Enabling Business Opportunity Through Platform Security

Intel Data Center Security Gold Deck

Release date: June 2025

Notices and Disclaimers

No product can be absolutely secure.

Your costs and results may vary.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

All product plans and roadmaps are subject to change without notice.

Intel technologies may require enabled hardware, software or service activation.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Cybersecurity Continues to Pose Significant Challenges

69% of organizations reported at least one hardware/ firmware-level attack[1]

$4.48M was the global average cost of a data breach in 2024[2]

Security for AI

77% of companies reported breaches to their AI in 2023[3]

Supply Chain Corruption

The worldwide fake semiconductor market is projected to reach $329 billion by 2031[4]

Increased Regulation

82% of the world's population is covered by some form of national privacy law[5]

1. The Futurum Group, Endpoint Security Trends 2023 / 2. IBM, Cost of a data breach 2024 | IBM / 3. Hidden Layer, AI Threat Landscape Report 2024
4. Counterfeit Electronic Components Detection | SMT Corp. / https://straitsresearch.com/report/electronic-components-market (May 2023) / 5. Identifying global privacy laws, relevant DPAs | IAPP

Security is Enabling Business Opportunities

Financial/ Payment Services

Microsoft — $25B/yr Processed in Public Cloud

Multi-Party Collaboration Around Data

GOLDBACH — Data Clean Rooms in AdTech

Post-Quantum Encryption (PQC)

ARQIT — Data Sovereignty with Confidential Computing and Networking

Privacy-Preserving Technology

BOSCH — Machine Learning for ADAS

Decentralized Health & Personal Data

AI MINDSystems Foundation — File-less Attack Detection

Blockchain-Based Services

Fireblocks — Crypto Exchange Key Vault

Remove Data-Sharing Barriers to Cancer Research

Penn University of Pennsylvania — Federated Learning for Distributed AI/ML

Cloud Economics and Scale

Deutsche Telekom — $17M Sovereign Cloud w/ Intel SGX

Intel's Investments Help Drive Better Security Outcomes

Our Roadmap is Aligned to Zero Trust Principles

Intel technologies help you build a Zero Trust strategy, establishing hardware as the root of trust

Endpoint Security

Strengthen defenses with AI-powered threat detection, insights, and hardware-based security measures

Network Security

Connect people with the resources they need through encryption-based identity and access control

Information & Data Security

Designed to isolate and protect your sensitive data while in use to enhance confidentiality, integrity, and availability

Physical Security

Help prevent real-world attacks by managing the convergence of AI, physical, and cyber security assets

Product Security Assurance: Built on a Foundation of Trust

Choose products designed with security in mind, backed by the industry's best security assurance[1]

[1] - As measured by ABI Research

Intel's Investments Help Drive Better Security Outcomes

Our Roadmap is Aligned to Zero Trust Principles

Intel technologies help you build a Zero Trust strategy, establishing hardware as the root of trust

Endpoint Security

Strengthen defenses with AI-powered threat detection, insights, and hardware-based security measures

Network Security

Connect people with the resources they need through encryption-based identity and access control

Information & Data Security

Designed to isolate and protect your sensitive data while in use to enhance confidentiality, integrity, and availability

Physical Security

Help prevent real-world attacks by managing the convergence of AI, physical, and cyber security assets

Product Security Assurance: Built on a Foundation of Trust

Choose products designed with security in mind, backed by the industry's best security assurance[1]

[1] - As measured by ABI Research

Product Security Assurance: Building More Resilient Products

Your data belongs on a **trusted foundation**

Modern systems need **performance and security**

Intel: 96% of vulnerabilities
discovered due to Intel's proactive product security assurance efforts[1]

AMD: 4.4x more
firmware vulnerabilities in their hardware root-of-trust than Intel[1]

Intel: Ranked #1
when compared to key competitors for Product Security Assurance[2]

Investment and Innovation

Rigorously testing and hardening the foundation you build on

Defense in Depth

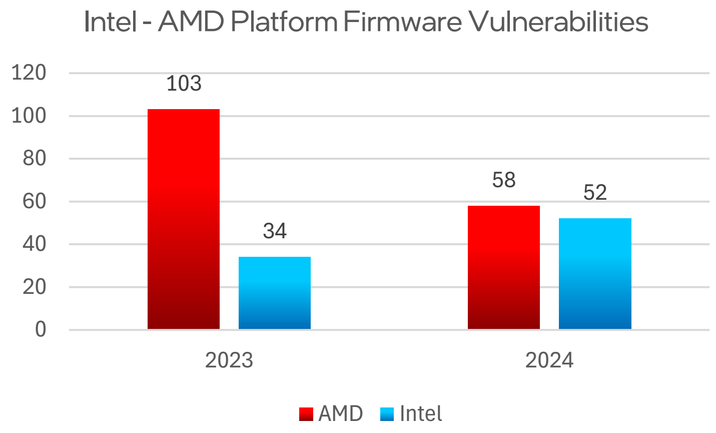
- Security Development Lifecycle
- Cutting-edge Security Research
- Mature Incident Response
- Supply Chain Excellence
- Industry Collaboration
- Community Engagement

1 - intel.com/securityreport / 2 – As measured by ABI Research

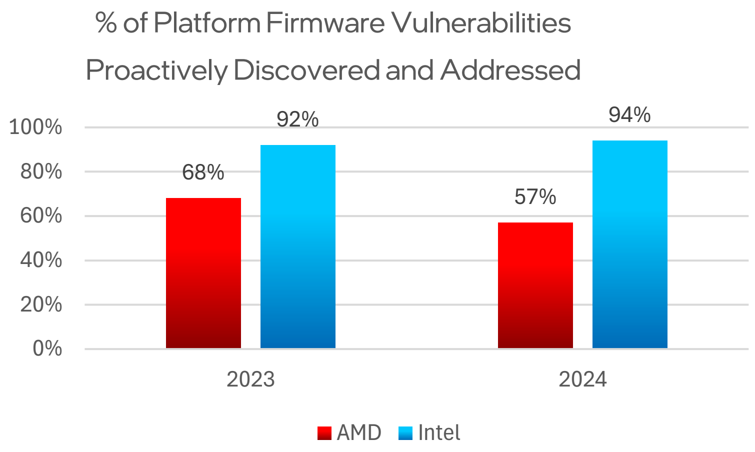
Platform Firmware Vulnerabilities

Key data points:

- In 2024, Intel reported 52 platform firmware vulnerabilities, while AMD reported 58.
- Intel’s proactive product security assurance efforts resulted in the discovery and mitigation of 94% of platform firmware vulnerabilities.
- According to AMDs public security bulletins, they proactively discovered 57% of the platform firmware vulnerabilities disclosed in 2024.



