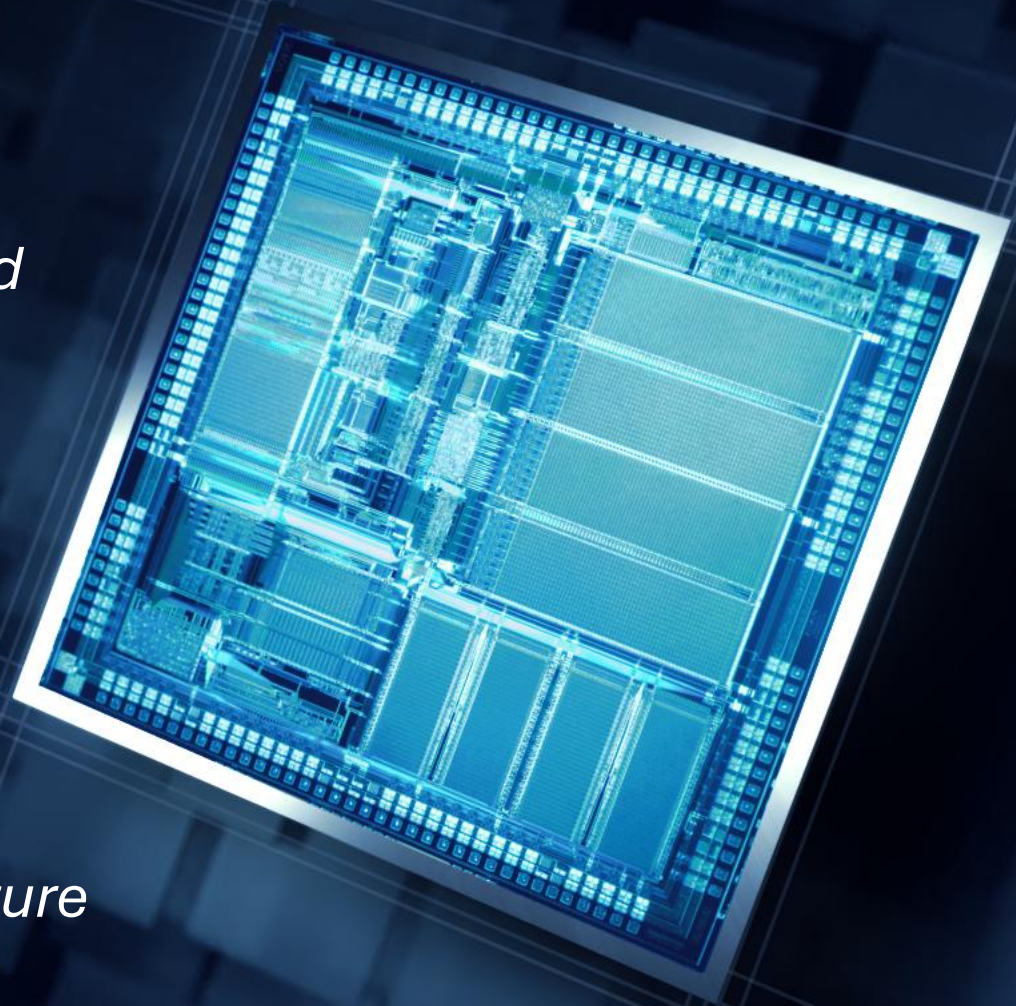
Azure Secure Hardware Architecture:

A Robust Security Foundation for Cloud Workloads

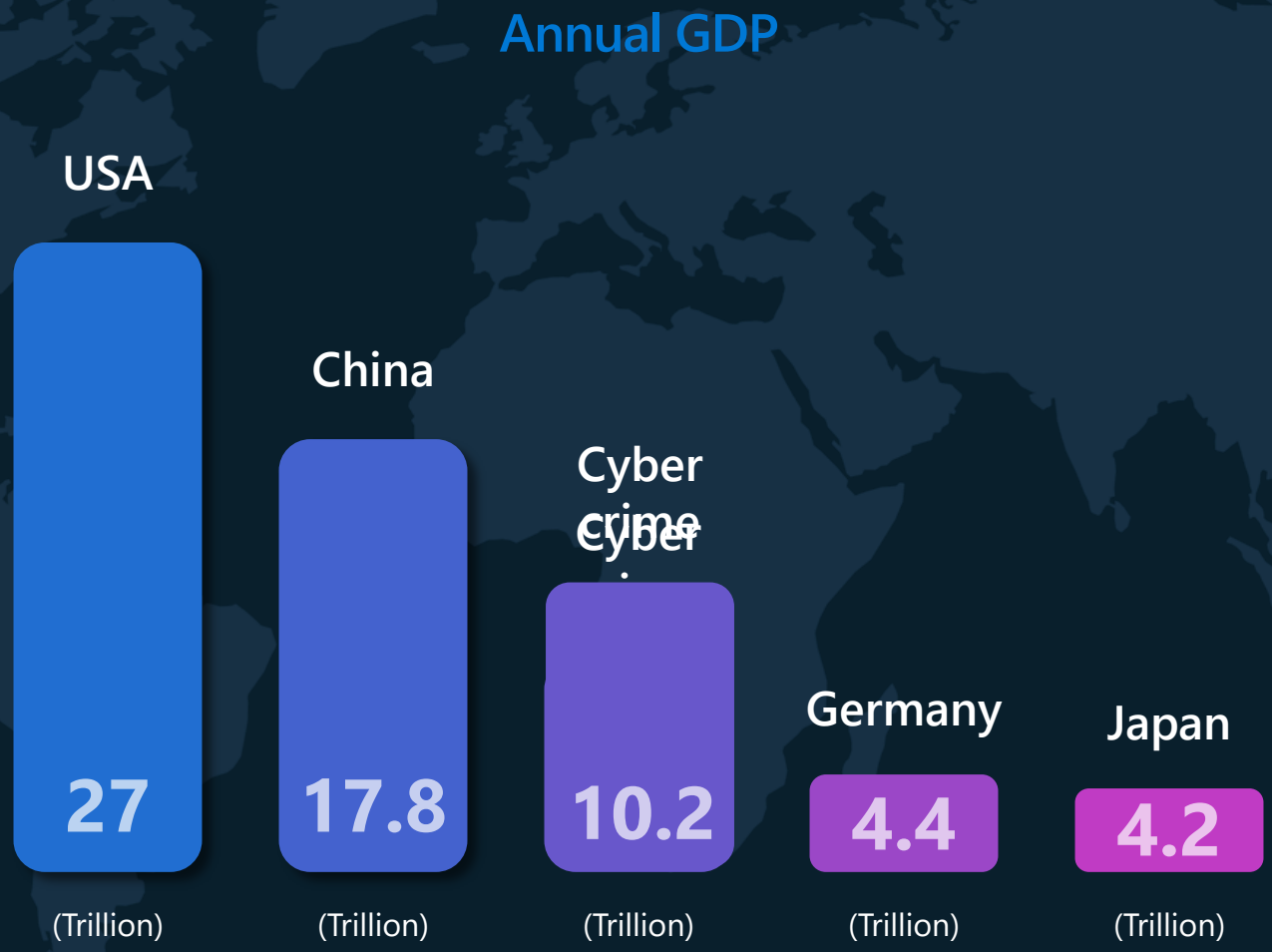


Bryan Kelly

Partner Architect

Azure Hardware Systems & Infrastructure

Cybercrime is the 3rd largest GDP



Source: Statistica

Azure: The World's Computer

70+ Azure regions

400+ Datacenters worldwide

275K+ Miles of fiber

190+ Network PoPs

Microsoft's unique vantage point
Global signal data and threat intelligence

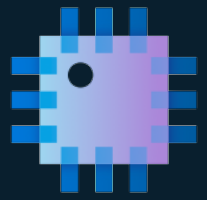
Monitoring 78 **trillion** daily security signals

34,000 dedicated security engineers

AI-powered detections and automated actions

Source: Microsoft Digital Defense Report

Microsoft's Secure Future Initiative (SFI)



