GUIDE

Sovereign AI cloud: A practical guide to *secure, compliant AI infrastructure*

ORI

ori.co

Contents

Introduction

In today's AI-driven world, organizations face a balancing act: they need to leverage powerful AI technologies while maintaining strict control over sensitive data. For CIOs, CTOs, and IT leaders across enterprises, government agencies, healthcare systems, and retail giants, the question is no longer whether to adopt AI—but how to do so with complete control and compliance.

75% of all countries have implemented **data localization rules**.[1]

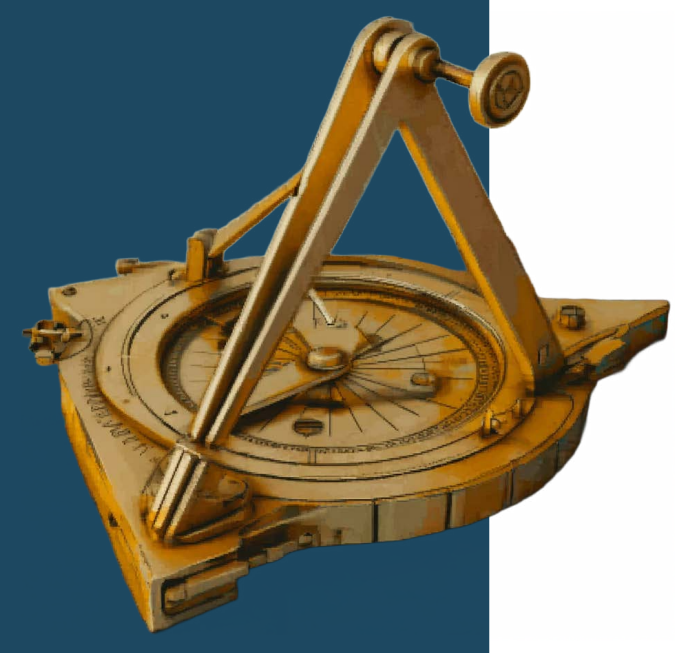
50% of European CXOs now see data sovereignty as a top issue **when selecting cloud vendors**.[2]

76% of consumers want to ensure their own country's laws and standard of care **are applied to personal data**.[3]

The concept of a **sovereign AI cloud** offers an elegant solution. This dedicated, private cloud environment empowers organizations with absolute ownership over their data and infrastructure, ensuring adherence to local laws and uncompromising security standards.

As digital sovereignty becomes both a regulatory imperative and a strategic asset, forward-thinking organizations increasingly demand an AI platform that seamlessly integrates advanced performance with stringent data privacy, auditability, and governance.

A sovereign AI cloud is poised to be the cornerstone of this next generation of secure, compliant AI initiatives.



1. McKinsey & Company. (n.d.). Localization of data privacy regulations creates competitive opportunities; 2. Accenture. (n.d.). Sovereign cloud: The foundation for trusted cloud-enabled transformation; 3. Cisco. (2024). Cisco consumer privacy report 2024.

Why a sovereign AI cloud is crucial for *modern enterprises and public sector organizations*

Data sovereignty is no longer a mere buzzword—it is a critical mandate. In an era defined by regulations such as the GDPR, HIPAA, and numerous national data protection laws, organizations must ensure that their sensitive information remains within designated boundaries and under strict oversight. This is particularly vital for government agencies entrusted with safeguarding citizen data and national interests.

A sovereign AI cloud offers several key benefits:

Absolute data control: By localizing data processing within prescribed jurisdictions, organizations can avoid conflicts with foreign legal mandates and ensure that sensitive information is managed exclusively under local oversight.

Enhanced trust and compliance: A dedicated cloud infrastructure, meticulously designed to meet regional standards, not only streamlines regulatory compliance but also reinforces stakeholder confidence.

Strategic differentiation: Organizations that embrace sovereign AI demonstrate a clear commitment to security and governance, positioning themselves as leaders in an increasingly competitive market where data integrity is paramount.

In contrast to multi-tenant public clouds—where data may inadvertently traverse borders—a sovereign AI cloud is purpose-built to meet the complex demands of today's digital environment, merging trust with performance.

