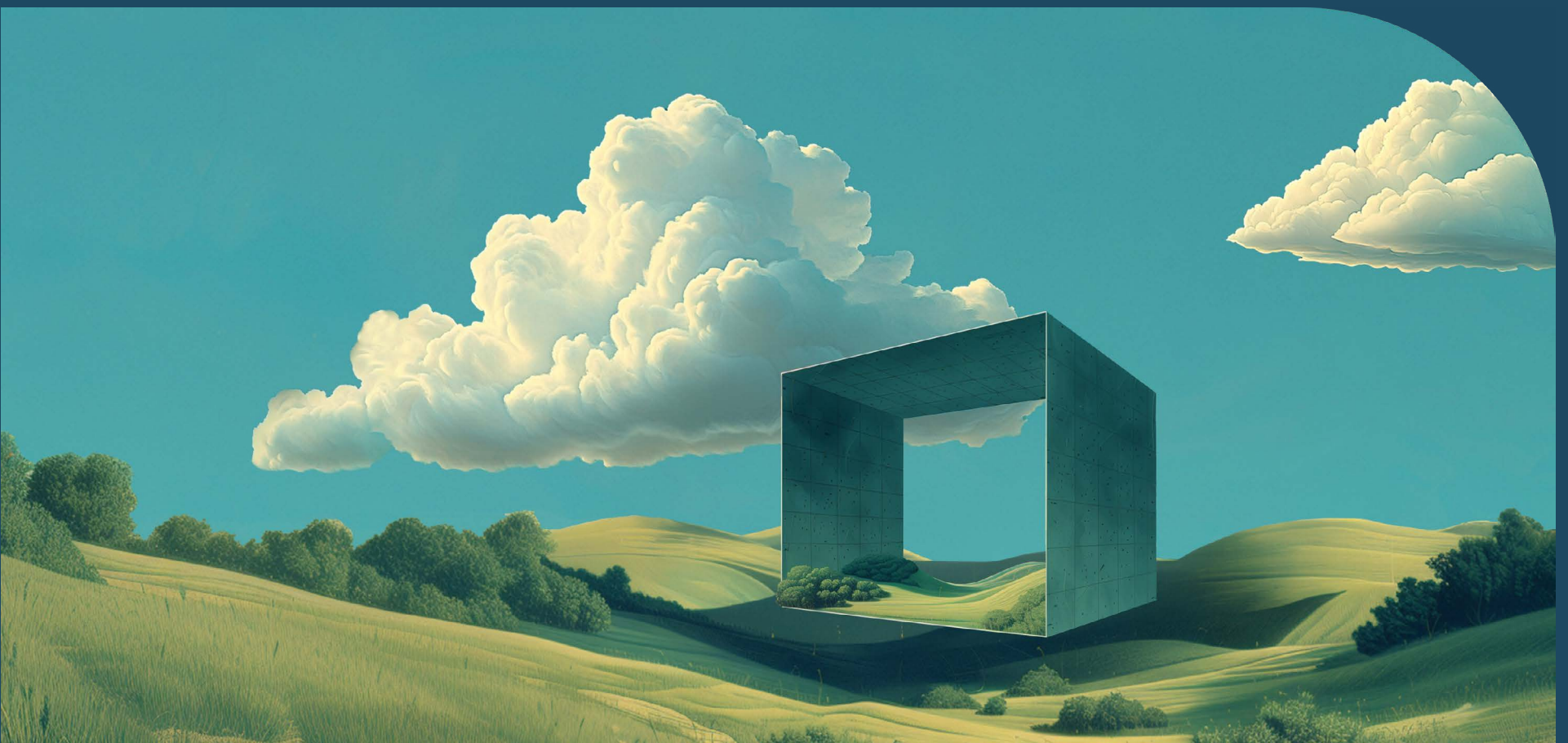




EBOOK

Build AI confidently with *a security-first* cloud



ORI

ori.co

Contents

Introduction	1
Weighing cloud security: Public vs Private cloud	2
How Ori Private Cloud fortifies your AI	4
Isolated and secure infrastructure	4
Flexibility that enhances your control over your workloads	5
Single-pane-of-glass monitoring	5
RBAC and granular security controls	6
Built-in traceability	6
Observability & resource tracking for optimization	7
Checklist for enterprise decision makers	8
Secure your AI journey	10
Build secure AI, faster	10

Introduction

Artificial intelligence (AI) is becoming a core driver of enterprise innovation, but security-first AI infrastructure is essential to protect sensitive data and intellectual property. Technology leaders are increasingly recognizing the need for secure cloud environments for AI, keenly aware that any breach or compliance failure in an AI deployment can be devastating.

