White Paper

Information Technology
Cybersecurity

Intel® Hardware Shield Overview

Intel Business Client Platform Security Marketing

Introduction

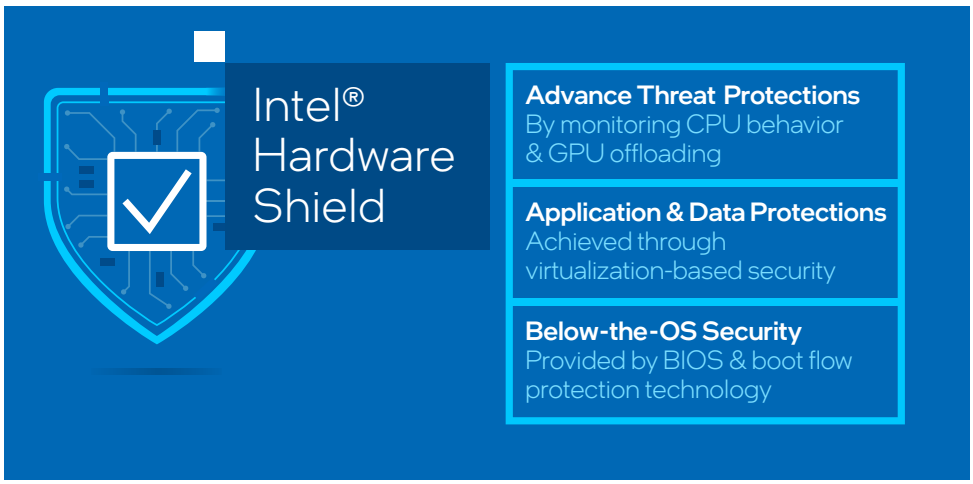
This document covers security features in Intel® Hardware Shield on the Intel vPro® platform. Intel Hardware Shield comes "out of the box" with the Intel vPro platform. Intel Hardware Shield has three groups of security technologies. The three groups are: below-the-OS security, application and data protections, 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 Hardware Shield?

Security matters more than ever as cyber-attacks 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. On top of all that, IT and information security professionals also face increasing regulatory compliance requirements for data localization and information privacy.

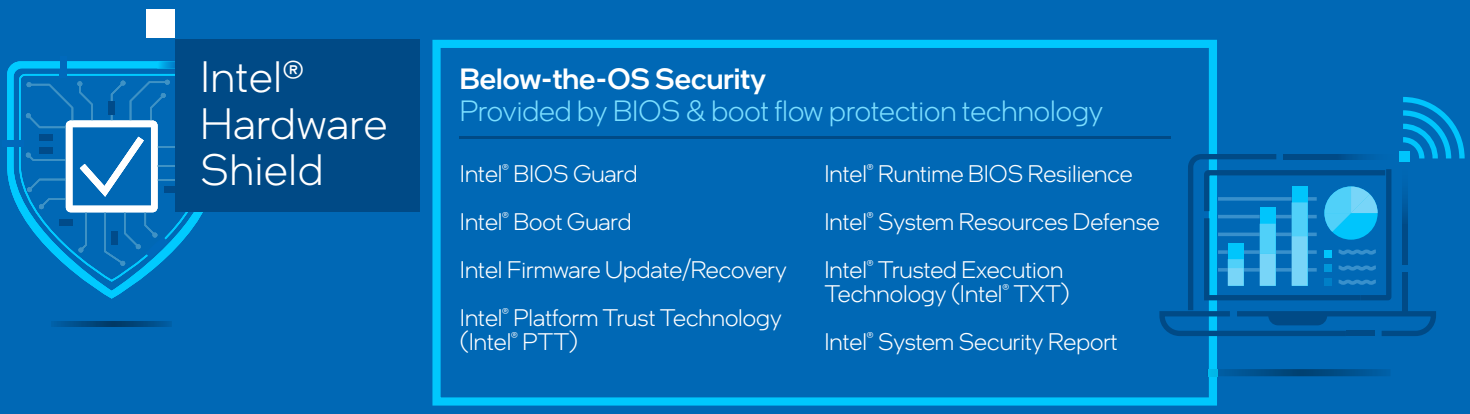
Many types of attacks target operating systems (OSs), browsers, applications, firmware and BIOS, in addition to system memory. According to TrendMicro's Zero Day Initiative, 63.2% of the 1,097 threats disclosed from 2019 to today were memory safety related.[1] In 2019, a leading data management solutions provider estimated that ransomware attacks alone had increased by 97% in two years causing $20 billion in damages,[2] while only 75% of companies attacked by ransomware ran up-to-date endpoint protection software.[3]

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 works with our partners to build security solutions that aim to help solve the toughest security problems. Intel Hardware Shield security technologies—the latest versions are available on the new 11th Gen Intel® Core™ vPro® mobile processors—aim to stay ahead of bad actors. Intel Hardware Shield provides built-in security features to help organizations protect, detect and recover from cyber-attacks in an increasingly challenging threat landscape.