Secure by Design

Secure by Default

Secure Operations

Continuous improvement

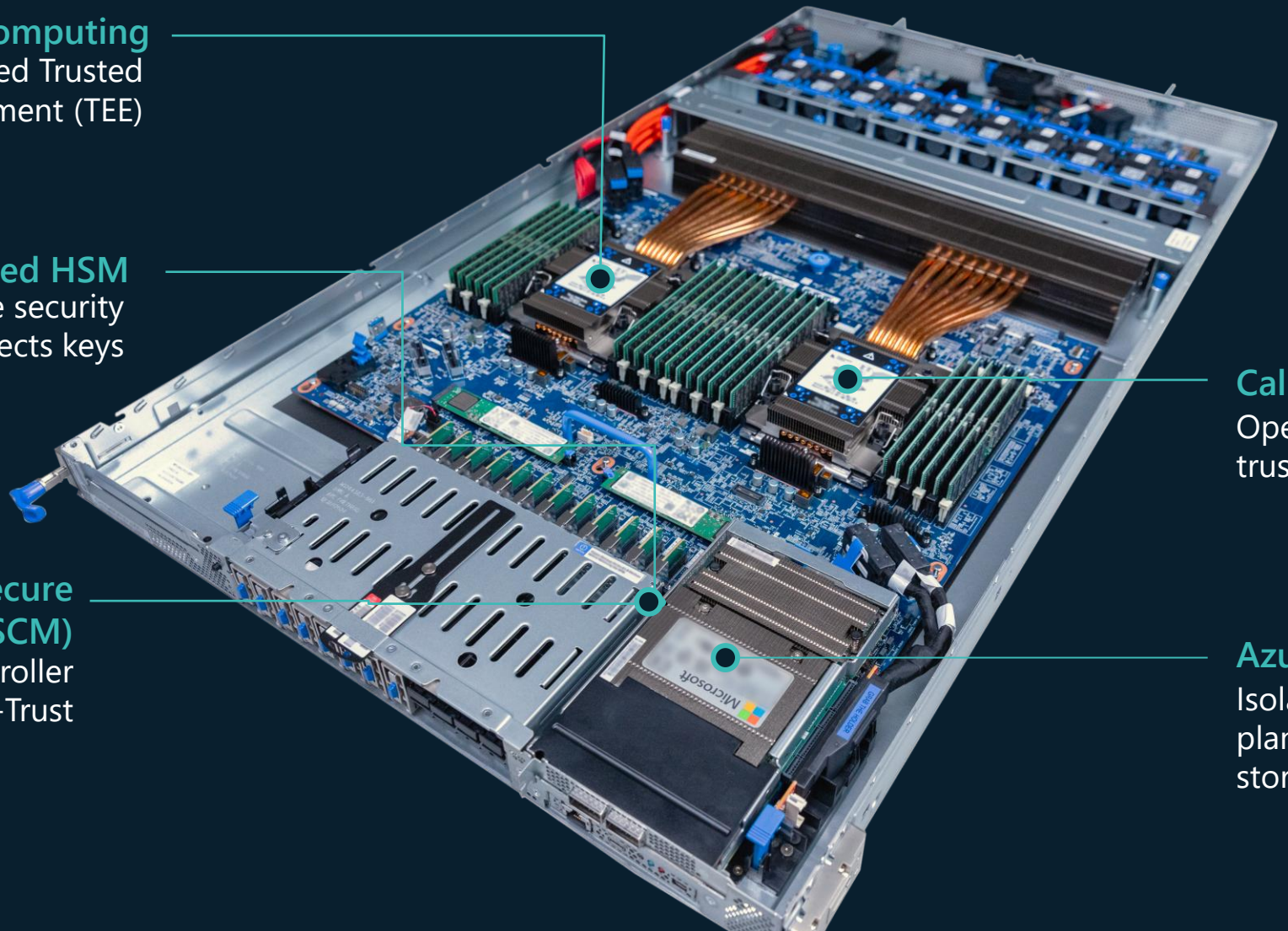
Paved path → Standards

Secure by Design - System Architecture

Confidential Computing
Hardware-based Trusted Execution Environment (TEE)

Integrated HSM
Hardened hardware security module protects keys

Datacenter Secure Control Module (DC-SCM)
Secure Management Controller & Platform Root-of-Trust



Caliptra
Open-source silicon for trustworthy computing

Azure Boost
Isolates control and data plane, network and storage offload

Microsoft’s Secure Future Initiative (SFI)

Blog home / News

Search the blog

News · 7 min read

Security above all else—expanding Microsoft’s Secure Future Initiative

By Charlie Bell, Executive Vice President, Microsoft Security

1. Protect identities and secrets

Reduce the risk of unauthorized access by implementing and enforcing best-in-class standards across all identity and secrets infrastructure, and user and application authentication and authorization. As part of this, we are taking the following actions:

- Protect identity infrastructure signing and platform keys with rapid and automatic rotation with hardware storage and protection (for example, hardware security module (HSM) and confidential compute).
- Strengthen identity standards and drive their adoption through use of standard SDKs across 100% of applications.

What are Hardware Security Modules (HSM)