82%

of data breaches were tied to data stored in cloud environments.¹

75%

of CISOs cite gaining control over cloud data as their top priority for managing risk.²

Up to 4%

of Global Turnover as fines for GDPR infractions.³

The risks of insecure cloud AI deployments include data breaches, IP theft, non-compliance fines, and even compromised AI models. To mitigate these risks, organizations are increasingly seeking isolated, compliant environments for their AI – which is why **79% of enterprises report implementing internal private clouds**⁴. Private clouds are emerging as the top choice for enterprise AI due to their robust data security, control, and flexibility.

Isolated & Secure



Ori Private Cloud is designed to be a security-first alternative to traditional public clouds for AI workloads. Ranging from secure, air-gapped environments to distinct workspaces for all your teams and robust enterprise controls, Ori makes it easy to build your AI securely and meet the growing security needs of your business.

1. SentinelOne. Private vs. public cloud security; 2. Big.ID 2024 CISO Report; 3. GDPR Info. Fines and penalties; 4. Forrester Infrastructure Cloud Survey in 2023.



Weighing *cloud security*: Public vs Private cloud


Not all cloud environments are equal when it comes to security. Public clouds and private clouds each have different risk profiles and benefits. Below is a comparison of key security aspects, highlighting how a private cloud can alleviate many security concerns associated with public cloud deployments:

	Public Cloud	Private Cloud
OWNERSHIP & CONTROL	Infrastructure is on shared, multi-tenant resources managed by a provider with limited direct control for the customer.	Infrastructure is dedicated to one organization, hosted privately or on-premise, giving the enterprise direct oversight and control.
ISOLATION OF RESOURCES	Shared environment with other tenants; potential for “noisy neighbors” and cross-tenant vulnerabilities if isolation fails. Data and workloads co-exist with others, raising concerns about data leakage between tenants.	Fully isolated environment with dedicated hardware and network segments for one enterprise, eliminating noisy-neighbor issues and vastly reducing attack surface. Greater ability to implement custom network segmentation and zero-trust architecture.
COMPLIANCE & DATA PRIVACY	Must rely on the provider’s controls and certifications. It’s a shared responsibility to meet regulations – the cloud vendor may be certified, but the customer must ensure their use of the cloud is compliant. Data may reside in global regions by default, raising sovereignty concerns.	Enhanced control over data location and handling , making it easier to comply with strict regulations (GDPR, HIPAA, etc.). Enterprises can choose where data is stored and processed. The environment can be tailored to specific compliance needs (e.g. keeping all data in-country and under specific encryption policies).
SECURITY RESPONSIBILITY	Follows a shared responsibility model – the provider secures underlying infrastructure (physical, hypervisor) while the customer secures the OS, apps, and data. Misconfigurations by users (e.g. open storage buckets) are a common risk. Security updates for managed services depend on the provider’s schedule.	Enterprise (and/or its private cloud provider) has end-to-end responsibility for security. With a private cloud like Ori’s, the dedicated infrastructure is maintained securely for the client, and the customer retains ultimate control over how data and workloads are secured and patched. This allows a more proactive security posture , everything from network to application can be locked down to the organization’s standards.
VISIBILITY & GOVERNANCE	Relies on provider’s tooling and APIs for monitoring. Visibility can be limited – e.g. only high-level logs or abstracted metrics are available, and multi-tenant setups mean less insight into underlying systems. Forensics and troubleshooting can be challenging in an ephemeral, shared environment.	Deep visibility into the stack – full access to logs, network data, and system metrics since the cloud is single-tenant. Enterprises can integrate the private cloud with their own SIEM, monitoring, and governance tools for a single-pane-of-glass view. This comprehensive observability simplifies auditing and incident response, as every action and flow in the environment is trackable by the organization.



