Confidential Computing and Hardware TEEs

Raghu Yeluri, Sr. Principal Engineer and Lead Security Architect

Office of the CTO / SATG

Outline

- Confidential Computing (CC)
- Technologies enabling Confidential Computing
- Use-cases Examples for Confidential Computing
- Challenges with Confidential Computing
- Intel's Project Amber - overview
- Summary

The “Last Mile” Problem with Data

Protect Data
at Rest

Storage Encryption

Protect Data
in Transit

Network Encryption

Protect Data
in Use

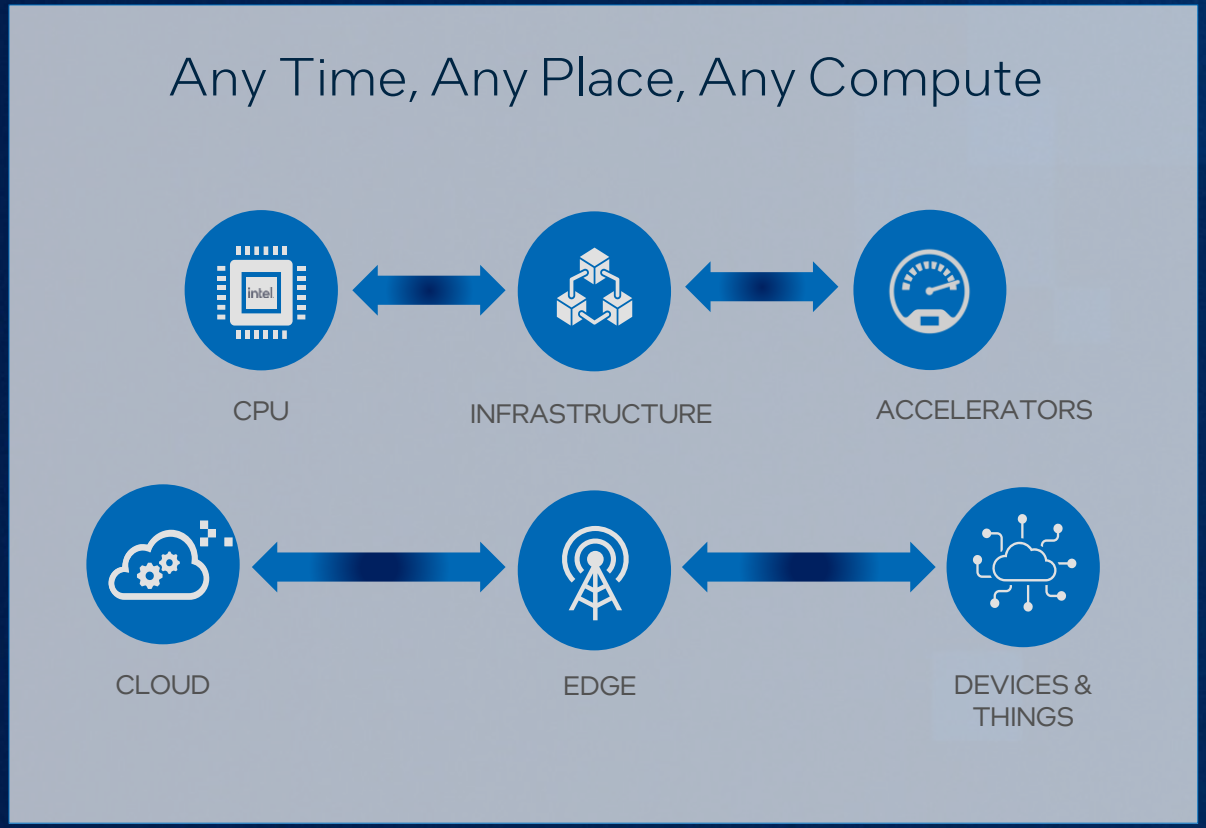
Confidential Computing

Confidential Computing (CC)

Protection/separation of data processing from the platform owner/administrator

- Enables data privacy & governance
- Accelerates cloud transformation for sensitive workloads
- Largest shift in computer security since the 1970's

Relies on a Trusted Execution Environment (TEE)

