intel

# Windows 11 Security Starts with an Intel Hardware Foundation

# A Secure Foundation Rooted Deep in Silicon

## According to a Windows 11 Survey Report, new Windows 11 PCs are more secure, with a reported 62% drop in security incidents and 3x reported reduction in firmware attacks.[1] But that doesn't tell the whole story.

That's because software, as critically important as it is, makes up only part of the compute system. With Windows 11, Microsoft and Intel continue a long-standing co-engineering commitment to platform performance, stability, fleet manageability, and – most importantly – security. Windows 11 security protections from Intel are part of a comprehensive strategy based on hardware layers of security from chip to cloud.

Intel vPro® Security is designed to meet and exceed Microsoft's Secured-core PC requirements, which are covered later in this document. Intel and Microsoft validated that Intel vPro Security provides over 90 hardware-assisted mitigations designed to prevent real-world attack techniques[2] as defined by the MITRE ATT&CK framework.

At runtime, Windows 11 takes advantage of Intel® Core™ Ultra features to help protect applications and data with accelerated encryption and accelerated virtual machine (VM) isolation. Intel hardware enables and accelerates advanced threat protections by enforcing OS-level program legitimacy and helps endpoint detection & response (EDR) tools such as Microsoft Defender for Endpoint respond to threats like ransomware, crypto jacking, and fileless malware attacks without degrading the user experience.

With Intel vPro® Security capabilities like threat detection and deep hardware and software integration across the stack, customers can experience the highest levels of security out-of-the-box. Using out-of-the-box security protections, Intel vPro® platforms offer a 70% attack surface reduction compared to older PCs[3]. Let's explore how Intel Core Ultra processors and Intel vPro® Security help drive these improvements.

# Secure AI: Preparing for the Future of AI

The advent of the AI PC is driving new software and productivity tools that will lean on artificial intelligence built into work machines. PCs powered by new Intel Core Ultra processors will fill many of those requirements.

The age of the AI PC started with the release of Intel Core Ultra processors, with both integrated GPU and NPU accelerators capable of running AI workloads entirely on client PCs. Intel has enabled over 400 AI features from 200 independent software vendors (ISVs) spanning all types of enterprise workloads. **Security for AI** is designed to protect AI models so users have peace of mind that their AI PC applications are better protected. It's critical that both models and data apply enterprise-grade security controls.

Since runtime attacks can target AI applications and user data, data needs to be encrypted and executed securely as it runs on the CPU, GPU, or NPU. Intel works with ISVs that develop holistic security controls that help protect AI. These ISVs scan models to detect malware, put guardrails around LLMs to prevent data poisoning attacks, firewall AI to help secure internal/external data calls, or protect personally identifiable information (PII) used for AI model inference.

Intel and Microsoft collaborated to document new AI attacks for the MITRE ATLAS project, bringing the industry together to outline attack tactics and countermeasures. Intel has documented over 30 attack tactics under MITRE ATLAS for which our hardware foundation can provide mitigations.

The updated Intel vPro platform has the most comprehensive security yet, integrated directly into the silicon. Features like advanced threat detection demonstrate **AI for Security**, using machine learning and CPU telemetry to improve detection of malicious code. Intel vPro Security can isolate sensitive operations and data, making it harder for malicious software to access them. It's the first time a hardware-assisted security system has been validated by the MITRE ATT&CK framework, which means it's been tested and proven to protect against over 150 real-world cyberattack techniques[4].

Combatting today's threats requires defense-in-depth — a robust security stack where hardware and software are tightly optimized to bolster overall security posture. Having insights into both software and hardware-based security measures can help enterprises unlock the full potential of a modern Intel AI PC fleet designed to advance the state of the art in cybersecurity.

# Designed for Windows 11 Security

In the Windows 11 Security Book, Microsoft defines six security categories ranging from chip to cloud.[1]

**Cloud Services** includes the remote out-of-band endpoint management and recovery capabilities of Intel® Active Management Technology (Intel® AMT) and Intel® Endpoint Management Assistant (Intel® EMA). With Intel AMT and Intel EMA, IT can install software or patch devices remotely, erase disks, reimage disks, and reboot remote devices—everything they could do if they were physically there, all from the cloud. Managed devices can reside in the public or private cloud, and the console can reside in a public or private cloud or at the edge.

The endpoint protection categories include:

- **Identity & Privacy:** secured identity and privacy controls
- **Application:** application security and privacy controls
- **Operating System:** encryption & data protection, network security, and virus & threat protection
- **Hardware:** hardware root-of-trust and silicon-assisted security
- **Security Foundation:** security assurance, certification, and secure supply chain

Intel hardware-based security capabilities help deliver maximum protection and minimum impact on users' productivity/experience. Intel technologies, programs, and practices range from hardware and firmware protections below-the-OS to application, data, and advanced threat protections up and down the stack.

Intel is an industry leader in creating and operating comprehensive ecosystem programs and practices to help assure the security of systems and their components throughout their lifecycle, across the value chain. Let's take a closer look.

## Mitigations for Windows 11, Secured-core PC, Microsoft Defender

**90**

MITRE ATT&CK® Mappings.[1]

## Proactive security posture

**70%**

Reduction in attack surface compared to 4-year-old devices with Intel vPro®.[2]

## Most comprehensive security

**30**

Unique vPro security features to help enable the most secure Windows 11.[1]

## Protect against evolving threats

**62%**

Reported drop in incidents.[3]

1. Intel, AI PCs Deliver an Industry Validated Defense vs. Real World Attacks, 2025.
2. Based on IQActive's "Intel vPro® 13th Gen Attack Surface Study" published March 2023 (commissioned by Intel), which evaluates Intel vPro® devices powered by 13th Gen Intel® Core™ processors against four-year-old Intel-based PCs.
3. Windows 11 Survey Report. Techaisle, September 2024. Windows 11 results are in comparison with Windows 10 devices.

