# Microsoft Cloud for Sovereignty

Pieter Kestelyn

# Transformation helps governments perform better and drive growth

Harnessing digital technologies enables governments to:

- Engage and support constituents
- Increase productivity
- Foster innovation
- Realize cost savings

**Digital transformation at scale and at pace requires the right policies**

# Hyperscale cloud is key to digital transformation

Cloud offers benefits beyond Cost Savings, Redundancy, Resilience and Scalability.
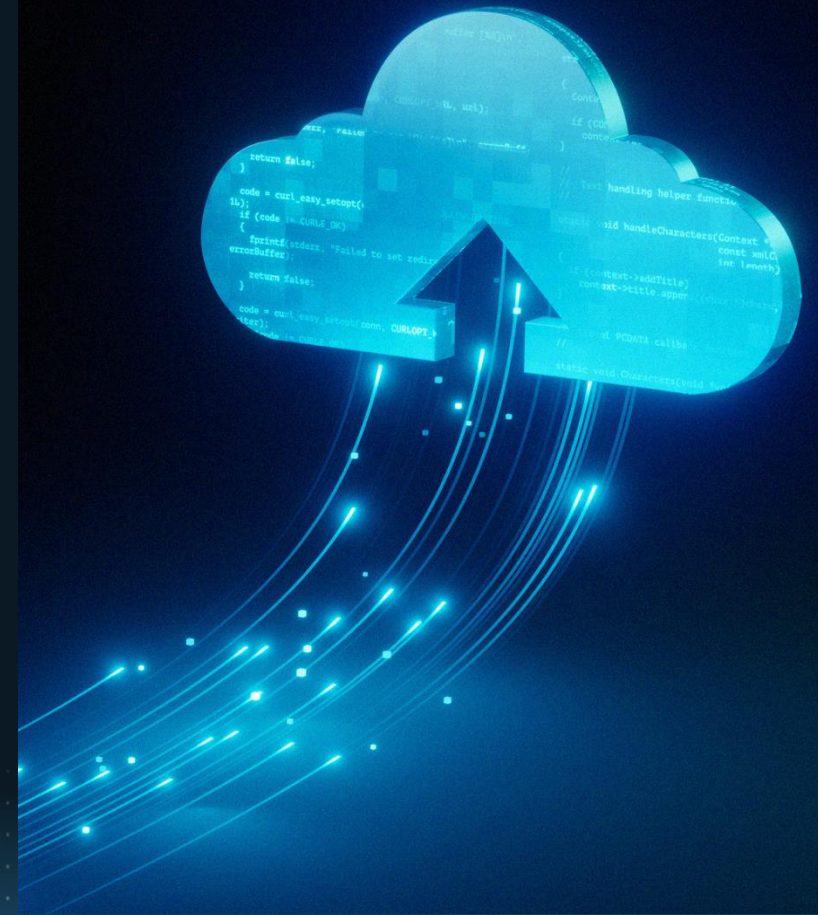
Agility – Reduce the cost of failure

Innovation – New technologies now come **first** to the cloud and soon will come **only** to the cloud

Cybersecurity – Hyperscale threats require Hyperscale protection

Compliance – Software-defined constraints, monitoring and auditing, adaptability to new compliance requirements

# With digital transformation, there are more concerns

Organizations want to safely leverage the benefits of the cloud, AI, and IoT, but...

