Microsoft | intel

Digital Sovereignty in the AI Era: Control and Verifiable Trust from Silicon to Cloud

A workload-based approach to control, verifiability, trust, and AI innovation

Introduction

Who this paper is for

Leaders responsible for digital sovereignty, security, and AI adoption, including CIOs, CISOs, CTOs, cloud and infrastructure executives, privacy and compliance leaders, and government and policy stakeholders.

AI is reshaping what digital sovereignty requires. AI now reaches critical infrastructure, essential services, and routine operations, making digital sovereignty an architectural concern rather than a question of data location alone. Decision makers must account for where models execute, who holds administrative authority, how sensitive information and intellectual property are safeguarded, and whether essential functions can withstand disruption. These are increasingly strategic decisions. Geopolitical instability, cyber risk, supplier dependencies, and service interruptions can all affect an organization's capacity to operate and innovate. Digital sovereignty brings those considerations together through four priorities: authority, resilience, verifiable trust, and choice. Digital sovereignty is therefore a question of control, resilience, trust, and choice.

Microsoft and Intel® contribute complementary layers to that architecture. Intel provides advanced computing technologies, hardware-based security, and AI acceleration. Microsoft adds cloud and local infrastructure, AI services, identity, security, governance, and sovereignty controls. In combination, they give organizations a clearer basis for placing workloads, protecting sensitive assets, and validating the execution environment.

Sovereignty architectures should reflect use-case risk. Public-facing AI, regulated analytics, and mission-critical government services can demand different degrees of administrative authority and operational independence. This paper uses that principle to examine deployment models, technical assurance, and continuity.

Contents

01 Introduction & Contents

02 Why sovereignty and security matter now

03 Defining digital sovereignty

04 A continuum of sovereign choices

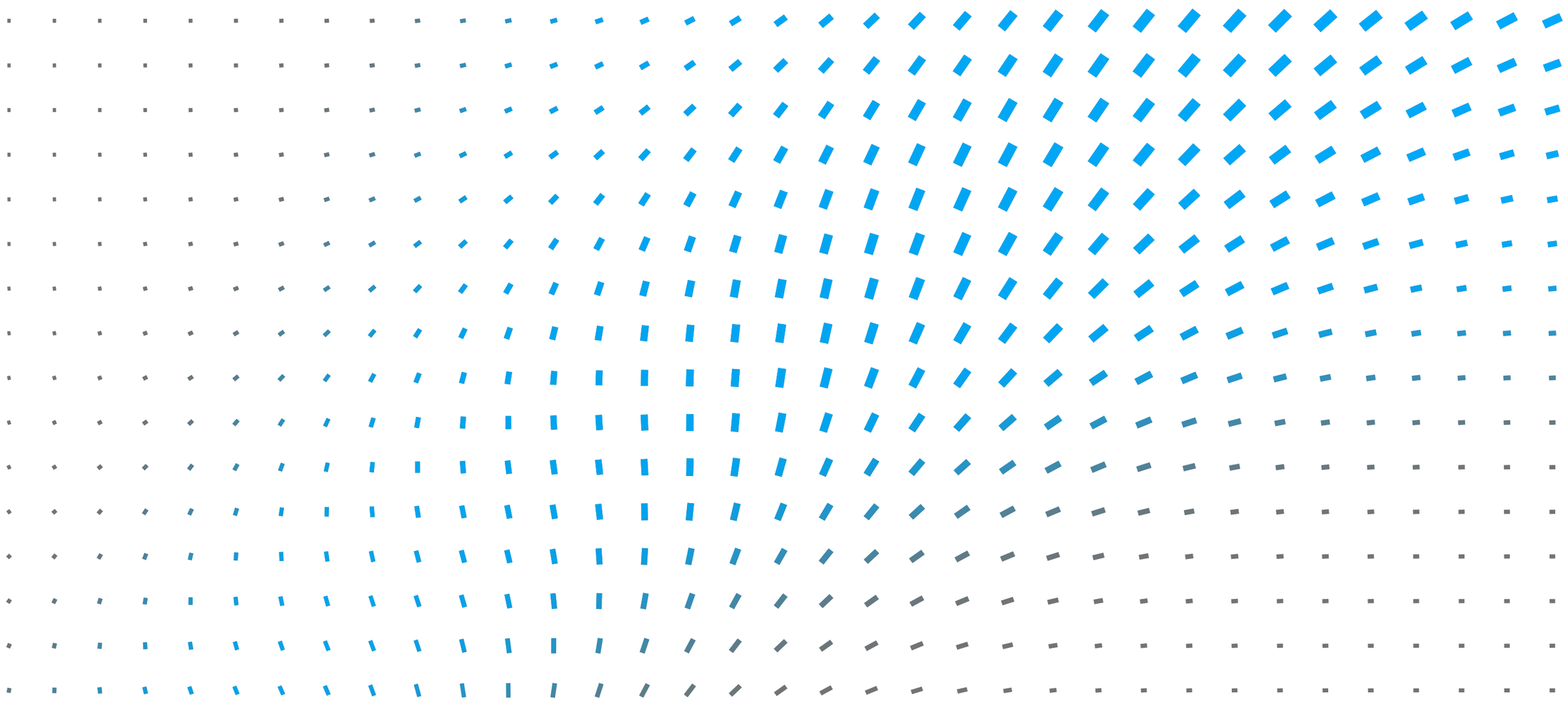
05 Verifiable trust from silicon to cloud