Intel - AMD Platform Firmware Vulnerabilities



% of Platform Firmware Vulnerabilities Proactively Discovered and Addressed

Intel continues to raise the bar with the proactive discovery and mitigation of 94% of its platform firmware vulnerabilities in 2024.

Source - intel.com/securityreport

Confidential Computing Firmware

Confidential computing is the protection of data in use by performing computation in a hardware-based, attested, Trusted Execution Environment.

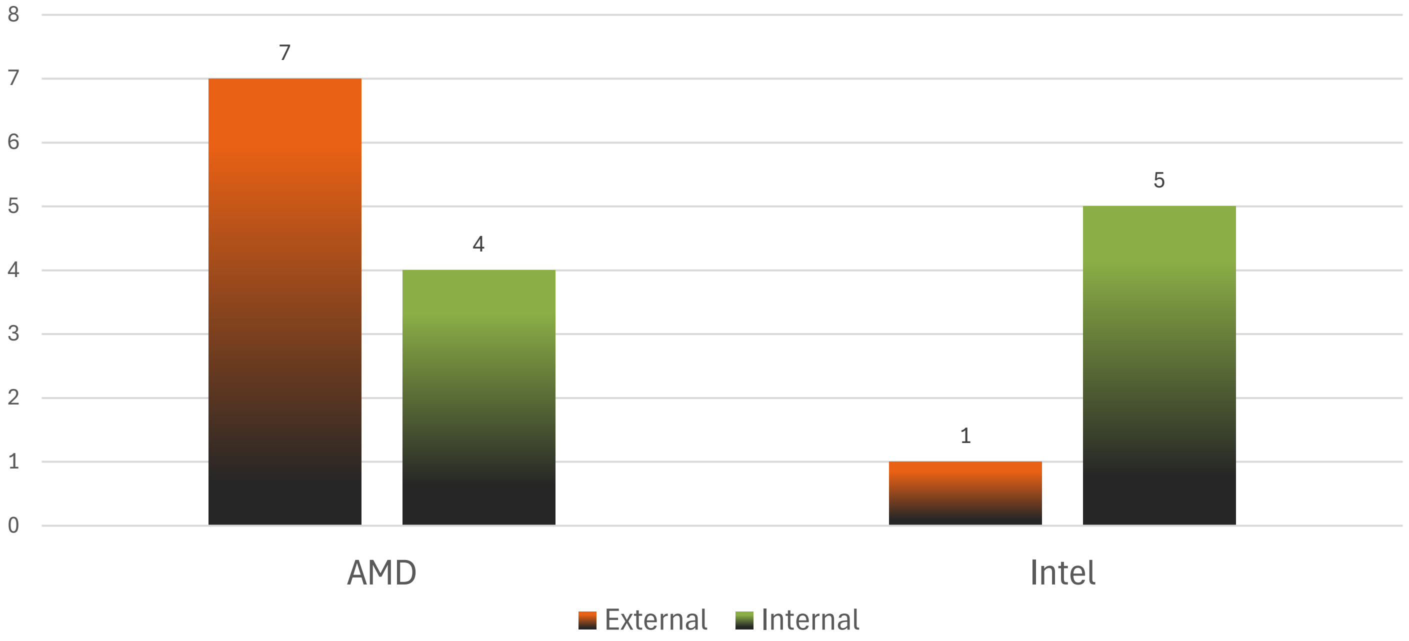
CONFIDENTIAL COMPUTING TECHNOLOGIES

Intel: Intel® Trust Domain Extensions (Intel® TDX) and Intel® Software Guard Extensions (Intel® SGX).

AMD: Secure Encrypted Virtualization (SEV), SEV-ES (Encrypted State), and SEV-SNP (Secure Nested Pages).

Source - intel.com/securityreport

Confidential Computing Hardware/Firmware Vulnerabilities Internally/Externally Found



In 2024, AMD reported 1.8x more vulnerabilities in their Confidential Computing firmware components and features than Intel.

Intel found 83% of Confidential Computing firmware vulnerabilities internally in 2024, while AMD found 36%.

Confidential Computing for Information & Data Security

3x

economic benefit

by data & analytics leaders who share data externally (vs those that do not)[1]

55%

of logged insider threats

rely on privilege escalation exploits[2]

82%

of the world's population

is covered by some form of national privacy law[3]

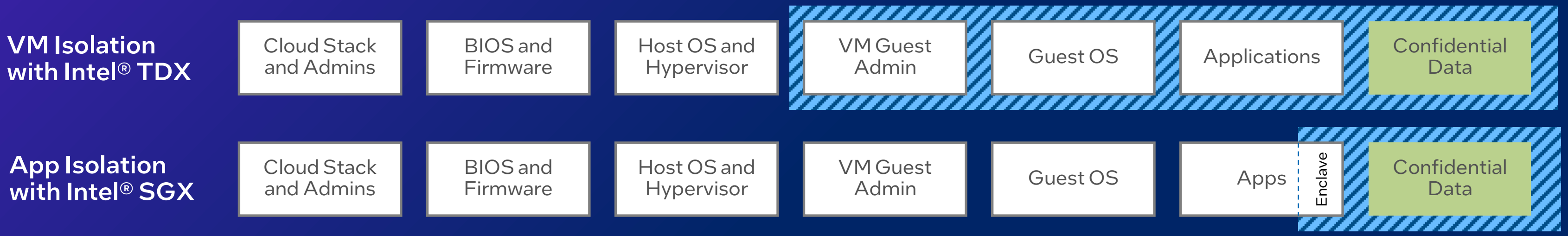
Activate sensitive data with silicon-based security

Intel® Software Guard Extensions (Intel® SGX)

Smallest Trust Boundary - Confidential data access is restricted to attested application code

Intel® Trust Domain Extensions (Intel® TDX)

Virtual machine isolation from cloud stack, admins, and other tenants



VM Isolation with Intel® TDX	Cloud Stack and Admins	BIOS and Firmware	Host OS and Hypervisor	VM Guest Admin	Guest OS	Applications	Confidential Data
App Isolation with Intel® SGX	Cloud Stack and Admins	BIOS and Firmware	Host OS and Hypervisor	VM Guest Admin	Guest OS	Apps | Enclave	Confidential Data

Intel® TDX Connect

Provides a high-performance encrypted connection between the CPU and PCIe devices

Intel® Tiber™ Trust Authority

ISO 27001:2022 certified independent attestation service for cloud service providers

[1] - Data Sharing is a Key Digital Transformation Capability (gartner.com) / [2] - Privilege elevation exploits used in over 50% of insider attacks (bleepingcomputer.com) / [3] - Identifying global privacy laws, relevant DPAs | IAPP.

