intel® security

At Intel, security comes first. Our culture and practices help ensure everything we build is designed to deliver the highest performance while optimizing protection. We are relentless in our pursuit of innovation with security that helps our customers tackle today's toughest challenges.

We innovate to help protect data and privacy, centered around three key priorities:

Software Reliability

Platforms that help protect against a range of cybersecurity threats and help assure software executes as intended.

Extended Page Tables Sub-page Write Protection (EPT-SPP)
Increased protection against rootkits via expanded runtime monitoring of Intel VT Extended Page Tables (EPT).

Intel® Control-Flow Enforcement Technology (Intel® CET)
Designed to protect against the misuse of legitimate code through control-flow hijacking attacks.

Intel® Threat Detection Technology (Intel® TDT)
Silicon-enabled, high-efficacy ransomware and cryptomining attack detection without compromising the user experience.

Page Protection Keys
Protection keys provide a user-level, page-granular way to grant and revoke access permission without changing page tables.

User-Mode Instruction Prevention
Designed to prevent address leakage of operating system structures & settings.

Workload and Data Protection

Trusted execution for hardware-isolated data protection.

Advanced Programmable Interrupt Controller Virtualization (APICv)
APICv reduces overhead by eliminating virtual machine exits triggered for virtual interrupt handling.

Intel® OS Guard
Designed to prevent instruction execution from user memory pages while the CPU is in supervisor mode.

Intel® Secure Key
A high-entropy random number generator designed to comply with ANSI/NIST standards. Formerly known as DRNG.

Intel® Software Guard Extensions (Intel® SGX)
Granular trusted execution environment with host level processing.

Intel® Virtualization Technology (Intel® VT)
Granular Extended Page Table execution control for user (XU) and supervisor (XS) pages.

Mode-Based Execution Control
Granular Extended Page Table execution control for user (XU) and supervisor (XS) pages.

Foundational Security

Critical protection to help verify the trustworthiness of devices and accelerate crypto performance.

Firmware Update/ Recovery
Comprehensive resiliency solution that keeps firmware more secure and resilient to malware attacks.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
Intel AES-NI dramatically reduces the compute cost for AES symmetric encryption.

Intel® Crypto Acceleration
Intel instruction set architecture (ISA) enhancements designed to significantly increase cryptographic performance.

Intel® BIOS Guard
Hardens flash storage to help prevent unauthorized BIOS modification and code execution.

Intel® Boot Guard
Hardware-based root of trust to help protect the integrity of the platform boot process.

Intel® Converged Security and Management Engine (Intel® CSME)
Cross-platform engine designed to support a range of Security and Manageability services.

Intel® Platform Firmware Resilience (Intel® PFR)
Verify firmware signatures prior to processor power-on, monitor boot progress, protect flash/recovery memory, and recover firmware to a healthy state.

Intel® Platform Trust Technology (Intel® PTT)
Credential storage and key management offering the capabilities of a discrete Trusted Platform Module (TPM 2.0).

Intel® QuickAssist Technology (Intel® QAT)
Platform based hardware-acceleration for cryptography and data compression.

Intel® Runtime BIOS Resilience
Reduces the risk that malware can be injected into System Management Mode (SMM) at runtime.

Intel® System Resources Defense
Extends the ability to enforce resource access policies for System Management Interrupt (SMI) handler firmware.

Intel® System Security Report
Communicates policies to the operating system in a trusted manner at runtime, in coordination with Intel TXT.

Intel® Total Memory Encryption (Intel® TME)
Provides memory data protection against physical attacks on lost or stolen platforms.

Intel® Trusted Execution Technology (Intel® TXT)
Validates the behavior of key components at system startup.

Learn more at intel.com/hwsecurity