intel

Memory Interposer Attacks

Out of Scope, but not forgotten

OC3 March 12th, 2026

OC3 Berlin 11th March 2026

Out of scope, but not forgotten

Simon Johnson
Intel Fellow, Confidential Computing

Simon Johnson
Intel Fellow

Simon Johnson is an Intel Fellow, and one of the industry's leading voices in confidential computing and hardware-rooted security. He leads the development of next-generation trusted computing technologies, including Intel® Trust Domain Extensions (Intel® TDX) — helping establish confidential computing as a foundational pillar of modern cloud and sovereign infrastructure.

A globally recognized technical leader and evangelist, Simon works closely with governments, cloud providers, and industry partners to strengthen platform security against emerging software and physical threat vectors while balancing performance, cost, and deployability at scale. With more than three decades in security, spanning both Intel and the UK government, he brings deep expertise in trusted systems, threat modeling, and resilient infrastructure design.

Simon is based in Hillsboro, Oregon.

Intel's Job ...

Security

… in Reality

Cost

- Resource Consumption
- Power Consumption
- Ease-of-deployment
- Operational Complexity

Performance

- Bandwidth
- Predictability
- Latency
- Throughput
- Availability
- Impact to non-security WL's

In practice, these three forces define the acceptable security envelope.

Security Assurance

- Threat Model Coverage
- TCB Size / Attack Surface
- Recoverability / Resilience
- Attestable and Verifiable
- Side-Channels Resistance
- Physical Attacks Resistance
- Post Quantum and Cryptographic agility

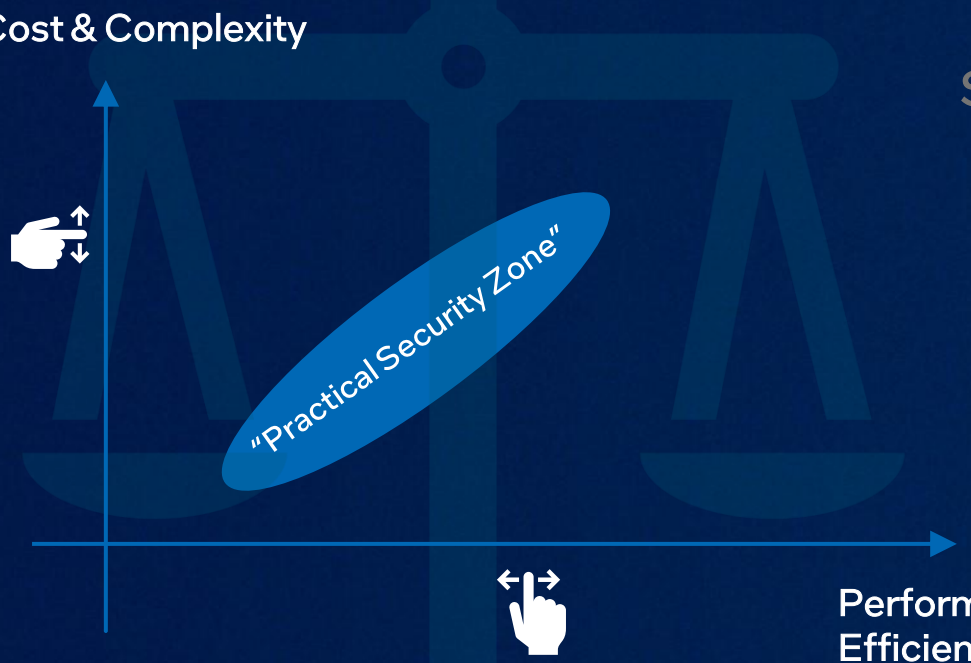
… in Reality, TCO defines the real security boundary

Cost

- Resource Consumption
- Power Consumption
- Ease-of-deployment
- Operational Complexity

Performance

- Bandwidth
- Predictability
- Latency
- Throughput
- Availability
- Impact to non-security WL's

