threats, you must protect AI applications and data during OS runtime. User data and files stored on AI PCs with Intel Core Ultra processors and Intel vPro can be protected with Windows BitLocker and CPU-based Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). Intel® Total Memory Encryption (Intel® TME) can help protect memory containing valuable AI model and data assets from cold boot attacks. Windows 11 encrypted VMs built on Intel® TME Multi-Key (Intel® TME-MK) help protect AI models and in-memory data during execution.

Intel® Virtualization Technology (Intel® VT-x) and Intel® Virtualization Technology with Redirect Protection (Intel® VT-rp) help protect virtualized environments by operating in memory during OS runtime. Intel VT-x assigns the hypervisor a higher privilege level, effectively isolating it from guest operating systems. Intel VT-x is also designed to prevent unauthorized access and enforce security policies. Intel VT-rp, only on Intel products, allows only authorized code to modify critical structures, preventing kernel memory corruption. It also mitigates page table attacks and isolates critical data.

Figure 1. Protect virtualized environments from in-memory attacks and unauthorized access with Intel VT-x and Intel VT-rp

Jump-oriented programming (JOP) and return-oriented programming (ROP) memory attacks, which are triggered by user interactions with web browsers, have long eluded software-only solutions. Intel® Control-flow Enforcement Technology (Intel® CET) helps protect against JOP and ROP attacks with hardware-based mechanisms, such as shadow stacks and indirect branch tracking, which block unauthorized software changes and malicious code execution.

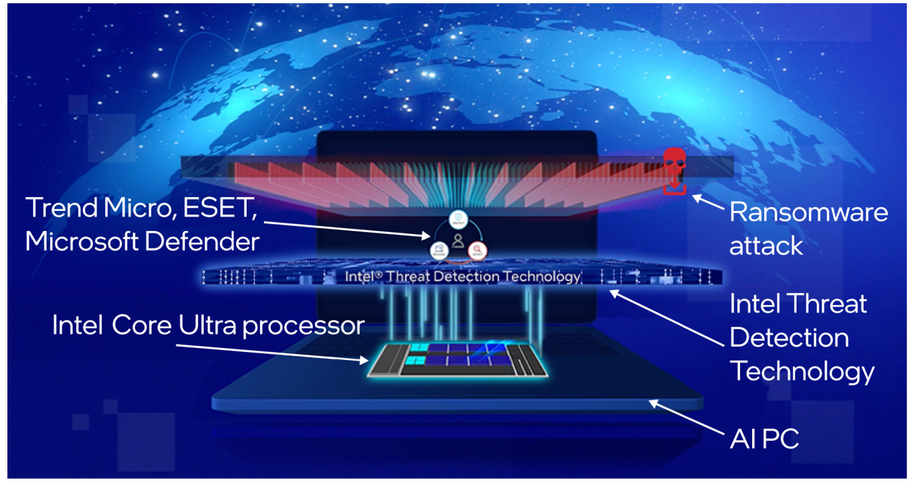
Stop ransomware with AI on client

Ransomware is on the rise. In 2023, 100 percent of businesses surveyed reported experiencing a ransomware attack in the past 24 months.[7] These attacks can be devastating, costing the victim as much as $10 million per incident—and possibly even more.[7]

Ransomware is a formidable threat that requires an equally indomitable security strategy. Traditional strategies built around software and data backups are no longer enough. Your security plan needs to include training users to recognize phishing attempts and suspicious behavior. Your endpoint security must evolve beyond heuristic algorithms; it must be smart enough to identify novel threats as they emerge.

Traditional endpoint detection-and-response software is often ineffective against sophisticated threats like ransomware because it relies on known signatures. Intel vPro with Intel® Threat Detection Technology (Intel® TDT) ups your security game by uncovering novel attack behaviors in real time and working with your security software to help stop ransomware in its tracks. This AI-driven, hardware-enforced approach is also effective against fast-evolving variants or attacks that use obfuscation techniques.

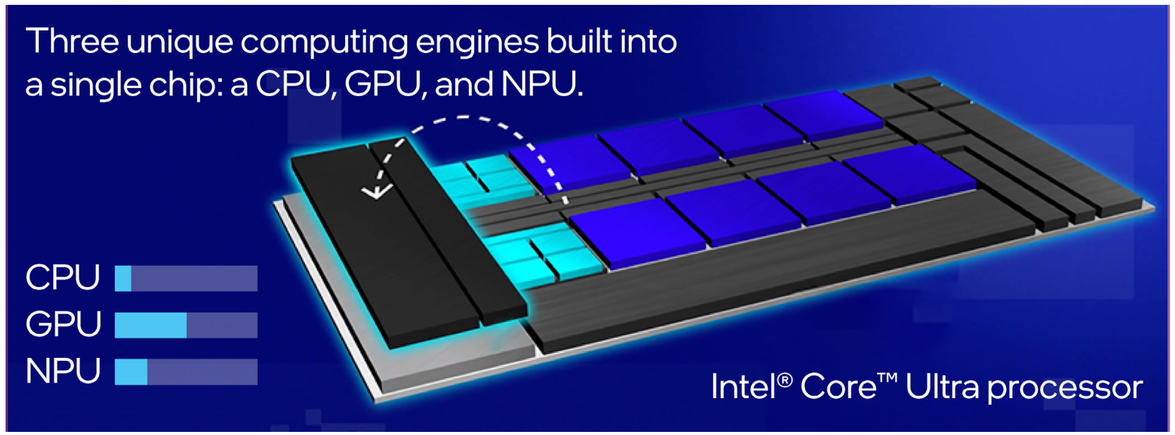
Trend Micro, ESET, Microsoft Defender, and other leading ISV solutions can make use of Intel TDT technology out of the box. As an added benefit, Intel TDT activity is offloaded to the GPU, which helps ensure that your users' computing experiences are not disrupted by the additional security processing.



