

Intel vPro® and Security

Adapting to the Evolving Landscape of Cybersecurity

Adapting to the Evolving Landscape of Cybersecurity

Since its introduction in 2006, Intel vPro® has been at the forefront of business computing, adapting to the ever-changing landscape of emerging threats and evolving technologies. As cybersecurity challenges have expanded from isolated system breaches to complex attacks across entire networks, Intel vPro® has consistently evolved to meet these new threats.

Today, malicious actors are no longer merely data thieves; they have become adept at commandeering entire computing resources, using PCs at remote endpoints as direct vectors into extensive networks, cloud, and SaaS applications. The shift from traditional office setups to remote work has also transformed the cybersecurity battleground, moving from reliance on firewall and VPN protections to a more dispersed security framework.

Hardware at the Heart of Security

Intel vPro® platform powered by Intel® Core™ Ultra™ Ultra processors, stands at the forefront of this battle. It offers a multi-layered defense strategy that is essential for robust cybersecurity. This integrated approach is crucial in a world where 75% of cyber-attacks begin as memory-resident, file-less malware, and 90% originate from endpoint breaches.

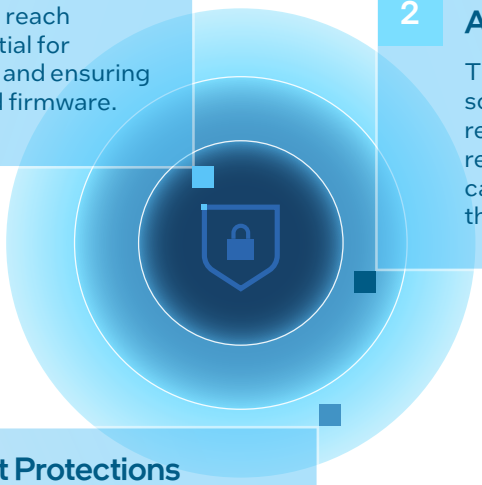
With Intel vPro®, security starts at the silicon level. The platform offers built-in security features that help protect, detect, and recover from cyber threats. By implementing defenses at the hardware level, Intel provides a foundational security layer that is harder for attackers to bypass, complementing and strengthening any software security measures.

Intel vPro®: A Comprehensive Security Structure

Intel vPro® platform's robust security architecture is structured around three core groups of solutions, each designed to fortify critical aspects of business security:

1 Below-the-OS Security

This foundational layer helps protect the system at the firmware and hardware levels, blocking threats before they can reach the operating system. It is essential for preventing unauthorized access and ensuring the integrity of the hardware and firmware.



2 Application and Data Protections

The highest layer involves deploying sophisticated techniques to detect and respond to advanced threats. This includes real-time monitoring and automated response capabilities that can identify and mitigate threats before they cause significant damage.

3 Advanced Threat Protections

At this layer, Intel vPro® helps secure the applications and data that are vital to business operations. This includes enhancing protection of sensitive information from unauthorized access and ensuring that applications run securely.

According to CrowdStrike's 2024 global threat report*, 75% of all attacks first execute as file-less malware in memory while 90% of attacks originate at the endpoint.

* https://www.crowdstrike.com/global-threat-report/

Below-the-OS Security

By providing a more secure and protected boot environment, these hardware-based technologies can verify the integrity of firmware and the OS as they are loaded and help protect the BIOS firmware and main memory starting at boot-up.

Intel® BIOS Guard

Firmware protection in non-volatile memory

Intel® BIOS Guard is a BIOS Flash update hardening technology that minimizes the trust boundary for updates, reducing the risk of Flash-based attacks like rootkits and persistent denial of service. It uses Model State Register (MSR) cycles to authenticate updates, creating a smaller attack surface and ensuring that Flash writes can only occur in a secure environment.

Intel Firmware Update/Recovery

Recovery to a last known good state if a firmware update fails

Intel® Firmware Update/Recovery enables secure firmware updates and recovery from failures, ensuring fault-tolerant deployment. In case of interruptions, the system automatically reboots to a last known good state and restarts the update process without requiring user intervention.