Workload Acceleration for Network Security

41%

Lower TCO than AMD

running NGNIX TLS workload[1]

9.7x

Perf Advantage per Server

Refresh and consolidate 2nd Gen Intel Xeon servers with Intel Xeon 6700P servers[2]

Up to **1.62x**

higher NGNIX performance

Intel Xeon 6952P vs AMD EPYC 9655[3]

Intel® QuickAssist Technology (Intel® QAT)

- Purpose-built accelerator that increases the performance of crypto operations and compression
- Supports AES-256 (quantum-resistant)
- Designed for high-throughput use cases including network encryption, VPNs, content delivery systems & more
- Higher crypto throughput while freeing CPU cores for other valuable workloads with higher power efficiency than CPU cores

Case Study: Performant Post-Quantum Cryptography (PQC)

- Arqit SKA-Platform™ adds quantum-threat resistance to high-performance IPsec throughput using 4th Gen Intel® Xeon® Scalable servers
- Adds quantum attack protection to existing 1.89 Tb IPsec throughput
- Testing with Arqit SKA-Platform demonstrates a quantum secure IPsec tunnel can be achieved without compromising performance

1. Estimated over 4 years. See [7T223] intel.com/processorclaims: Intel Xeon 6. Results may vary.
2. Estimated over 4 years. See [7T26] intel.com/processorclaims: Intel Xeon 6. Results may vary.
3. See [9W220] intel.com/processorclaims: Intel Xeon 6. Results may vary.

Intel® Security Engines

Enhance Data Security to Drive Innovation

Confidential Computing

Intel® Software Guard Extensions (Intel® SGX)

Intel® Trust Domain Extensions (Intel® TDX)

Workload Acceleration

Intel® Crypto Acceleration

Intel® QuickAssist Technology (Intel® QAT)

Advanced Protection

Intel® Control-Flow Enforcement Technology (Intel® CET)

Intel® Boot Guard

Intel Technologies for Confidential Computing

Privacy First with Confidential Computing

The confidential computing benefit:

Designed to Protect Data In Use

Trusted Execution Environment (TEE)

Secure and isolated environments to prevent unauthorized access and modification to applications and data when in use

Increased assurance for sensitive data

- Data confidentiality
- Computational integrity
- Data privacy

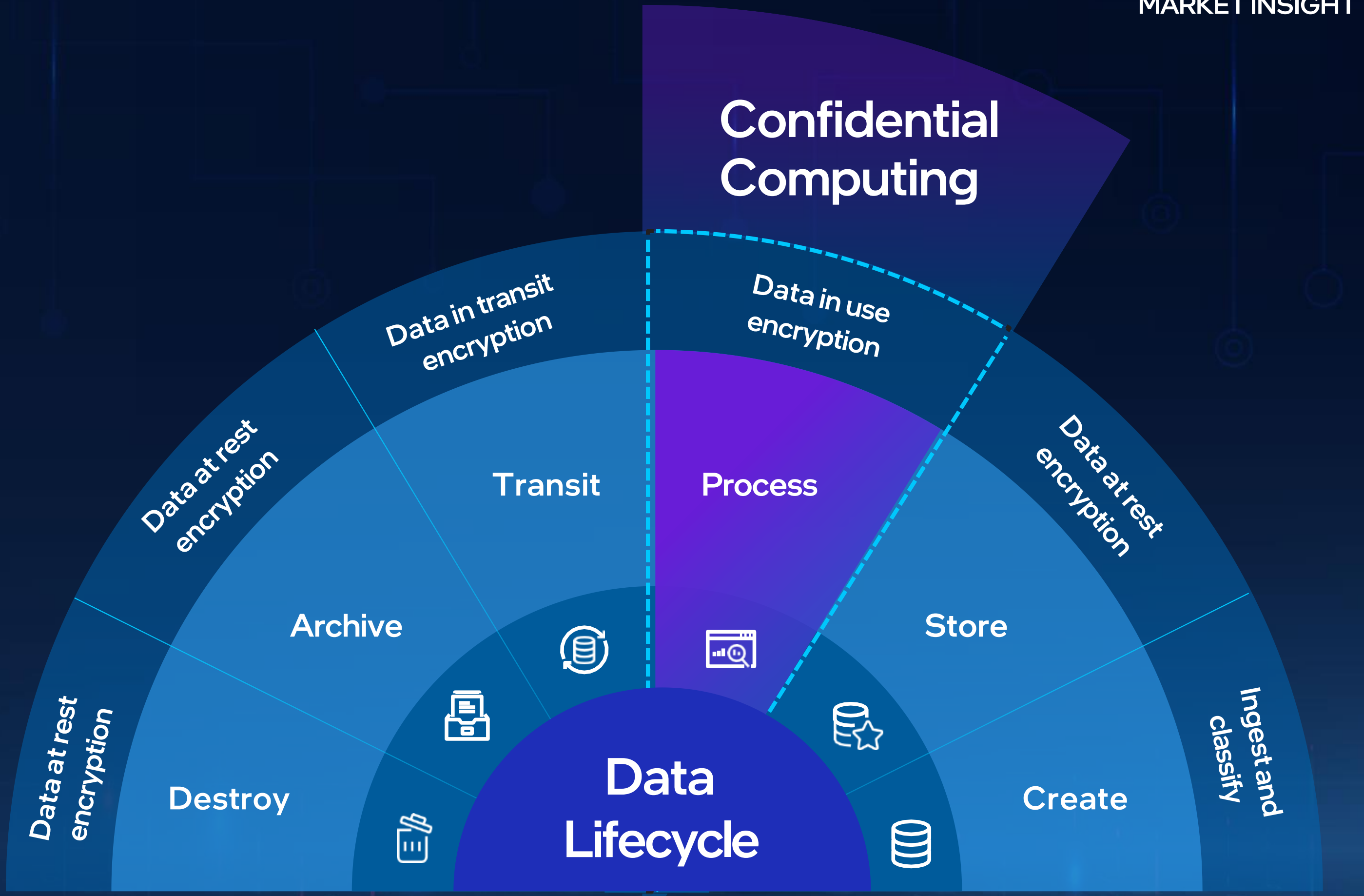
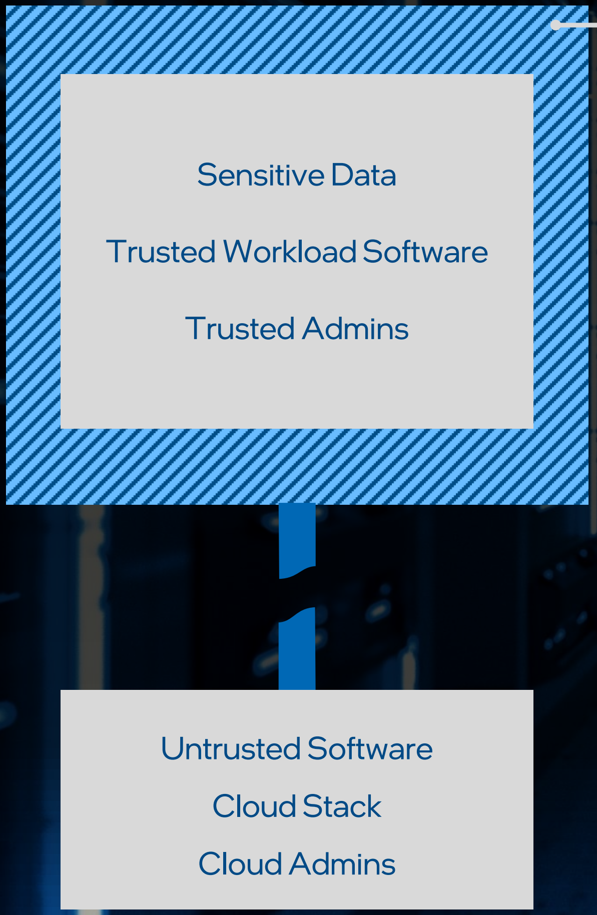