Private clouds offer greater control, isolation, and custom security measures at the cost of additional management overhead. In contrast, public clouds provide convenience and rapid scalability but require trusting a third-party platform and diligently managing shared security responsibilities. Notably, using a public cloud means closely watching security configurations, since the slightest oversight (e.g. misconfigured access rules) could expose data to the internet.

On the compliance side, private clouds are often preferred for keeping sensitive data local and meeting strict regulatory requirements, whereas public clouds might offer more built-in services that ease daily management but could complicate compliance audits.

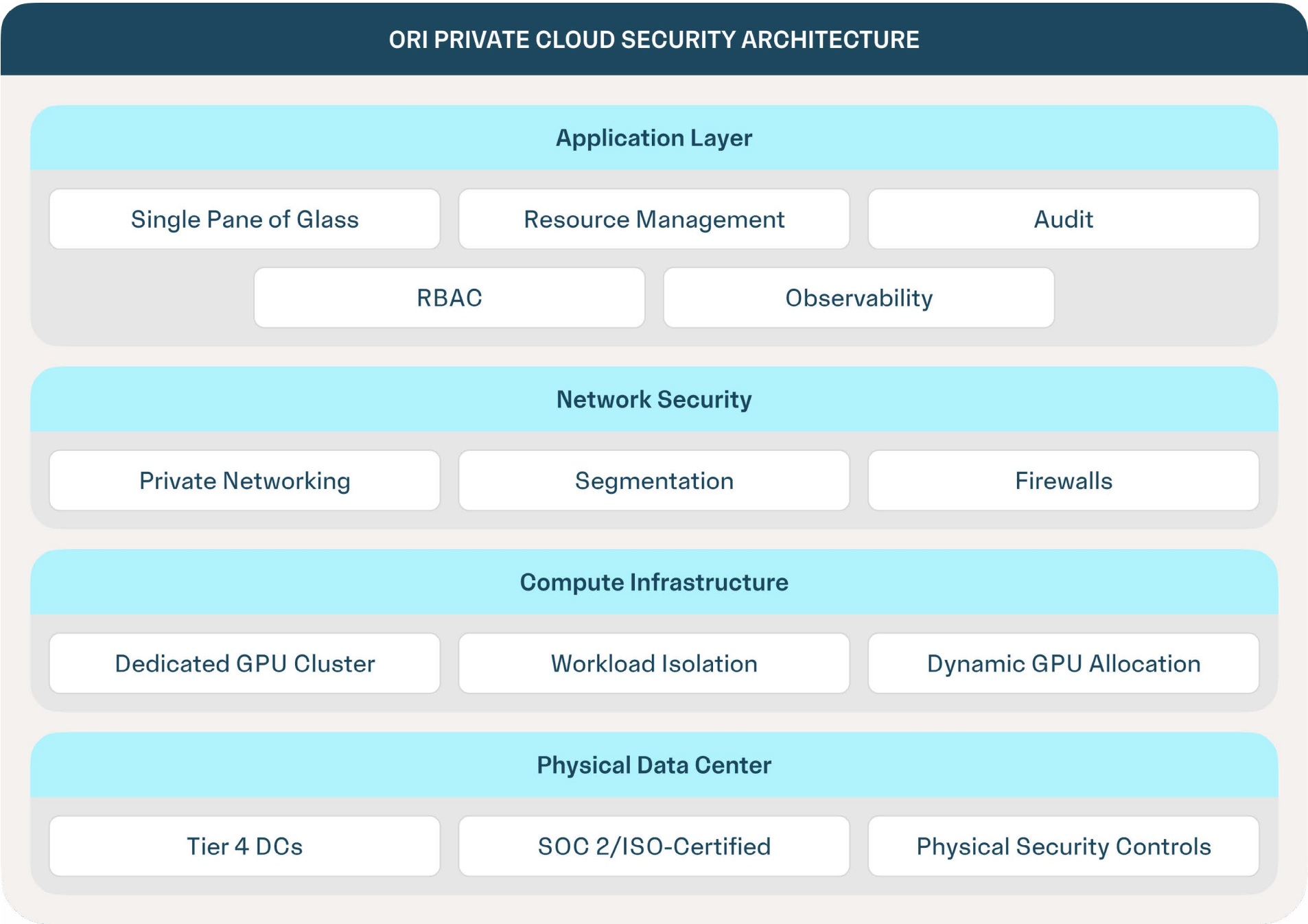


For enterprises with low risk tolerance and high governance needs, a private cloud can significantly mitigate the security risks inherent in public cloud services.