| | | | | |
|---|---|---|---|---|
| **Cloud** | **Cloud Services**<br>**Protecting your work information**<br>Azure Active Directory<br>Modern Device Management<br>  MDM Security Baseline<br>Windows Autopatch | Microsoft Endpoint Manager<br>  Remote Wipe<br>Secured-core Configuration Lock<br>Windows Autopilot and Zero-Touch Deployment | Universal Print<br>Microsoft Azure Attestation Service<br>Azure Code Signing<br>Microsoft OneDrive | **Protecting with Microsoft Accounts**<br>Microsoft Account<br>Find my Device<br>OneDrive Personal Vault |
| **Identity** | **Secured Identity**<br>Enabling Passwordless Sign In<br>Windows Hello (for Business)<br>  Temporary Access Pass<br>  Cloud Trust<br>Microsoft Authenticator<br>Fast Identity Online (FIDO) | Windows Hello<br>  PIN<br>  Windows Presence Sensing<br>  Enhanced Sign in Security<br>Simplified Sign in for EDU<br>Enhanced Phishing Detection/Protection | Advanced Credential Protection<br>  Windows Credential Guard<br>  Windows Defender Remote<br>  Credential Guard<br>Smart Cards<br>Access Management | **Privacy**<br>Transparency and Audit Trail<br>location, camera, and microphone<br>Use of diagnostic data |
| **Application** | **Application Security**<br>Smart App Control<br>User Account Control (UAC) | Windows Defender Application Control (WDAC)<br>App isolation | App containers<br>Developing secure applications | |
| **Operating System** | **Encryption and Data Protection**<br>BitLocker<br>Encrypted Hard Drive<br>Personal Data Encryption<br>Email Encryption | **Network Security**<br>Transport Layer Security (TLS)<br>DNS Security<br>Bluetooth protection<br>Securing Wi-Fi Connections<br>Windows Defender Firewall<br>VPN<br>SMB File Services | **Virus and Threat Protection**<br>Microsoft Defender AntiVirus<br>Additional Protection for Local Security Authority<br>Attack Surface Reduction<br>Tamper Protection<br>Microsoft Vulnerable Driver Blocklist<br>Controlled Folder Access<br>Exploit Protection<br>Enhanced Phishing Protection Microsoft Defender SmartScreen<br>Microsoft Defender for Endpoint | **System Security**<br>Trusted Boot<br>Cryptography<br>Certificates<br>Cookie Signing and Integrity<br>Device Health Attestation<br>Windows Security Policy Setting and Auditing<br>Windows Security App |
| **Hardware (Chip)** | **Hardware Root-of-Trust**<br>TPM 2.0<br>Microsoft Pluton Security Processor | **Hardware Root-of-Trust**<br>Secured Kernel (HVCI enabled by default)<br>Hardware Enforced Stack Protection | Secured-core PCs<br>Firmware Protection | |
| **Security Foundation** | **Offensive Research**<br>Software Development Lifecycle<br>Microsoft Offensive Research and Security Engineering<br>OneFuzz | Microsoft Insiders and Bug Bounty Program | **Certification**<br>CC<br>FIPS | **Secure Supply Chain**<br>Software Bill of Materials (SBOM)<br>Azure Code Signing |

**Figure 1. Microsoft Windows 11 Security from Chip to Cloud**
Windows 11 security categories, as defined in the Windows 11 Security Book.

| | | | | |
|---|---|---|---|---|
| **Cloud** | **Cloud Services**<br>Intel® AMT with Intel® Active Management Technology<br>Intel® EMA with Intel® Endpoint Management Assistant<br>Intel® Remote Platform Erase | Intel® One Click Recovery<br>Intel® PTT<br>Intel® Boot Guard | Intel® Runtime BIOS Resilience<br>Intel® System Security Report<br>Intel® System Resources Defense | Intel® AES-NI |
| **Identity** | **Secured Identity**<br>Intel® VT-x<br>Intel® VT-d | Intel® TME<br>Intel® TME-MK | Intel® PTT | N/A |
| **Application** | **Application Security**<br>Intel® VT-x<br>Intel® VT-d | Intel® TME<br>Intel® TME-MK | | |
| **Operating System** | **Encryption and Data Protection**<br>Intel® AES-NI<br>Intel® PTT | **Network Security**<br>N/A | **Virus and Threat Protection**<br>Intel® TDT<br>Intel® VT-x<br>Intel® UMIP<br>Intel® VT-d<br>Intel® TME<br>Intel® MBEC<br>Intel® TME-MK<br>Intel® VT-rp<br>Intel® CET | **System Security**<br>Intel® TDT<br>Intel® TXT<br>Intel® Boot Guard<br>Intel® Secure Key<br>Intel® PTT<br>Intel® VT-x<br>Intel® AES<br>Intel® TME<br>Intel® AES-NI<br>Intel® TME-MK<br>Intel® Runtime BIOS Resilience<br>Intel® System Security Report<br>Intel® System Resources Defense<br>Intel® BIOS Guard |
| **Hardware (Chip)** | **Hardware Root-of-Trust**<br>Intel® CSME<br>Intel® PTT | **Silicon Assisted Security**<br>Intel® CET<br>Intel® TXT<br>Intel® MBEC<br>Intel® VT-d<br>Intel® PTT<br>Intel® VT-x | Intel® VT-rp<br>Intel® TME<br>Intel® Boot Guard<br>Intel® TME-MK | Intel® Runtime BIOS Resilience<br>Intel® System Security Report<br>Intel® System Resources Defense |
| **Security Foundation** | **Offensive Research**<br>Intel® Security Assurance | | **Certification**<br>Intel® CSME<br>Various Crypto | **Secure Supply Chain**<br>Intel® Tiber™ Transparent Supply Chain |

**Figure 2. Hardware-Enabled Security**
All six Windows 11 security categories described in Microsoft's Windows 11 Security Book include substantial endpoint security capabilities enabled by Intel.

# Security-Processing Hardware

The OS alone cannot protect from the wide range of attackers' tools and techniques used to compromise a computer. These evolving threats call for multilayered silicon-assisted security, including hardware to process and store sensitive business information.

Building silicon-assisted security helps address entire classes of vulnerabilities that cannot be addressed by software alone and provide performance advantages compared to implementing the same capability in software. Using hardware-based isolation, Windows 11 stores sensitive data like encryption keys and user credentials behind additional security barriers, isolated from the OS.

Hardware security engines, running firmware designed by Intel, are the foundation of system security. Our latest engines address sophisticated attacks and advanced multi-tile architecture by isolating functions in separate engines.

- The **Intel® Converged Security and Management Engine (Intel® CSME)** provides system-level security features integrated in silicon for technologies like **Intel® Active Management Technology (Intel® AMT) and Intel® Platform Trust Technology (Intel® PTT)**.
- Intel Core Ultra processors introduced the **Intel® Silicon Security Engine (Intel® SSE)** to function as Silicon Root of Trust (RoT), which cryptographically identifies and attests Intel silicon. Separating this low-level functionality from manageability and graphics security helps provide the secure isolation needed for RoT.
- As we strengthen our silicon security, our partners and customers continue to innovate through software- and firmware-based system security solutions. That's why we introduced the **Intel® Partner Security Engine**, a separate, dedicated engine based on Intel® SSE hardware architecture.

Microsoft Pluton will leverage the Security capabilities of Intel Partner Security Engine starting with Intel® Core Ultra processors (Series 2). As the Microsoft Pluton roadmap continues to evolve to meet the needs of Windows Security, Intel® Partner Security Engine will continue to provide secure, performant, and efficient hardware capabilities to support Pluton as well as other partner usages.

