Microsoft

Attested, Transparent, Sovereign: The Evolution of Confidential Computing

Mark Russinovich
CTO, Deputy CISO and Technical Fellow,
Microsoft Azure

@markrussinovich
@mrussinovich

Microsoft Azure Confidential Computing

Services

- Confidential containers on Azure Red Hat OpenShift — Generally Available
- SQL always encrypted with secure enclaves — Generally available
- Azure Virtual Desktop on confidential VMs — Generally available
- Azure Confidential Databricks — Generally available
- Azure Database for PostgreSQL — Generally available
- Azure Batch on confidential VMs — Generally available
- Managed HSM — Generally available
- Microsoft Azure Attestation — Generally available
- Azure Confidential Ledger — Generally available
- Azure Container Apps — Generally available
- Azure AI Search — Generally available
- Azure Data Explorer — Public preview
- Azure Event Hub — Private preview
- Azure Service Bus — Private preview
- Azure Event Grid — Private preview
- Confidential inferencing with Azure Open AI Whisper — Preview
- Azure Confidential Clean Rooms — Preview

Note: Regional availability will depend on availability of ACC SKUs

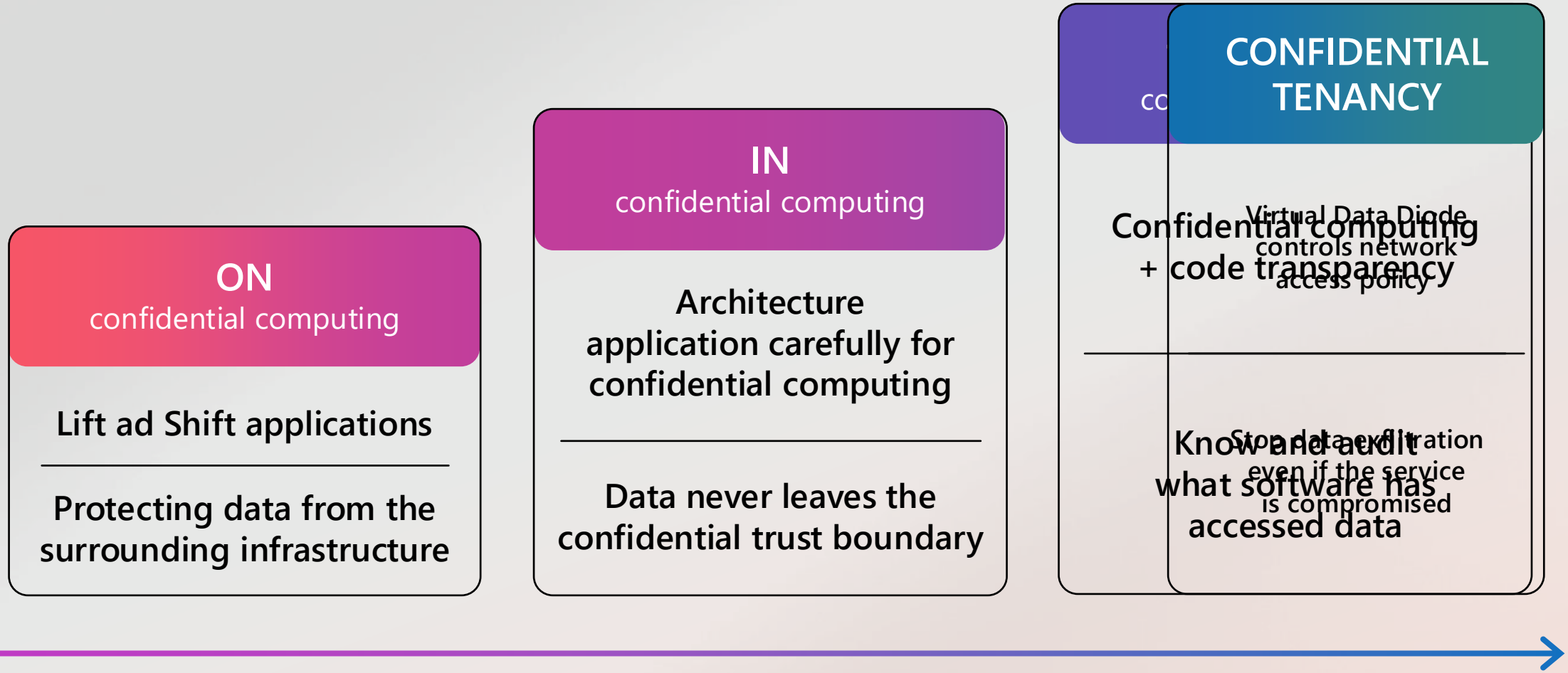
Containers

- Confidential VM AKS worker nodes — Generally available
- Confidential containers on ACI — Generally available
- Confidential containers on AKS — Public preview

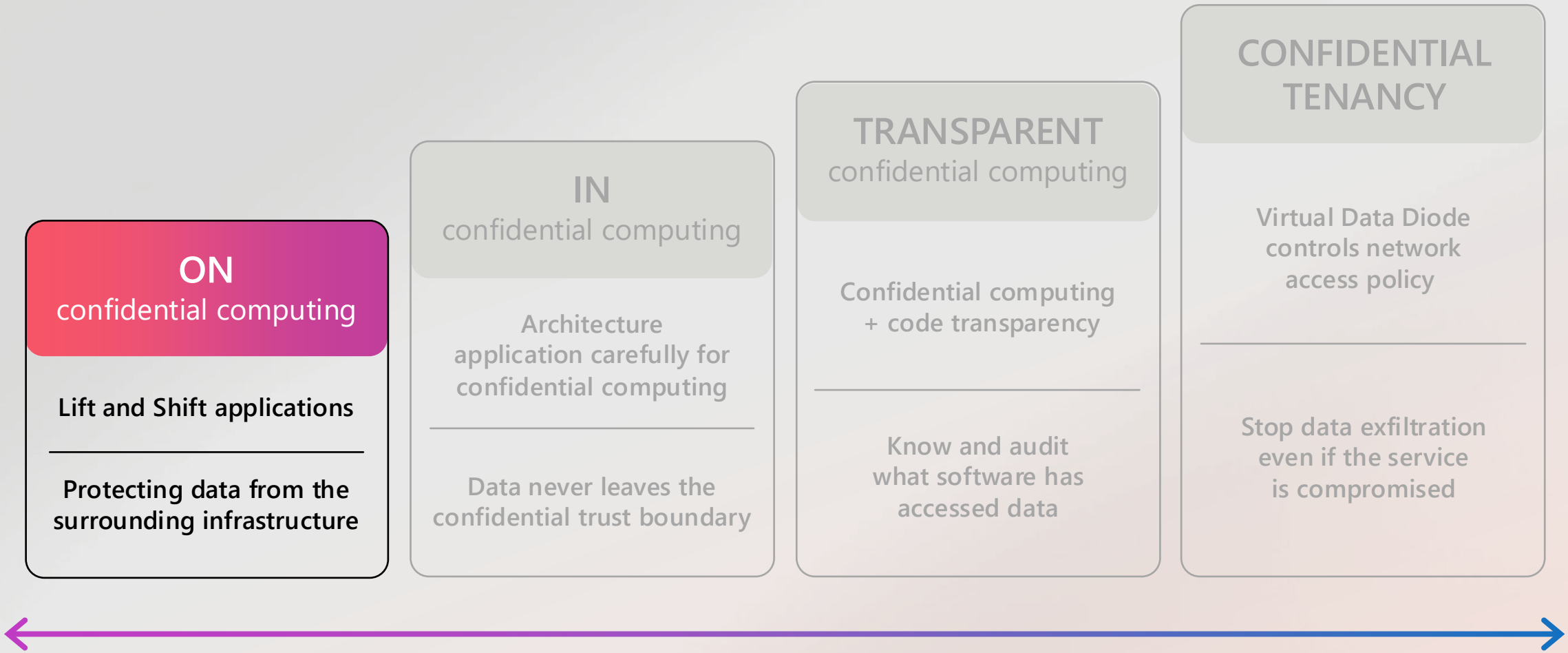
Infrastructure

- AMD — DCasv5 & ECasv5 DCasv6 & ECasv6 AMD SEV-SNP CVMs — Generally available
- intel — DCesv6 & ECesv6 Intel TDX CVMs — Generally available
- NVIDIA — NCCH100v5 VMs NVIDIA GPUs — Generally available
- Azure Integrated HSM — Generally Available