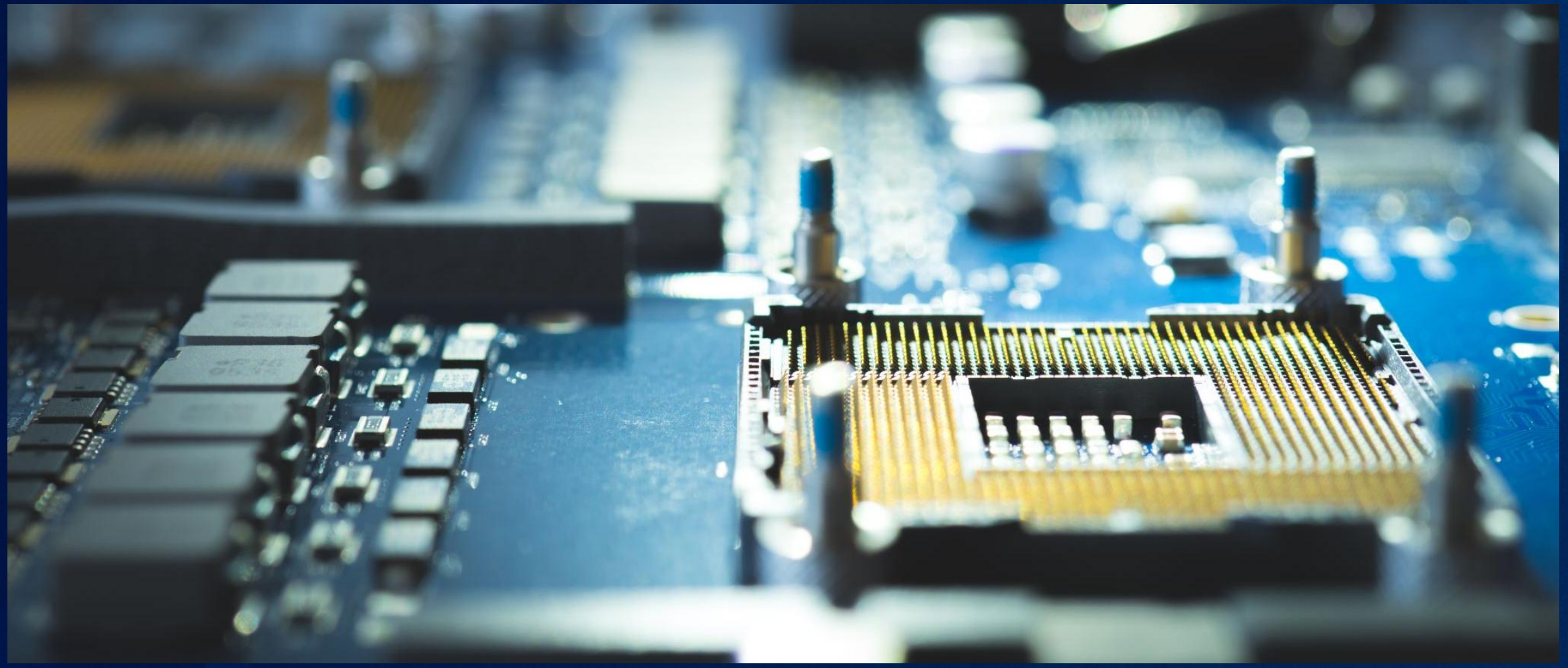


Security Assurance

- Threat Model Coverage
- TCB Size / Attack Surface
- Recoverability / Resilience
- Attestable and Verifiable
- Side-Channels Resistance
- Physical Attacks Resistance
- Post Quantum and Cryptographic agility

