ORACLE
Cloud Infrastructure

Bringing Always-On Cloud Security to Your Data Center

Oracle Dedicated Region Cloud@Customer helps provide layered security for on-premises cloud environments.

The security of a public cloud in the customer data center

Services available in a public cloud environment, including vendor-managed products for cloud native, AI/machine learning, analytics, database, integration, and security, are now available in your data center with Oracle Dedicated Region Cloud@Customer. Run the portfolio of IT workloads on a single-tenant, flexible cloud infrastructure with Oracle's end-to-end service-level agreements (SLAs) covering performance, availability, and manageability of services—with the Oracle Cloud Infrastructure (OCI) portfolio within your physical data center.

Dedicated Region Cloud@Customer helps Oracle customers meet their regulatory, data residency, latency, and internal security requirements while enabling them to gain the benefits of OCI in the customers' data center. IT departments can use their own perimeter network security while adopting OCI's built-in security and security services of the platform, data, and applications.

With Dedicated Region Cloud@Customer, customer data, including control plane operations (for example, start/stop/terminate operations), stays on-premises and won't flow out of the region. Management data for Dedicated Region Cloud@Customer that helps Oracle achieve its SLAs and provide continuous security and functionality updates will flow in and out as required but without affecting your data residency requirements. In addition, you control the inbound and outbound connections to and from your Dedicated Region Cloud@Customer network. The traffic flow will be subject to your perimeter security.

Oracle's security-first approach operates on three pillars: architected-in, automated, and always-on security once it has been configured by our customers for their requirements. In this ebook, you will discover more about how Oracle delivers the highest levels of security to both the cloud and data centers.

Only 25% of organizations feel they can provide greater security controls within their data center versus that of a cloud service provider.*

* Oracle and KPMG Cloud Threat Report 2020

1 Protecting the data center: hardware security

SHARED PHYSICAL SECURITY

Oracle Dedicated Region Cloud@Customer employs hardware protection deployed within server cages with racks that Oracle provides and manages. This includes installation, monitoring, and maintenance of all physical security controls for the cages. These controls include cameras, two-factor access control, and intrusion-detection mechanisms. Cage walls extend below the raised floor and above the ceiling tiles, enclosing the Oracle Dedicated Region Cloud@Customer equipment within the customer data center.

The higher levels of security relied on in the public cloud can now be part of your physical data center.

AUTHORIZATION AND ACCESS

Oracle designed Dedicated Region Cloud@Customer to help isolate and protect your services and database data from unauthorized access, using Oracle Cloud Infrastructure. The cloud management duties are shared between the customer and Oracle. You, as the customer, will control access to your customer services, databases, and database data. Oracle will control access to Oracle-managed infrastructure components. Oracle has no access to customer cloud instances or data. You also control access to your VMs, databases, and data via three types of controls.

Authentication

- Credentials to access your customer services, customer VM operating system and databases, and database data

Network

- Layer 2 virtual LANs to access customer VMs
- Network access rules implemented in the customer VM operating system and Oracle database

Encryption

- Application to database encryption
- Database to storage encryption

Security of on-premises cloud infrastructure

- Housed inside the customer's data center
- Remotely managed by Oracle
- Data remains on the customer's premises

2 Unified security control

Oracle's customers, such as your organization, control access to and use of your own applications, workloads, and data. Dedicated Region Cloud@Customer, like other regions of OCI, provides authentication and authorization services such as OCI Identity and Access Management for all OCI resources and services. You can use a single tenancy on Dedicated Region Cloud@Customer shared by your various business units, teams, and individuals while maintaining security, isolation, and governance.

> Oracle Data Safe offers a unified security control center that helps you quickly understand the security of your databases with security assessments, user risk assessments, activity auditing, sensitive data discovery, and data masking that provides automated risk alerts that may require attention.

> OCI Identity and Access Management helps IT organizations ensure that sensitive application data isn't viewed by unauthorized users while Oracle Database Vault implements security controls that help enable database administrators to perform necessary maintenance and administrative tasks without accessing the data itself.