Navigating *security, compliance, and data sovereignty* in AI

Deploying AI at scale introduces a multifaceted set of challenges that extend well beyond Compute and Data Storage. AI workloads often involve highly sensitive information—from personal data to proprietary research—that demands an environment with unparalleled security and rigorous compliance. Key considerations include:

Data privacy and residency

Regulatory mandates require that sensitive information remain within specific national or regional confines. Public clouds, with their global footprints, may inadvertently disperse data or metadata across multiple jurisdictions.
A sovereign AI cloud ensures that every element of your data remains within the designated geography.

Regulatory compliance

Industries face diverse regulatory landscapes, from financial oversight to stringent healthcare standards. The complexities of these frameworks can render shared cloud environments problematic. A sovereign AI cloud enables organizations to architect their infrastructure in strict accordance with regulatory requirements, facilitating smoother audits and demonstrable compliance.

Enhanced security posture

Shared-tenant environments naturally broaden the attack surface, increasing the risk of unauthorized access and data breaches. In contrast, a dedicated cloud environment minimizes these risks by eliminating cross-tenant exposure and enabling robust, customizable security measures.

Control and ownership

In conventional public cloud settings, control over encryption keys and operational protocols is often diluted. A sovereign AI cloud places complete control in the hands of the organization, enabling precise management of security protocols and data governance.

Today’s digital imperatives demand more than just state-of-the-art AI capabilities—they require an environment engineered for transparency, control, and trust. Modern cloud architectures are evolving to meet these standards by combining advanced AI acceleration with stringent security and compliance measures.

Power your sovereign AI with a *dedicated* cloud environment

A defining characteristic of a sovereign AI cloud is isolation, achieved through both single-tenant architectures and, where necessary, air-gapped configurations.

Dedicated-tenant architecture

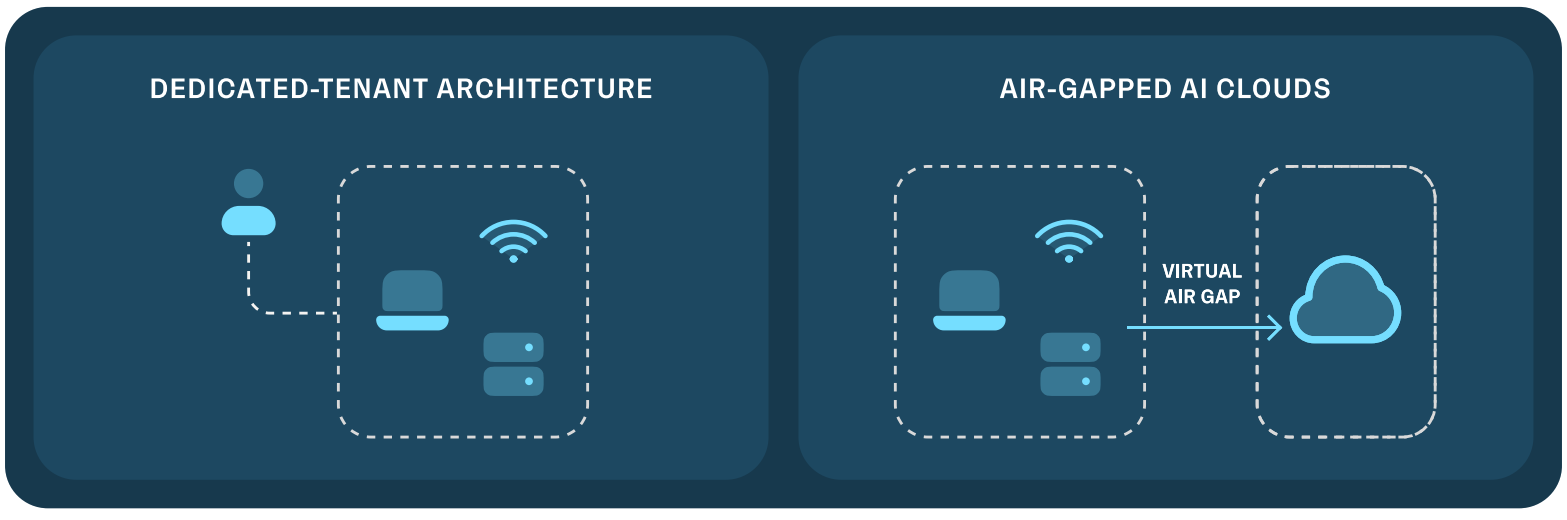
In a dedicated-tenant environment, your organization's AI workloads run on dedicated hardware. There's no sharing of compute, storage, or network resources with other tenants, ensuring that your sensitive processes remain isolated. This exclusivity:

- **Eliminates "noisy neighbors"**: Performance is consistent because no other workload interferes with your resources.
- **Enhances security**: With no cross-tenant access, the risk of unauthorized access or data leakage is drastically reduced.
- **Amplifies customization**: Tailor the environment to your specific security and performance needs without being constrained by the limitations of a shared infrastructure.

Air-gapped AI clouds

For the most sensitive projects, an air-gapped environment offers an extra layer of security. By physically or logically isolating the cloud from external networks, organizations can:

- **Maximize protection**: Create an environment that is virtually impervious to external cyber threats.
- **Control connectivity**: Maintain rigorous oversight over any temporary network connections, ensuring that data exchange occurs only under strict, pre-approved protocols.
- **Blend performance and compliance**: The combined benefits of single-tenancy and air-gapped configurations culminate in an AI platform that offers both exceptional performance and an uncompromising security posture—attributes that are indispensable for organizations that need to stay ahead of competition but also adhere to compliance requirements.



The strategic advantage of a *dedicated private AI cloud*

For enterprises and government agencies, the decision to adopt a dedicated, private AI cloud is not merely about technology—it is a strategic imperative. Here's why taking complete control over your AI infrastructure is essential:

- **Assured compliance**: A dedicated private cloud is meticulously designed to respect local data residency requirements, simplifying the task of meeting diverse regional and industry-specific compliance standards.
- **Robust security framework**: Full control over every aspect of your AI stack—ranging from custom encryption keys to comprehensive monitoring systems—ensures that your data is protected at every layer.
- **Optimized performance and customization**: A private AI cloud empowers you to tailor your hardware and software configurations to meet the specific demands of large-scale AI training and high-performance inference, unencumbered by the limitations of shared environments.
- **Cost predictability at scale**: For organizations operating at scale, a private cloud model offers more predictable operational expenses, avoiding the variable costs associated with public cloud usage.
- **Elevated trust and transparency**: Being able to unequivocally state that your AI infrastructure operates within a secure, sovereign environment enhances stakeholder confidence and strengthens your market position.

Modern digital strategies recognize that the most effective AI solutions are those that seamlessly blend *advanced computational capabilities* with stringent controls and *full ownership of data*.

Sovereign AI cloud *in action*: Diverse use cases

The versatility of a sovereign AI cloud is evident across a broad spectrum of organizations:

Government agencies and public sector organizations

A government analytics department can leverage AI to enhance public services—ranging from traffic pattern analysis to processing citizen feedback. A dedicated, air-gapped environment ensures that all data remains strictly within national borders, with robust access controls and comprehensive audit trails that support both innovation and regulatory compliance.

Global financial institutions

A multinational financial services company employs AI for fraud detection and risk management. By deploying region-specific instances within a dedicated private AI cloud, the bank ensures that sensitive financial data remains localized and is processed under stringent regulatory standards. This approach minimizes cross-border data exposure and meets the exacting requirements of global financial regulators.

AI-first tech companies

An innovative startup specializing in foundation models requires substantial computational power without compromising proprietary data. Utilizing a dedicated high-performance private cloud, the company gains exclusive access to thousands of GPUs in an optimized environment, ensuring that its critical training processes are both secure and cost-effective.