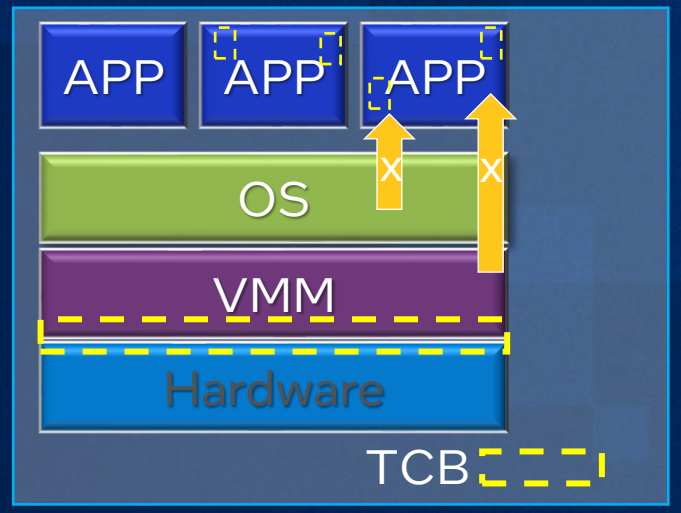


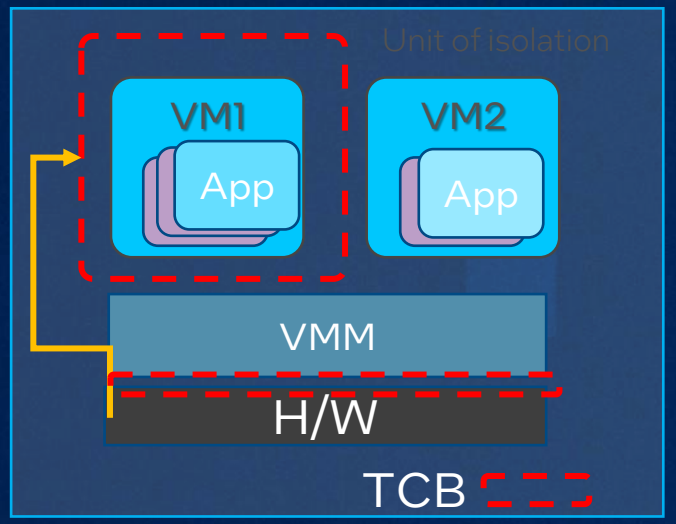
Confidential Computing: Workloads run in Trusted Execution Environment (TEE) to protect against unauthorized viewing and tampering of code and data

TEE enables Confidential Computing

- ✓ A **Trusted Execution Environment (TEE)** is a secure area protected by the processor. (aka. Enclave)
- ✓ Provides hardware-enforcement so that:
  - Code loaded inside TEE is operator-authorized code.
  - Data inside TEE cannot be read/modified from the outside.
  - Confidentiality and integrity for both code and data.
- ✓ Threats protected:
  - Malicious/compromised admin
  - Malicious/compromised tenant of a hypervisor
  - Malicious/compromised network
  - Compromised operating system/BIOS