Fault-injection attacks seek to physically disrupt the behavior of integrated circuits, causing devices such as Intel CSME to behave incorrectly. Intel developed and calibrated the Intel Tunable Replica Circuit - Fault-Injection Detection (Intel TRC-FID) to detect and help mitigate these attacks in the security processor. It helps protect against fault-injection attacks that use voltage glitching, clock pins, or electromagnetic interference. Intel TRC-FID detects dynamic variation in circuits and is calibrated to a point where such timing violations could only be the result of an attack. When Intel TRC-FID detects a glitch, to prevent further execution of security processor firmware, hardware isolation prevents any further interaction of the firmware with hardware.

Intel CSME also helps meet two important goals:

1. Securely boot the system by verifying the SOC firmware so malware cannot hide its presence and infect boot code.
2. Provide a highly secure area isolated from the OS and applications for storing cryptographic keys, data, and code. This helps safeguard critical resources that rely on the Trusted Platform Module (TPM) and secure boot.

The TPM is designed to provide hardware-based security functions and prevent unwanted tampering. The TPM 2.0 specification includes enhancements including cryptographic algorithm flexibility. With Windows 11, both new and upgraded devices require TPM 2.0 for a stronger security posture.

TPMs provide security and privacy benefits for system hardware, platform owners, and users. Windows Hello, BitLocker, Windows Defender System Guard, and other Windows features rely on the TPM for key generation, secure storage, encryption, boot integrity measurements, attestation, and other capabilities. These, in turn, help customers strengthen the protection of their identities and data.

# Platform Trust Technology

Intel PTT provides an integrated TPM implementation to assist with hardware root-of-trust at boot, including providing a provisioned key for **Intel® Boot Guard**. Intel PTT includes the capabilities of an Intel® TPM 2.0 within the System on Chip (SoC) for storing keys, passwords and digital certificates. This credential storage and key management solution meets Windows OS hardware requirements and is optimized for low power consumption. Intel PTT supports the Trusted Computing Group (TCG) TPM 2.0 specifications and FIPS 140-3 certification.

Intel® Secure Key, within the SoC crypto subsystem circuitry, helps to protect sensitive keys, even from the firmware running within the security engine. This is a critical feature for a sensitive application like a TPM. But some customers require TCG-certified TPMs as part of their purchase criteria, and Intel supports customer choice to enable discrete TPMs. Intel PTT is typically turned off in the BIOS in configurations that also support a discrete TPM. Refer to PC OEM documentation to learn how to enable Intel PTT. For more, see Choose the Right TPM Type for Your Use Case.

# OS Protection

Windows 11 uses built-in hardware protection with OS security out-of-the-box to help keep your system, identity and information safe.

As the boot process begins, the PC will first verify that the firmware is digitally signed, reducing the risk of firmware rootkits. Secure Boot then checks all code that runs before the OS, checking the OS bootloader's digital signature to ensure that it is trusted by the Secure Boot policy and hasn't been tampered with. Trusted Boot takes over where Secure Boot leaves off. The Windows bootloader verifies the digital signature of the Windows kernel before loading it. The Windows kernel, in turn, verifies every other component of the Windows startup process.

Windows relies on Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Boot, Dynamic Root-of-Trust Measurement (DRTM), and other low-level security features to help protect your PC from attacks. From the moment you power on your PC until your anti-malware starts, Windows, enabled with Intel hardware, helps keep you safe.

Measured Boot, implemented by bootloaders, BIOS, and the Windows boot process, verifies and cryptographically records each step of the boot in a chained manner. These events are bound to the TPM that functions as a root-of-trust. Remote attestation is the mechanism by which these events are read and verified by a service to provide a verifiable, unbiased, and tamper-resilient report. Remote attestation is the trusted auditor of system boot, allowing relying parties to bind trust to the device and its security.

In addition to the use of measured boot for remote attestation, the use of local attestation by solutions such as BitLocker help ensure integrity of early boot components.

# Trusted & Secure Boot

On leading Intel Core Ultra processor-based systems, you can use trusted and secure boot processes that meet and go beyond Secured-core PC specifications, based on the following hardware security technologies from Intel:

- **Intel® Trusted Execution Technology (Intel® TXT)** is used by the OS or hypervisor to initiate a Measured Launch Environment (MLE)—generally at OS boot time. Intel TXT measures key components executed during launch of 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® System Security Report** is a patented, trusted hardware-to-software channel for gaining below-the-OS security visibility. In coordination with Intel TXT, Intel System Security Report communicates policies to the OS, and it provides a one-time report at Intel TXT launch to indicate the system hardware or resources that may be accessible from firmware System Management Interrupt (SMI) handlers.
- **Intel® System Resources Defense** extends the ability to enforce resource access policies for SMI handler firmware beyond memory resources. This mechanism 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 for hardware access from SMI handlers. Intel System Resources Defense can help to harden the platform by reducing the attack surface in SMM.
- **Intel® Boot Guard** provides a hardware-based trust chain for boot integrity that roots the Microsoft Windows requirements for UEFI Secure Boot to the hardware. Intel Boot Guard cryptographically verifies and/or measures BIOS components before executing them.
- **Intel® BIOS Guard** is a UEFI-BIOS Flash update technology that creates a very small trust boundary for BIOS image updates to flash memory, eliminating from the trust boundary the SMI handler and nearly all the power-on self-test (POST) BIOS, as well. This small trust boundary reduces the risk of flash-based attacks on Intel Core Ultra platforms.

# Virtualization Technologies

In Windows 11, hardware and software work together to help protect the operating system, with virtualization-based security (VBS) and Secure Boot built-in and enabled by default on Intel Core Ultra processors. Even if bad actors get in, they don't get far. VBS isolates a secure region of memory from the OS and increases protection from OS vulnerabilities.

VBS uses **Intel® Virtualization Technology (Intel® VT-x)**, Intel® VT-x2 with Extended Page Tables (EPT), and more for performance optimization and security. For example, VBS uses **Intel® VT for Directed I/O (Intel® VT-d)** to accelerate advanced security capabilities and improve reliability and security through device isolation using hardware-assisted remapping. Intel VT-d also improves I/O performance and availability by direct assignment of devices. These features work in concert to enable virtualized workloads that help to prevent malicious code injection in the OS and protect data such as log-in credentials from direct memory access attacks and other modern threats.

Windows Virtual Secure Mode (VSM) uses Intel VT-x to protect key data and credentials (tokens) on the system's main storage drive. VSM and Intel VT-x help prevent hackers from obtaining credentials and infiltrating the enterprise infrastructure. Beyond VSM, Microsoft Defender Credential Guard can isolate secrets so that only privileged system software can access them, preventing credential theft attacks. Credential Guard utilizes Intel Virtualization Technologies helping to prevent credential theft attacks. Credential Guard can be enabled via Microsoft Intune, Group Policy, editing the Windows Registry, or using the Device Guard and Credential Guard hardware readiness tool. In addition, Windows includes a set of Intel VT-x enabled technologies called Windows Defender Device Guard. A Device Guard feature called Configurable Code Integrity restricts devices to run only authorized applications. Simultaneously, a Device Guard feature called Hypervisor-Protected Code Integrity (HVCI) helps protect the OS against kernel memory attacks.