Governments want control over their data

Demand for privacy is increasing

New regulations on technology

Ethical implications of AI are being studied

Cloud Value vs Control Burden

**LEGEND**
- Hyperscale Cloud
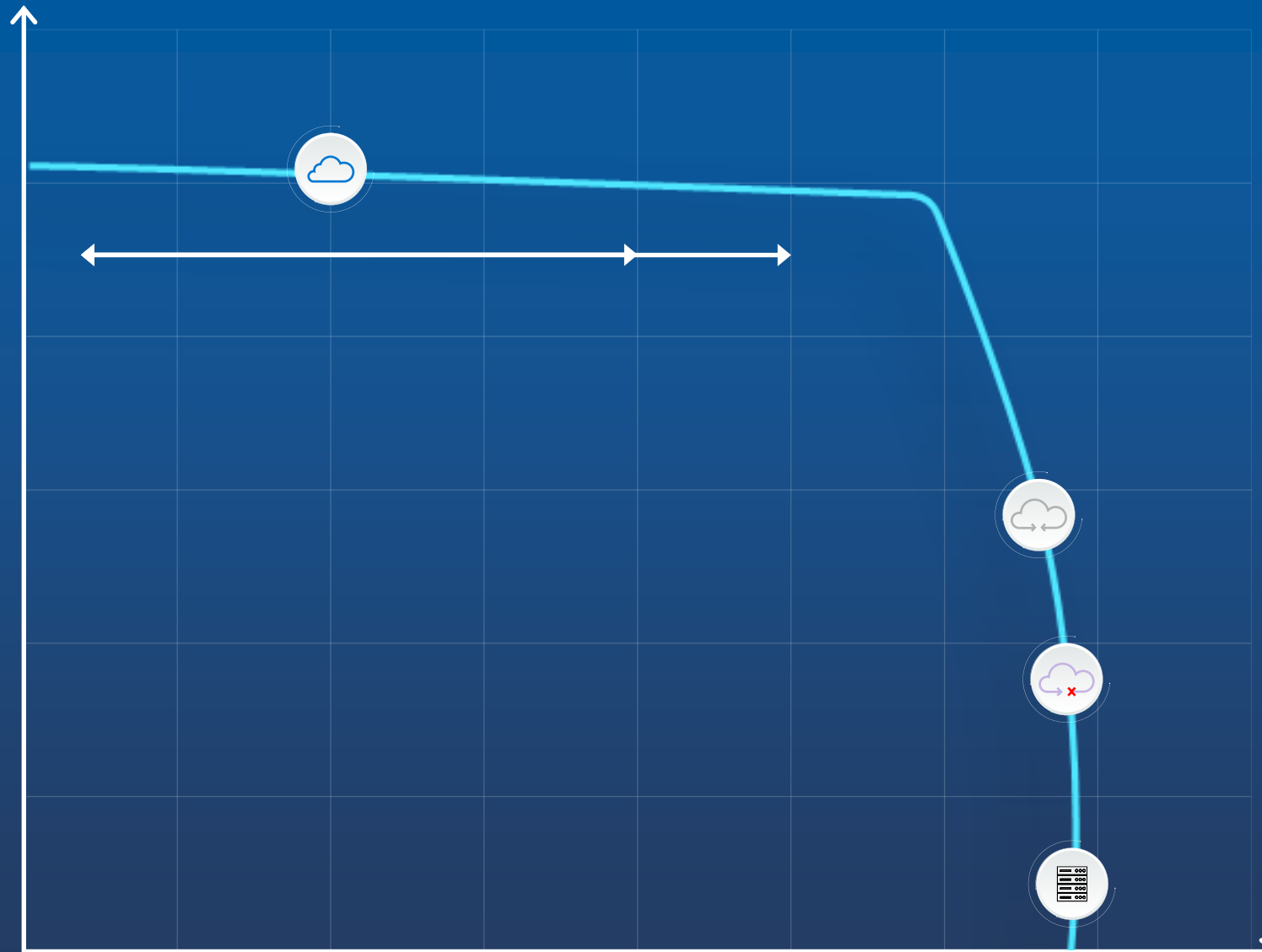- Hybrid Cloud (connected)
- Hybrid Cloud (disconnected)
- On-premise

**CLOUD VALUE**
(Scalability, Innovation, Cybersecurity, Reliability, Compliance, Cost Savings, Agility, Managed, Redundancy, Economic Benefit)

**CONTROL BURDEN**
(Sovereignty, Autarky, Residency, Operations)

# Microsoft Cloud for Sovereignty | Value Proposition

**Helps enable regulatory compliance:**

**Easily use with all your Azure workloads:**

**Reduce perceived risk of cloud adoption:**

Help ensure compliance with future regulatory changes using sovereign guardrails and controls in your cloud environment.