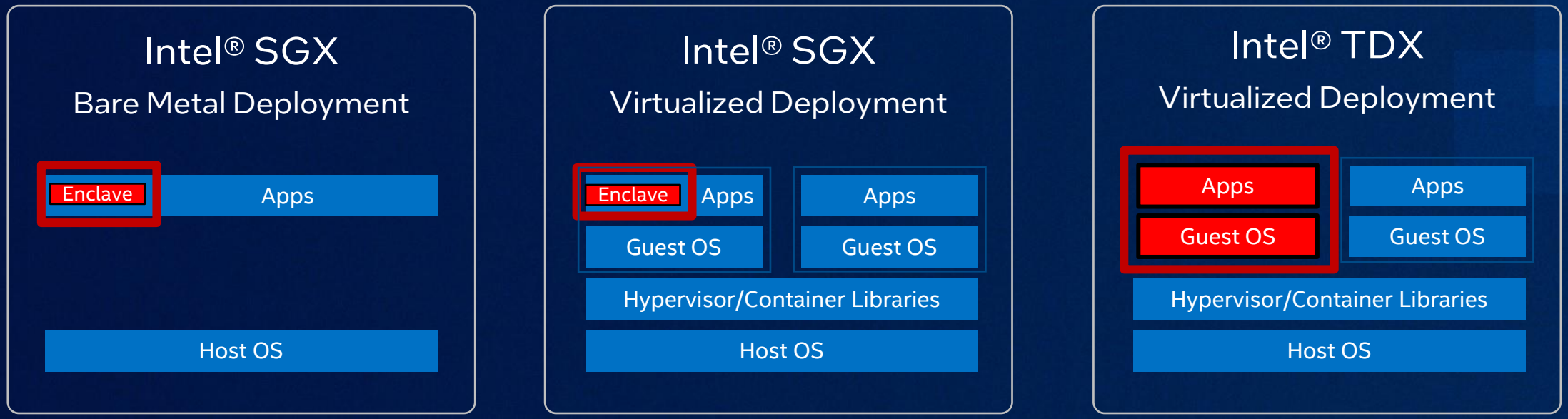
Examples of TEEs: Intel® SGX, Intel TDX, AMD SEV-SNP, ARM Realms