In addition, malicious attacks on the OS kernel and the page table threaten applications and data across the platform. **Intel® Virtualization Technology - Redirect Protections (Intel® VT-rp)** delivers hardware acceleration for an otherwise performance-intensive attack mitigation. Using dedicated processor instructions, Intel VT-rp accelerates the execution of alternate page table root/page tables that the OS can trust. Intel VT-rp is used by the Microsoft Hyper-V hypervisor virtual machine monitor (VMM) to enforce guest linear translation to guest physical mappings. Intel VT-rp comprises three related technologies: a Hypervisor-managed Linear Address Translation (HLAT) mechanism, a new EPT control bit called "paging-write," and another new EPT control bit called "verify paging-write." When combined with the existing Extended Page Table (EPT) capability, Intel VT-rp enables the VMM to ensure the integrity of combined guest linear translation cached by the processor translation lookaside buffer (TLB) via a reduced software TCB managed by the VMM. This helps make the VMM-enforced guest translations far less vulnerable to tampering without degrading performance.

# Control-Flow Enforcement

Control-flow hijacking is another threat to the OS and beyond. Control-flow hijacking attacks system memory to target OSs, browsers, readers, and other legitimate programs. These attacks are hard to detect or prevent because they use existing code running from executable memory to change program behavior. For example, Return Oriented Programming (ROP) attacks rely on the RET (return) instruction, where the address of the next instruction to execute is fetched from a stack; stack corruption is used to control the return address.

Intel works closely with Microsoft, and Microsoft works closely with developers, so the industry can offer better protection against control-flow hijacking. Intel® Control-Flow Enforcement Technology (Intel® CET) helps to protect against the misuse of legitimate code. Intel CET enables the OS to create a Shadow Stack, which is designed to be protected from application code memory accesses, and stores CPU-stored copies of the return addresses. This helps ensure that even when an attacker is able to modify/corrupt the return addresses in the data stack for the purpose of carrying out a ROP attack, the attacker is not able to modify the Shadow Stack. The Intel CET state machine in the CPU detects mismatches between the address on the shadow and data stack to help prevent the attack via an exception reported to the OS.

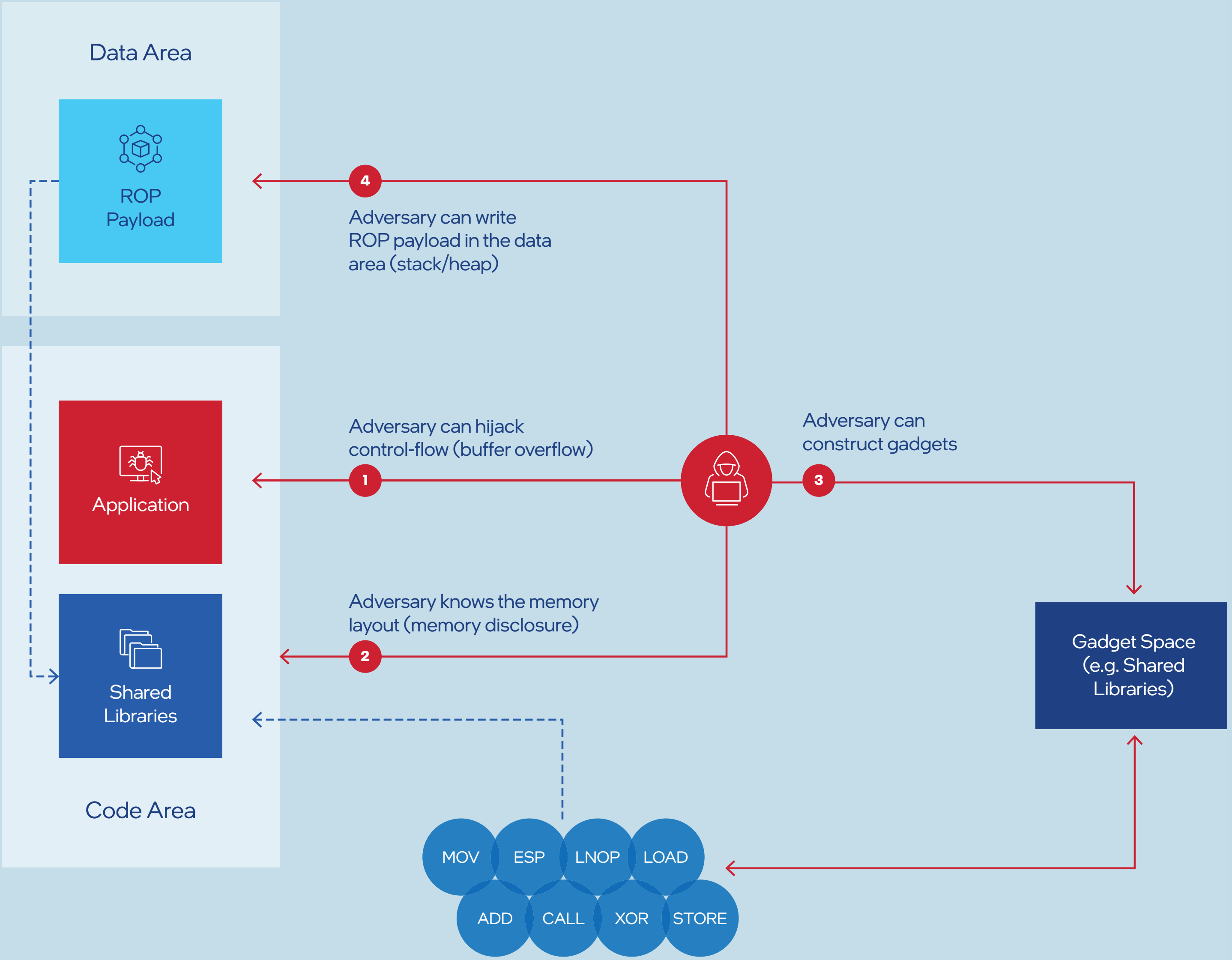


**Figure 3.** Control-flow hijacking co-opts legitimate application code to subvert a remote system and all vulnerable machines.

# AI-Powered Threat Detection

System-wide protection from ever-evolving, advanced threats like ransomware, software supply chain attacks, and crypto jacking requires a holistic approach. That's why Windows 11 supports **Intel® Threat Detection Technology (Intel® TDT)** to help rapidly detect and respond to these threats. Intel TDT is enabled in leading security vendors' software (including Microsoft Defender for Endpoint) to improve efficacy and performance, resulting in better detection of advanced threats on Intel Core Ultra platforms.

Intel TDT equips EDR software to go beyond signature and file-based techniques with malware behavior monitoring, and with Full-Stack Visibility, Intel TDT helps close blind spots to expose and differentiate malware from legitimate data encryption as it hides in memory or in VMs to evade detection.