Apply your sovereign controls and guardrails quickly and easily to all Azure workloads, no manual configuration required.
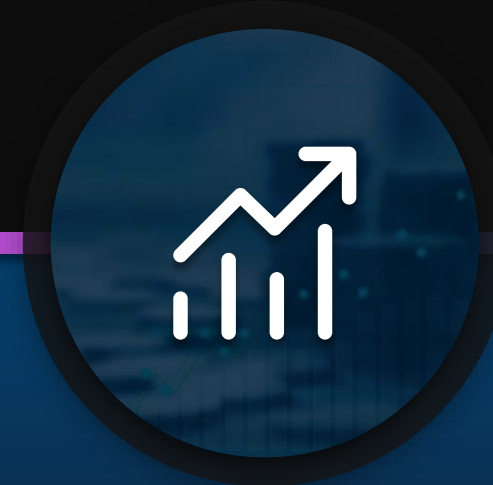
Provide public sector customers with a future-proof solution that helps reduce the risk perception associated with cloud adoption.

# Microsoft Cloud for Sovereignty
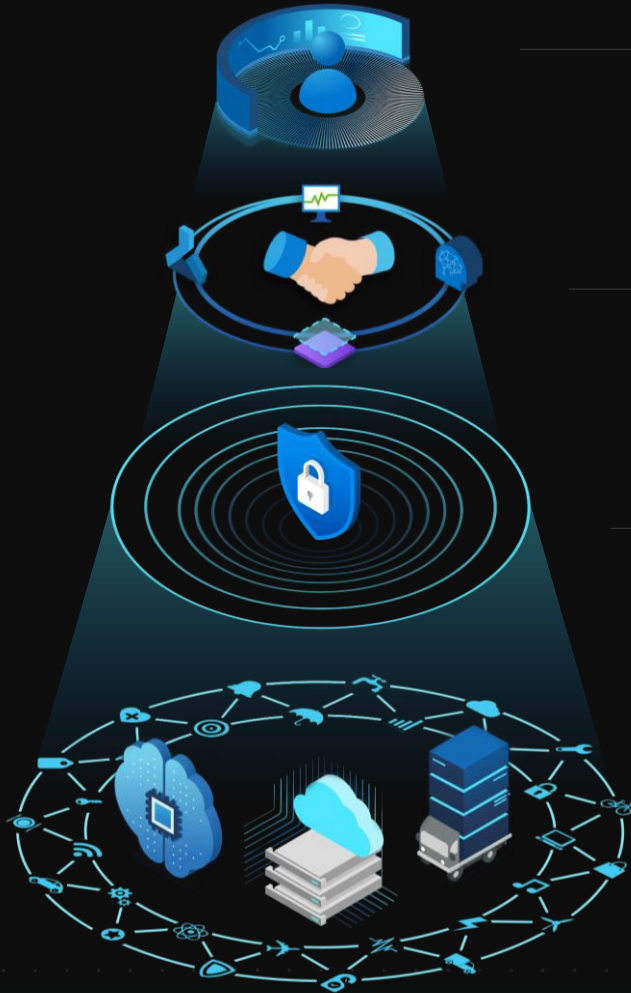
## Sovereign Control Portfolio

Protect workloads from outside access using advanced sovereignty and encryption controls such as confidential computing and cloud HSMs.

## Sovereign Guardrails & Guidance

Get access to codified architectures, workload templates, and tooling to assist in creating compliant architectures and answer sovereign questions.

## Compliance & Transparency

Ensure local compliance with policy packs for your region and increased transparency over—and into— your environment's operations.

## Public Cloud Capabilities

Get the innovation, scale, and security of the public cloud, with capabilities significantly beyond private or on-prem datacenters.

## Data Residency

60+ Azure regions for local data residency, + EU data boundary

**Microsoft Cloud for Sovereignty**

**Sovereign Control Portfolio**

| Azure Confidential Computing | Sovereign Tooling | SQL Always Encrypted |
| Managed HSMs | Azure Policy | Azure Monitor |

