



### Software Reliability

Harden the software to help protect against a range of cybersecurity threats

#### 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 cryptojacking detection with minimal impact to the user experience by offloading compute-intensive AI algorithms and security workloads to the Intel integrated GPU.

#### Anomalous Behavior Detection for Intel TDT

Monitors applications for early indicators of compromise with the ability to help detect supply chain style attacks.

#### 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 (UMIP)

Designed to prevent address leakage of operating system structures & settings.



### Workload and Data Protection

Protect data using accelerated encryption and trusted execution enclaves

#### 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)

Hardware assisted virtualization of the CPU context, I/O devices, and direct memory access (DMA).

#### Intel Virtualization Technology – Redirect Protection (Intel® VT-rp)

Extends hardware-rooted virtualization-based security to Intel vPro® PCs, helping boost security for virtualized environments.

#### Mode-Based Execution Control

Granular Extended Page Table execution control for user (XU) and supervisor (XS) pages.



### Foundational Security

Secure the foundation to help systems start and operate as intended

#### 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® Firmware Guard

Collaboration with OEMs for better firmware resiliency, faster adoption of mitigations, data protection, and improved recovery from update failures.

#### 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® Total Memory Encryption – Multi-Key (Intel® TME-MK)

Encrypts DRAM to help protect against physical cold boot attacks, with multiple keys that the OS can use to encrypt sections of memory.

#### Tunable Replica Circuit – Fault Injection Detection

Monitors voltage droop, temperature, and aging variation in circuits to help detect timing violations that can mitigate fault-injection attacks.

#### Intel® Trusted Execution Technology (Intel® TXT)

Validates the behavior of key components at system startup.