06 Sovereign AI infrastructure where you need it

08 Sovereignty without sacrificing innovation

09 Microsoft and Intel: A shared foundation for digital sovereignty

Why sovereignty and security matter now



As cloud and AI become integral to critical operations, traditional approaches to security and compliance must evolve. Data residency, regulatory requirements, and contractual commitments remain important, but they don't fully address questions of who can access and control systems, how sensitive workloads are protected while in use, how technology dependencies affect resilience, and whether essential services can continue through disruption. Addressing these risks requires a comprehensive approach to security, governance, technology, and operational resilience. Organizations need to understand who can access and manage their systems, identify potential vulnerabilities, and assess whether essential services can continue during disruptions.

Increasingly, they also need technical evidence that security protections are in place and operating as intended, complementing contractual assurances, policies, and certifications. The goal isn't to eliminate every risk, but to make informed, workload-specific choices about control, dependency, and assurance applying protections where the sensitivity or criticality of a workload requires them while preserving the ability to innovate.

5 questions leaders should ask:

1. Which critical workloads and datasets require geographic, operational, or access controls?
2. Who can administer systems and authorize access to sensitive information, including during exceptional circumstances?
3. What external technology and service dependencies could affect operations, continuity, or recovery?
4. What technical evidence is needed to confirm that required security protections are in place?
5. Where can AI create value while keeping sensitive data and processing within approved boundaries?

Defining Digital Sovereignty

For Microsoft and Intel, digital sovereignty means giving organizations greater control over their data, infrastructure, technology, and operations, with the flexibility to choose the technologies and deployment models that best meet their needs. Three inter-connected priorities help guide this approach.

Continuum of sovereign choices

Match each workload's risk profile to public cloud, customer-controlled infrastructure, or partner-operated environments, considering data, access, connectivity, resilience, continuity, and administrative authority.

Verifiable trust from silicon to cloud

Use hardware-based security alongside identity, encryption, cloud protection, and governance to safeguard sensitive workloads and produce technical evidence of defined security properties.

Sovereign AI and innovation at scale

Build and operate AI across compatible cloud and local environments, accounting for data protection, performance, resilience, and administrative authority throughout the AI lifecycle.

A continuum of sovereign choices

The Microsoft Sovereign Cloud portfolio spans Sovereign Public Cloud, Sovereign Private Cloud, and the Sovereign Partner Ecosystem. This range lets organizations align individual workloads with the required mix of flexibility, authority, and operational independence.

Sovereign Public Cloud

- Use Microsoft public cloud services with added sovereignty capabilities for data protection, access transparency, and operational governance
- Best suited for workloads that need broad public cloud services and can meet sovereignty objectives through available safeguards.

Sovereign Private Cloud

Run supported workloads on customer-controlled infrastructure with greater administrative authority.

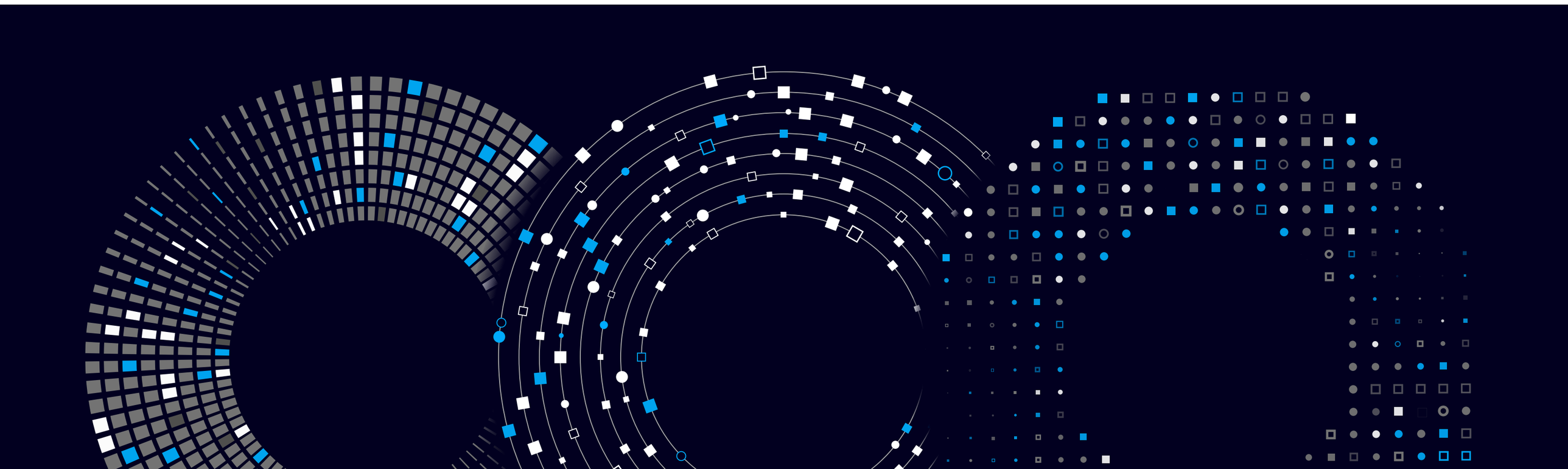
.