PCIe Card

Server & Rack Mount Solutions

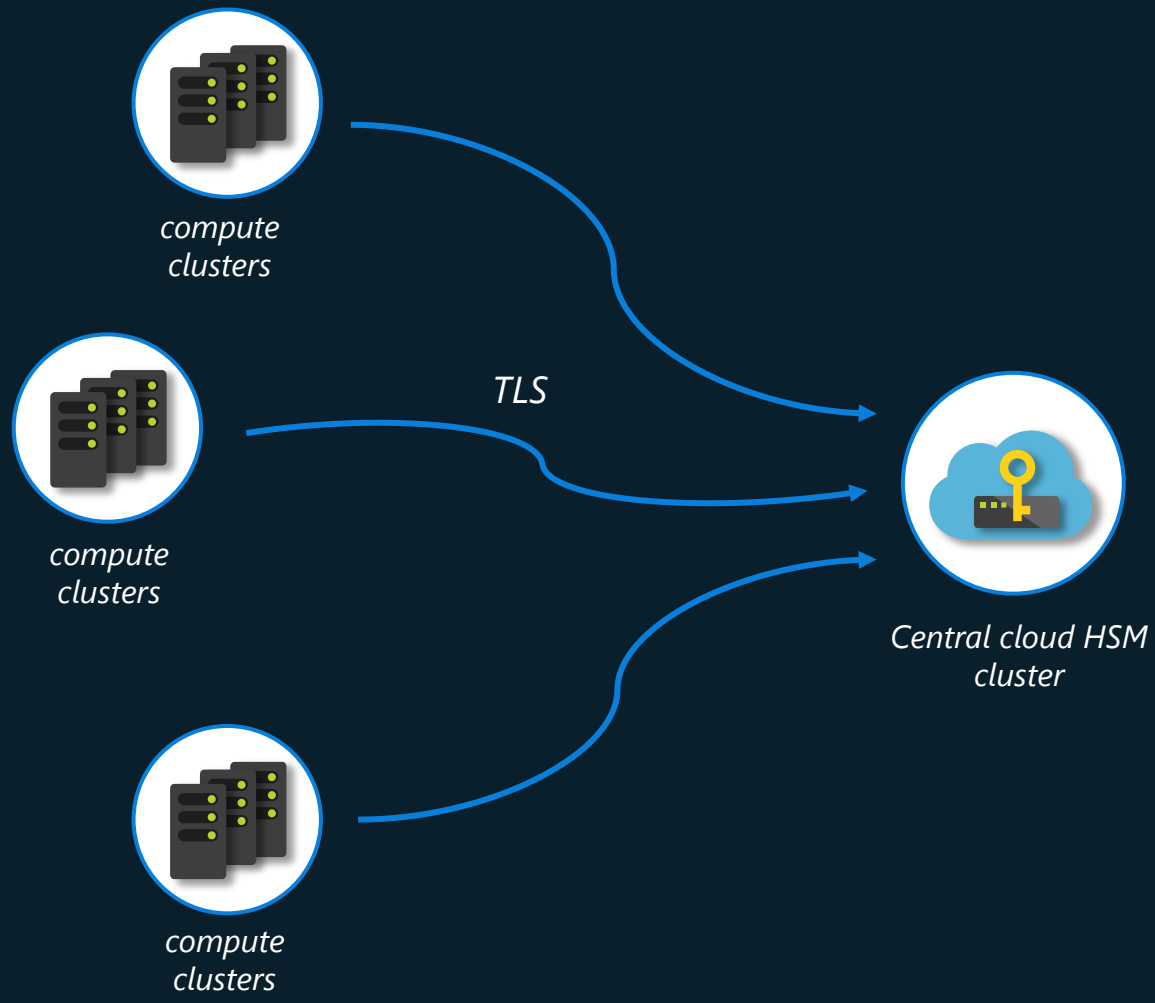
Typical HSM Architecture

Deployed independently

Scaling challenges

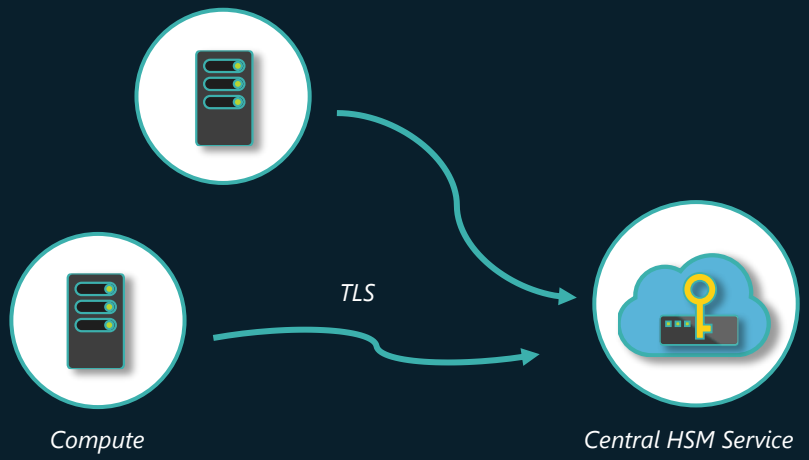
Remotely accessed by servers

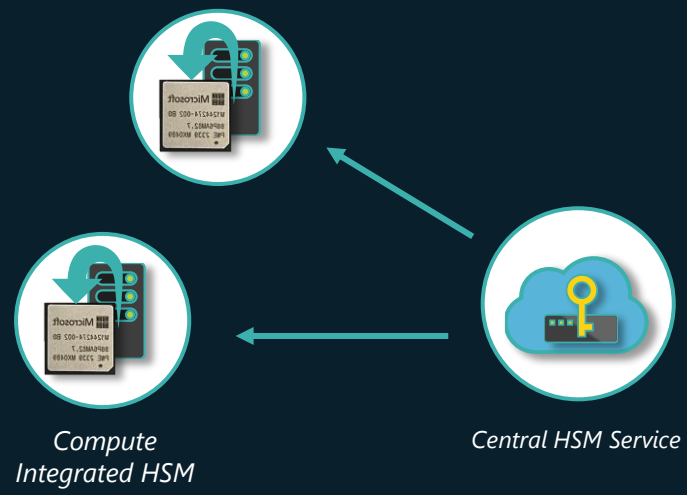
Impractical for some workloads



Evolving from Central to Integrated

Integrated HSM - Key Cache





2000's

1U, Rack-Mount - Central HSM Clusters

2025 (Azure)

Azure Integrated HSM, Cloud-Optimized, Integrated into Every Server.

Azure Integrated HSM

Microsoft's in-house security chip

Industry leading Key Protection

Isolates cryptographic keys in dedicated vault	Designed to meet HSM security standards for key protection (FIPS 140-3 Level 3)	Deployed in all new Azure servers in 2025