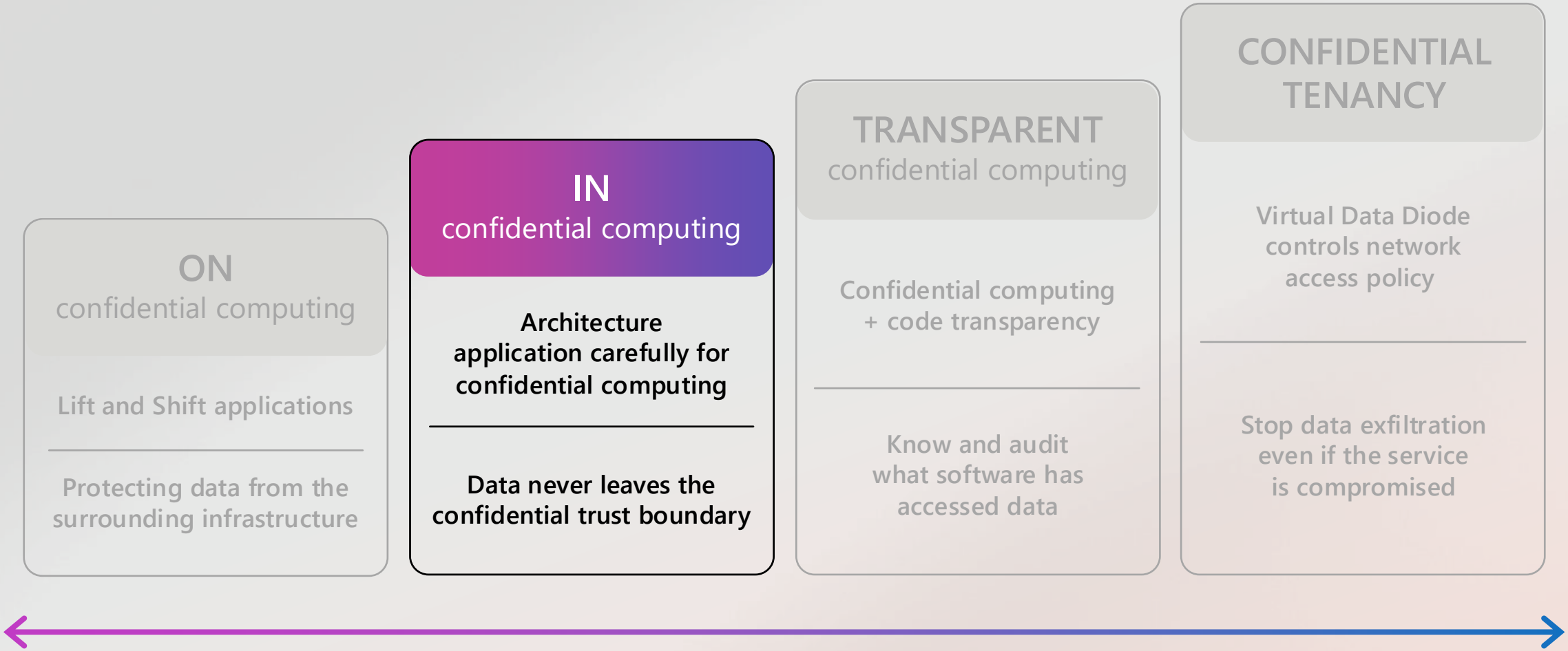
Confidential computing guarantees



Confidential computing guarantees



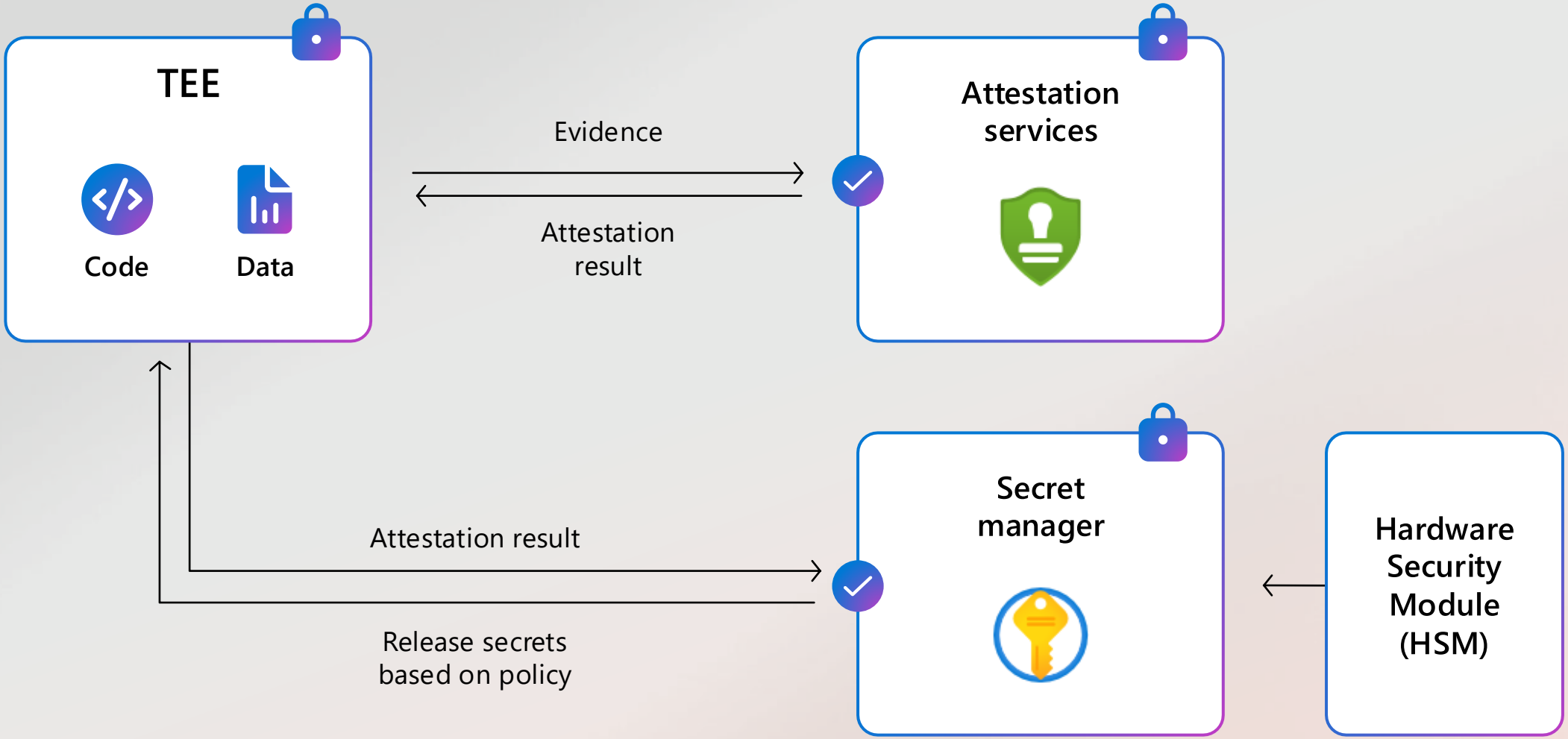
Confidential computing guarantees



The cloud confidential trust boundary

Confidential Trust Boundary (CTB) Root of Trust

Attestation and secure key management



Protecting signing keys

News · April 21, 2025 · 6 min read

Securing our future: April 2025 progress report on Microsoft's Secure Future Initiative ›

By Charlie Bell, Executive Vice President, Micros

To better protect signing keys, in September 2024 we announced that we have moved Entra ID and Microsoft Account (MSA) access token signing keys to hardware-based security modules (HSMs) and virtualization-based security in Windows, with automatic rotation. Since then, we've applied new defense-in-depth protections in response to our Red Team research and assessments, migrated the MSA signing service to Azure confidential VMs, and are migrating Entra ID signing service to the same. Each of these improvements help mitigate the attack vectors that we suspect the actor used in the 2023 Storm-0558 attack on Microsoft.