- Azure Local provides a consistent infrastructure foundation across edge and datacenter environments, with connected and disconnected operating options.
- Best suited to scenarios that require local infrastructure, greater operational control, or the ability to operate with limited or no cloud connectivity.

Sovereign Partner Ecosystem

- Engage local partners and independently operated cloud providers when national requirements call for specific ownership, operational oversight, or governance arrangements.
- Best suited for organizations that depend on local or national operators, specialized oversight, or partner expertise.

Availability, operating responsibilities, safeguards, and support boundaries differ by environment. Evaluate each configuration against the workload's risk profile before deployment.



Verifiable trust from silicon to cloud

Data location alone does not establish sovereignty. Organizations also need assurance about workload protection, access authority, and the security properties of the execution environment. Microsoft and Intel combine hardware-based isolation and attestation with Microsoft security and governance capabilities to provide that assurance. This is where confidential computing and hardware-based attestation can add another layer of assurance. Microsoft's digital sovereignty blog explicitly positions Azure confidential computing as protecting supported data while it is processed in a hardware-based and attested trusted execution environment.

Protect sensitive workloads

Confidential computing complements encryption at rest and in transit by protecting data in use. In supported Azure confidential virtual machines, Intel® Trust Domain Extensions (Intel TDX) isolates virtual machines in hardware and can reduce exposure to certain infrastructure-level threats.

Verify the environment

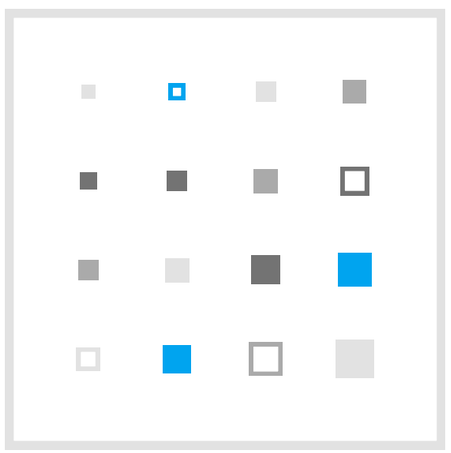
Attestation supplies cryptographic evidence about defined properties of the computing environment. That evidence can inform access decisions before sensitive data or encryption keys are released. It does not establish the security of an entire workload or platform; its assurance is limited to the measured properties and eligible configurations.

Maintain control

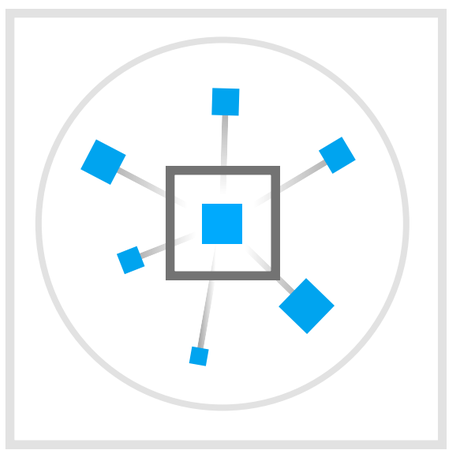
Microsoft identity, encryption, key management, operator access, policy, governance, and sovereignty features enable organizations to administer access, enforce security requirements, and retain oversight across eligible cloud and local environments The approach: isolate the workload, verify the environment, and authorize access.