Although no feature or set of features provide absolute security, Intel Hardware Shield delivers the world's most comprehensive hardware-based security for business, as delivered by 11th Gen Intel Core vPro mobile processors. As security threats continue to adapt and attack lower levels within a system's resources, the feature roadmap of Intel Hardware Shield continues to evolve. Continuing product improvement and investment is crucial to meeting customer needs. Intel technologies and products operate 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 Hardware Shield: **Below-the-OS Security**

The Intel Hardware Shield category of below-the-OS security is comprised of hardware-based technologies to help provide a trusted execution environment and to help protect the 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 from the trust boundary the System Management Interrupt (SMI) handler and nearly all of the power-on self-test (POST) BIOS, as well. 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 writes 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 also 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 is a form of an Intel® Trusted Platform Module. This feature of Intel Hardware Shield includes the capabilities of an Intel TPM 2.0 within the Intel vPro platform for storing keys, passwords, and digital certificates. 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 of Intel Hardware Shield 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

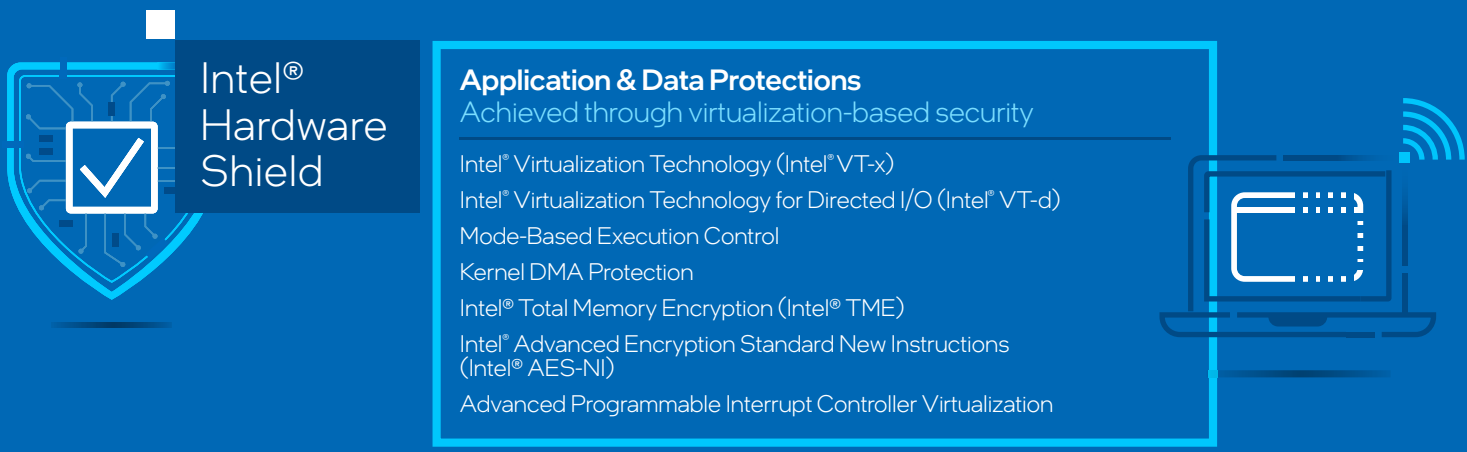
Intel® Trusted Execution Technology (Intel® TXT) is the technology that the OS or hypervisor can use to initiate a measured and controlled launch of system software called the Measured Launch Environment (MLE). The MLE is a protected environment. Generally, the OS or hypervisor uses Intel TXT to establish 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 supports Intel TPM 2.0. It also supports the Intel PTT (a form of TPM 2.0). Intel TXT can work with a discrete Intel TPM or with Intel PTT. In addition, Intel TXT with Intel 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 Hardware Shield: **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. The security technologies in this category include: Intel® Virtualization Technology (Intel® VT-x), Intel® Virtualization Technology for Directed I/O (Intel® VT-d), Mode-Based Execution Control, Kernal DMA Protection, Intel® Total Memory Encryption (Intel® TME), Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and Advanced Programmable Interrupt Controller Virtualization.