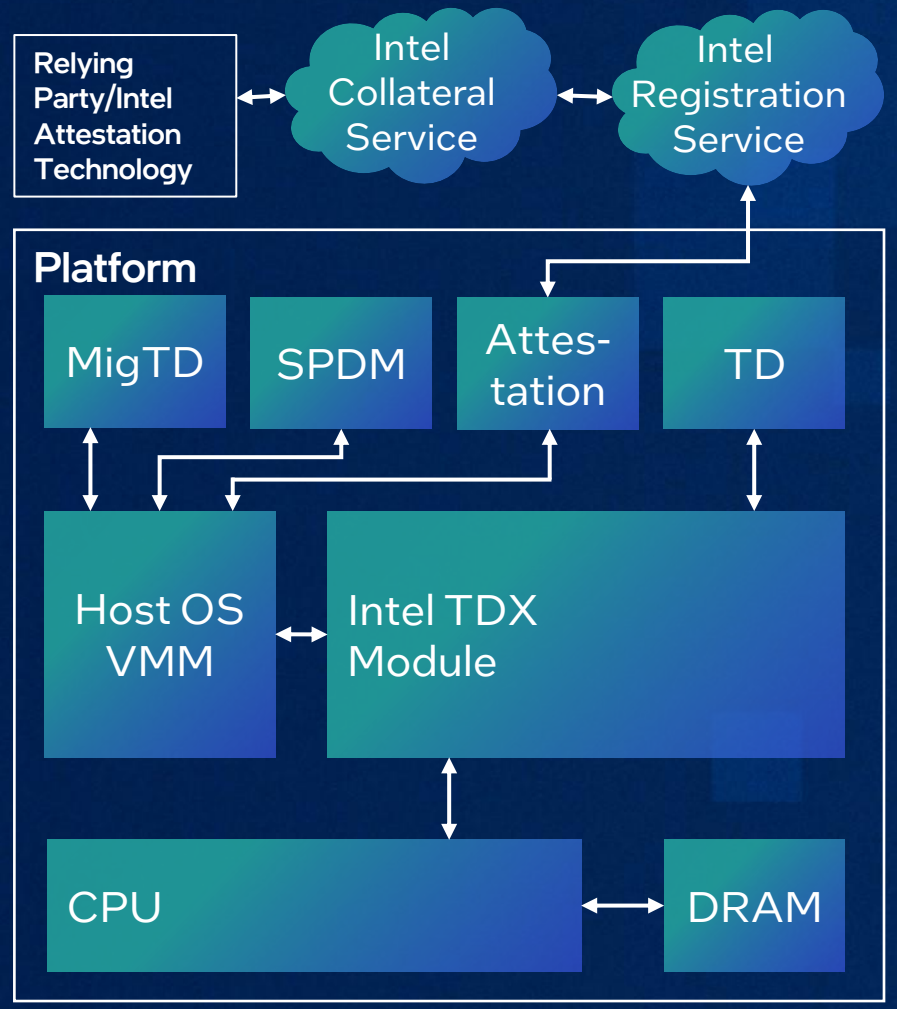
The optimal architecture maximizes verifiable security within an economically sustainable envelope