Platform telemetry in the CPU helps profile exploits for behavioral detection. Targeted exploit detection combines machine learning with hardware telemetry unique to Intel processors. This capability adds a highly effective, low-overhead tool to the arsenal of security providers without requiring intrusive scanning techniques or signature databases, leading to improved and proactive malware detection.

For example, using silicon telemetry, Intel TDT helps detect new ransomware variants not yet profiled by the security solution vendor. Likewise, a known attack may be running in a VM and be undetectable by the security vendor. Again, Intel TDT signals can be useful to the third-party solution in detecting these attacks. In fact, SE Labs documented up to a +24% detection assist from Intel TDT for EDR solutions*.

Ransomware is downloaded through malicious links from phishing schemes targeting user devices. It can encrypt endpoint files and move across the network to infect servers and shared applications. Intel TDT helps detect ransomware variants not yet profiled by EDR solutions.

Crypto jacking attacks are still common and often fluctuate based on the market price of cryptocurrency. Intel TDT applies machine learning to low-level hardware telemetry from the CPU Performance Monitoring Unit (PMU) to help EDR solutions detect crypto jacking at runtime with minimal overhead.

Crypto jacking operations trigger a signal when a certain PMU usage threshold is reached, and the signal is unaffected by common antimalware evasion techniques such as binary obfuscation or memory-only payloads. Thanks to AI and machine learning, Intel TDT can recognize the footprint of this style of attack.

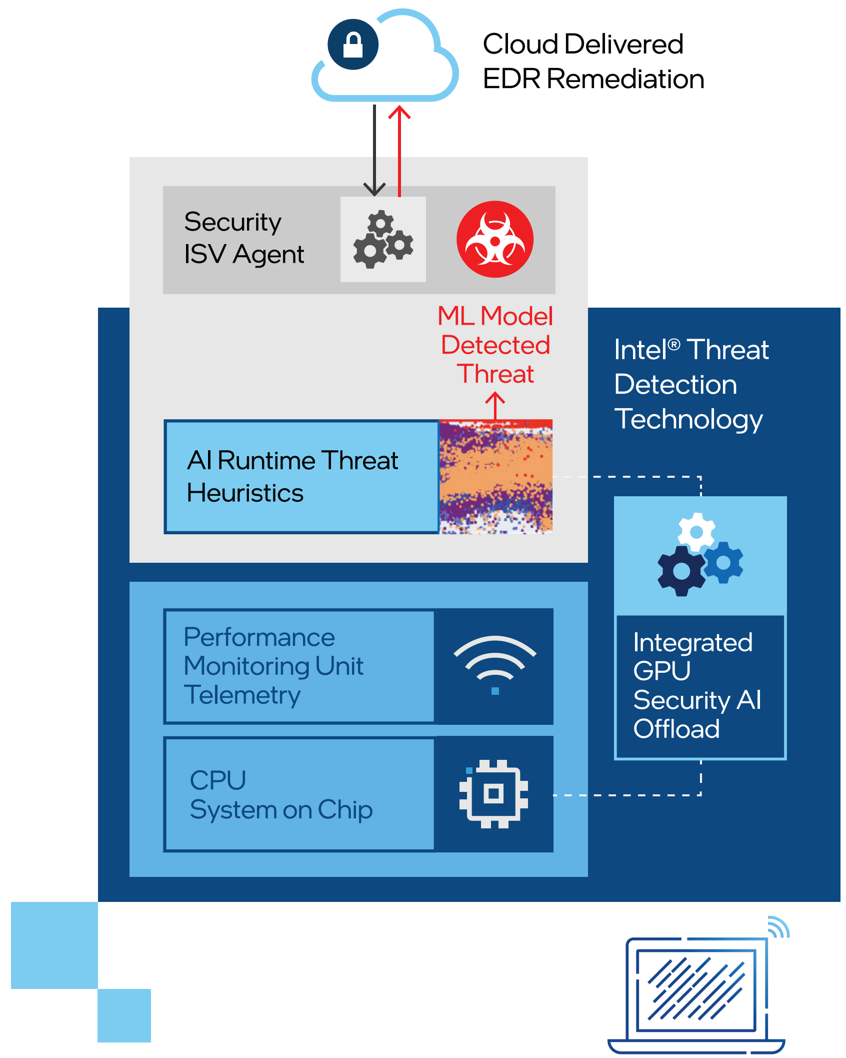


**Figure 4.** Intel TDT uses CPU telemetry and Intel integrated GPU offloading to accelerate and enable advanced threat protections such as advanced memory scanning (AMS) and machine learning (ML)-based real-time monitoring.

* "SE Labs Intelligence-Led Testing: Enterprise Advanced Security (Ransomware)," SE Labs, February 2023.
https://selabs.uk/reports/enterprise-advanced-security-ransomware-intel-threat-detection-technology-2023-02/

# Reducing Performance Impacts

Security software vendors and enterprise IT professionals need to run more security workloads to detect new classes of emerging threats. However, CPU performance can limit how much they can do without affecting the user experience.

Intel TDT enables security software vendors to efficiently and easily offload some workloads from the CPU to the integrated GPU. The performance of Intel Core Ultra processors, coupled with the large pool of shared system memory, allows endpoint protection to take advantage of graphics compute that is mostly idle on enterprise client systems. For example, Intel TDT crypto mining and ransomware detectors use the integrated GPU to run the Random Forest Classifier toolkit workload.

**Intel TDT Advanced Memory Scanning (AMS)** was the first security workload Intel TDT offloaded from CPU to the Intel integrated GPU. Current scanning technologies can detect system memory-based cyberattacks, but many security software vendors turn them off by default because they impact CPU performance.

With AMS, offloading to the Intel integrated GPU enables EDR software solutions to scan more frequently, improving overall system security and uncovering hard-to-detect fileless attacks to the memory layer. For example, Microsoft integrates Intel TDT-enabled AMS into the Microsoft Defender for Endpoint Advanced Threat Protection (ATP).

# Application & Data Protections

Most cyberattacks occur at the application and data level, and those attacks are getting more sophisticated. The security perimeter erodes as cyberthreats evolve and become more complex.

For IT professionals, balancing user experience against security priorities can be daunting. That's especially true today, as home and business PC uses converge with more people working remotely than ever before. That means IT must provide high-performance devices and enhanced support for employee productivity while also taking proactive measures to improve security by protecting valuable assets and data.

Cybercriminals regularly gain access to valuable data by hacking poorly secured applications. Common security failures include "code injection" attacks, in which attackers insert malicious code that can tamper with data, or even destroy it. Wherever confidential data is stored, it must be protected against unauthorized access, whether through physical device theft or from malicious applications. Intel Core Ultra processor-based platforms include security capabilities to isolate and help protect login credentials, sensitive data and business-critical applications in secure virtual machines. In addition, Intel Core Ultra platforms include advanced hardware-based encryption technologies to help protect data in flight, at rest, and in applications.