Healthcare organizations

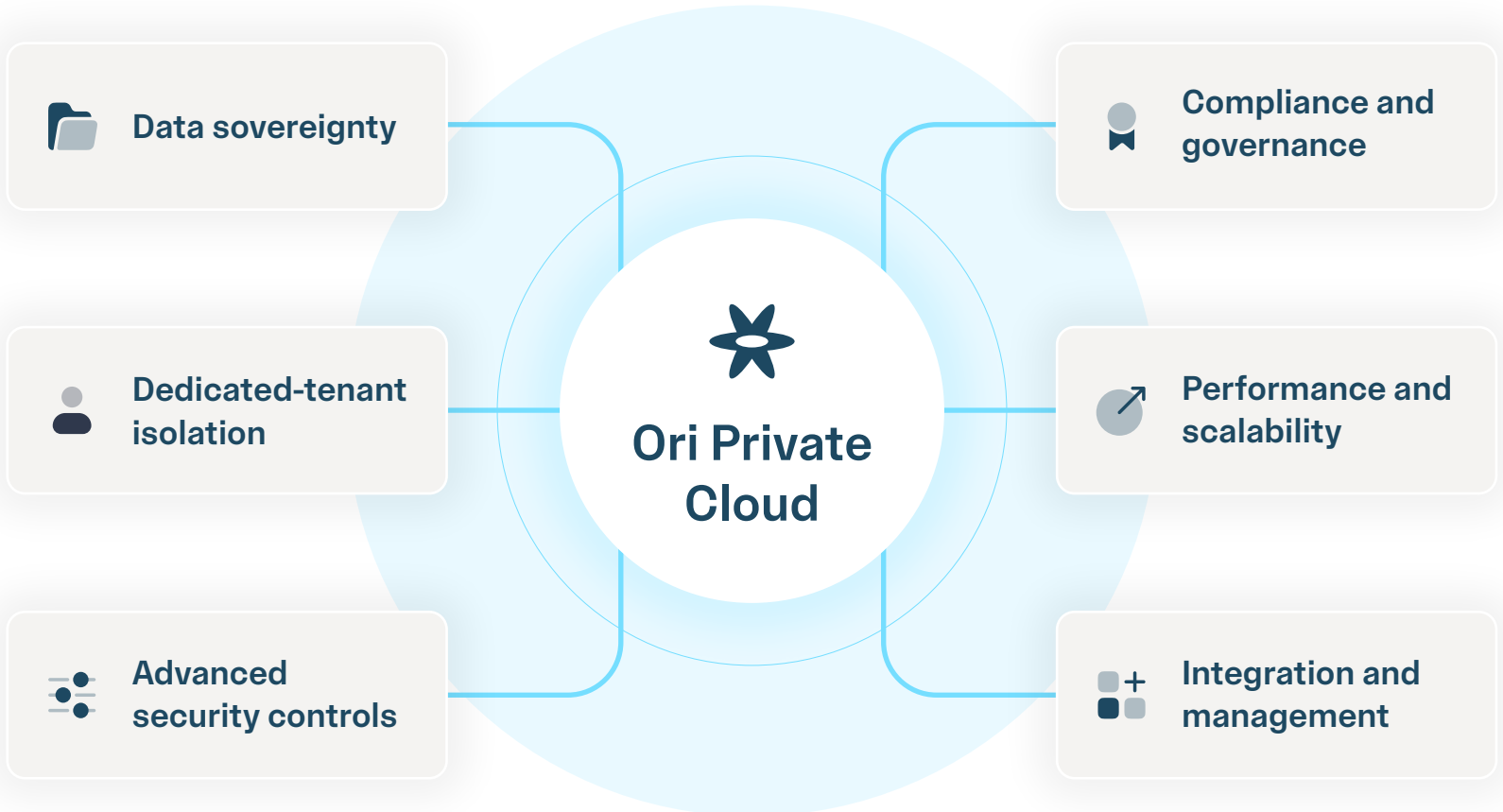
Healthcare providers and research institutions increasingly depend on AI to enhance patient care, streamline diagnostics, and accelerate drug discovery. By deploying AI on a sovereign AI cloud, these organizations can process sensitive patient data—including records, imaging, and research findings—within an environment that strictly adheres to HIPAA and other regional healthcare standards. This configuration guarantees that patient privacy and data integrity are preserved at every stage.

