ORACLE

Oracle Cloud Infrastructure Security Architecture

May 2024, Version 3.0

Public

ORACLE

Purpose Statement

This document provides an overview of features and enhancements included in Oracle Cloud Infrastructure (OCI). It's intended solely to help you assess the business benefits of OCI and to plan your IT projects.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Revision History

The following revisions have been made to this document.

DATE	REVISION
May 2024	• Removed references to first and second generations of public cloud • Updated figures 1, 3, and 4. Deleted figure 2 (RoT)
September 2021	Added information about OCI Dedicated Region
March 2020	Initial publication

ORACLE

Table of Contents

Overview

Oracle Cloud Infrastructure (OCI) is an infrastructure-as-a-service (IaaS) offering architected on security-first design principles. These principles include isolated network virtualization and reproducible known-good-state physical host deployment, which significantly reduce risk from advanced persistent threats.

OCI benefits from tiered defenses and highly secure operations that span all layers in the infrastructure stack, from physical hardware to the web layer, in addition to the protections and controls available in our cloud. Many of these protections should also work with third-party clouds and on-premises solutions to help secure modern enterprise workloads and data where they reside.

This document describes how OCI's features help to address the security requirements of customers who run critical and sensitive workloads. It details how security is fundamental to the architecture, data center design, personnel selection, and processes for provisioning, using, certifying, and maintaining OCI.

Security-First Design

As cloud adoption has increased, so has the incentive for bad actors and the corresponding need for a greater focus on security. From its inception, OCI has been able to build on the learnings of security issues identified in first-generation clouds.

Oracle Public Cloud

OCI is a complete IaaS platform. It provides the services needed to build and run applications in a highly secure, hosted environment with high performance and availability. Customers can run the Compute and Database services on bare metal instances, which are customer-dedicated physical servers, or as virtual machines (VM) instances, which are isolated compute environments on top of bare metal hardware. Bare metal and VM instances run on the same types of server hardware, firmware, underlying software, and networking infrastructure, so both instance types have the OCI protections built into those layers.

Dedicated Realms

With OCI Dedicated Region and Oracle Alloy, Oracle offers dedicated realms, which are cloud regions that bring all of Oracle's cloud services to data centers chosen by customers or Alloy partners. Oracle delivers these dedicated realms to help address local data compliance and regulatory requirements. Under this model, customer data is kept at the local sites to help customer address latency and data residency requirements. Oracle builds dedicated realms with the same security-first design principles as the rest of OCI.

Platform Security

OCI platform security has several key architecture features, including isolated network virtualization, secure firmware installation, and hardware root of trust.

Isolated Network Virtualization

The hypervisor is the software that manages virtual devices in a cloud environment, handling server and network virtualization. In traditional virtualization environments, the hypervisor manages network traffic, enabling traffic to flow between VM instances and physical hosts. This traffic flow adds considerable complexity and computational overhead to the hypervisor. Proof-of-concept computer security attacks that demonstrate escaping hypervisor isolation have highlighted the substantial risk that can come with this design. These attacks exploit hypervisor complexity by enabling an attacker to "break out" of a VM instance, access the underlying operating system, and gain

control of the hypervisor and embedded network virtualization. The attacker can then potentially alter the network configuration to access other hosts.