AZURE CONFIDENTIAL COMPUTING BLOG 4 MIN READ

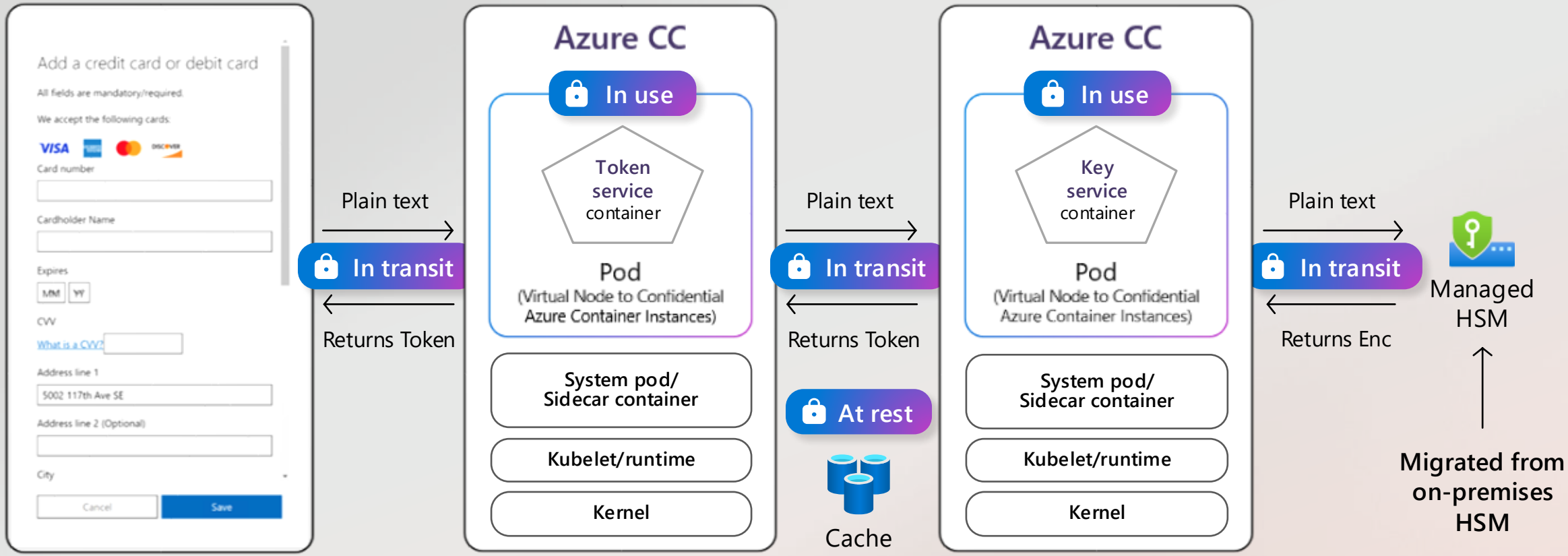
Announcing: Microsoft moves $25 Billion in credit card transactions to Azure confidential computing

Brad_Turner MICROSOFT

Nov 15, 2023

Microsoft is proud to showcase that customers in the financial sector can rely on public Azure to add *confidentiality* to provide secure and compliant payment solutions that meet or exceed industry standards.

Microsoft Payment services



Customer adds a credit card

AZURE CONFIDENTIAL COMPUTING BLOG 4 MIN READ

Announcing: Microsoft transforms Licensing with Cloud Security and Confidential Computing

Sumithra_Shekhar MICROSOFT

Jul 07, 2025

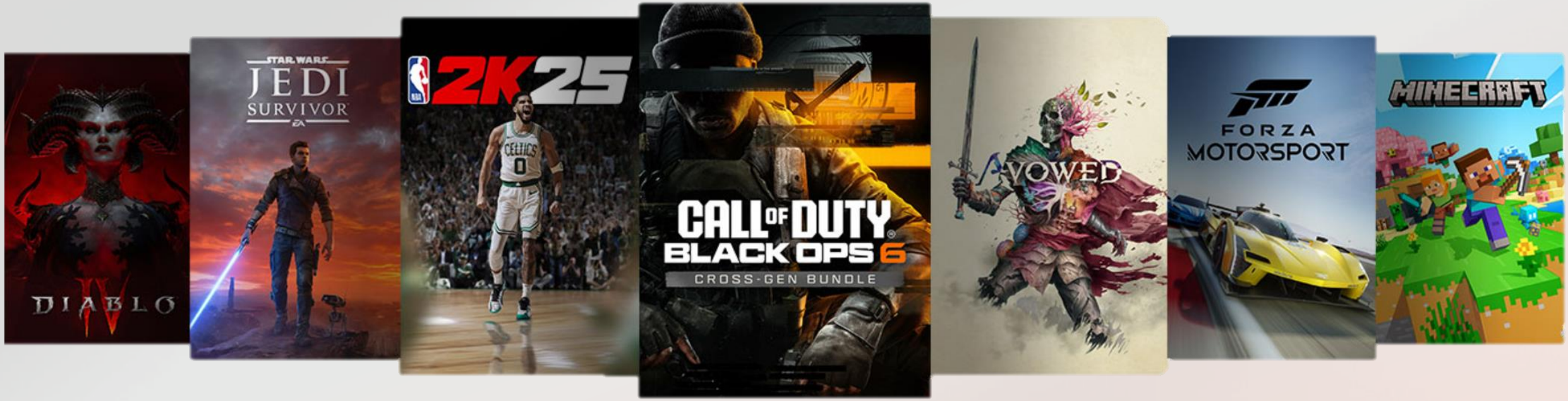
Enhance Confidentiality with Secure, Compliant, and Cost-Effective High-Scale Cryptographic Solutions in Public Azure

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.