aka.ms/AzureIntegratedHSM

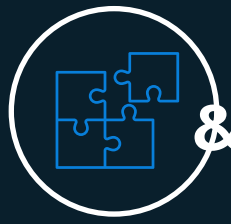
Designing for scale

Performance

vs

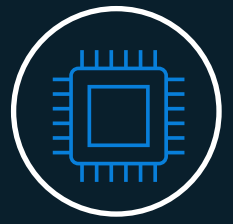
Power

&



Area

&



Packaging

Dedicated Circuit

Programmability

Azure Integrated HSM - ASIC

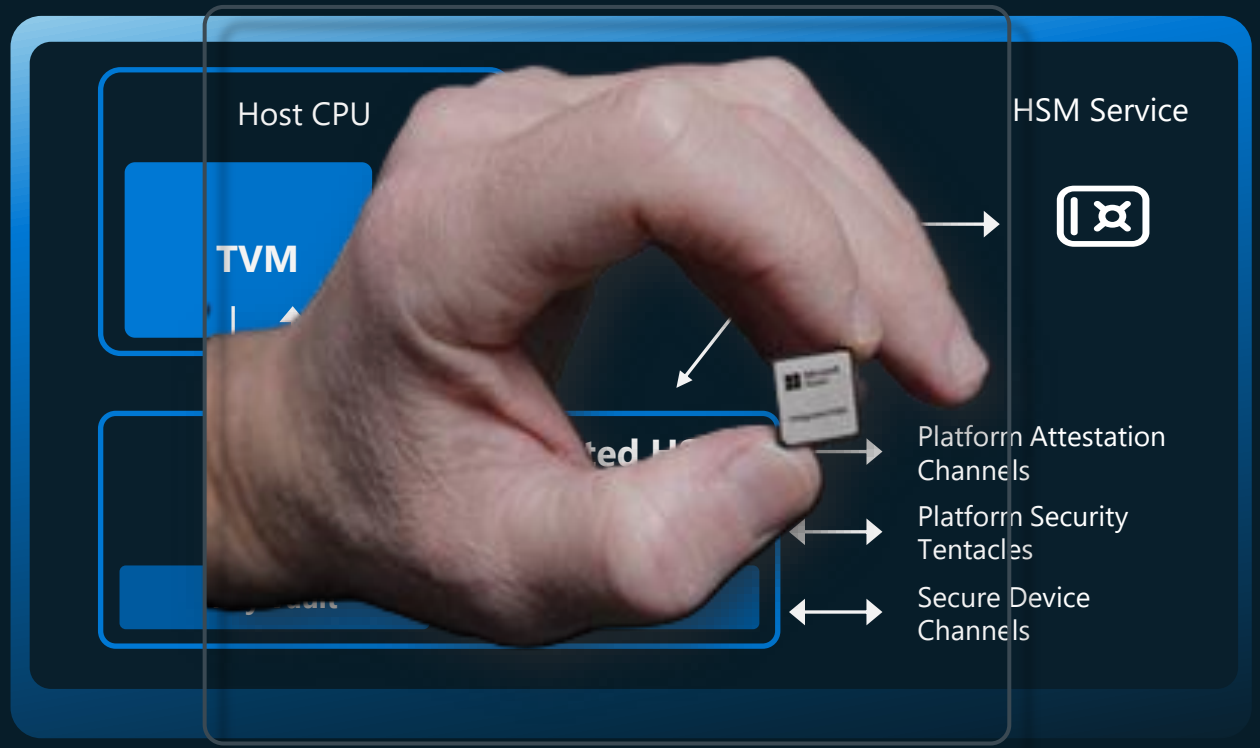
HSM optimized hardware

- Hardware crypto acceleration for AES and PKE operations
- Realtime cores for control logic.

Hardened interfaces and security standards

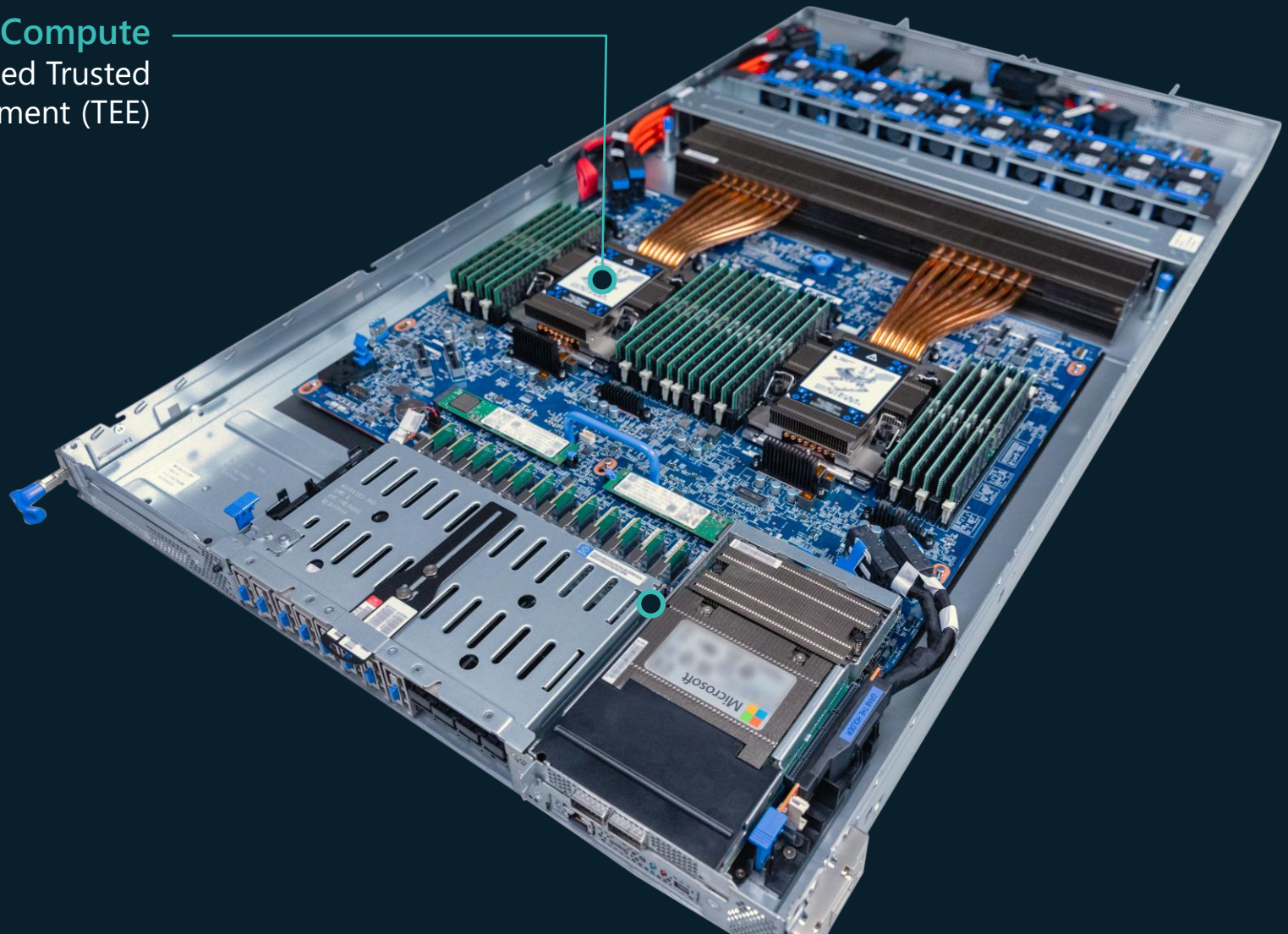
- TEE Interface Security Protocol (TDISP)
- Federal Information Processing Standards (FIPS) 140-3 Level 3