Intel Confidential Computing Innovations to drive down TCO



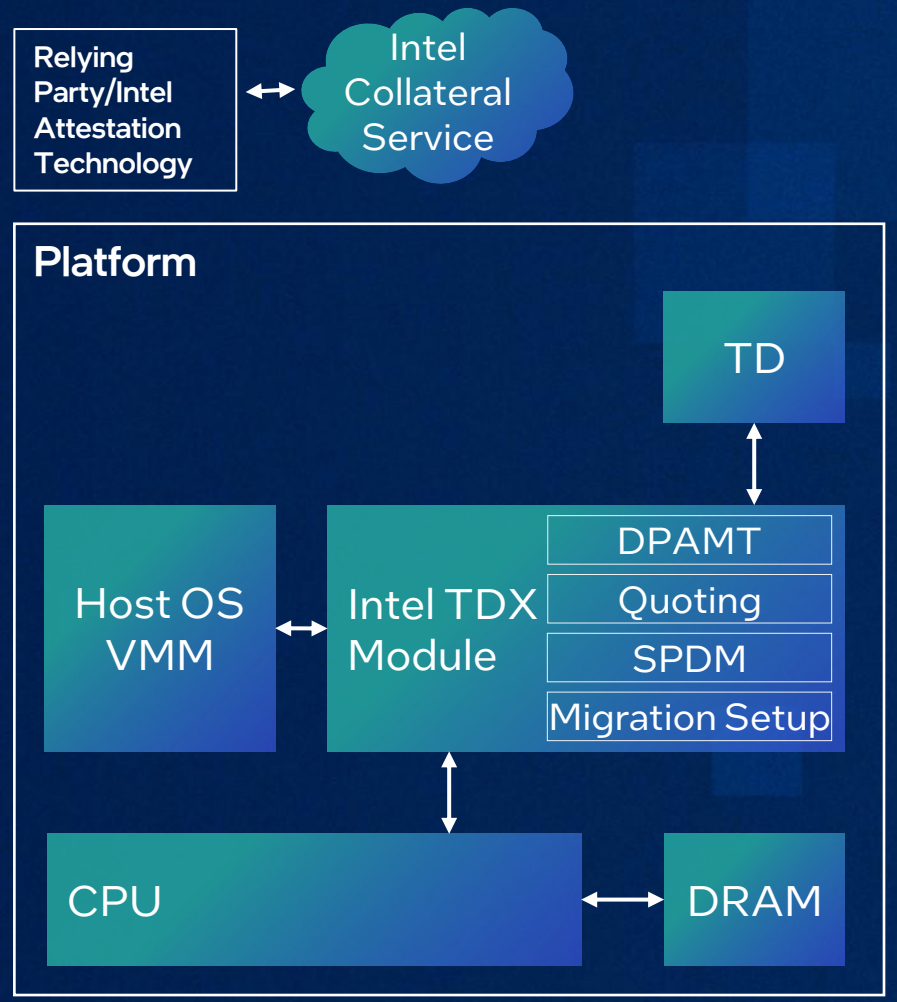
Customer TCO Requirements for Intel TDX

- Run Confidential and Non-confidential side by side
  - Reduce Memory Consumption when idle
  - Reduce the need for reboots on updates
  - Enable Migration with TDISP devices
  - Better Diagnostics on Failure Cases
- Reduce Enabling Complexity
  - Remove external service TD's
  - Support a single multi-vendor stack for TEE-IO
  - Intel TDX should not rely on Intel SGX
  - Support full virtualization of Linux guests
- Provide additional security
  - Harden attestation mechanisms



Advancing Intel TDX for Maturity, Operability and Scale

- Run Confidential and Non-confidential side x side
  - Dynamic PAMT
  - Linux Kernel Updates of Intel TDX Module*
  - Non-blocking migration export*
  - Enhanced Intel TDX Module diagnostics for detecting fatal errors
- Reduce Enabling Complexity
  - Refactor of Intel TDX Connect*
  - Integrated Migration Setup support*
  - DICE based attestation w/o Intel SGX*
  - Virtualization Exception Support extended
- Provide additional security
  - DICE based attestation
- Intel TDX Module Quarterly Updates aligned to Intel Update Cycle



*Under development

Cryptographic Error Correcting Code (ECC)

Next-Generation Rowhammer Protection

The Innovation

On write, Cryptographic Blinding Algorithm ***removes determinism*** from exploitable error patterns

The Mitigation

Reduces the risk of attackers manipulating ECC behavior to induce controlled memory corruption

The Protection

Attempted Rowhammer attacks can be detected, corrected, or handled as memory corruption errors

Delivers stronger memory protection with no additional ECC overhead and negligible performance impact, all within the existing platform TCO envelope.

Post-Quantum Cryptography (PQC) Update

Addressing PQC Threats

Complete

Resilience to Data Harvesting

Larger key sizes for symmetric crypto to protect against Harvest Now Decrypt Later attacks.

Near Completion

Code Signing & Authentication of Firmware

CNS A 2.0 compliant PQC algorithms for CPU and SoC firmware.

In-progress

Secure Internet with new Digital Signature & Key Establishment Standards

Develop NIST PQC standard and implement them in our products.

Intel's PQC Roadmap

PQC Algorithm Standards

Intel is deeply engaged in the development of PQC algorithms across the industry. Standards development is expected to continue for the next several years.

PQC Technology Implementation

Intel began offering PQC capabilities in its platforms in 2023.

Full PQC Compliance

All new Intel platforms will incorporate PQC resistant algorithms across the full stack by 2030.