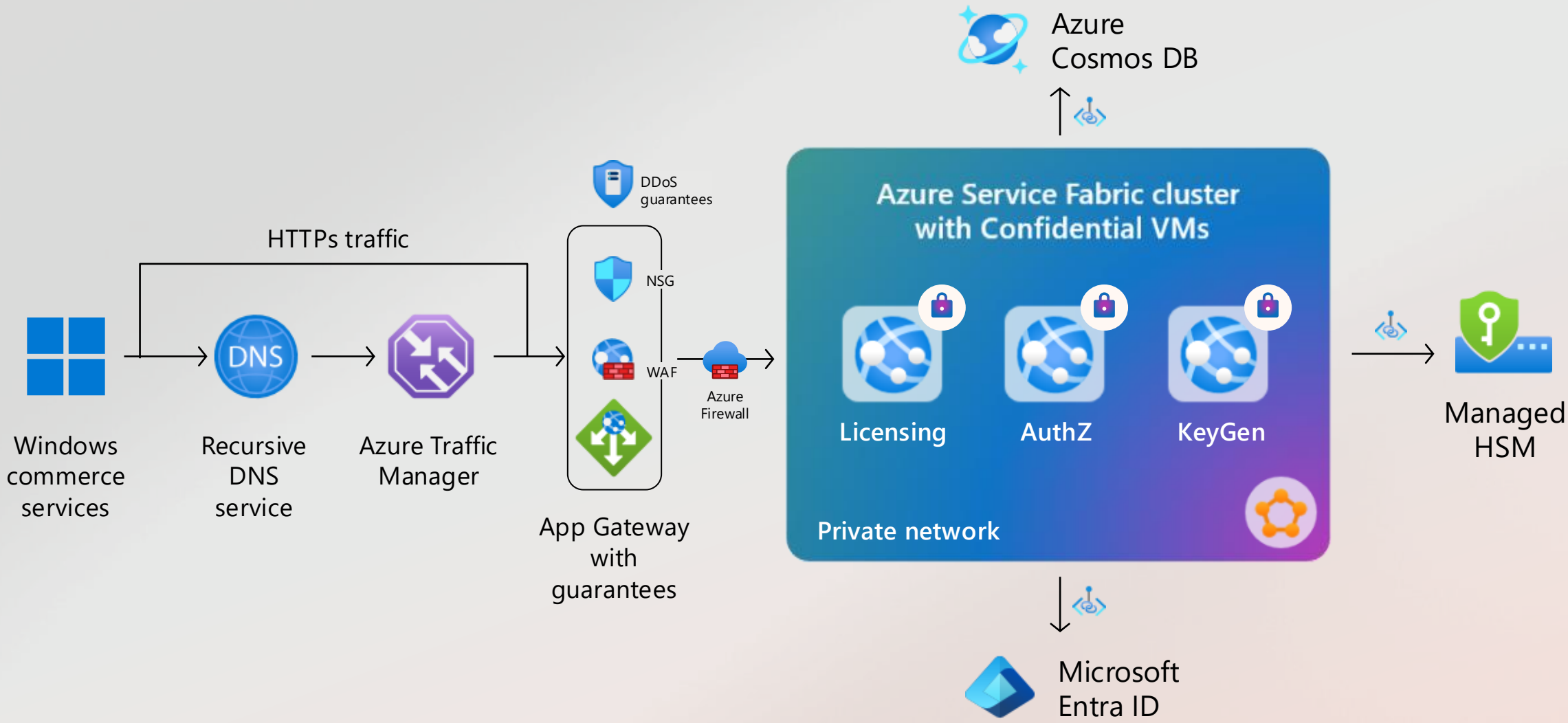
But what did it really take to move one of Microsoft's most security-critical services to the cloud? Read on to uncover how the team enabled the largest cryptographic workload ever run in Azure—built on high-assurance infrastructure designed for secure, high-throughput operations.

Migrating highly secure workloads is made possible with the help of Confidential computing and Managed HSM empowering organizations handling highly secure, high-throughput, and confidential workloads to operate with greater confidence, flexibility, and value.

XKMS Token Signing Service
100% on confidential computing



Microsoft Licensing Service



Engineering secure passkey sync in Microsoft Password Manager

Written By

Kamaraj Gandhirajan

published

April 22, 2026

Passkeys are designed to repl
and secure. With Microsoft Pa
their Microsoft account.

Syncing passkeys enables a se
signed in. Instead of being tie
to leverage device-based auth

However, enabling this experi
must be protected during cre

In this post, we'll walk throug
Manager.

Confidential compute for passkey operations

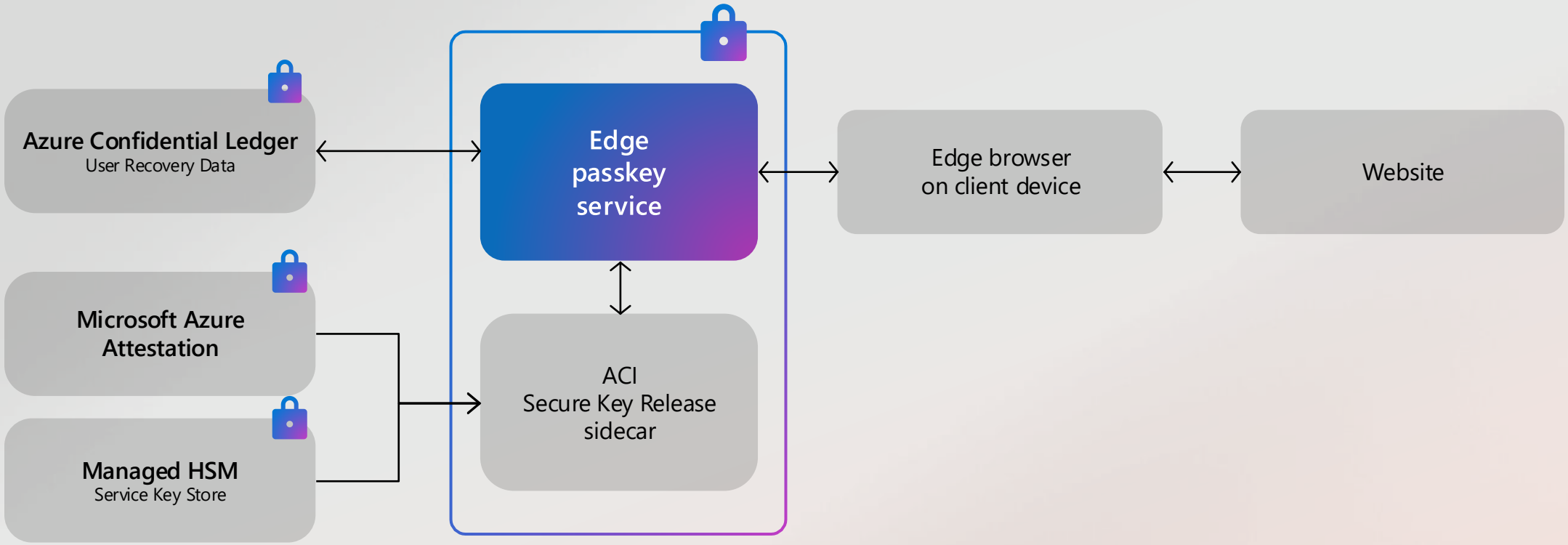
Sensitive passkey operations, including credential creation, assertion, and recovery validation, execute inside the Azure confidential computing environments backed by hardware isolation.

This ensures that:

- Cryptographic material is processed inside protected memory.
- The host environment cannot inspect sensitive cryptographic material (such as passkeys and encryption keys) while in use.
- Only attested service code can access protected encryption keys.

By strictly controlling where passkey material can be decrypted and used, we ensure that sensitive cryptographic material remains protected within trusted execution boundaries, while strengthening operational integrity. Access to these operations is further gated by user verification using platform authenticators (for example, Windows Hello or device biometrics), with device-bound cryptographic keys used to authorize passkey operations.

Edge passkey service



AZURE CONFIDENTIAL COMPUTING BLOG 4 MIN READ

Preview of multiparty analytics with Azure Confidential Clean Rooms

Deepak_JV MICROSOFT
Jun 02, 2026

Securely collaborate on sensitive datasets across organizations with Spark SQL big-data analytics inside a verifiable Trusted Execution Environment.