Intrusion detection, tamper detection



Secure by Default – Hardware Isolated Services

Confidential Compute
Hardware-based Trusted Execution Environment (TEE)



Azure confidential computing

Services

Confidential containers on Azure Red Hat OpenShift
Public preview

SQL always encrypted with secure enclaves
Generally available

Managed HSM
Generally available

Mic
Azu
Ger

ing

Containers

Intel SC
nodes
Genera

Infra

AMD

DCasv
AMD S
Genera

DCasv
Gated p

Azure Integrated HSM
In Deployment

AZURE CONFIDENTIAL COMPUTING BLOG 4 MIN READ

Announcing: Microsoft moves $25 Billion in credit card transactions to Azure confidential computing

AZURE CONFIDENTIAL COMPUTING BLOG 3 MIN READ

Confidential agentic AI on Azure helps ServiceNow respond to sales commission inquiries in seconds

Krishnaprasad_Hande MICROSOFT
Jun 17, 2025

odels, solve previously
AI agents leveraging
ands of commission
onse times while

AZURE CONFIDENTIAL COMPUTING BLOG 4 MIN READ

Announcing: Microsoft transforms Licensing with Cloud Security and Confidential Computing

Sumithra_Shekhar MICROSOFT
Jul 07, 2025

Enhance Confidentiality with Secure, Compliant, and Cost-Effective High-Scale Cryptographic Solutions in Public Azure

Microsoft is proud to announce the successful migration of its Windows Licensing Service to Azure, leveraging cutting-edge Confidential Computing and Managed Hardware Security Modules (mHSM) technology. This marks a significant breakthrough in the cloud adoption journey for workloads operating in highly secure environments, reshaping the way Microsoft's licensing services operate securely at scale.

Confidential Computing

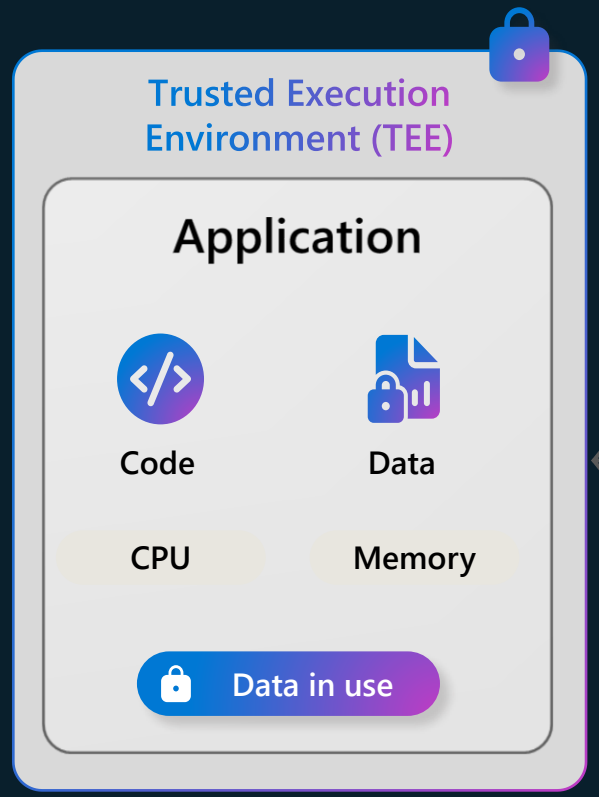
Protect “data in use”

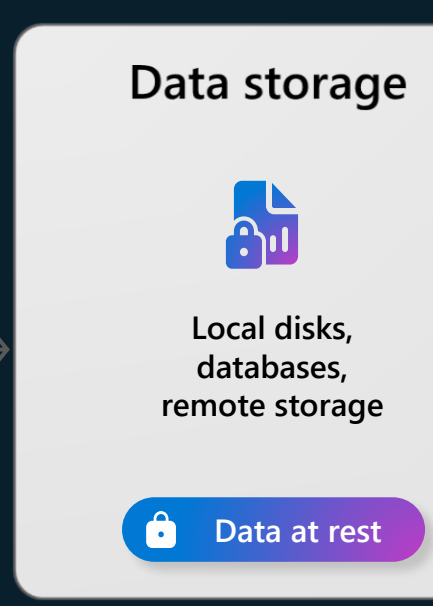
Data Protection

Data at rest
Encrypt data on disk

Data in transit
Encrypt data on the network

Data in use
Encrypt/Protect data that is in use, while in RAM and during computation