**Intel® Advanced Encryption Standard-New Instructions (Intel® AES-NI)** accelerates the encryption of data to make pervasive encryption feasible in areas where previously it was not—that gives IT environments faster, more affordable data protection and more security. Intel AES-NI is used by Microsoft BitLocker to accelerate encryption and decryption, and to improve key generation and matrix manipulation, all while aiding in carry-less multiplication. This accelerates cryptographic processing and addresses side channel attacks associated with traditional software methods of table look-ups.

**Intel® Total Memory Encryption (Intel® TME)** provides the base functionality to allow for full physical memory encryption. It is designed to work with existing software applications and systems (without modification). Intel TME helps protect against "cold boot" memory attacks where an attacker dumps memory by performing a hard reset of the target machine. Intel TME encrypts DRAM using NIST standard AES-XTS encryption. It leverages Intel expertise in process/circuit design to help provide data protection through high-performance and low-power crypto circuits.

Intel TME is enabled via the BIOS during the initial boot process with very minor modifications. Once activated, all data sent on the external memory buses of the chip are encrypted using the standard NIST AES-XTS algorithm. It generates the 256-bit key using a hardware random generator. The key is not accessible by software or through any external interface. A new platform key is generated by the processor on every boot. Intel TME is an out-of-box capability that provides memory data protection for end users' sensitive/confidential data if their client system is lost or stolen. Hooks are available for anti-theft service to wipe out the keys for Intel TME.

Virtualized and containerized environments need more granular, page-level memory encryption. **Intel® Total Memory Encryption – Multi-Key (Intel® TME-MK)** enhances Intel TME for page-granular memory encryption through support for multiple encryption keys. Intel TME-MK can effectively work with non-volatile memory, various attestation mechanisms or other key provisioning services.

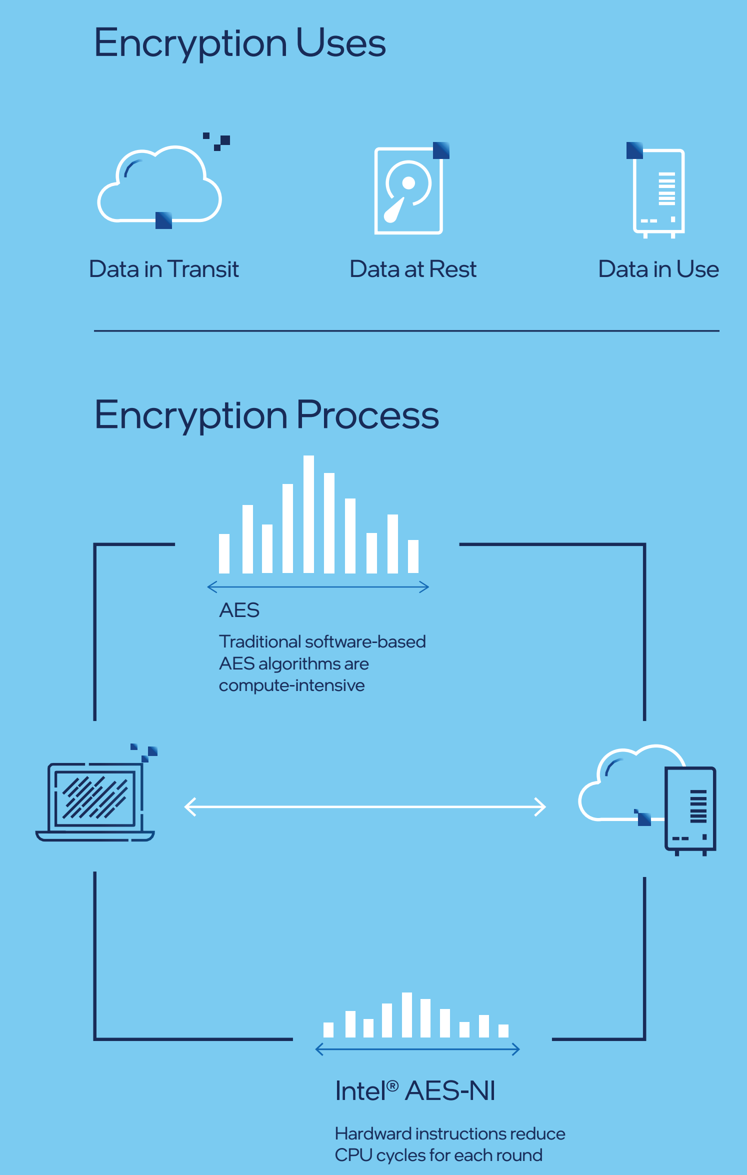


**Figure 5.** Intel AES-NI accelerates cryptographic processing for data in flight, at rest, and in applications.

For virtualized workloads, Hyper-V can manage the keys to transparently provide memory encryption support for legacy OSs without modifications. OSs also can take advantage of Intel TME-MK to provide support in native and virtualized environments—e.g., each guest OS can take advantage of Intel TME-MK for itself and encrypt its own data.

In addition to encryption, Intel Core Ultra processor-based PCs use hardware-accelerated virtualization techniques to abstract the physical hardware, creating logical resources consisting of CPUs, memory, storage and networking and providing those resources in the form of agile, scalable, consolidated virtual machines (VMs). Because VMs are sandboxed from the rest of the client system, they provide complete isolation from the PC OS and other VMs. That enables isolation of workloads, reducing the opportunity for malware to easily spread and enabling improved protection of credentials and other secrets, as well as for running entire workloads in separate VMs.

**Intel VT-x** provides silicon-assisted security to isolate critical system resources from VMs and containers running various system- and application-level processes. Intel VT-x supports usages for activity partitioning, workload isolation, embedded management, legacy software migration, and disaster recovery.

A related technology built-in to Intel Core Ultra processors, **Intel® Virtualization Technology for Directed I/O (Intel® VT-d)**, helps protect against faulty device Direct Memory Access (DMA) and interrupts. That helps to secure workloads from unauthorized DMA initiated from the main OS. That's especially important on the latest mobile PCs that feature hot-plug PCIe ports such as Thunderbolt™ 4 technology for greater extensibility but at the risk of "drive-by" DMA attacks.

DMA-capable devices can read and write to system memory without having to engage the system processor. Intel VT-d provides the foundation for Kernel DMA Protection on Microsoft Windows. Windows leverages the system IOMMU to block external peripherals from starting and performing DMA unless the drivers for these peripherals support memory isolation.

Intel Virtualization Technologies also help protect Windows 11 kernel-level code integrity with **Mode-Based Execution Control (MBEC)**. MBEC virtualization provides an extra layer of protection from malware attacks in a virtualized environment. It enables the Windows Hyper-V hypervisor to more reliably and efficiently verify and enforce the integrity of kernel-level code. Memory integrity is a powerful system mitigation that leverages MBEC hardware virtualization and Hyper-V to protect Windows kernel-mode processes against the injection and execution of malicious or unverified code. Code integrity validation is performed in a secure environment that is resistant to attack from malicious software, and page permissions for kernel mode are set and maintained by the hypervisor.