Image Source: Intel Confidential Computing: Market Sales Deck (an IDC Infobrief, sponsored by Intel)

Confidential Computing



Trusted Execution Environment (TEE)

Isolation

Separation of the TEE from underlying software, admins, and other cloud tenants

Encryption and Control

Workload owner holds key to decrypt data, retaining control and preventing access by cloud provider or other entities

Verification

Cryptographic confirmation that TEE is genuine, correctly configured, and software is exactly as expected

Highly Active in Confidential Computing

Sectors

Healthcare

Financial Services

Retail

Government

Industrial and Edge

Usages

Collaborative Analytics

Confidential AI

Privacy-preserving AdTech

Privacy-preserving Blockchains

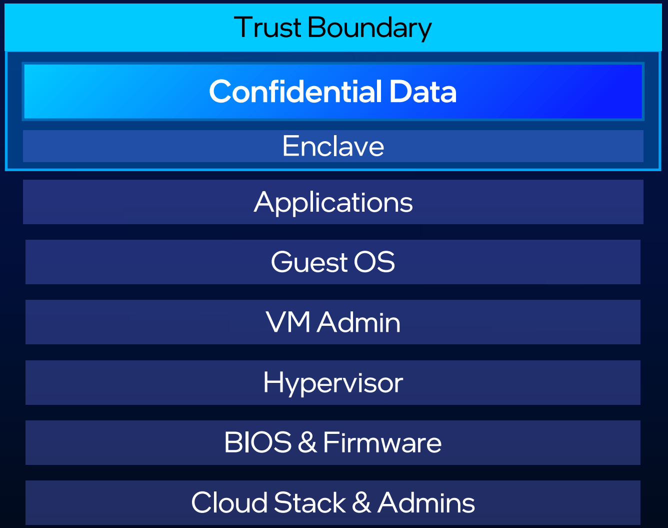
Data and Software IP Control

The Most Comprehensive Confidential Computing Portfolio

App Isolation

Intel® SGX

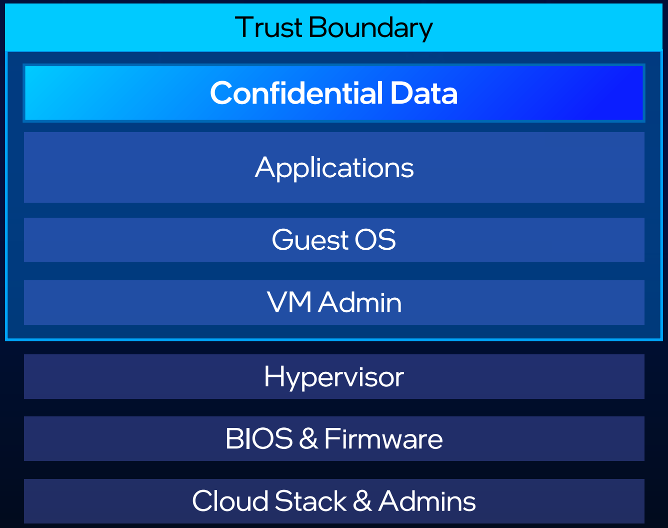
Smallest trust boundary for greatest data protection & code integrity



VM Isolation

Intel® TDX

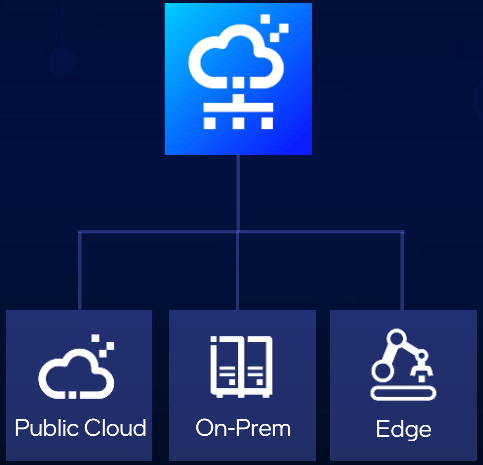
Most straightforward path to greater security and control for legacy apps



Independent Attestation

Intel® Tiber™ Trust Authority

Uniform, independent attestation of trustworthy environments



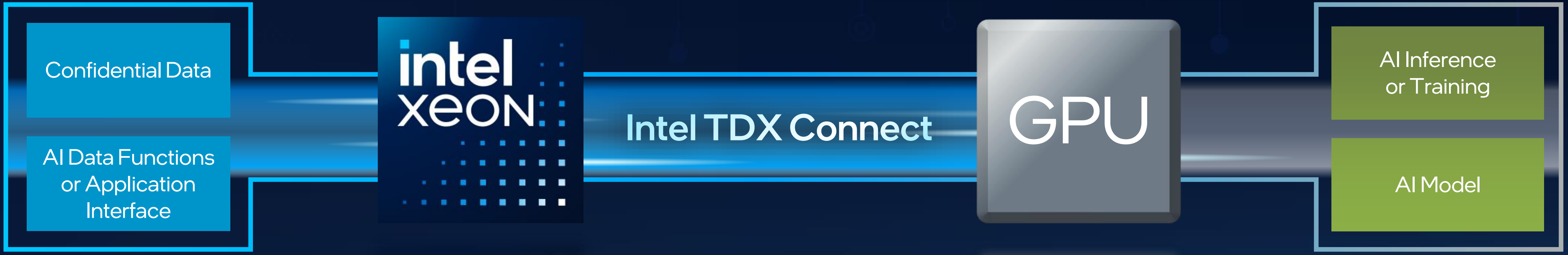
Intel Xeon 6 introduces AES-256 encryption (quantum-resistant) for Intel SGX & Intel TDX