PQC-enablement of Intel TDX

Memory Encryption

Supports AES-XTS w/256bit keys

Measurements

SHA384 measurements are standard in Intel TDX

TDX Connect

Support for SPDM 1.4 in development

Attestation

Support for ML-DSA based attestation in development

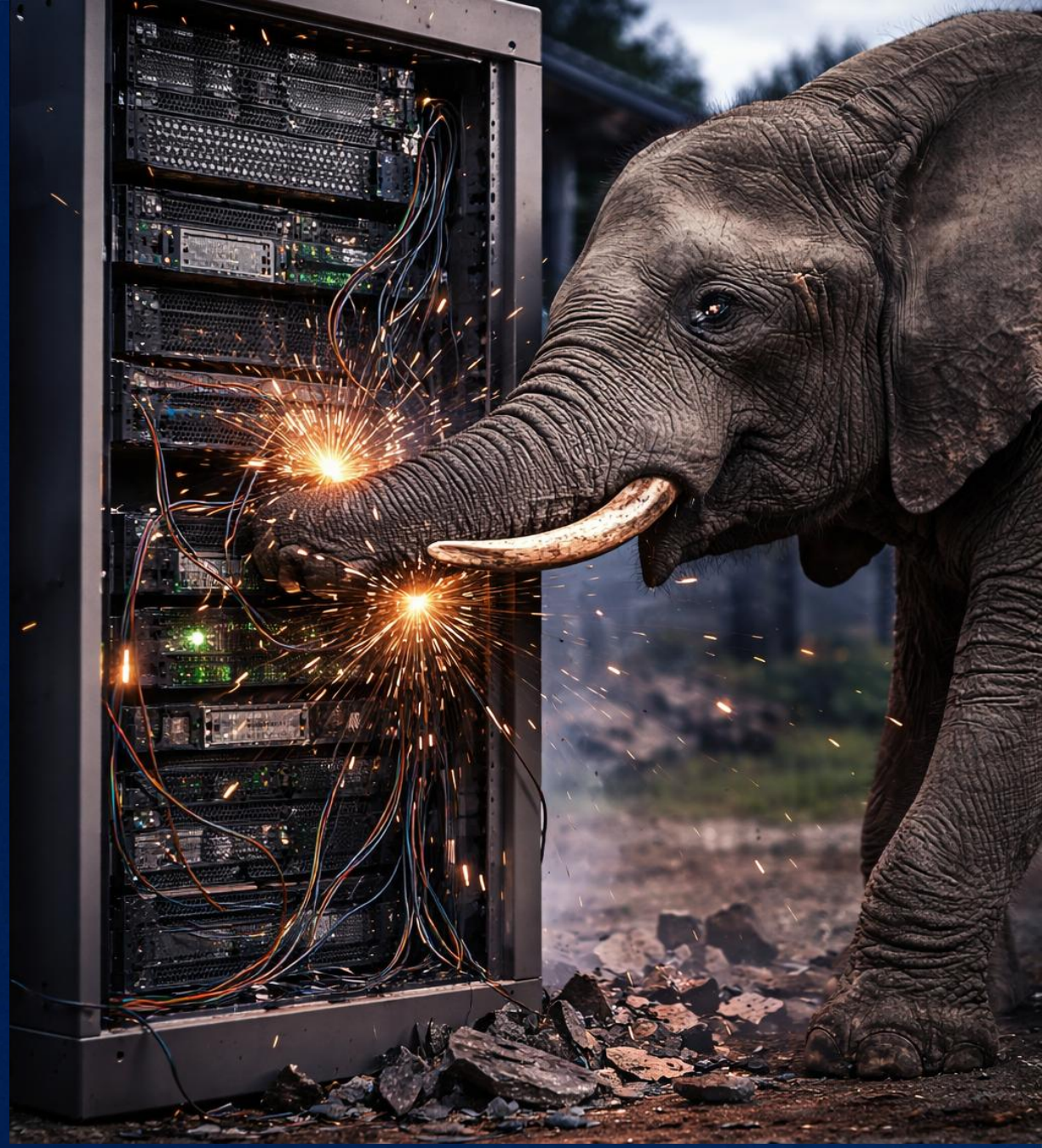
Migration

ML-KEM Key Negotiation w/ ML-DSA Attestation in development

Physical Attacks – the elephant in the room

- Physical access changes the threat model
  - Memory probing & bus observation
  - Fault injection & Rowhammer-style manipulation
  - Cold-boot & DMA attacks
  - Ciphertext observation & tampering
- When attackers reach the hardware, new protections are required

So how do we strengthen protection without increasing TCO



Out of Scope, but not forgotten

- **AES-XTS based memory encryption has become the de facto standard across the industry**
  - Its relatively efficient and widely deployed
  - However, it provides limited protection when attackers can observe or manipulate encrypted memory
- Recent academic research has demonstrated attacks against several AES-XTS based implementations
- Stronger cryptographic protections are possible — but cannot be delivered without increasing platform TCO
- So how do we improve security while minimizing cost and performance impact?
- Through incremental, hardware-native security improvements — delivered piece by piece