Hardware Trust Anchor

Open Source - Silicon Root of Trust

Caliptra 2.0

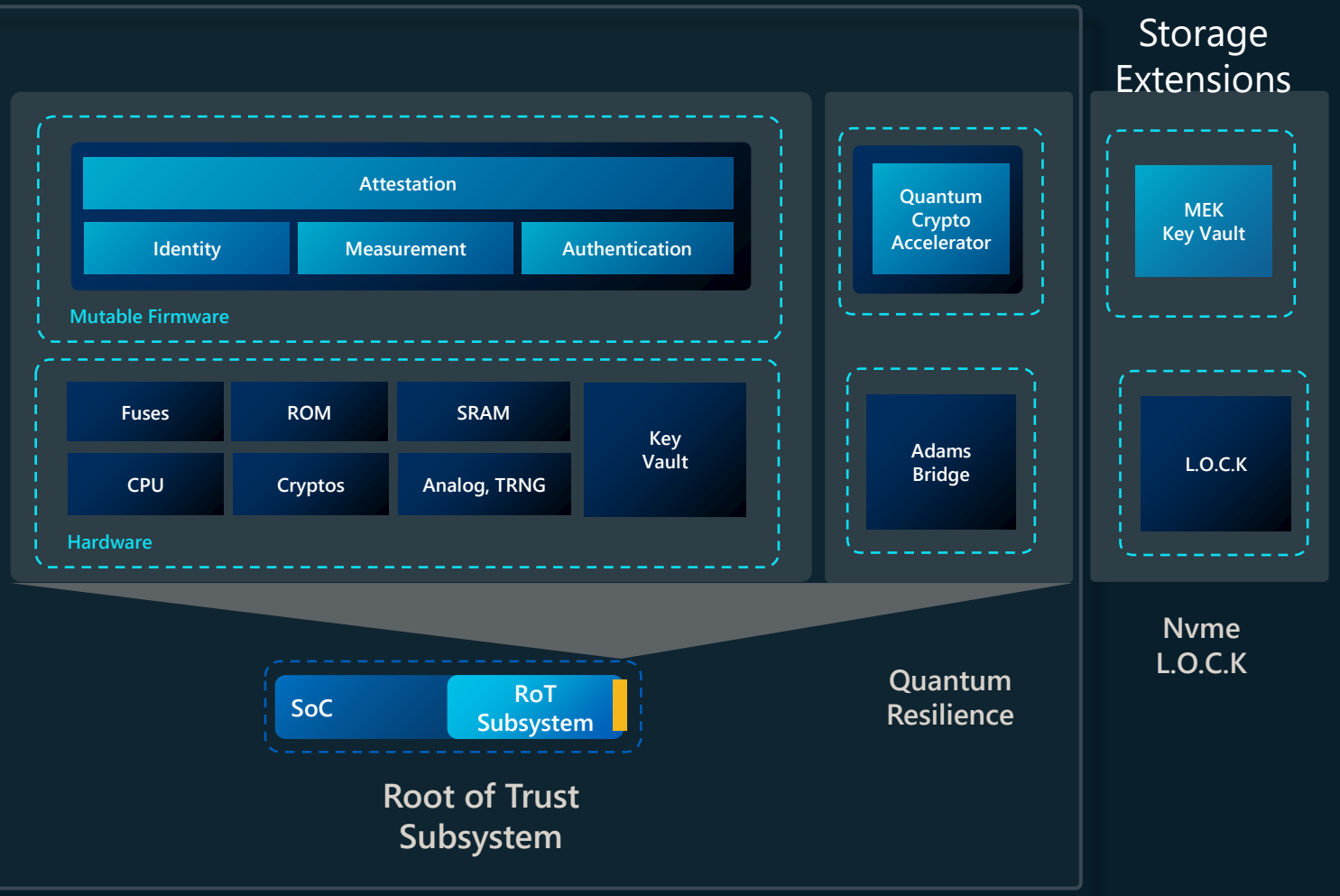
Transparency of complete Root of Trust – **Security Subsystem**

Adams Bridge

Complete open-source silicon quantum resilient crypto accelerator

OCP L.O.C.K

Nvme Key Management block, secures keys for storage devices



Caliptra by numbers

- Hardware cryptos take up ~62% of the area
- Caliptra SRAM = 521KB (FW) + 64KB (ABR)

Adam's bridge	521,368
ECC engine	270,156
RISC-V processor	117,796
Key vault	84,576
HMAC engine	73,264
SOC interfaces	116,899
AES engine	61,019
Entropy source distributer	36,387
RNG digital side	31,396
SHA512 engine	22,200
De-obfuscation engine	15,472
SHA256 engine	7,918
MCU processor	131,826
OTP controller	58,157
I3C recovery interface	48,472
MCI	36,597
Life cycle controller	3401
ROM interface	990
Total Gate Count	**1,640,145**