Support for up to 2048 encryption keys for trust domains with Intel TDX

Intel® Software Guard Extensions (Intel® SGX), Intel® Trust Domain Extensions (Intel® TDX)

The Next Milestone in Confidential AI with **Intel® TDX Connect**

Provides a high-performance encrypted connection between the CPU and PCIe devices with direct memory access and lower overhead

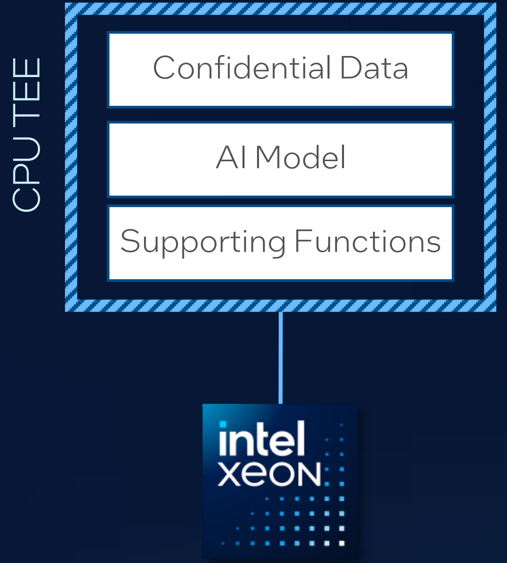


More Info: Announcing Intel® TDX Connect Support on Intel® Xeon® 6 - Intel Community

*Activating Intel TDX Connect will require Intel Xeon 6 with P-cores, TDX Module updates, an enabled OS, and an enabled device

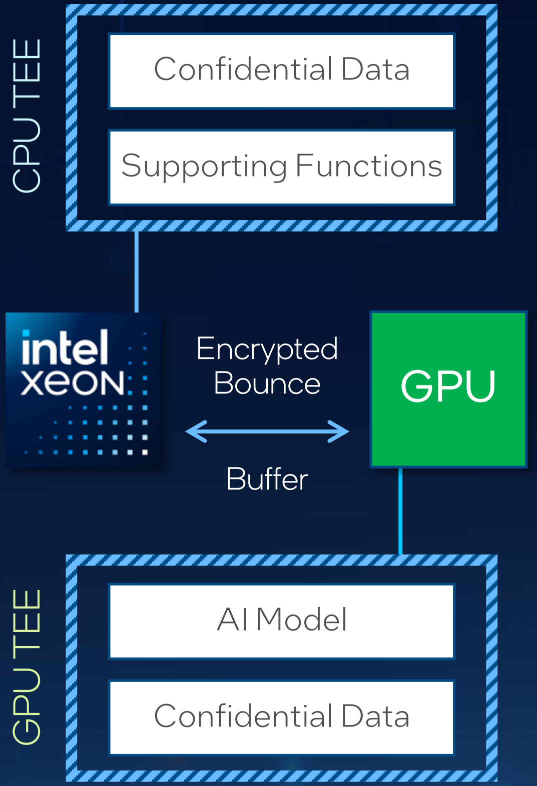
Confidential AI Options & Evolution

CPU-Based AI



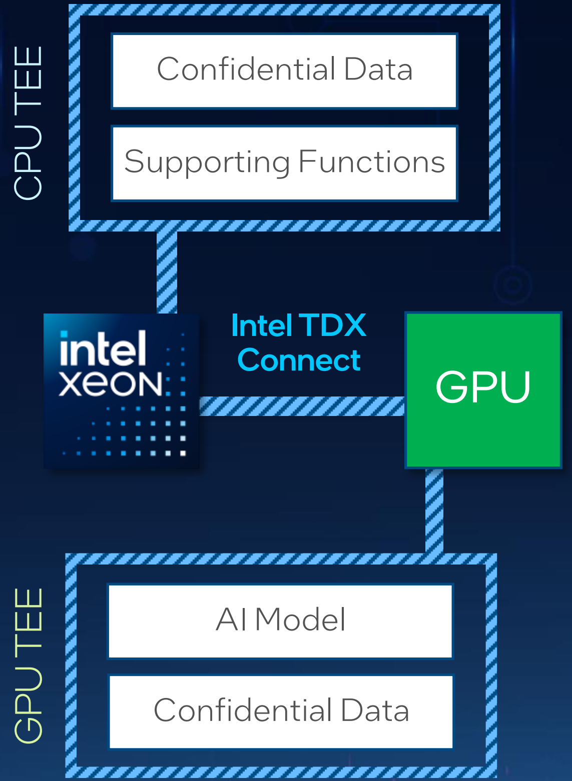
- Most inference workloads
- Training <10B parameters
- Intel® AMX acceleration

Accelerated AI with Bounce Buffer



- Models >10B parameters
- Data passed via encrypted "bounce buffer"

Accelerated AI with Intel® TDX Connect



- Models >10B parameters
- Single logical TEE across CPU & GPU (performance)

[More Info: Announcing Intel® TDX Connect Support on Intel® Xeon® 6]

*Activating Intel TDX Connect will require Intel Xeon 6 with P-cores, Intel TDX Module updates, an enabled OS, and an enabled device