**Sovereign Guardrails & Guidance**

| Reference Architectures | Sovereign Landing Zones | Policy Initiatives |

Orchestrate deployment, configuration, monitoring and management

**Compliance & Transparency**

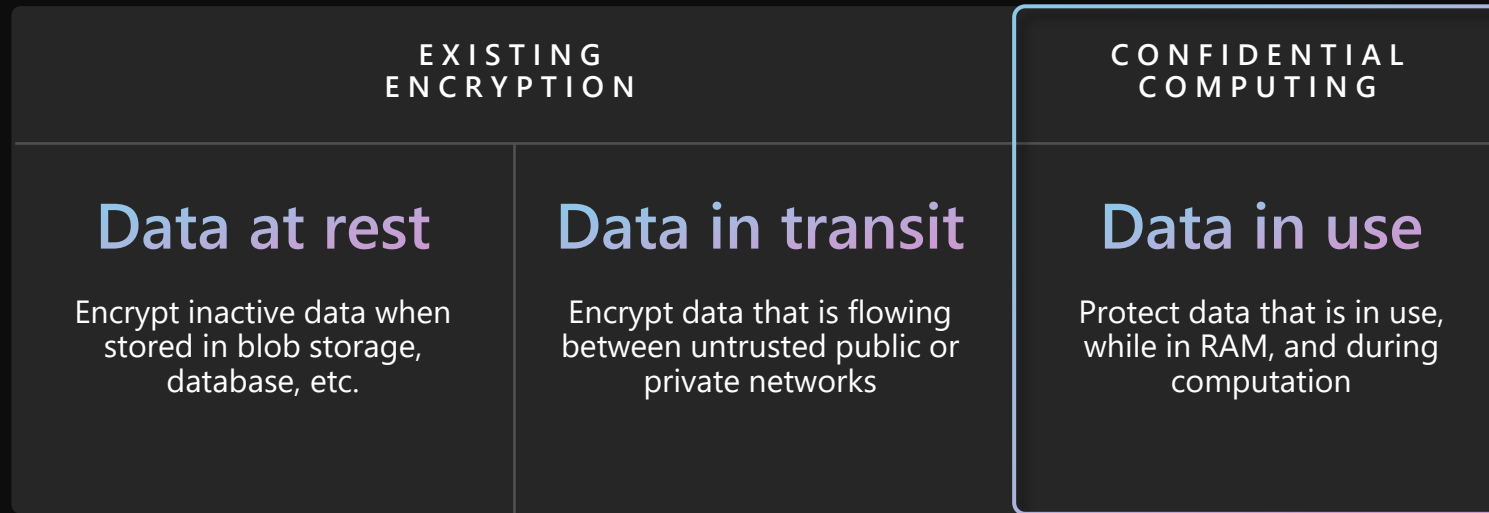| Operator Logs | Government Security Program | Right to audit |

**Public Cloud Capabilities**

| 60+ Azure Regions | Azure Services |

Provides Local Data Residency and the resiliency and connectivity of a hyperscale cloud

# Data protection through encryption

| EXISTING ENCRYPTION | | CONFIDENTIAL COMPUTING |
|---|---|---|
| **Data at rest** | **Data in transit** | **Data in use** |
| Encrypt inactive data when stored in blob storage, database, etc. | Encrypt data that is flowing between untrusted public or private networks | Protect data that is in use, while in RAM, and during computation |

In Azure, confidential computing means…

**A hardware root-of-trust, customer verifiable remote attestation, and memory encryption**

## PROTECT AGAINST

**Malicious**
privileged admins or insiders

**Hackers**
exploiting bugs in the Hypervisor/OS

**Third parties**
accessing data without customer consent

# Microsoft Cloud for Sovereignty | Generally Available Today

Microsoft Cloud for Sovereignty became generally available in December 2023 with key components of the offering vision, including:

- The Sovereign Landing Zone (SLZ), provides opinionated, easy to deploy, repeatable infrastructure-as-code to help meet sovereignty and regulatory compliance requirements for the public sector and government agencies.

- Sovereignty Baseline policy is a special set of built-in Azure Policy initiatives meant to supplement the environments with sovereignty controls, like data residency, key management and customer managed keys, and confidential computing.

- Policy for Italy's ACN requirements, Netherlands BIO regulation, and CSA Cloud Controls Matrix (CSA CCM v4) which help customers more easily monitor, guard and report on their compliance in Azure.

- Transparency Logs provide customers with visibility into instances when Microsoft engineers temporarily access their subscriptions for customer support or service reliability issues.

- Automated workload templates for Azure Confidential Computing and Azure Lighthouse as examples for building workloads using these technologies for sovereign environments to speed learning and adoption.

- Technical documentation and guidance on Microsoft Learn, integrated with WAF, CAF, and guidance around workload migration to address sovereign needs.

- Additional Azure services in the GSP program, including Azure Fabric Controller and Azure Virtual Desktop.

Microsoft

# Questions?

Thank You!