How Ori Private Cloud fortifies your AI

Ori's Private Cloud is purpose-built to address enterprise AI security priorities, providing a secure and controlled environment without sacrificing performance.



Isolated and secure infrastructure

Ori Private Cloud runs on dedicated infrastructure for each customer. Your AI workloads operate on hardware exclusively allocated to your organization, ensuring complete isolation from any other tenant or workload. This dedicated approach means **no shared resources, no noisy neighbors**, and strong isolation at the compute, storage, and network layers – dramatically reducing the risk of cross-tenant data leakage or interference. Enterprises gain full control over their AI environment: you decide where data resides and how it's secured, meeting data sovereignty requirements.



Moreover, Ori's data centers meet rigorous security standards (**SOC 2 and/or ISO 27001 certified**), so the physical infrastructure and facilities are audited and compliant. In short, Ori Private Cloud gives you a **cloud that's yours alone** – tightly secured from the ground up with full control over your most sensitive AI data and models.

Flexibility that enhances your control over your workloads

Ori Private Cloud provides the flexibility to **Bring your Own Compute** (BYOC). With BYOC, you can keep particularly sensitive data on your hardware and still use Ori's tools to process it, avoiding potential cloud storage of certain datasets if that's a compliance requirement. That means you can **leverage Ori's platform to run workloads in air-gapped environments within your own data centers**.

Designed for distributed teams, Ori Private Cloud enables every team to innovate in an isolated workspace while maintaining central oversight. By providing **distinct workspaces for each team (a multi-tenant architecture within the enterprise)**, organizations can segregate projects and data per team.

Each team's data, models, and pipelines are isolated from the ground up, at the software, network and compute levels. This data isolation guarantees that even though teams share the underlying cloud platform, their data does not accidentally mix. One team cannot access another team's datasets or models appropriate privileges. Isolation not only protects sensitive information but also reduces the risk of cross-team errors and aids compliance with data sovereignty rules.

Single-pane-of-glass monitoring

Ori provides a unified monitoring and management interface that offers real-time **visibility into your AI workloads spanning teams across your organization**. This “single pane of glass” approach means your team can monitor GPU/CPU utilization, memory, storage I/O, and network performance for every AI job or service.

Centralized logs and metrics allow security and ops teams to watch for anomalies or unauthorized activities across the entire AI stack. Because the Ori Private Cloud environment is fully under your control, **you can integrate with your existing security monitoring tools** – by feeding Ori's telemetry into your SIEM or analytics platforms to extend enterprise-wide observability.

The result is end-to-end situational awareness: from model training runs to inference endpoints, you have **real-time insights** at your fingertips. This level of visibility not only helps detect potential security issues early but also aids in optimizing AI performance by catching bottlenecks or inefficiencies quickly.



RBAC and granular security controls

Ori Private Cloud includes robust Role-Based Access Control (RBAC)

capabilities and fine-grained permission settings. You can define roles and assign privileges so that users only access the data and functions they require. This principle of least privilege reduces risk by minimizing unnecessary access. For example, a data scientist might deploy and monitor models but not have rights to alter core infrastructure settings. Ori's platform enforces these controls consistently across all services.

In addition, Ori supports two-factor authentication, ensuring that **only authenticated, authorized personnel can launch AI workloads or view sensitive data**. These granular controls form the backbone of **AI security governance** – together with monitoring, they allow enterprises to confidently share an AI platform among teams without fear of unchecked access.