Another Intel Virtualization Technology, called **Advanced Programmable Interrupt Controller Virtualization (APICv)**, helps execute interrupts more securely, in hardware. Interrupts are either external or internal.

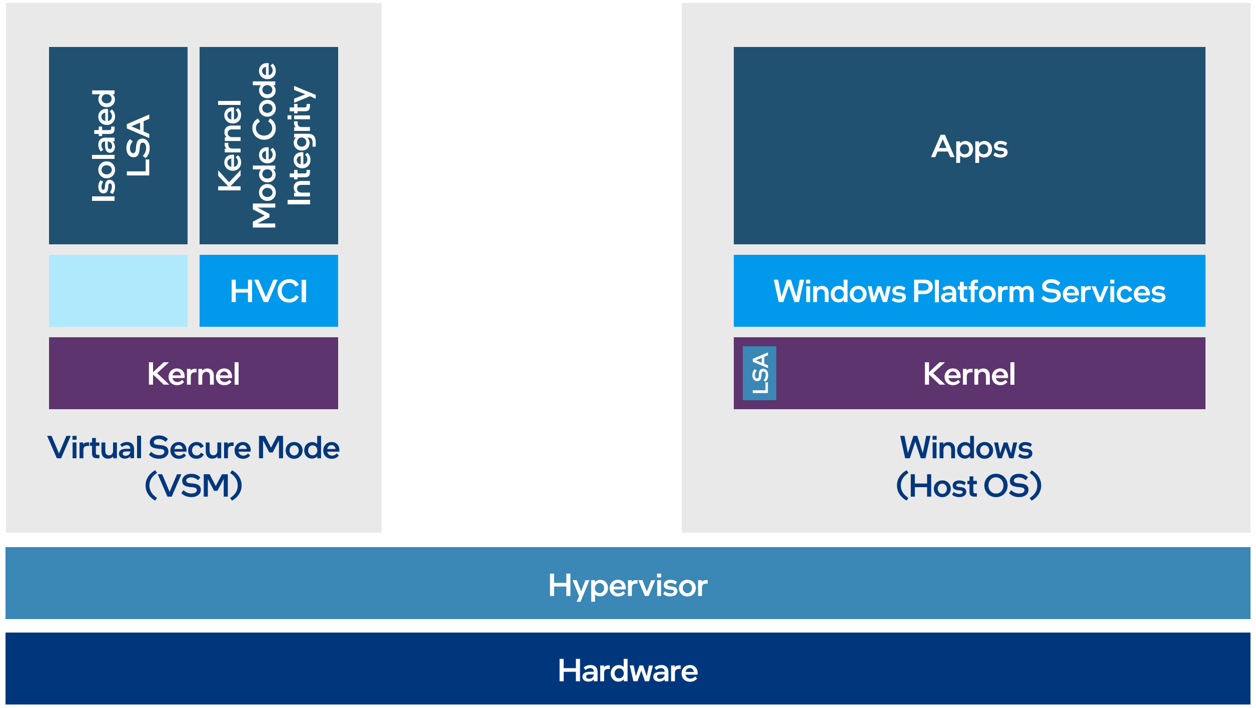


**Figure 6.** MBEC from Intel provides finer-grain control on execute permissions to help protect the integrity of system code from malicious changes.

External interrupts originate from other partitions or devices, and internal interrupts originate from within the partition itself. Interrupt delivery requires the exit and reentry of VMs—typically time-consuming task and a major source of overhead.

To minimize that, Intel Core Ultra processor-based platforms emulate those activities in hardware using APICv circuitry. APICv eliminates the VM exits triggered by privileged register access during the handling of virtual interrupts. APIC register virtualization and virtual interrupt handling eliminate a major source of virtualization overhead, greatly reducing the attack surface.

# Identity & Privacy Protection

Malicious actors launch an average of 921 password attacks every second—nearly doubling in frequency over the past 12 months, according to the Microsoft Security Blog.

> **Hackers don't break in, they log in**," says Microsoft Chief Information Security Officer Bret Arsenault.

That's why Windows 11 uses Intel Virtualization Technologies to enable secure biometric authentication.

Biometric authentication is becoming a mainstream use case driven by Windows Hello (Enhanced Sign-in Protection). Securing the entire biometric data path is important to enable mainstream adoption of biometrics, which enhances both security (by elimination of passwords) and ease of use. Intel enables this capability with **Virtualized Trusted I/O (VTIO)**. Windows Hello supports VTIO with secure VM infrastructure based on Hyper-V. VTIO works in conjunction with the hypervisor and trusted I/O drivers running in a secure VM (which isolates and protects I/O data via VT Extended Page Table-based memory views). VTIO protects I/O for USB/MIPI cameras used for biometric face authentication—the camera data can be securely delivered to a biometric match engine running in the secure VM (which also protects the biometric match template).

# No-Compromise, Silicon-Enabled Security

Intel builds in security from the ground up, for powerful defense in today's threat environment. Together, Intel hardware and Windows 11 software meet the modern threats of today's hybrid work environments by delivering hardware-based isolation, end-to-end encryption, and advanced malware protection. With Windows 11 on Intel Core Ultra processor-based PCs, customers get business-class productivity and intuitive new experiences without compromising security.

# Security Foundation

In addition to our hardware, the Intel Security First Pledge helps keep your business safe with industry-leading support and programs such as the **Intel Security Development Lifecycle**, the **Intel® Bug Bounty Program**, and more.

## Intel Security Development Lifecycle

The Intel Security Development Lifecycle guides us in applying privacy and security practices across hardware, firmware, and software throughout the product lifecycle. It is a set of processes that implement security principles and privacy tenets into product development. These processes incorporate security-minded engineering and testing at the onset of product development when it is more effective and efficient to employ. While the Intel Security Development Lifecycle is most common in software development, Intel has been applying these principles across software, firmware, and hardware development since at least 2009.

The physical nature of hardware security offers a unique set of challenges and opportunities. One challenge is that hardware generally has longer development cycles and support lifetimes than software. The opportunity is to impose security objectives early in the product definition before doing so becomes increasingly costly to change. Due to the length of time for hardware development and manufacturing, architects must attempt to anticipate new usage models and potential threats years in advance. Unlike software, though, hardware offers opportunities to improve the robustness of product security beyond what is possible in code. For example, trust boundaries can be enforced through physical separation of trusted and untrusted memory regions. Moving up the stack, the Intel Security Development Lifecycle is applied to BIOS, drivers, open-source software that Intel maintains, and myriad products across the company. Although every product differs, the same mindset and methodology are applied where relevant and broadly enforced.