TCB: Trusted Compute Base

Intel Hardware TEEs

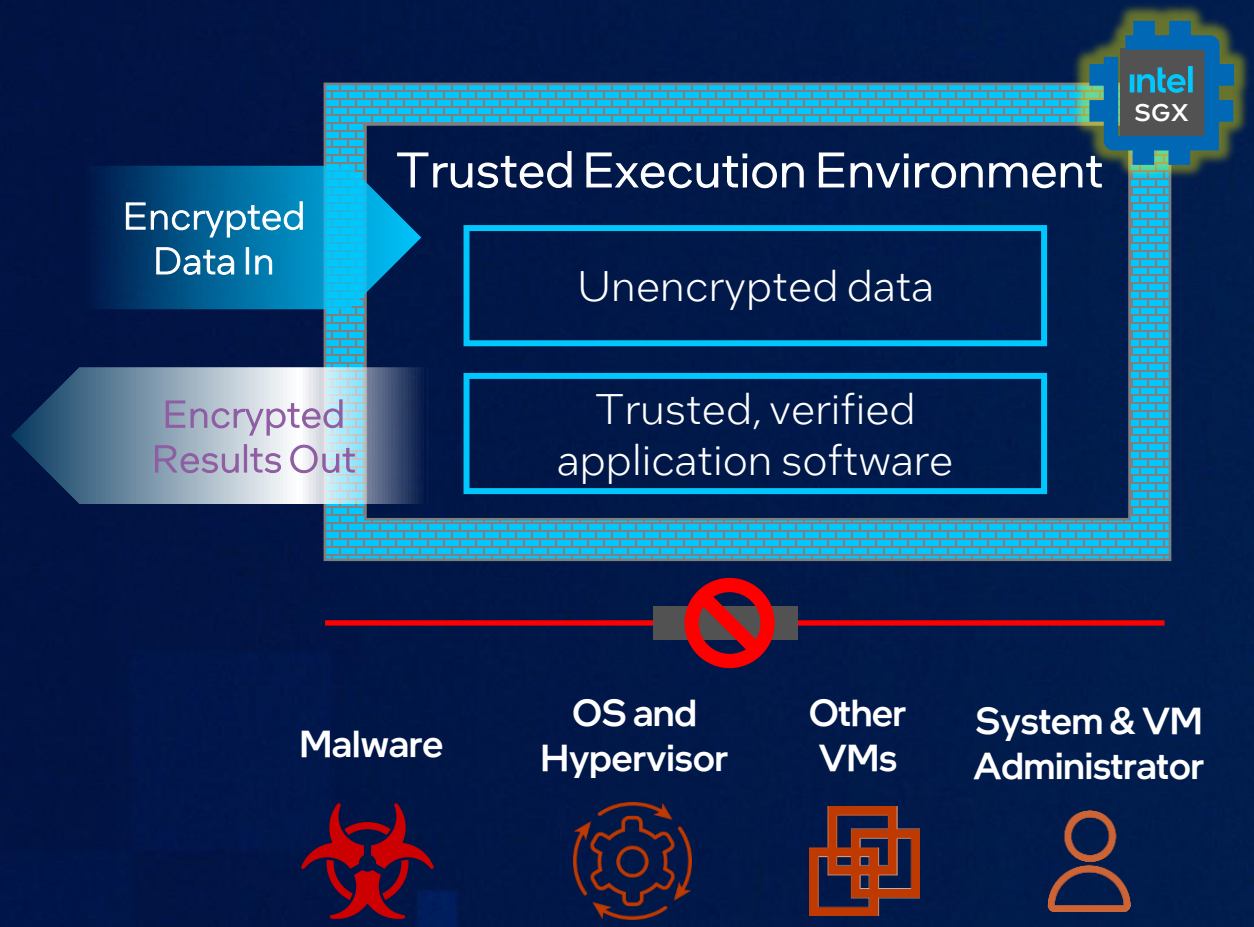


- Maximum data isolation
- Single tenancy

- Simplest migration of existing software
- Multi-tenancy

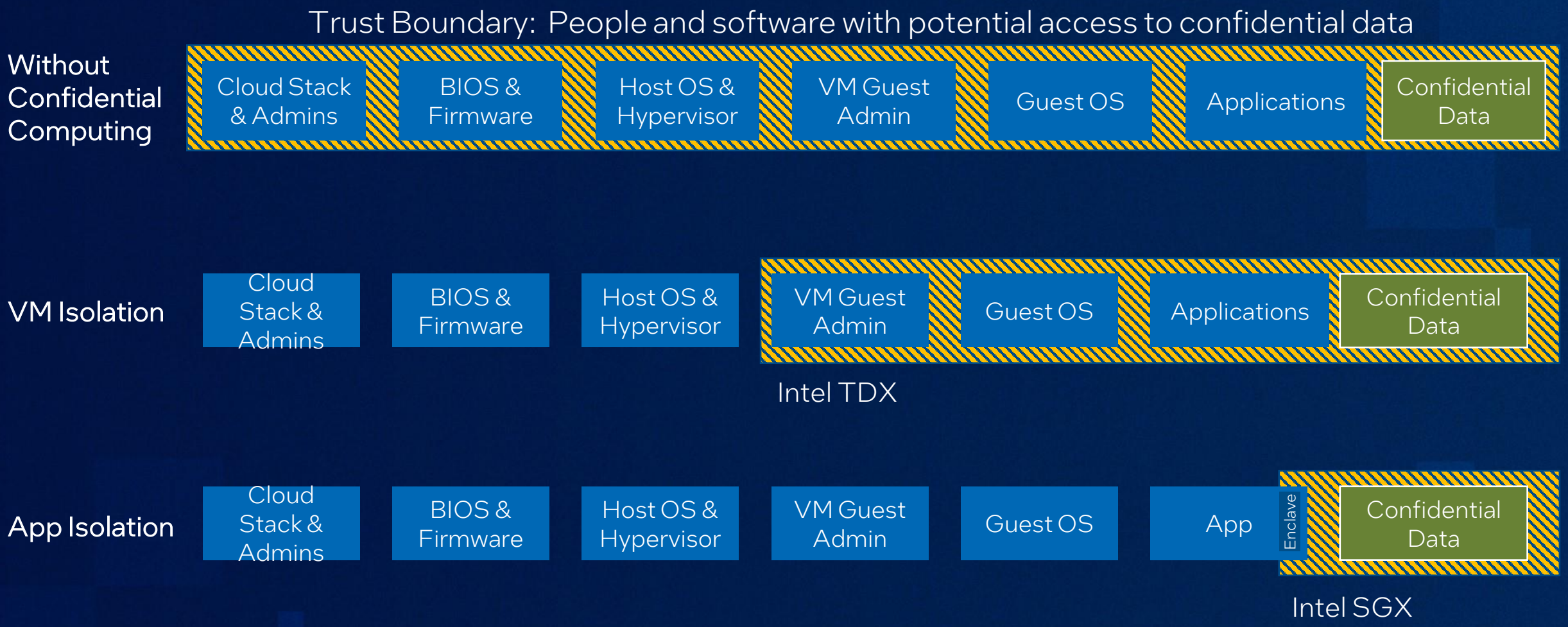
Trust Boundary: Software with access to Confidential Data