Intel® Tiber™ Trust Authority

Zero Trust Attestation Service Without High Cost or Complexity

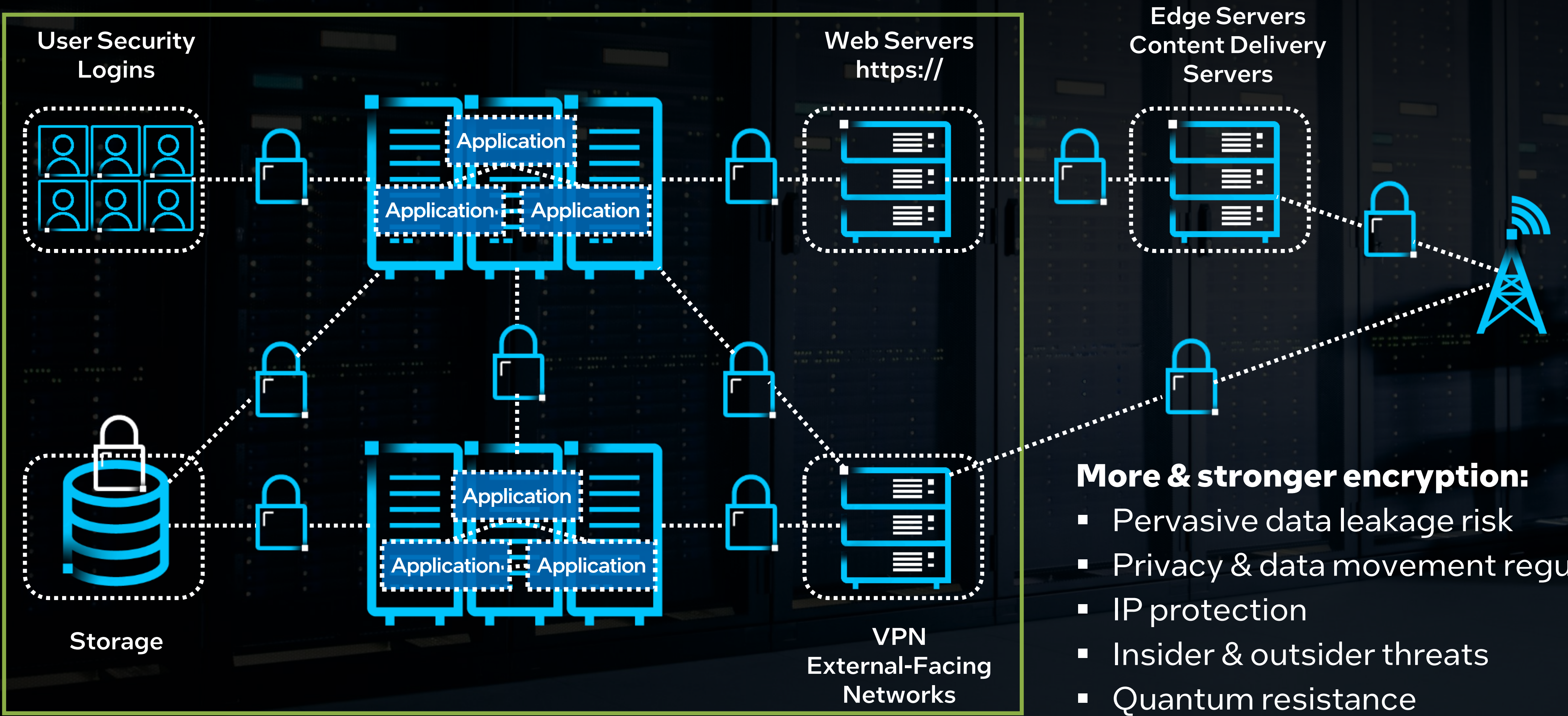
Public Cloud Flexibility – Private Cloud Security

- Zero Trust Independent Verification
- Confidential Compute Verification
- CPU + GPU Unified Verification
- Service Plugin for Relying Parties
- Tamper-resistant Ledger Platform
- Auditable Logs

MSP = Managed Service Provider

Intel Technologies for Security Workload Acceleration

Crypto Operations are Everywhere



More & stronger encryption:

- Pervasive data leakage risk
- Privacy & data movement regulations
- IP protection
- Insider & outsider threats
- Quantum resistance

Accelerate High-Volume Cryptography Workloads

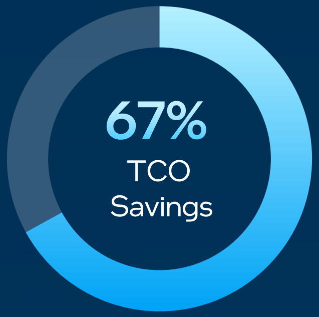
Intel® QuickAssist Technology (Intel® QAT)

- Increases the performance of crypto operations and compression
- Supports AES-256 (quantum-resistant)
- Designed for high-throughput use cases including network encryption, VPNs, and content delivery systems
- Higher crypto throughput while freeing CPU cores for other valuable workloads
- Higher power efficiency than CPU cores

Web Services: NGINX TLS (1S) on 6760P

Refresh Aging Infrastructure to Save Space and Cost

10:1 Consolidation[1]

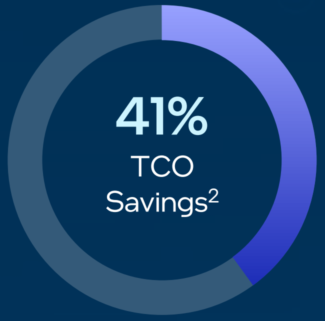


90% fewer servers
83% less power

Replace 2nd Gen Intel® Xeon® processor-based servers with Intel Xeon 6 processor-based servers

Save Power and Money on New Server Purchases

1.55x Perf/Server[2]



Performance advantage and TCO savings vs AMD EPYC 9005 servers

1. Estimated over 4 years. See [7T26] intel.com/processorclaims: Intel Xeon 6. Results may vary.
2. Estimated over 4 years. See [7T223] intel.com/processorclaims: Intel Xeon 6. Results may vary.

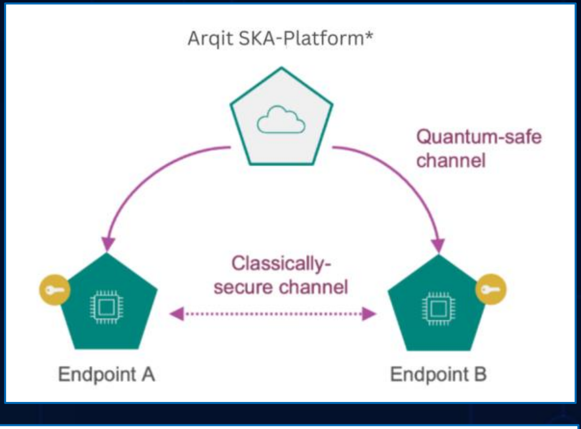
intel.