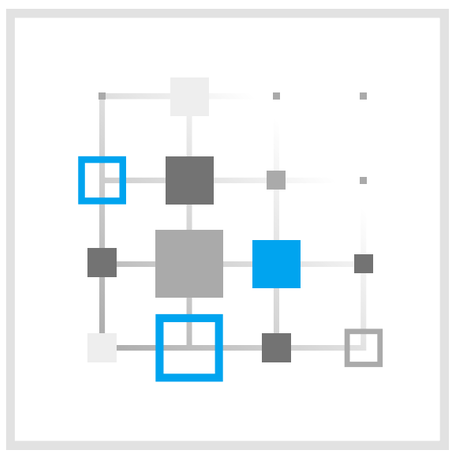
Isolate the workload. Verify the environment. Authorize access.

Hardware-based isolation, attestation, and policy-based access rules work together to establish trust in sensitive computing environments.









Sovereign AI infrastructure where you need it

AI deployment now spans core business processes, creating a placement decision for every model and data flow. Public cloud may suit some scenarios; others call for processing near sensitive data, operational systems, or users.

Microsoft and Intel support both cloud and local deployment models. Azure Local provides the infrastructure for running supported applications and services in customer-managed environments. Foundry Local enables AI models to run locally. Intel® Xeon® processors deliver compute and AI acceleration for relevant workloads. Deployment, configuration, and availability should be validated for each scenario.

Together, these technologies let organizations align AI placement with data governance, performance, connectivity, and resilience objectives. Sovereign AI encompasses not only the model, but also the applications, data pipelines, development tools, infrastructure, and operating processes across its lifecycle.

Critical Industries: When trust becomes mission critical

Sovereignty is especially consequential in sectors that handle sensitive information or deliver essential services. The examples are illustrative rather than specific customer deployments; the appropriate safeguards depend on the workload, industry, jurisdiction, and validated configuration. The challenges vary by industry. Hospitals must protect patient information while using AI to improve care. Financial institutions need to safeguard transactions and meet compliance requirements. Governments, utilities, and manufacturers depend on resilient infrastructure to keep essential services running.

Industry scenarios

Healthcare

Protect sensitive clinical data during supported AI analysis with hardware-based isolation and access control.

Manufacturing:

Run supported AI inference near plant systems where connectivity, latency, and operational continuity matters.

Government:

Process restricted information in approved environments with sovereign deployment and layered security controls.

Sovereignty without sacrificing innovation

Organizations can pursue innovation while retaining authority over critical systems. With a workload-based sovereignty strategy, they can:

- Select deployment models from the workload's risk, regulatory obligations, operating conditions, and recovery objectives Apply consistent governance and lifecycle practices where supported.
- Bring new AI capabilities closer to sensitive data and existing applications.
- Strengthen resilience through business continuity planning, recovery capabilities, and management of critical dependencies.
- Respond to changing requirements without unnecessarily limiting technology choices.

Digital sovereignty enables organizations to have the confidence to innovate on their own terms while remaining accountable for critical systems and data. With the right combination of infrastructure, security, and governance, they can adopt new technologies while maintaining accountability for their most critical systems and data. Organizations can begin with five workload-level questions.

Applying sovereignty to your workloads

- Data sensitivity: What information requires additional protection?
- Operational control: Who must be able to administer and operate the environment?
- Technical assurance: Which security properties must be verified, and what evidence is required?
- Connectivity and resilience: Must the workload continue operating during a network or service disruption?
- AI requirements: Where should models and data processing run to meet performance and control needs?

Microsoft and Intel: A shared foundation for sovereignty

Digital sovereignty requires more than choosing where data resides. It calls for a foundation that brings together deployment flexibility, verifiable security, and operational control built on a trusted foundation A practical sovereignty strategy begins with classification: determine the sensitivity, criticality, assurance needs, and operating constraints of each workload.

Microsoft and Intel bring together complementary layers for that strategy. Intel's computing technologies, hardware-based security, and AI acceleration work alongside Microsoft's cloud infrastructure, AI services, and integrated security and governance capabilities. This connection from silicon to cloud helps organizations strengthen security and protect sensitive workloads across the technology stack while maintaining choice in where and how workloads run.

As cloud and AI continue to evolve, organizations need the flexibility to respond to changing sovereignty requirements without limiting innovation. Together, Microsoft and Intel are helping organizations build digital sovereignty on a trusted foundation, with the control, resilience, and choice to innovate with confidence.

Learn more

Microsoft Sovereign Cloud
Explore digital sovereign solutions across cloud, AI, security, and productivity.
aka.ms/sovereignty

To identify which sovereign cloud solution may fit your organization's needs, take the Microsoft Sovereign Cloud assessment

Azure local
Learn about running Azure services and workloads on customer-controlled infrastructure.
aka.ms/azurelocal

Intel Confidential Computing
Learn about Intel hardware-based security technologies and trusted execution environments.
intel.com/confidentialcomputing