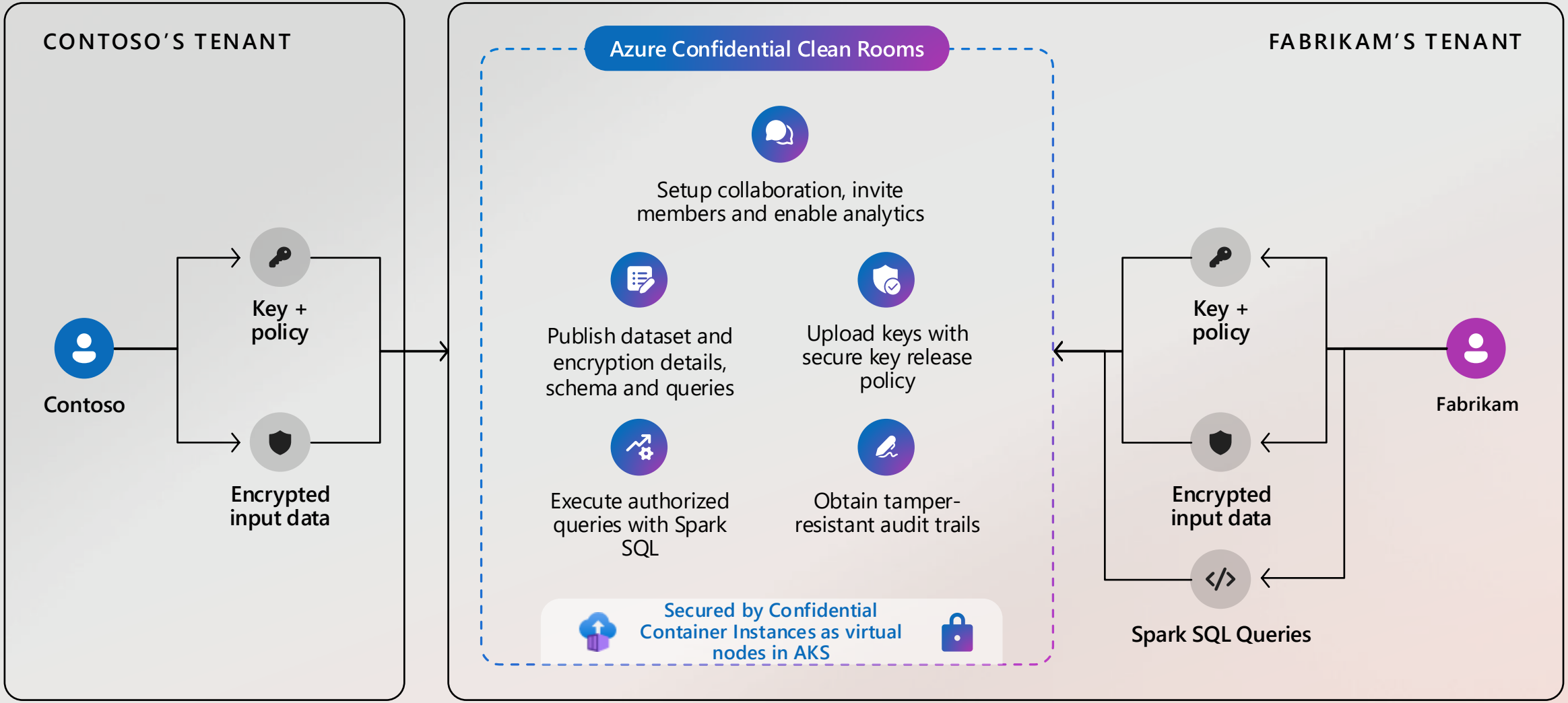
Today, we are excited to announce the preview of multiparty analytics feature of **Azure Confidential Clean Rooms**, a **fully managed service** that allows customers and their partners to securely analyze privacy-sensitive datasets from multiple parties. It uses **confidential compute enabled Apache Spark-based big-data analytics (Spark SQL)** which helps protect their raw data from other collaborators and from the Azure operator by performing computations in a Trusted Execution Environment (TEE). Privacy-sensitive datasets include personally identifiable information (PII), protected health information (PHI) and cryptographic secrets.

Organizations across industries are increasingly looking to supplement their data with data from business partners, to build a complete view of their business. For example, brands, publishers, and their partners need to collaborate using datasets containing Intellectual Property (IP) to improve the relevance of their campaigns. Confidential data clean rooms help solve this challenge by enabling organizations to share and analyze granular datasets in a secure environment that helps prevent raw data exfiltration—protecting intellectual property, preserving customer privacy, and addressing concerns around regulatory compliance.