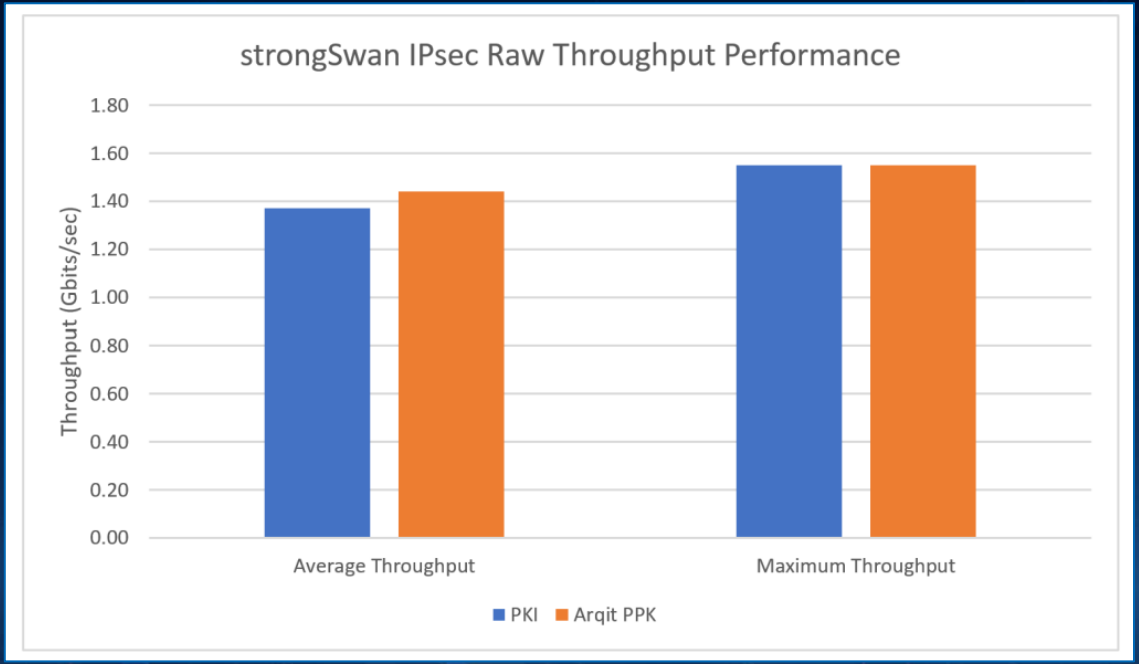
Case Study: Arqit SKA-Platform*

Testing demonstrates a quantum secure IPsec tunnel can be achieved without compromising performance[1]

Address "Harvest Now, Decrypt Later" threats

- Arqit adds RFC 8784 compliant post-quantum cryptography (PQC) without performance impact to single server 1.89 Tbps VPP IPsec tunnel [2]
- Arqit NetworkSecure* deployed with Intel® Trust Domain Extensions (Intel® TDX) to help protect PQC keys generated and enhance protection of encrypted networks[3]
- Solution can also be fully deployed on the Intel® NetSec Accelerator Reference Design[1]





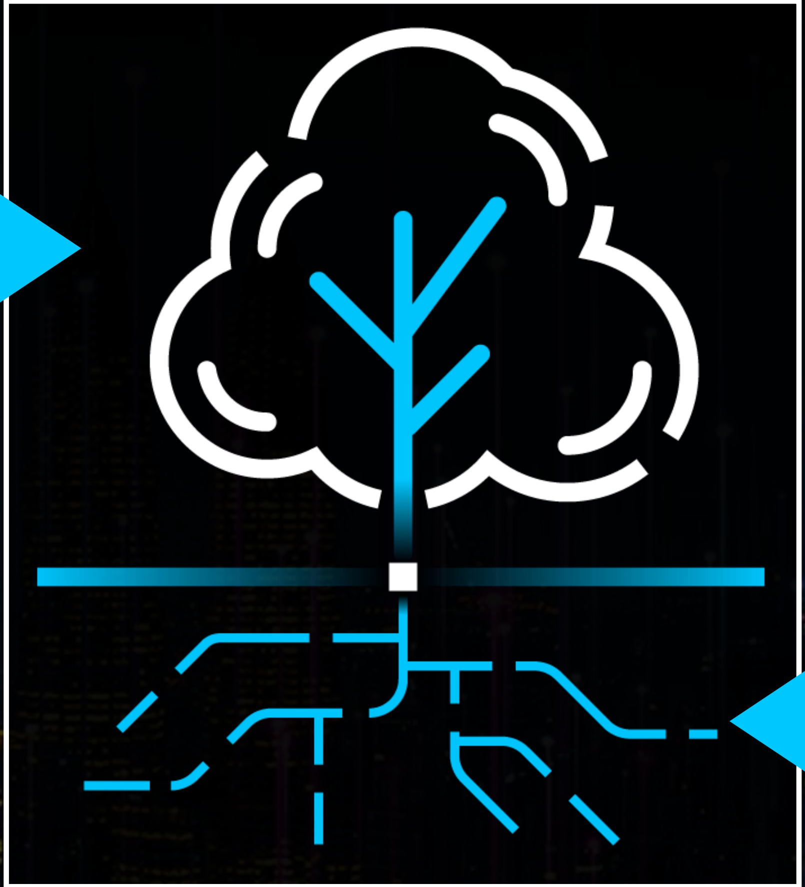
IPsec throughput performance with and without Arqit SKA-Platform[1]

[1] – Intel, Arqit and Intel Test Post Quantum Cryptography (PQC) Solution
[2] – Intel, FD.io VPP-SSwan and Linux-CP – Integrate StrongSwan with World's First Open Sourced 1.89 Tb IPsec Solution Technology Guide (intel.com)
[3] – Arqit, Data Sovereignty with Confidential Computing and Networking

Intel Technologies for Advanced Protection & Software Safety

Hardware Can Help Mitigate Many Software Attack Vectors

- Applications, OS and hypervisor, represent a huge attack surface
- Attacks exploit structural software vulnerabilities can be mitigated by hardware



- BIOS and platform firmware form the foundation for entire software environment
- Hardware can mitigate attacks on BIOS and low-level firmware that can compromise the entire stack

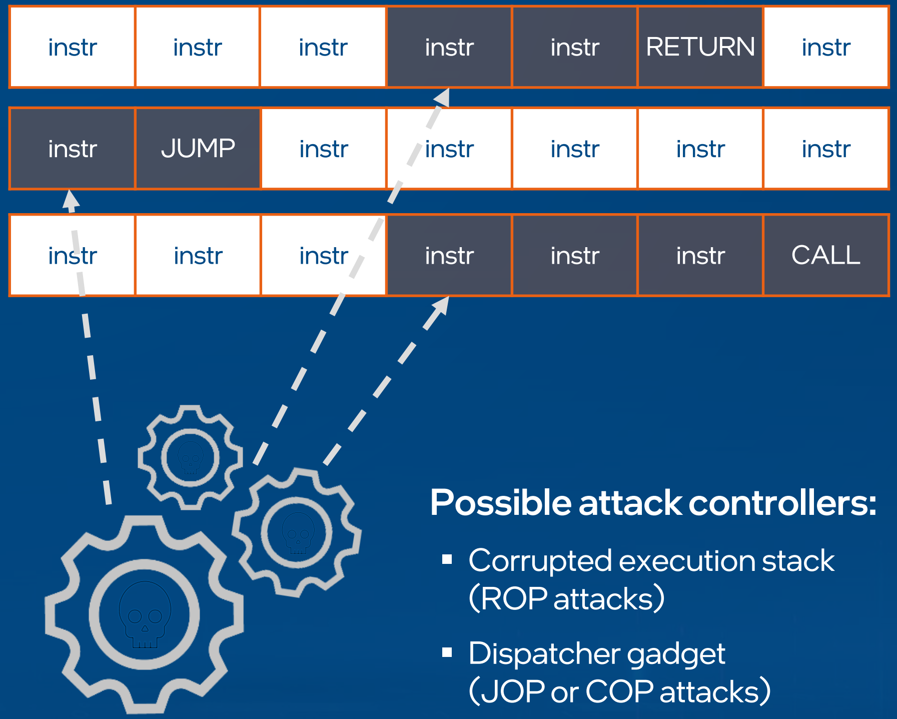
Intel® Control-Flow Enforcement Technology (Intel® CET)

Intel CET helps keep software behaving as intended.