Built-in traceability

To help customers meet regulatory and internal compliance requirements, Ori Private Cloud provides comprehensive **audit and compliance tooling**. Every action in the environment – from data uploads to model deployments, from user logins to configuration changes – can be logged and tracked.

Audit logs help keep a record of all activities, showing who accessed what and when. This level of traceability creates a verifiable chain of custody for data and models, which is invaluable for compliance audits and incident investigations.

Ori's compliance-oriented features don't stop at logging; the platform is designed in alignment with major security standards. Ori undergoes annual **ISO 27001 audits and is advancing towards SOC 2 compliance**, reflecting a commitment to security best practices. For customers, this means the private cloud environment inherently meets high security benchmarks, and built-in tools like compliance dashboards or reporting templates can simplify aligning your usage with frameworks like GDPR or industry-specific rules.



Observability & resource tracking for optimization

Ori's platform offers deep **observability into AI workloads and resource utilization**, which not only bolsters security but also helps optimize performance and costs. Through detailed metrics and resource tracking, you can see how every model training or inference job consumes GPUs, CPUs, memory, and storage. This transparency enables **optimization of AI workloads**: teams can identify under-utilized resources, spot performance anomalies, and right-size their clusters for efficiency. In practice, such observability leads to optimal training times and higher resource utilization, translating to cost savings via greater efficiency.

Real-time observability thus serves a dual purpose – strengthening security (through continuous oversight of system behavior) and driving cost-effective scaling of AI by ensuring you're getting the most out of your dedicated infrastructure. With Ori Private Cloud's rich telemetry, enterprise AI teams can confidently innovate, knowing they have the data to keep the environment both **secure and optimized**.



Checklist for enterprise decision makers

When evaluating a **security-first cloud provider** for AI workloads, enterprise decision-makers should consider the following checklist. Use these criteria to ensure any solution will meet your organization's security and compliance requirements:



Compliance & certifications: Does the provider demonstrate adherence to industry security standards? Verify they have relevant certifications (e.g. ISO 27001, SOC 2, GDPR readiness) and can support your compliance needs (such as data residency or specific regulatory frameworks in your industry).



Dedicated infrastructure: Confirm that the cloud environment offers private, isolated resources for your workloads. True isolation means your data and computations won't share hardware with other customers, greatly enhancing security.



Secure and distinct workspaces for each team: Does the cloud provide a multi-tenant access for your teams to segregate projects and data per team?



Flexibility to bring your own compute: If you already own Compute or prefer your compute for certain projects, consider a cloud that lets you to bring your own compute (BYOC) or integrate it with the provider's compute infrastructure.





Access controls & data protection: Evaluate the strength of identity and access management. Look for robust RBAC (role-based access control) to restrict user permissions and integration with your Identity Provider (SSO/MFA). The provider should enforce least privilege and protect sensitive data through every layer.



Monitoring & visibility: Ensure the solution provides real-time monitoring, logging, and observability into your AI processes. You should have a single pane of glass to oversee all AI jobs, with alerts for any anomalies. This visibility is key to quickly detecting issues like unauthorized access or data misuse in AI workflows.



Audit logging & reporting: Check that comprehensive audit logs are available and easily accessible. Built-in logs and reporting will simplify proving adherence to policies and investigating incidents if they occur.

This checklist will help you identify a cloud partner that treats security as a first-class priority, not an afterthought. A provider like Ori Private Cloud, which meets all these criteria, can empower your enterprise to pursue AI initiatives without compromising on protection.



Secure your AI journey

Enterprises must prioritize a security-first cloud infrastructure for AI to protect their data, ensure compliance, and build AI solutions with confidence. AI initiatives can deliver immense value, but without the right security foundation, they also introduce new risks. A security-first AI cloud means you can accelerate innovation without compromising on governance or peace of mind.

Build AI confidently knowing that your models and sensitive data are running in a hardened environment designed for enterprise needs. Ori Private Cloud delivers the performance and scalability for AI, plus the security and control that public clouds often lack. It empowers your organization to harness AI's full potential while keeping your risk low and your compliance on track.

Build *secure AI, faster*

Talk to a Private Cloud Expert →

Don't leave the security of your AI to chance. Take the next step towards building AI confidently with the right cloud foundation.



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