Intel TDT uses AI and hardware to improve threat detection by at least 24 percent compared to software-only mechanisms.[8]

Boost your existing security software with three unique computing engines

AI PCs with Intel Core Ultra processors combine three computing engines built into a single chip: a CPU, GPU, and neural processing unit (NPU, an AI and machine learning [ML] engine). Intel works closely with ecosystem partners to provide holistic security solutions that protect end users and devices from below the OS and up through the stack. Intel also collaborates with ISVs to ensure your third-party solutions integrate seamlessly and perform reliably.



The following software solutions are optimized for Intel Core Ultra processors:

LiveDrop
Utilizes the NPU and GPU for hardware-accelerated file transfers, making it ideal for environments that require secure offline data transfers.

Proofpoint
Uses the NPU to run sophisticated data loss prevention (DLP) tools on endpoint devices without impacting user productivity. Proofpoint also adds autonomous protection of sensitive data, blocking of unauthorized exfiltration, and real-time security notifications.

BUFFERZONE SafeBridge AI
Uses the NPU or GPU to create isolated virtual environments and document analysis for malware using content disarm and reconstruction (CDR) technology.

BUFFERZONE Safe Data
Uses the NPU or GPU to intelligently scan and classify files containing sensitive data directly on the device, securing them in a virtual vault accessible only by authenticated users. This threat detection and analysis happens quickly and efficiently, without impacting user productivity.

Take a holistic approach to security

New and emerging threats require a more intelligent security approach. Intel Core Ultra processors and Intel vPro provide AI-boosted endpoint protections that start at the hardware layer, run through the software stack, and extend across the ecosystem. It takes AI-powered tools to protect against today's pervasive and AI-enhanced threats like ransomware and phishing attacks. If you deploy AI PCs with Intel Core Ultra processors and Intel vPro, these intelligently adaptive and proactive safeguards deliver a "hidden layer" of protection that works without you needing to configure anything.

When it's time to upgrade your organization's PCs, feel confident in your decision by opting for solutions based on generations of tested IT development, built with security integrated at every step, and backed by dedicated teams evaluating security resilience.

With their advanced AI and security capabilities, AI PCs powered by Intel Core Ultra processors and built on the Intel vPro platform offer a security solution that is smart enough to safeguard your data, comply with regulatory requirements, and maintain operational continuity. So, why not put them to work and turn your efforts toward driving innovation and growing the business?

Learn more at intel.com/AIPC and intel.com/vpro.

Intel ranked #1 in product security assurance

An independent study from ABI Research assessed top silicon vendors on the innovation and implementation of their security assurance practices.[9]

[1] McKinsey. "The state of AI in early 2024: Gen AI adoption spikes and starts to generate value." May 2024.
[2] Searce. "STUDY: AI Adoption Spends Jump Among Enterprises as Eliminating Data Privacy Concerns Remains a Foremost Opportunity for Driving Long-Term Growth and ROI." *BusinessWire*. August 2024.
[3] DigitalOcean. "AI and Privacy: Safeguarding Data in the Age of Artificial Intelligence." Accessed October 2024.
[4] IBM. "Cost of a Data Breach Report 2024." July 2024.
[5] Based on an Intel-commissioned study by Forrester Consulting, which surveyed 500 IT decision-makers (ITDMs) at enterprises across the world using Intel vPro, including ITDMs in the US, Canada, France, Germany, the UK, Australia, China, India, and Japan. For the study's findings, Forrester Consulting aggregated the data and experiences from the interviewees into a composite organization with an assumed revenue of $1 billion per year and 10,000 employees. Source: Forrester Consulting. "The Total Economic Impact™ of the Intel vPro® Platform." Commissioned by Intel. January 2024.
[6] Cisco. "Cisco Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette." June 2024.
[7] Cybereason. "Ransomware: The True Cost to Business 2024." 2024.
[8] Intel. "Intel® Threat Detection Technology: Protect Your PC Fleet from Advanced Cyberattacks." Accessed February 2025.
[9] ABI Research. "Embracing Security as a Core Component of the Tech You Buy."Accessed February 2025.