ORACLE

Oracle Cloud Isolated Region
## Disconnected Cloud for Highly Sensitive Workloads

Your challenge

As a private or public sector organization with sensitive data requirements, you face complex challenges while managing your critical operations. Legacy IT environments can no longer keep pace with today's demands, which have outgrown on-premises capacity and capabilities. You know a hyperscale cloud platform is the solution, but you are unsure if it will meet your security requirements. So, how can you securely run your highly sensitive, mission-critical workloads in an air-gapped cloud while having access to the same services and innovation as public clouds?

Our solution

Committed to organizations with stringent security requirements globally, **Oracle Cloud Isolated Region** is a full-featured, air-gapped hyperscale cloud that offers the same services as our public regions, as depicted below.
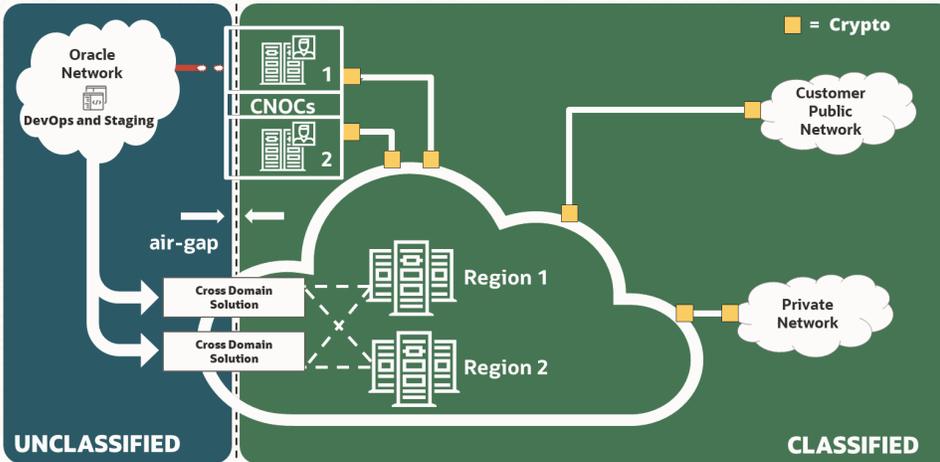
Oracle Cloud Isolated Regions are not connected to the internet, but they are connected via encryption devices to your secure networks. The regions can be located on-premises or in a co-located data centre that meets your compliance standards. Only authorised, onsite personnel can operate these regions from secure, in-country Cloud Network Operations Centres (CNOCs).

Code is deployed securely across the air-gap, and Oracle's global teams have no knowledge of or access to data or workloads inside the region. The region is also designed to function without a persistent connection between the Oracle network and the Cross Domain Solution. Designed to securely and predictably run your highly sensitive, mission-critical workloads—Oracle Cloud Isolated Region is the hyperscale cloud solution for public and private sector organizations with the most demanding security requirements.

Refer to our press release, announcing Singapore Defence and Technology Agency's selection of Oracle Cloud Isolated Region.

Oracle Cloud Isolated Region Highlights

Everything Everywhere
Offers the same services as public cloud and all the latest innovation—just disconnected

Security-first by design
Oracle cloud is engineered with security at the core, enabling zero trust architecture

Comprehensive solution for continuity of operations
Two regions provide high availability and disaster recovery for mission-critical workloads

Global expertise operating sovereign & disconnected environments
Proven 24/7 sovereign operations—live today in the US, UK, and EU

Fastest time to delivery
Building Oracle Cloud Isolated Regions in as little as 12 months—from data centre whitespace-ready to region isolation

Best value proposition
The same transparent and globally consistent pricing as public cloud with no escalation for highly sensitive workloads

Small footprint
As small as 100m² means minimum financial commitments that are manageable for any country's budget—and the footprint can grow with your forecasted demand plan

Core-to-Edge capabilities
Oracle Cloud Isolated Region provides the air-gapped cloud core to deploy and manage your Roving Edge Infrastructure

Industry Applications

Financial Services
- Protect sensitive financial data and trading systems

Healthcare
- Secure protected health information and research data

Energy & Utilities
- Safeguard critical infrastructure management systems

Telecommunications
- Secure customer data and network operations

Government
- Defense missions: safeguarding your nation's classified data and workloads
- Support sensitive public sector operations

Regulatory Compliance

- Oracle Cloud Isolated Region helps organizations meet stringent regulatory requirements in highly regulated industries such as healthcare (HIPAA), financial services (PCI-DSS, GLBA), and public sector (FedRAMP, FISMA)
- Oracle will work with you to support your unique security and compliance requirements

Private Sector Use Cases

- Drug research and development
- Financial trading platforms
- Critical infrastructure management
- Healthcare data analysis
- Intellectual property protection

Security by Design

Oracle's cloud is built on security-first principles for uncompromising cloud security. Oracle believes cloud security should be a default, built-in feature. Here are some examples:

Customer isolation: Oracle fully isolates networks with our custom-designed SmartNIC which prevents network traversal attacks, offering greater security and isolation at the infrastructure level.

Zero-trust security: Our security model employs a robust portfolio of easy-to-use, always-on security innovations. Data is encrypted by default, both at-rest and in-transit. Identity access is role-based, managed with deny-by-default policies.

Cloud Guard: Automatically monitor your tenancies against user misconfiguration, warning users and alerting administrators of potential risks. Cloud Guard can suggest improvements or even automatically implement corrective actions.

Data sovereignty: You have complete control of log and audit data, cross domain solution activity, and security analytics. Oracle Cloud Isolated Regions can operate with no automated data egress.

Secure supply chain: Oracle uniquely designs and tests our own hardware, maintains presence in supplier factories, and keeps verifiable chain of custody throughout our hardware lifecycle. Your secure cloud infrastructure is protected from the factory to your data centre.

Hardware Root of Trust: Reduce the risk of firmware-based attacks with Oracle's custom-built, hardware-based technology to wipe and reinstall firmware every time a server is provisioned or tenancy is created.

Oracle Cloud Isolated Region

Disconnected Cloud for Highly Sensitive Workloads