Intel® SGX: A Trusted Execution Environment for Protecting Date In-Use



- Data in-use is protected inside a hardware-enforced Trusted Execution Environment (TEE) called an “Enclave”
- Designed so software outside the enclave cannot access data inside it, even with escalated privileges
- Enclave configuration & Software load is verified with strong attestation

Trust Boundary: Smaller is Better



Real World Usages

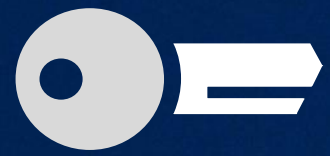
Trusted Multi-party Compute

Federated Learning

Privacy Preserving Analytics

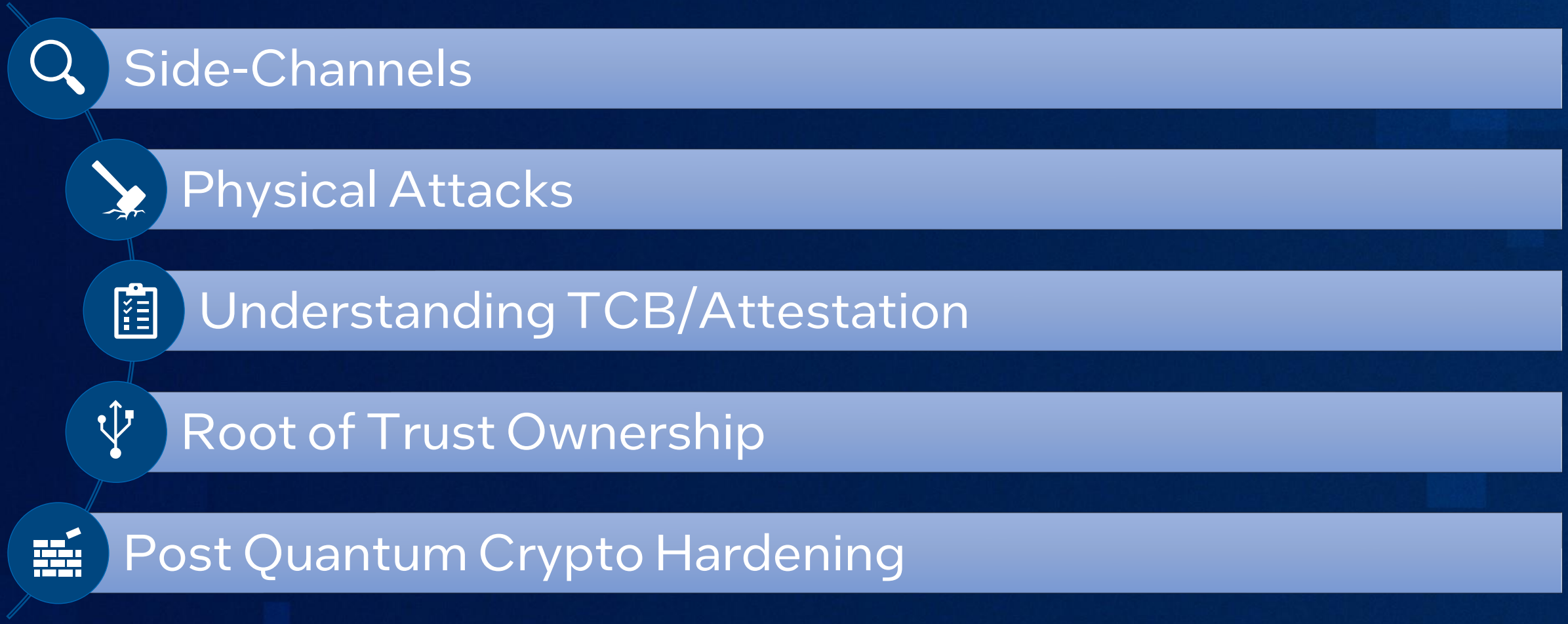
Blockchain

Cloud & Edge Infrastructure

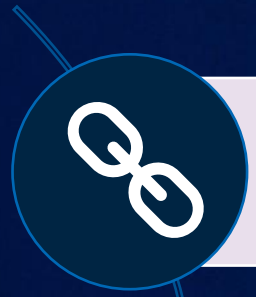


Key Management

Security Challenges



Attestation: Challenges in Today's CC Model



Linking infrastructure & attestation

Scaling attestation across vendors & geos

Complexity of home-grown attestation

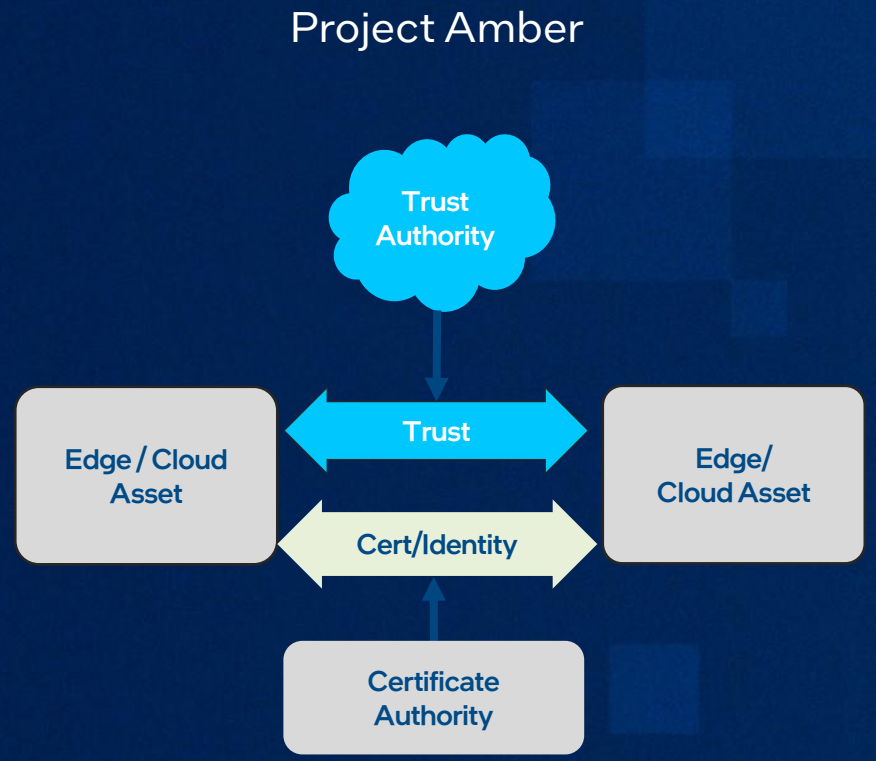
Expanding Confidential Computing Requires Better Attestation Solutions

What is Project Amber?

An Intel® service to remotely verify and assert trustworthiness of compute assets (TEEs, devices, Roots of Trust, etc.)

Enables Zero Trust Model for Confidential Computing

Operationally independent from the Cloud/Edge infrastructure provider that is hosting confidential compute customer workloads



Zero Trust: Extending Attestation Services
In Cloud Environments

Project Amber 1.0 Objectives:

- SaaS service w/ 99.9% uptime SLA
- Multi/Hybrid cloud & Edge Workload support
- Multi-TEE support
  Initially: Intel® Software Guard Extensions (Intel® SGX) and Intel® Trust Domain Extensions (Intel® TDX)
- Federated model for Geo-support
- Provable Integrity of Verification Process
- CSP agnostic & Multi-cloud deployment

Summary

- Confidential Computing (CC) is the biggest change to computer security in multiple decades.
- Confidential Computing enables data privacy & governance solutions.
- Ground truth of Trust in CC is via a process called Attestation.
- Expanding Confidential Computing requires better Attestation solutions.
- Project Amber is a new multi-cloud, multi-TEE SaaS for 3rd party attestation.
- Project Amber Pilot engagements are starting in Q4 2022, target launch in 2H 2023.

Notices & Disclaimers

Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com.

Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

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

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 Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.


intel