> Oracle Advanced Security provides Transparent Data Encryption (TDE) of data at rest as well as the ability to redact sensitive data entirely.

Oracle helps organizations reduce risk with an expanded set of security offerings that are simple, integrated, and economically attractive.

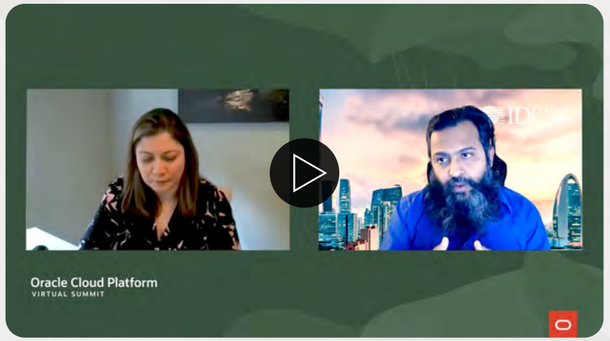
3 Meet data residency requirements

You want to know precisely where your data is stored and take the necessary steps to help ensure that you comply with regulatory compliance requirements that govern your organization. You also seek a cloud provider that offers tools to help implement and monitor security controls and has protocols to follow in case of a data breach or in the case of data disposal. This is where a choice of cloud technology and cloud service provider can make a huge difference in the life of a business—and their data.

With Dedicated Region Cloud@Customer, Oracle goes further than other cloud providers by providing the same database capabilities in the cloud, on-premises, or in hybrid environments. By using the same Autonomous Database and Exadata capabilities in Oracle Cloud Infrastructure public cloud regions and Cloud@Customer deployments in customer data centers, organizations can develop databases and applications in one location and deploy them everywhere they're needed—especially when data residency or security is a concern.

Dedicated Region Cloud@Customer helps your IT department implement additional isolation controls to guard data and workloads. It is a self-contained region where customer data, including API operations and metadata, remain local to the region.

Oracle manages and monitors Dedicated Region Cloud@Customer in the same manner as the other regions of Oracle Cloud Infrastructure, so you can have a consistent experience across both. It helps organizations such as yours with their obligations to data residency rules, regulations, and laws.



"This is a major step toward enabling more choice for government to access world-leading cloud services in a data centre managed by a 100% Australian sovereign company focused on connectivity, security, and simplified deployment."

Rob Kelly, Managing Director, Australian Data Centres

Watch the video

4 Automated end-to-end encryption

With Oracle Dedicated Region Cloud@Customer, data is encrypted at rest and in transit with Oracle-managed encryption and the keys are protected through the Oracle Cloud Infrastructure Vault service.

AT-REST DATA

All data at rest is encrypted by Oracle by default in Dedicated Region Cloud@Customer. Your IT department can also choose to control its own keys by using the Vault service to create and manage those keys. If you have an external key management system, keys can be imported and generated keys can be used in OCI Vault to secure data at rest in the dedicated region.