## Intel Bug Bounty Program

The Intel® Bug Bounty program invites security researchers to partner, discover, and eliminate issues on Intel products. Established in 2018, the community of security researchers from around the world continues to contribute to improving the security of technology in many ways. Collaboration on security research yields improved identification and mitigation of potential vulnerabilities, and coordinated vulnerability disclosure allows all parties time to develop and deploy mitigations.

In 2021, Intel expanded the Intel Bug Bounty Bonus program across Pentium®, Celeron®, and Atom® Processors. This marked the first of several planned expansions to the program, and we began rewarding researchers with bonus multipliers for findings in specific areas of interest. Across the entire Intel Bug Bounty program, top areas of findings for researchers were in GPUs, system and devices, and software, leading to mitigations and improved security across an array of products.

We're fostering a community dedicated to offering training to security researchers, exciting new hacking challenges, and opportunities to work at unprecedented levels with new and pre-release products, as well as new collaborations with Intel hardware and software engineers. Learn more.

# Platform Update

The Intel Platform Update process proactively and transparently enables product security updates across the ecosystem, and Intel has unrivaled product security incident response with coordinated processes to help keep your business safe. Participating OEMs integrate signed updates and robust Intel recovery capabilities into firmware update architecture. **Intel® Firmware Guard**, in collaboration with OEMs, provides the ability to update the firmware on an end user's system and recover from a firmware failure. Firmware updates are signed, 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 during the update, the system automatically boots to a last known good state and restarts the firmware update process—all without user intervention.

# Transparent Supply Chain

Intel Firmware Guard works hand-in-glove with our Secure Supply Chain program, **Intel® Tiber™ Transparent Supply Chain**, to help detect changes to PC configuration in transit, in cooperation with supply chain partners. Policies and procedures trace system components from the point of manufacture. Intel® Tiber™ Transparent Supply Chain helps identify counterfeit or malware-infected PC components (requires OEM setup/implementation).

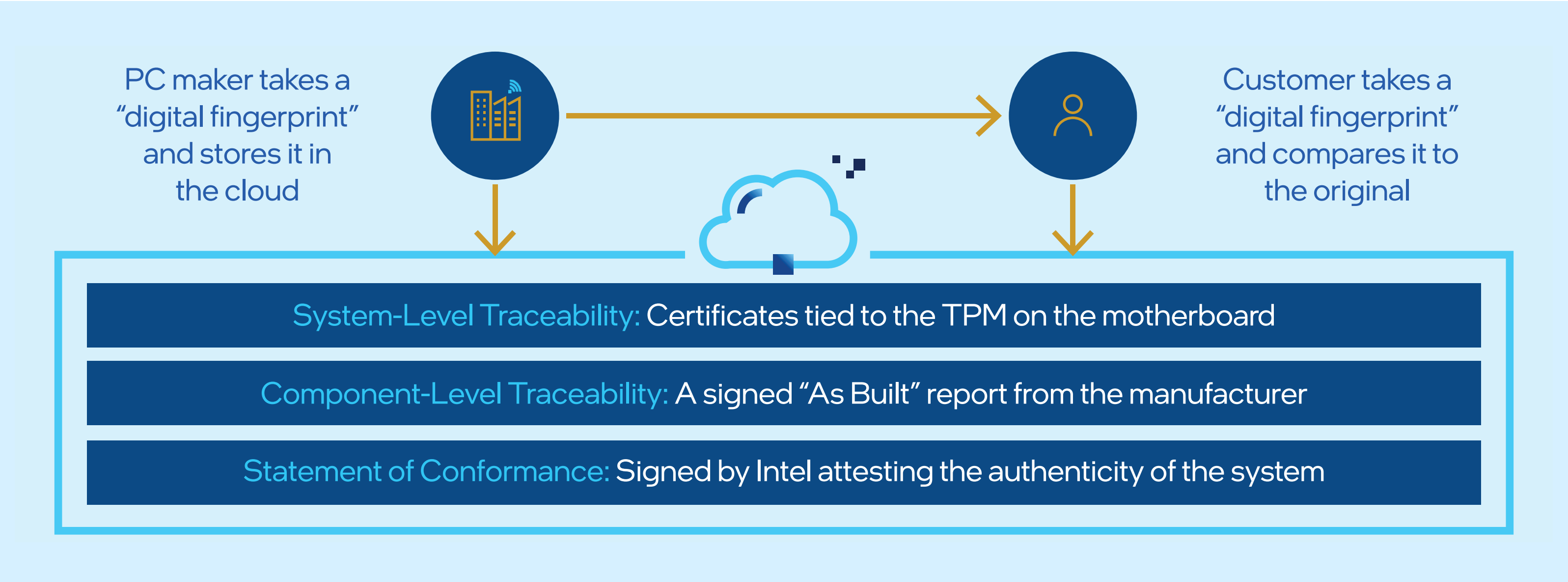


**Figure 7.** Together with supply chain partners, Intel® Tiber™ Transparent Supply Chain helps identify counterfeit or malware-infected PC components.

# Certification

Certification is another aspect of the Intel security foundation—specifically, cryptographic certification. Cryptography is a mathematical process to protect user and system data, for example, by encrypting data so that only a specific recipient can read it by using a key possessed only by that recipient. Cryptography is a basis for privacy to prevent anyone except the intended recipient from reading data, provides integrity checks to ensure data is free of tampering, and authentication that verifies identity to ensure that communication is secure.

**The Federal Information Processing Standard (FIPS) Publication 140 is a U.S. government standard that defines the minimum security requirements for cryptographic modules in IT products. FIPS 140 certification ensures that U.S. government-approved algorithms are correctly implemented. These include RSA for signing, ECDH with NIST curves for key agreement, AES for symmetric encryption, and SHA2 for hashing. FIPS 140 also tests module integrity to prove that no tampering has occurred and proves the randomness of entropy sources.**

**Intel CSME is certified as a FIPS 140-3 cryptographic sub-system. This is the embedded subsystem for Intel PTT, designed to act as the security and manageability controller for the integrated TPM implementation and other key cryptographic functions.**

Attestation provides assurance of trust, as it can verify the identity and status of critical components. It can also help verify the device firmware and boot process have not been altered. This capability helps organizations manage access with confidence. Once the device is attested, it can be granted access to resources.

# Windows 11 Security Starts with Intel

From power-on through boot-up and beyond, Windows 11 security protections from Intel are part of a comprehensive strategy based on hardware layers of security, from chip to cloud. Intel and Microsoft co-engineering continues to build zero-trust/verify-everything capabilities across the entire solution stack.

Today, Intel Core Ultra processor-based business client platforms deliver highly effective, low-overhead security protections for Windows 11 and the applications and data that run on it.

## Learn More

[Intel vPro®: An Unrivaled Business PC Platform]

[Intel vPro® Security: Out-of-the Box PC Security]

[Intel® Core™ Ultra Processors]

[AI PCs Built for Business]

[Intel® Threat Detection Technology: Protect Your PC Fleet from Advanced Cyberattacks]

[Security Starts with Intel]