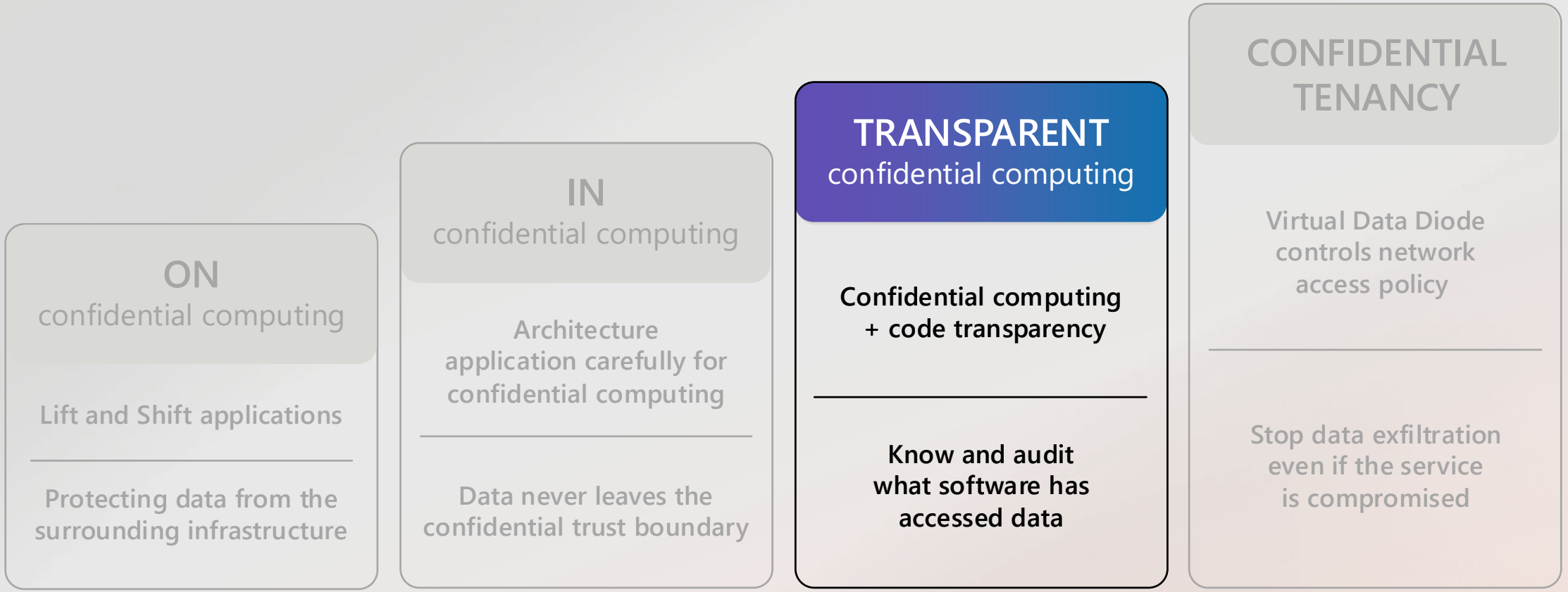
You can sign up for the preview here

Preview

Multiparty Analytics with Azure Confidential Clean Rooms

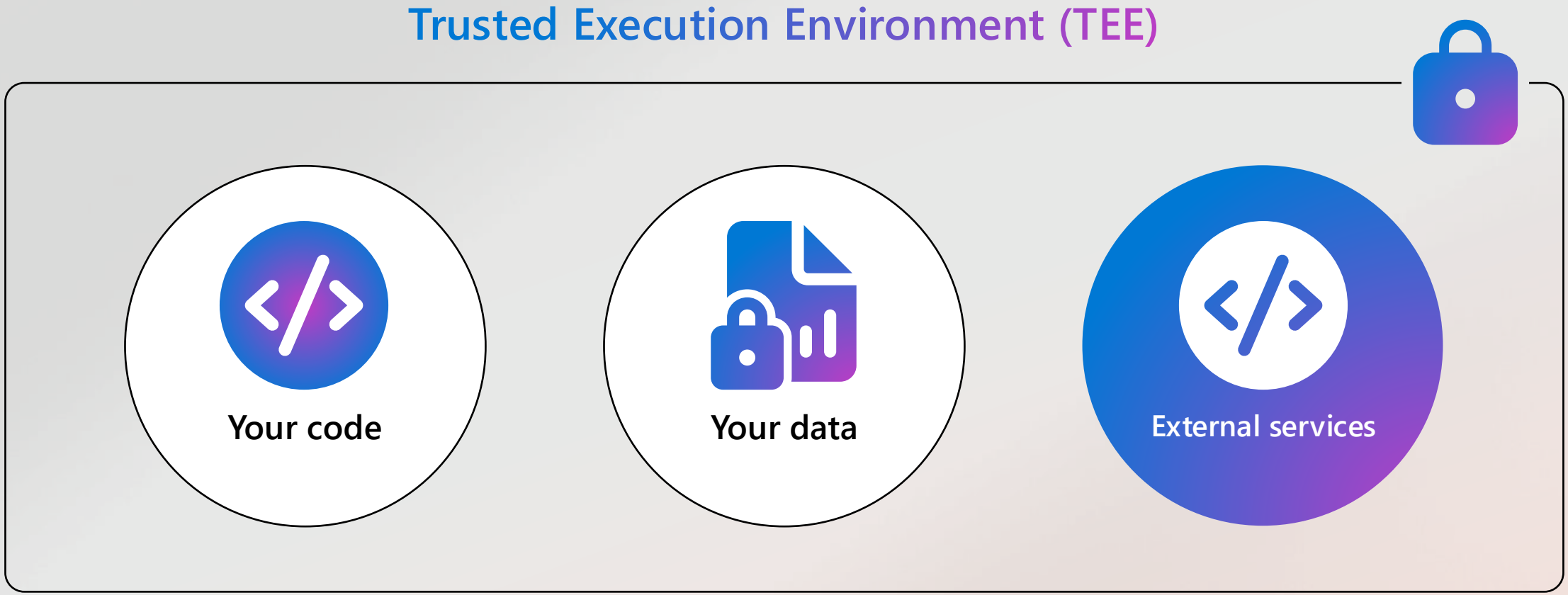


Confidential computing guarantees



The cloud confidential trust boundary

The cloud confidential trust boundary



acmqueue

Current Issue Past Issues Topics

September 7, 2023

Volume 21, issue 4

PDF

Why Should I Trust Your Code?

Confidential computing enables users to authenticate code running in TEEs, but users also need evidence this code is trustworthy.

Antoine Delignat-Lavaud, Cédric Fournet, Kapil Vaswani, Sylvan Clebsch, Maik Riechert, Manuel Costa, Mark Russinovich

MICROSOFT SECURITY COMMUNITY BLOG 4 MIN READ

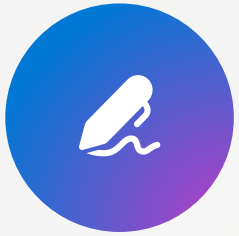
Microsoft Leads a New Era of Software Supply Chain Transparency

ShubhraS MICROSOFT
Jun 15, 2026

Microsoft has launched the general availability of Microsoft's Signing Transparency (MST), a pioneering solution for software supply chain integrity based on the SCITT standard. This initiative enhances trust by logging every critical software build in an open, tamper-evident ledger. This advancement exemplifies Microsoft's commitment to Zero Trust principles and industry-wide transparency. This service is currently providing transparency for Microsoft services like Microsoft Azure Attestation, Managed HSM, Azure confidential ledger, and Microsoft Signing Transparency.