Key Innovations Strengthening Confidential Computing Assurance

1. **Platform Ownership Endorsement:**
   Enable verifiers to establish trusted platform ownership and execution context
2. **Architectural Enclave Improvements:**
   Continuously reduce attack surface and strengthen workload isolation
3. **Hardware-Based Attestation:**
   Enable stronger, hardware-rooted, automated trust verification
4. **Tamper Detection Research:**
   Detect and respond to physical tampering and intrusion attempts
5. **Next-Generation Memory Encryption:**
   Advance beyond AES-XTS to protect against emerging memory attack vectors

Dedicated OC3 Session:

Toward ownership-aware attestation: Contrast meets Platform Ownership Endorsement

Simplified, Hardware-Native Attestation for Confidential Workloads

- Hardware-native attestation without requiring Intel® SGX
  - New hardware-rooted signing capability from the platform security engine
  - No external service VM required means simpler architecture and lower overhead
  - Attestation requests handled directly through the Intel® TDX Module interface
  - Supports both direct and indirect use of the hardware security engine for optimal performance and flexibility
  - Recently published draft Intel® TDX Module interface definitions for attestation quoting https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/documentation.html

Simplifies attestation architecture, reduces operational overhead, and improves scalability of confidential computing deployments.

Next-Generation Memory Encryption for Scalable Confidential AI

- Scaling Confidential AI is stressing the limits of traditional AES-based memory encryption and its TCO model.
- Intel is exploring an ASCON-based construction designed to both strengthen security and reduce the cost of memory encryption.
- Industry collaboration is essential to standardize next-generation memory encryption and enable Confidential AI at scale.

1	**Improve security, bigger block sizes, and optional cache line versioning:** Stronger resistance to physical memory tampering and replay attacks delivered with minimal performance, power, and silicon overhead—preserving overall platform TCO
2	**Reduce Latency Costs of Encryption** Lower performance overhead and power consumption from memory encryption, improving workload efficiency while reducing overall platform TCO
3	**Optimize silicon efficiency (power and area):** Reduced silicon area and power requirements, lowering platform cost and improving overall TCO efficiency at scale

Security Research on Intel Confidential Computing

We encourage offensive research on our products to continuously strengthen our security

2022 — Google

Intel collaborated with Google Project Zero on a 9-month evaluation of Intel® TDX in 2022 prior to initial availability.

2024 — Microsoft Azure

Intel collaborated with Microsoft Offensive Research & Security Engineering to examine 29 attack vectors on Intel® TDX in 2024.

2025 — Google

Extension of previous review covering major changes since Intel® TDX module 1.0, with a focus on live migration and Trusted Domain partitioning (nested VMs within TDs).

https://cloud.google.com/blog/products/identity-security/rsa-google-intel-confidential-computing-more-secure
https://www.intel.com/content/dam/www/public/us/en/security-advisory/documents/intel_tdx_joint_security_review_with_microsoft.pdf
https://www.intel.com/content/www/us/en/content-details/846149/2024-intel-product-security-report.html

Proactive Security Validation

At Intel, we're dedicated to making our Confidential Computing technology as secure as possible. This kind of collaborative research extends our internal threat models and helps uncover and address security vulnerabilities that can emerge in these complex environments before malicious actors can take advantage of them.

> *Intel TDX is an instrumental technology helping to achieve our confidential computing goals. Now that we are finished, it's even more secure, and I'm very confident, after this hackathon, with this technology."*
>
> — **Yair Netzer,** Principal Security Research Manager, Microsoft

> *Our deep collaboration with Intel allows us to battle-test and strengthen the security of foundational technologies that power Confidential Computing. By proactively identifying vulnerabilities in critical features like Live Migration and TD Partitioning using advanced AI tools like Gemini, we are helping to raise the security bar for the entire ecosystem."*
>
> — **Andrés Lagar-Cavilla,** Distinguished Engineer, Google Cloud

Verifiable Trust Within an Economically Viable Envelope

Confidential Computing is now a foundational technology

- Protects data *in use* across cloud, sovereign, and enterprise environments
- Enables confidential AI, regulated workloads, and secure multi-tenant platform

Innovation must balance security benefits with TCO to be broadly adoptable

- Stronger security delivered without prohibitive cost or performance impact
- Enables scalable, real-world deployment of confidential workloads

Innovation to address the next set of security challenges

- New tools will be needed to address issues within the TCO envelope
- Addressing some challenges may take time and industry co-operation

intel® security

Notices & Disclaimers

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

No product or component can be absolutely secure.

Your costs and results may vary.

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