Intel® Runtime BIOS Resilience

BIOS environment lock-down during runtime

Intel® Runtime BIOS Resilience secures the System Management Mode (SMM) environment by locking the page table during runtime, preventing unauthorized modifications. This ensures OS memory remains inaccessible from SMM, significantly reducing the risk of malware injection and enhancing platform security against runtime attacks.

Intel® Trusted Execution Technology

Dynamic root of trust

Intel® Trusted Execution Technology (Intel® TXT) enables the OS or hypervisor to establish a Measured Launch Environment (MLE), ensuring a secure and controlled system launch. By verifying behaviors and configurations against a "known good" benchmark, it quickly detects and prevents tampering during boot time and supports TPM-based attestation for UEFI firmware and OS authenticity.

Intel® Boot Guard

Cryptographically-verified boot

Intel® Boot Guard provides hardware-based boot integrity by verifying the correctness of the Initial Boot Block (IBB) code before the CPU starts execution, ensuring a secure boot process. By acting as a hardware root of trust, it strengthens the chain of trust and reduces the risk of malware exploiting hardware or software vulnerabilities during system boot.

Intel® Platform Trust Technology

Integrated trusted platform module

Intel® Platform Trust Technology (Intel® PTT) is an integrated Trusted Platform Module (TPM) that securely stores keys, passwords, and digital certificates within the Intel vPro® platform. It meets Windows OS hardware requirements while optimizing for low power consumption and supports Trusted Computing Group 2.0 and FIPS 140-2 certifications.

Intel® System Resources Defense

System management mode protections

Intel® System Resources Defense enhances platform security by restricting System Management Interrupt (SMI) handlers' access to hardware resources, reducing the attack surface in System Management Mode (SMM). By isolating the OS's trusted compute base from SMI handlers, it minimizes the risk of vulnerabilities being exploited to compromise OS security.

Intel® System Security Report

Security configuration communication to the OS

The Intel® System Security Report provides a trusted, one-time hardware-to-software report during OS boot, offering below-the-OS security visibility. Working alongside Intel® TXT, it communicates critical policies to the OS, ensuring that hardware and resource access from firmware SMI handlers are securely monitored.

Intel® Partner Security Engine

Enables third-party firmware to run securely on Intel silicon

The Intel® Partner Security Engine, powered by Intel® Core™ Ultra processors, is a dedicated security engine that securely runs third-party signed firmware on Intel silicon. It isolates sensitive data, such as encryption keys, from the rest of the system, protecting it from advanced attack techniques like speculative execution.

Application & Data Protections

Intel vPro® employs advanced virtualization and encryption technologies to establish robust protections at the application and data level, effectively countering a spectrum of attacks that bypass traditional software-only solutions.

Intel® Virtualization Technology

Hardware support for virtualization-based security

Intel® VT-x enhances security by isolating secure workloads from the main OS, creating a firewall that prevents malware in the OS from accessing sensitive data in virtual machines. It combines hardware-enforced isolation and encryption to protect memory confidentiality, ensuring high performance while enabling quick recovery from compromised systems without disrupting other workloads.

Intel® VT-d

Intel® Virtualization Technology for Directed I/O

Detects unauthorized DMA and interrupts

Intel® VT-d enhances security by isolating I/O devices and protecting workloads from unauthorized Direct Memory Access (DMA) initiated by the main OS. It improves system reliability by detecting and reporting DMA or interrupts that could otherwise compromise memory or VM isolation. It maintains a secure firewall between malware running in the main OS and secure workloads running inside a secure VM.

Intel® VT-rp

Intel® VT-Redirect Protections

Hardware-based protection for the OS kernel

Intel® VT-rp provides hardware-based support for kernel page protections, defending against memory corruption and page table attacks. By preventing aliasing and page remapping with minimal performance impact, it ensures the OS kernel and critical data remain secure from malicious threats.