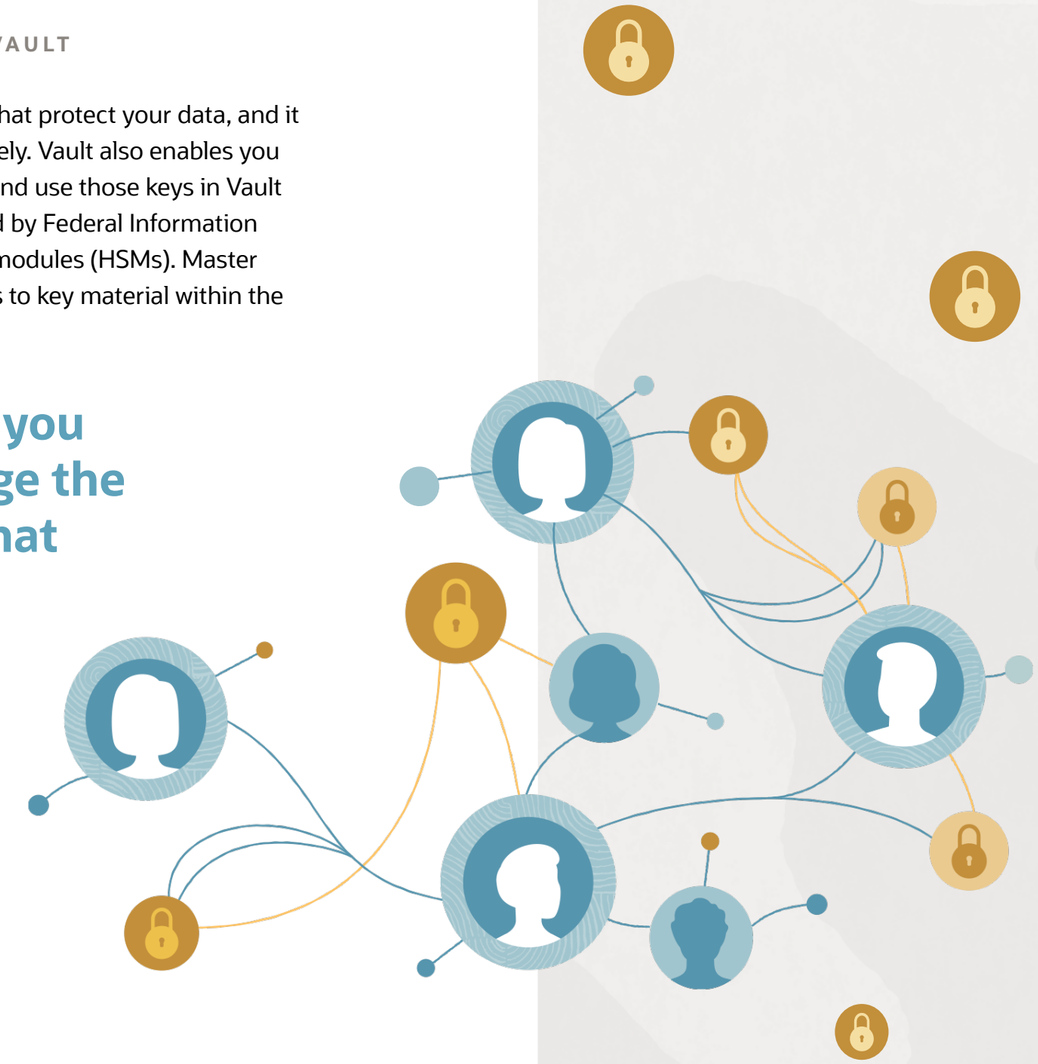
IN-TRANSIT DATA ENCRYPTION

Data in motion between your compute instances and Dedicated Region Cloud@Customer cloud services is also encrypted, as are all OCI APIs and OCI Object Storage traffic. Encryption of traffic for boot and block volumes is supported for Oracle-supplied images, and OCI provides a client for wrapping Network File System traffic to and from File Storage with Transport Layer Security 1.2. Your IT department can also control the data in motion between your compute instances, to and from bare metal and VM databases, and for data destined outside Dedicated Region Cloud@Customer.

ENCRYPTION KEY AND SECRETS MANAGEMENT IN VAULT

OCI Vault enables you to centrally manage the encryption keys that protect your data, and it helps manage the credentials you use to access resources securely. Vault also enables you to bring your own keys from another key management system and use those keys in Vault to help protect your data in the dedicated region. Vault is backed by Federal Information Processing Standards 140-2 Level 3 certified hardware security modules (HSMs). Master encryption keys never leave the HSMs, and Oracle has no access to key material within the Vault service.

OCI Vault enables you to centrally manage the encryption keys that protect your data



5 Get started with Oracle at your data center

Dedicated Region Cloud@Customer brings the benefits of a public cloud to your data center. That includes automated security that helps reduce risks, manages access, and monitors activity with a unified platform.

The security controls that are available in Oracle Cloud Infrastructure commercial regions can now be contained in your data center with Dedicated Region Cloud@Customer, which includes tools you use to help manage your cloud security posture by uncovering vulnerabilities, addressing threats, and remediating security misconfigurations.

Discover how Oracle brings the public cloud security to data centers

Learn more | Start for free

ORACLE