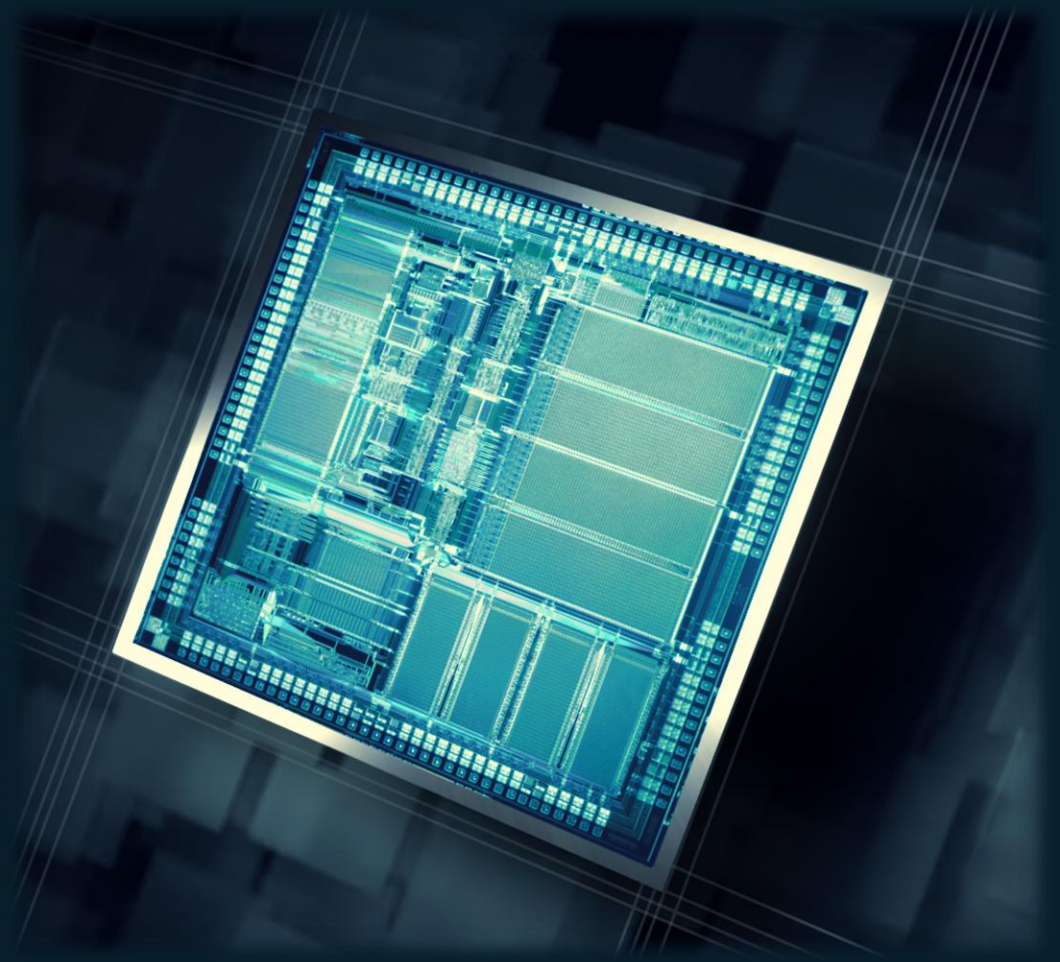
Caliptra Verification

Release Gates:

- Verification plans executed.
- CDC, Lint, RDC, Synthesis runs are clean.
- Release label created.
- Tests, Test benches, coverage reports all open.

	Type	Coverage	Hit	Total
👁	line	98.9%	6127	6193
👁	branch	99.6%	7118	7145
👁	cond	98.7%	4618	4677
👁	toggle	99.4%	85356	85881

Why open-source Silicon?



Transparency: open-source allows greater security transparency.

Consistency: facilities Secure by Default and Secure operations.

Standard: cryptography is heavily standardized.

Fortification: building layers of defense. ~diversification.

How to get involved

Caliptra

https://Caliptra.io

CHIPS ALLIANCE

https://www.chipsalliance.org/workgroups

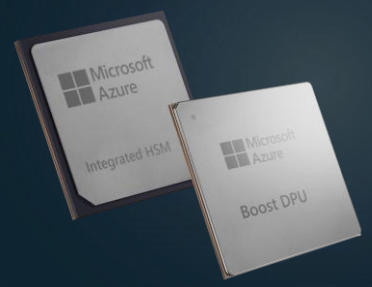
OPEN Compute Project

https://www.opencompute.org/projects/security

Microsoft's SFI – Hardware Infrastructure

Secure by Design

Purpose built Secure Silicon



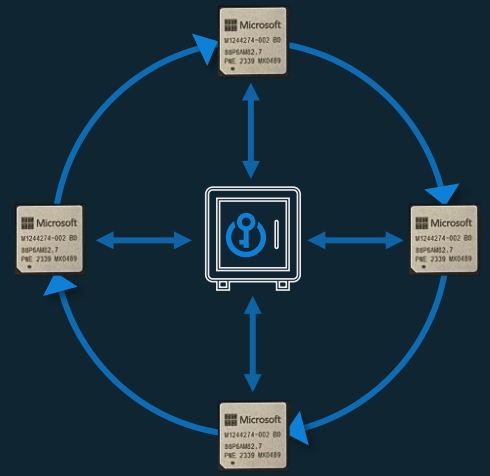
Secure by Default

Azure Confidential Cloud

- Data at rest
- Data in transit
- Data in use

Secure Operations

Secure Operating Model



Thank you

For more information visit: TODO