Intel® LASS

Intel® Linear Address Space Separation

Protects against Kernel Exploitation

Intel® LASS enhances security by separating privilege levels based on linear addresses, preventing attackers from using various techniques to expose the layout of the kernel address space and gain memory address mappings. This defense protects against kernel exploitation techniques, such as meltdown-style side-channel attacks, ensuring the safety of critical data and credentials.

MBEC

Mode-Based Execution Control

Enforce the integrity of kernel-level code

MBEC virtualization provides an extra layer of protection from malware attacks in a virtualized environment. It enables hypervisors to verify and enforce the integrity of kernel-level code more reliably. It refines permissions through Extended Page Tables, separating execution rights for user and supervisor pages.

Kernel DMA Protection

Blocks peripheral devices from unauthorized access to system memory

DMA-capable devices can read and write to system memory without having to engage the system processor. Kernel DMA Protection prevents unauthorized access to system memory by blocking malicious peripheral devices. Built on Intel® VT-d, this feature is supported on modern Windows, macOS, and Linux systems.

Intel® AES-NI

Intel® Advanced Encryption Standard New Instructions

Makes pervasive encryption feasible

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.

Advanced Programmable Interrupt Controller (APIC) Virtualization

Better inter-partition protection through virtualization

Virtual machine monitors (VMM) emulate most guest accesses to interrupts and the APIC in a virtual environment. APICv enhances security by handling guest interrupts directly in hardware rather than through the VMM, reducing overhead and increasing I/O throughput.

Intel® Total Memory Encryption (Intel® TME)

Encryption of data in endpoint system memory

Intel TME encrypts all system memory and enables confidentiality of DRAM/NVRAM that is outside the system processor package. 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.

Advanced Threat Protections

Advanced Threat Protections within Intel vPro® encompass a suite of cutting-edge technologies designed to detect sophisticated cyber threats that traditional methods may miss. These technologies leverage hardware capabilities to enhance system performance and efficiency while targeting and mitigating threats such as ransomware and cryptomining with minimal impact on the user experience. Intel vPro® platform powered by Intel® Core™ Ultra processors delivers a comprehensive suite of hardware-based security technologies for advanced threat protection.

Intel® TDT

Intel® Threat Detection Technology

Increases the effectiveness/efficiency of security software

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.

Intel® Threat Detection Technology – Accelerated Memory Scanning

Offloads memory scanning to enhance malware detection

Accelerated Memory Scanning enhances malware detection by offloading memory scanning to the integrated GPU, increasing efficiency while reducing performance overhead. This approach enables ISVs to expand detection coverage for file-less malware hiding in system memory, providing faster and more detailed threat identification.

Intel® Threat Detection Technology – Advanced Platform Telemetry

Combines machine learning with hardware telemetry

Advanced Platform Telemetry combines machine learning with hardware telemetry to detect exploits and suspicious behavior without relying on intrusive scanning or signature databases. Offloaded to the GPU for minimal performance impact, it enhances ransomware protection and is particularly effective against zero-day threats and undetectable malware.

Intel® CET

Intel® Control-flow Enforcement Technology

Helps protect against memory safety attacks

Intel® CET defends against control-flow hijacking attacks like Return-Oriented Programming (ROP) and Jump-Oriented Programming (JOP) by providing hardware-based protections. With features like indirect branch tracking and shadow stack, Intel CET ensures control flow integrity and safeguards systems against malicious code misuse.

These Advanced Threat Protections form a critical component of Intel's comprehensive security architecture, providing robust defenses against evolving cyber threats while maintaining optimal system performance and user transparency.

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:

https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-security/overview.html



Performance varies by use, configuration and other factors. Learn more at intel.com/PerformanceIndex
Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for additional details.
No product or component can be absolutely secure.
Your costs and results may vary.
Intel technologies may require enabled hardware, software or service activation.
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 intel.com/performance-vpro for details.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.
Other names and brands may be claimed as the property of others.