Microsoft Signing Transparency

Guaranteed auditability for Microsoft service code in external services

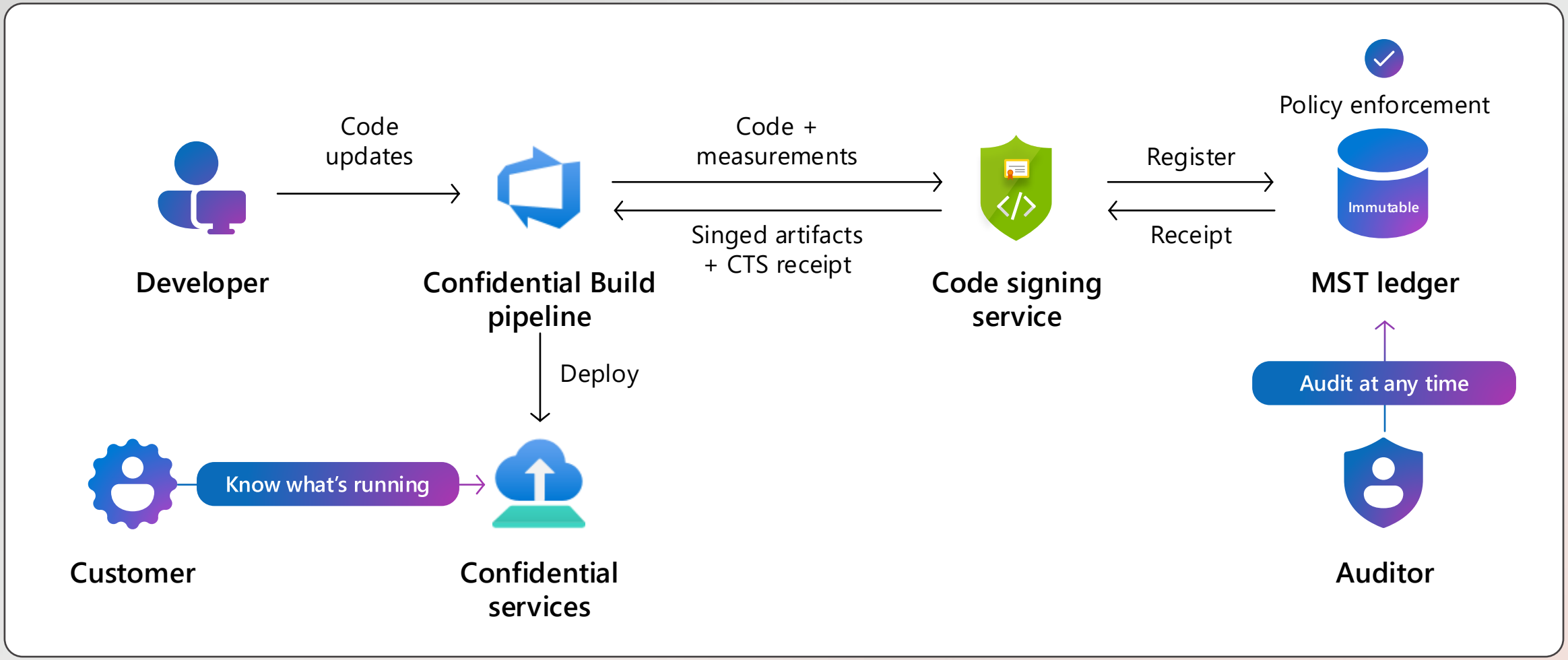


Signing code that matches policy

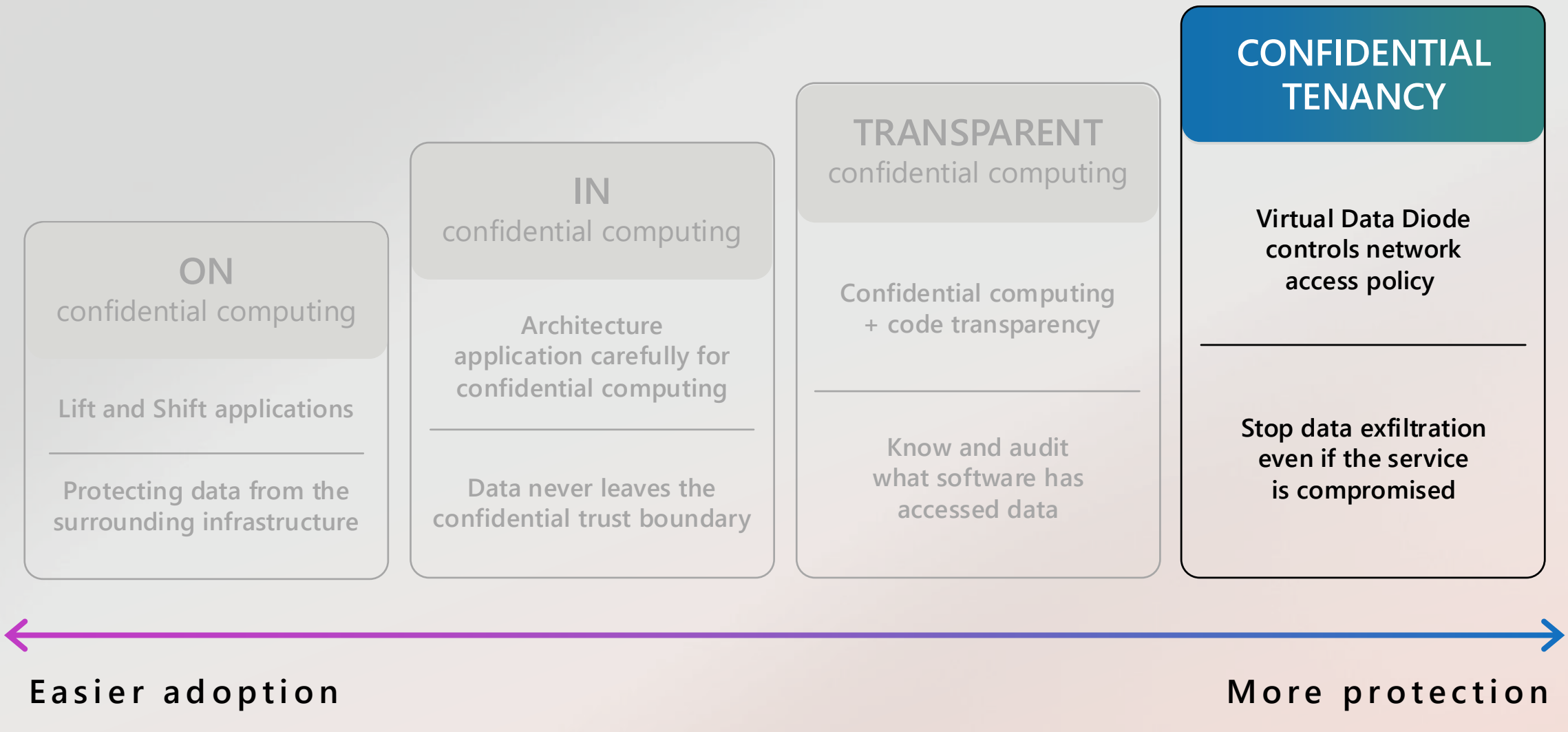
Reproducible build based on confidential computing