Designed to stop Return, Jump, and Call-Oriented Programming (ROP, JOP, COP) attacks:

1. Shadow Stack: Helps stop corrupted execution stack from redirecting Return commands to gadget addresses
2. Indirect Branch Tracking: Introduces new software flag called "ENDBRANCH" placed at the legitimate beginning of code branches

Attack executed by sequencing code "gadgets" in a legitimate program



instr	instr	instr	instr	instr	RETURN	instr
instr	JUMP	instr	instr	instr	instr	instr
instr	instr	instr	instr	instr	instr	CALL

Possible attack controllers:

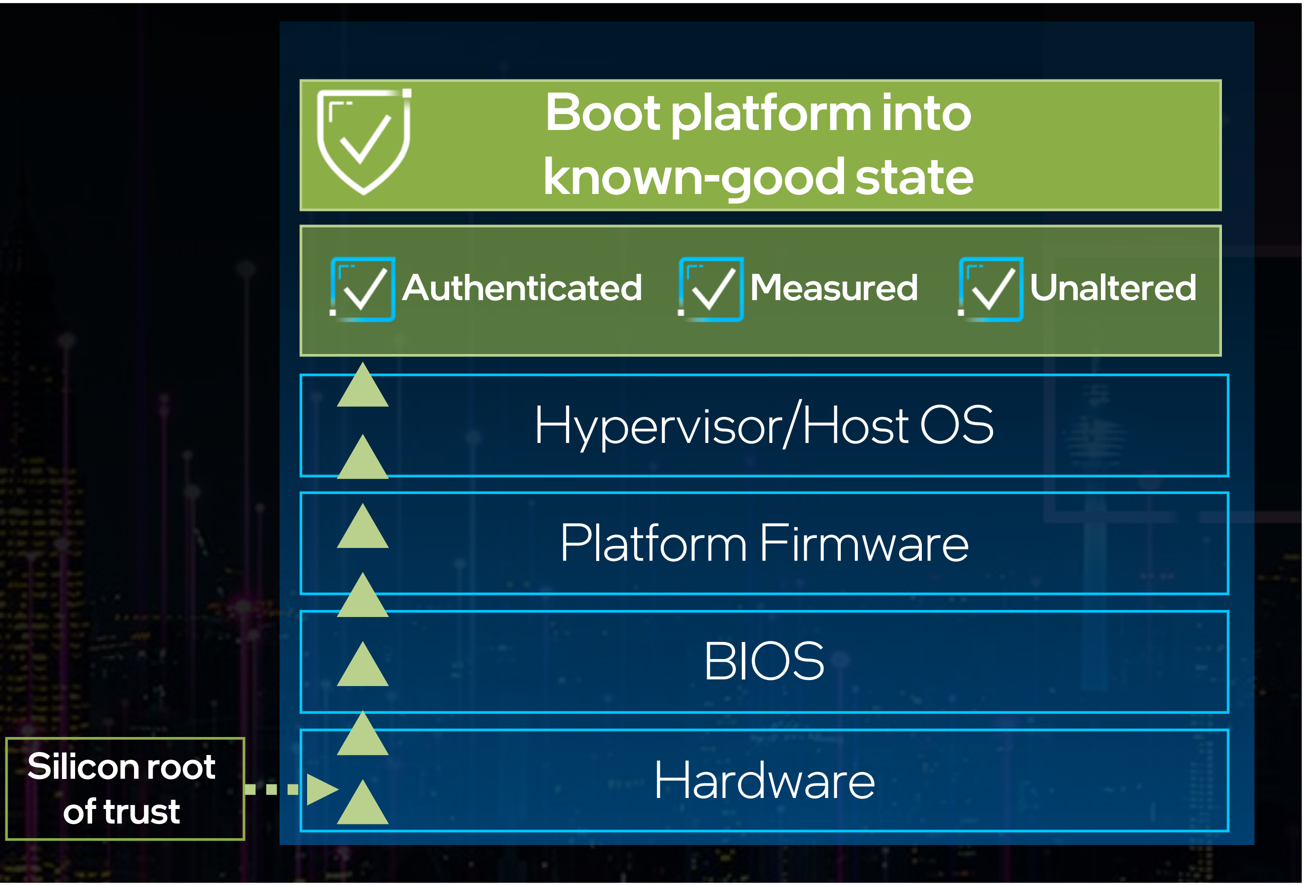
- Corrupted execution stack (ROP attacks)
- Dispatcher gadget (JOP or COP attacks)

Intel Technologies Boot Platforms into a Known-Good State

Intel® Boot Guard
Protects integrity of BIOS launch, starting chain of trust with HW

Intel® Trusted Execution Technology
Measured, verified launch of authenticated launch code modules

Intel® Platform Firmware Resilience
Can detect unauthorized firmware changes in BIOS, BMC, SPI Flash and more , and recover to known state



Intel's Investments Help Drive Better Security Outcomes

Our Roadmap is Aligned to Zero Trust Principles

Intel technologies help you build a Zero Trust strategy, establishing hardware as the root of trust

Endpoint Security

Strengthen defenses with AI-powered threat detection, insights, and hardware-based security measures

Network Security

Connect people with the resources they need through encryption-based identity and access control

Information & Data Security

Designed to isolate and protect your sensitive data while in use to enhance confidentiality, integrity, and availability

Physical Security

Help prevent real-world attacks by managing the convergence of AI, physical, and cyber security assets

Product Security Assurance: Built on a Foundation of Trust

Choose products designed with security in mind, backed by the industry's best security assurance[1]

[1] - As measured by ABI Research

What Intel Security Can Do For You

Better protect sensitive data, applications, and infrastructure

Create new business possibilities without compromising data privacy

Resource: Security Product Messages

More Info: Security Engines - Intel

Intel® Software Guard Extensions

Protect and isolate your confidential data while it is actively in use. Uniquely establish granular control and protection with private memory enclaves designed to be protected from higher privilege processes.

Intel® Trust Domain Extensions

Increase confidentiality, enhance privacy, and gain control over your data at the VM level. Deliver guest OS and VM application isolation in as few as one click during VM configuration.

Intel® Control-flow Enforcement Technology

Designed to protect against the misuse of legitimate code through control-flow hijacking.

Intel® Quick Assist Technology

Expedite the encryption and decryption of data to help reduce system resource consumption for your AI workloads.