Defense and aerospace organizations

Defense and aerospace sectors increasingly rely on AI to enhance project planning, expedite threat detection, and accelerate research and development for next-generation systems. Highly sensitive or classified data—ranging from mission-critical sensor outputs to strategic intelligence can be securely managed in a sovereign AI environment that meets strict national security standards. This approach not only fortifies data against unauthorized access or external interference but also empowers defense and aerospace agencies to innovate more rapidly, free from the operational and regulatory risks often associated with shared or non-sovereign platforms.

Ori private cloud: A sovereign AI cloud engineered for *secure, faster AI*

To achieve the ideal balance between cutting-edge AI performance and rigorous security, Ori Private Cloud presents a purpose-built solution that meets the highest standards of data sovereignty, compliance, and innovation.



Complete data sovereignty: Ori Private Cloud is deployed within your chosen region, ensuring that every facet of your data—from raw inputs to processed outputs—remains within local regulatory boundaries. This guarantees that your organization retains unequivocal control over its data.

Dedicated-tenant isolation: Every deployment of Ori Private Cloud is strictly single-tenant, meaning your AI workloads operate on dedicated hardware isolated from other clients. This configuration provides unmatched security and performance, enabling you to run critical applications without compromise.

Advanced security controls: Security is integral to the architecture of Ori Private Cloud. Featuring robust role-based access control (RBAC), resource monitoring and observability, the platform affords you comprehensive control over data access and integrity.

Tailored compliance and governance: Recognizing that no two organizations share identical requirements, Ori Private Cloud offers a highly customizable platform. Whether it is aligning with specific data retention policies or meeting unique audit logging standards, the platform can be tailored to your precise regulatory needs, streamlining compliance and enhancing governance.

Unmatched performance and scalability: Ori Private Cloud is engineered to support the most demanding AI workloads. With access to state-of-the-art hardware—including advanced GPUs and high-speed interconnects—your organization can scale its AI initiatives seamlessly, whether for intensive model training or rapid, high-volume inference.

Seamless integration and expert management: Designed to integrate effortlessly with your existing tools—ranging from Kubernetes clusters to bespoke AI frameworks—Ori Private Cloud is available as a fully managed service. This means you benefit from expert configuration, proactive maintenance, and continuous support, allowing your team to focus on strategic innovation rather than infrastructure management.

In an era where the control of digital assets is synonymous with competitive advantage, Ori Private Cloud delivers an environment that is as secure as it is powerful—a true enabler of next-generation AI innovation.

Chart a new course for secure *AI innovation*

As AI becomes a cornerstone of strategic enterprise initiatives, the imperative for sovereign, secure, and compliant AI infrastructure grows ever more pronounced. Forward-thinking executives understand that the transition to a sovereign AI cloud is not merely a technological upgrade—it is a strategic transformation. By merging unparalleled computational capabilities with comprehensive control and regulatory assurance, a Sovereign AI Cloud redefines what is possible in today's digital era.

Ori Private Cloud offers an environment meticulously engineered to meet these exacting standards, delivering a platform that is as secure as it is high-performing. It provides the requisite control and transparency for organizations to innovate boldly, all while ensuring that sensitive data remains exclusively under your control.

Now is the time to *transform* your approach to AI

Discover how a dedicated, sovereign cloud environment can accelerate your strategic initiatives, fortify your data governance, and pave the way for sustained innovation.

Talk to a Private Cloud Expert →

Accelerate AI development and market *readiness*

Develop AI in a secure, compliant *environment*

Optimize operational costs and *maximize* your ROI

About Ori

Ori is the first AI Infrastructure provider with the native expertise, comprehensive capabilities and end-to-endless flexibility to support any model, team, or scale. We're building the backbone of the AI era so that the technology of tomorrow can advance our world.

Ori believes that the promise of AI will be determined by how effectively AI teams can acquire and deploy the resources they need to train, serve, and scale their models. By delivering comprehensive, AI-native infrastructure that fundamentally improves how software interacts with hardware, Ori is driving the future of AI.

Learn more at www.ori.co →

ORI

ori.co