Automate upgrade with Microsoft Signing Transparency bootstrapped

Microsoft Signing Transparency

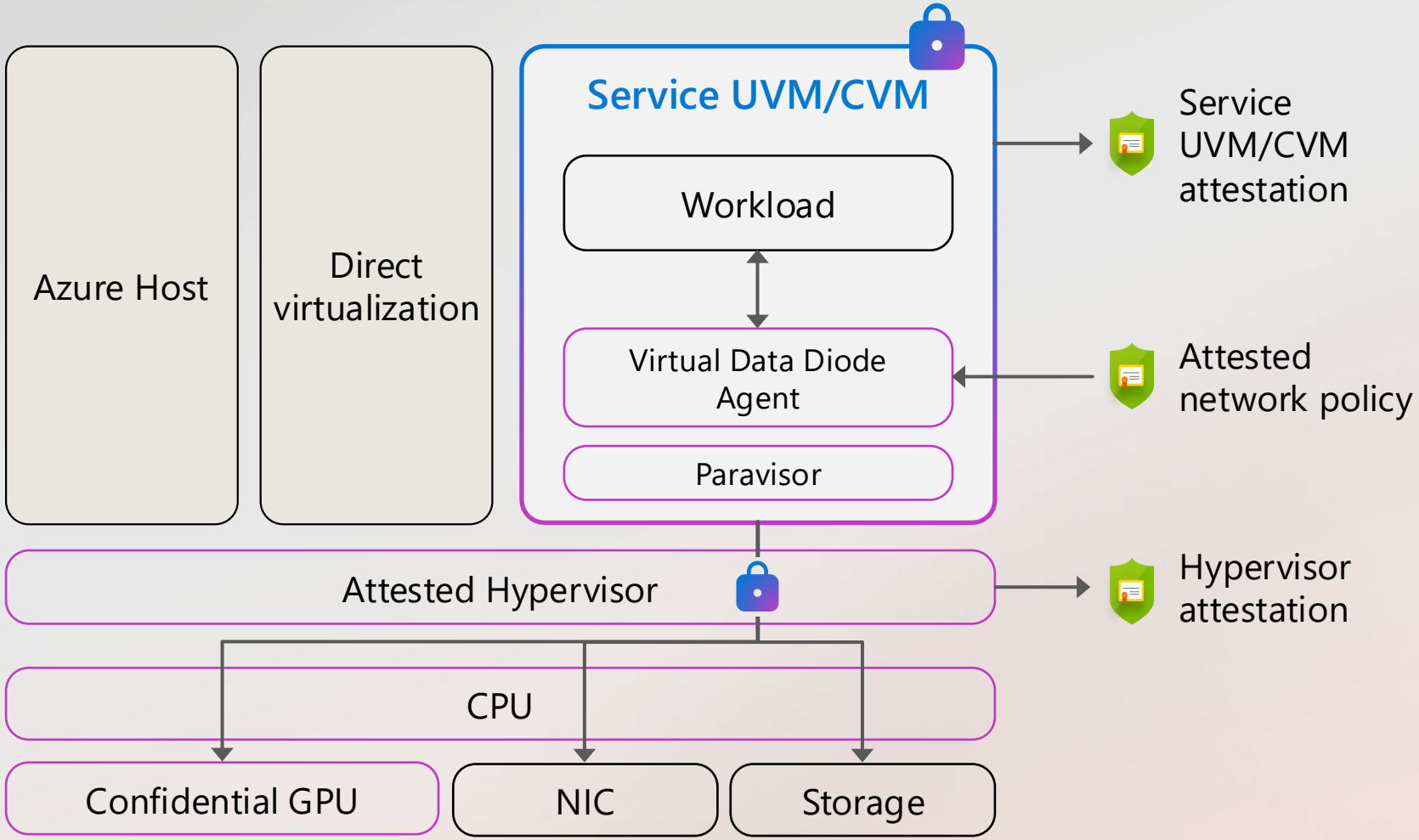


Confidential computing guarantees

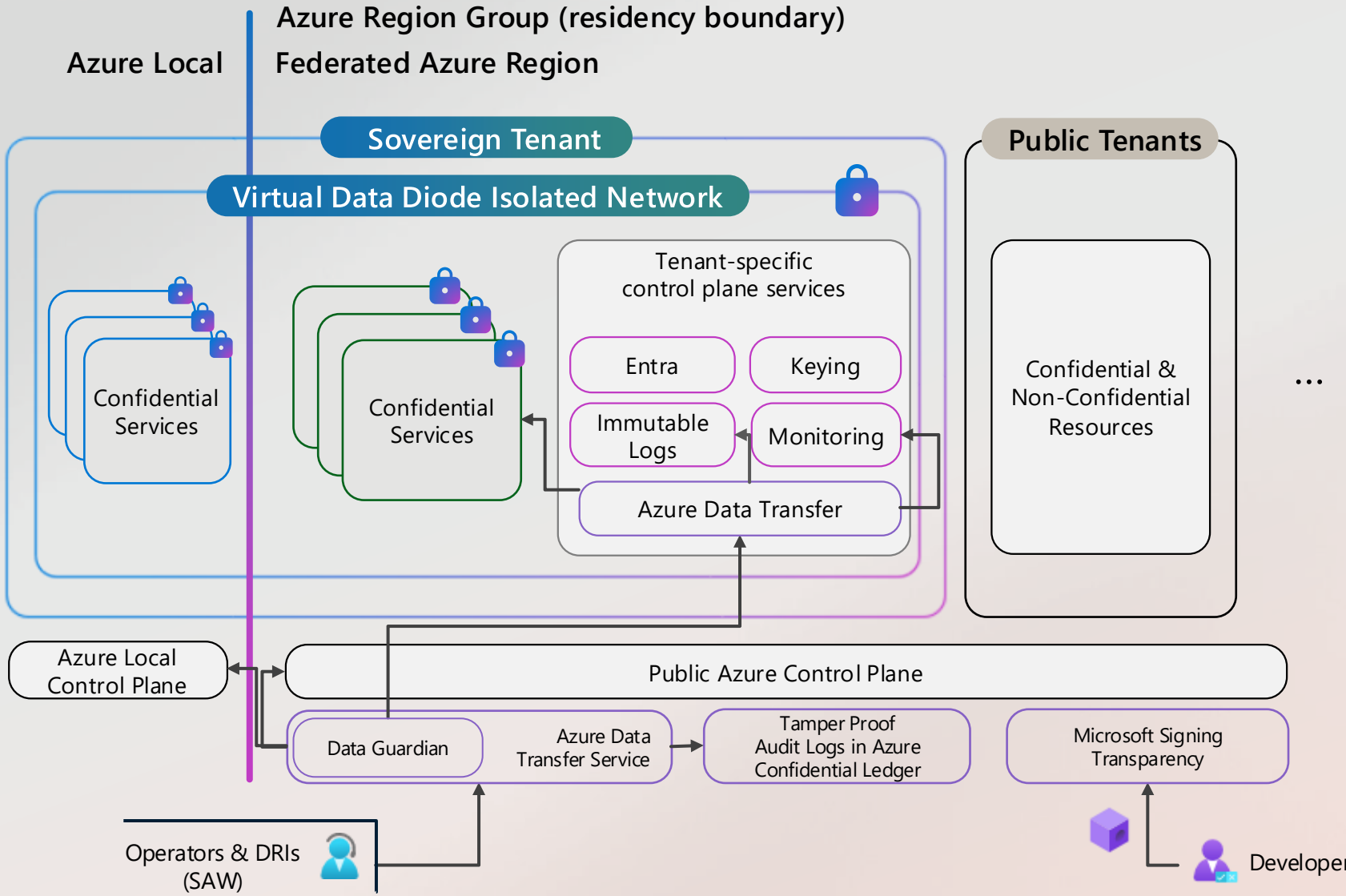


Virtual Data Diode

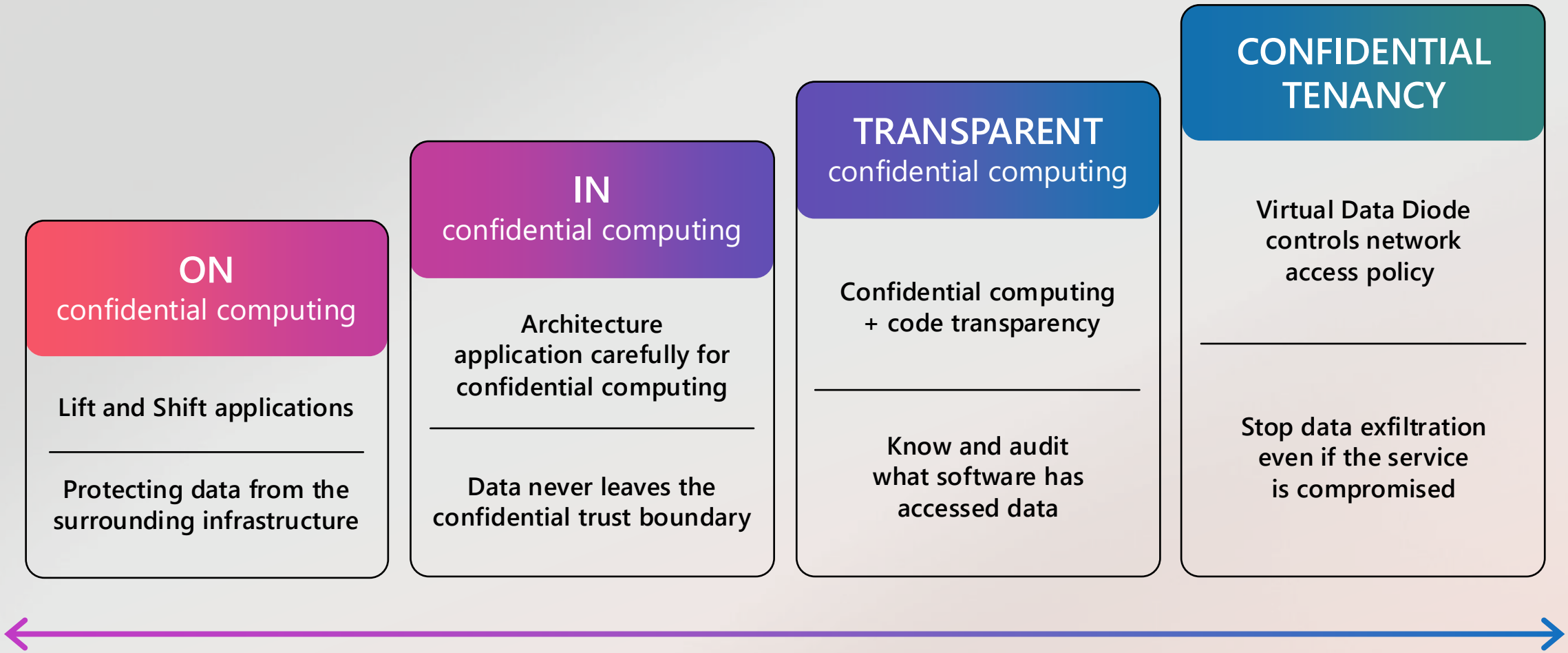
Attestable Network Policies



Sovereign confidential computing



Confidential computing guarantees



Confidential cloud

Data is fully in the control of the customer at rest, in transit, or in use.

The cloud platform provider is **outside the trusted compute base.**

Code running in the cloud is protected and **verified by the customer.**

Activity history is **immutable and auditable.**

Confidential computing is the future of computing