Intel® Virtualization Technology

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 also protects confidentiality of memory content from a physical attacker, while providing the performance needed to run virtualization-based workloads without impact to the user experience. An example of how an isolated execution environment provides security is 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 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

For more system security, Intel Hardware Shield complements virtualization security with memory encryption. 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 improves on the Advanced Encryption Standard (AES) algorithm and accelerate 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 AES-NI 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 Virtualization

Virtual machine monitors (VMMs) emulate most guest accesses to interrupts and the advanced programmable interrupt controller (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® Hardware Shield

Advance Threat Protections
By monitoring CPU behavior & GPU offloading

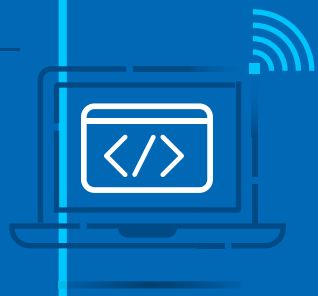
Intel® Threat Detection Technology (Intel® TDT)

Intel® Threat Detection Technology – Accelerated Memory Scanning

Intel® Threat Detection Technology – Advanced Platform Telemetry

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

*Available on 11th Gen Intel® Core™ vPro® mobile processors



Intel Hardware Shield: **Advanced Threat Protections**

Advanced threat protections are a group of technologies 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® Threat Detection Technology (Intel® TDT) is a set of technologies that harness silicon-level telemetry and acceleration capabilities to help identify threats and detect anomalous activity. Intel TDT analyzes data to help identify polymorphic malware, file-less scripts, cryptomining, and other targeted attacks – in real time, and with minimal end user impact.

In today's threat environment, security systems must do more than log events. They must also reduce false-positive alerts, long the bane of security applications. Intel TDT uses machine learning heuristics to both detect persistent attacks in real-time while also reducing false positives. Developers now can leverage Intel TDT detection functions to improve threat detection, while tuning performance variables and false-positive rates that deliver the proper balance for their security solutions.

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

Intel Threat Detection Technology – Accelerated Memory Scanning (AMS) enables memory scanning for malware to be offloaded to the GPU. This method improves memory-scanning efficiency while lowering performance overhead, which ultimately expands detection coverage for malware hiding in system memory.

Current scanning technologies can detect system memory-based cyberattacks, but at the cost of CPU performance. CPU based scanning involves scanning memory for thousands of patterns. CPU usage becomes very high, leaving little room for other programs. AMS enables certain real time memory scanning operations to be migrated from the CPU to the Intel integrated GPU. As a result, threat detection is enhanced without impacting the user experience or reducing battery life. Because it does not slow down the end user's system, users will allow more scanning, resulting in more security coverage.

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 highly effective, low-overhead tool that does not require intrusive scanning techniques or signature databases—leading to improved malware detection. 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® Control-flow Enforcement Technology (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. JOP or ROP 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 return-oriented programming (ROP) attack methods.

Intel Hardware Shield 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.

Intel Hardware Shield, 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.

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, and Intel TDT provides advanced threat detection against ransomware and cryptomining without compromising performance.

Additional Resources

Intel vPro® Platform
Intel.com/vPro

Intel.com/HardwareShield

Intel vPro Expert Center

Intel vPro Platform Support
Intel.com/support

[1] https://www.zerodayinitiative.com/advisories/published/, 2020
[2] https://www.veeam.com/ransomware-protection.html, 2020
[3] Sophos, Understanding ransomware and the impact of repeated attacks, February 2018
[4] In thin & light Windows-based PCs, as measured by December 2020 IOActive study (commissioned by Intel.) The study compared the 11th Gen Intel Core vPro mobile Intel Hardware Shield hardware-based security capabilities within these categories: Below-the-OS, Application & Data Protection, and Advanced Threat Protection, with all available corresponding technologies of the AMD Ryzen Pro 4750U. IOActive also analyzed respective security assurance processes and performed some feature testing. Visit www.Intel.com/11thgenvpro for details. No product or component can be absolutely secure. Results may vary.

0521/MZ/DCC/PDF