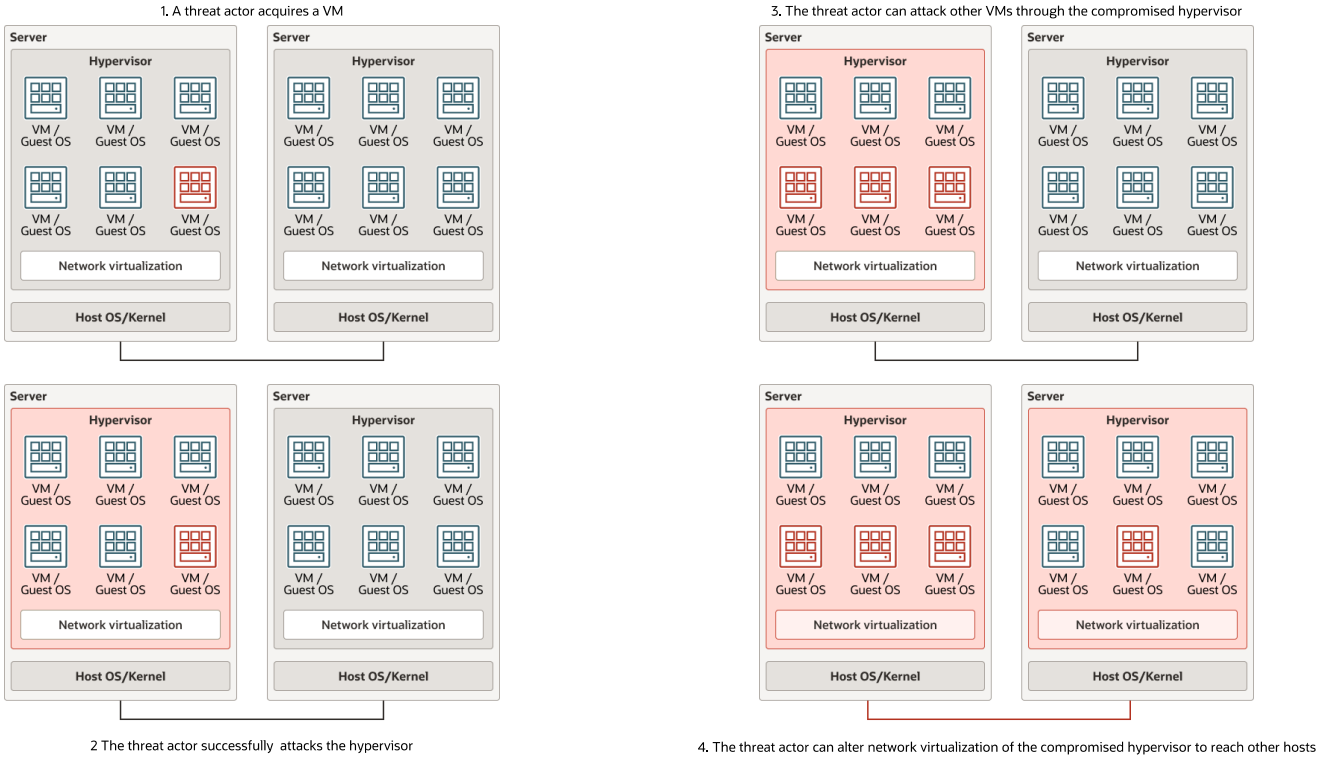

Figure 1: A VM Escape Attack on a Single Host Spreading to Other VMs

OCI reduces threat proliferation between hosts by implementing network virtualization outside the hypervisor. Even if a bad actor escapes a VM and compromises the hypervisor, they will not be able to reconfigure the network virtualization, limiting lateral movement to other hosts.

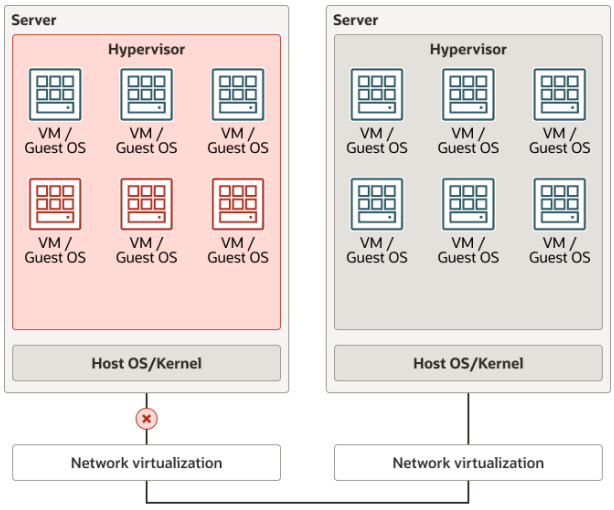

Figure 2: Isolated Network Virtualization Reduces Risk of Lateral Threat Proliferation in OCI

OCI's physical network architecture adds a layer of defense to the network virtualization by further isolating customer tenancies and limiting the risk of lateral threat proliferation. The physical network components are the racks, routers, and switches that form the physical layer of OCI.

Access control lists (ACLs) are enforced for the top-of-rack (ToR) switches. ACLs enforce adherence to the communications pathways within the topology. For example, the ToR switch drops any packet in which the virtual network source IP address and its corresponding physical network port don't match the expected mapping. This mismatch occurs if an attacker spoofs the virtual source IP address to pretend to be a legitimate traffic source to reach other tenants. Oracle designed the ACLs to help prevent IP spoofing by associating the expected IP addresses for an isolated network virtualization device with the physical ports that the device is connected to. In addition, the destination device performs a reverse-path check on packets to address encapsulation header tampering.

The design of the physical layer is a simple, flat network connected to virtual ports on the virtual cloud network (VCN). This design reduces the complexity of managing allowed traffic paths and heightens the visibility of attempts to circumvent them.

Hardware

A primary design principle of OCI is protecting tenants from firmware-based attacks. Threats at the firmware level are becoming more common, which raises the potential risks for public cloud providers. To ensure that each server is provisioned with clean firmware, Oracle has designed, built, and implemented a hardware root-of-trust for the process of wiping and reinstalling server firmware. Oracle uses this process every time a new server is provisioned for a tenant or between tenancies, regardless of the instance type.

The hardware root-of-trust is a protected hardware component that's manufactured to Oracle's specifications. It's limited to performing the specific task of wiping and reinstalling firmware. It triggers a power cycle of the hardware host, prompts for the installation of known firmware, and confirms that the process has been completed as expected. This method of firmware installation tends to reduce the risk of firmware-based attacks, such as a permanent denial of service (PDoS) attack or attempts to embed backdoors in the firmware to steal data or make it otherwise unavailable. In addition, internal servers are configured to use secure boot.

Network Segmentation

OCI network design is segmented to provide customer and service isolation. These network segments each have a unique communications profile with access into and out of these segments controlled, monitored, and policy driven.

The public edge network contains bastions, service endpoints, network devices, and the gateways and proxies from private networks and VCNs.

The private network is segmented into a core service enclave, the overlay enclave, and Integrated Lights Out Manager (ILOM) network. An enclave is a network segment with a specific security profile and controls—physical or logical.

The core service enclave hosts services like Networking, Identity and Access Management (IAM), Block Volumes, Load Balancing, Key Management, Host Management, Security services, and Audit. These services are provisioned in separate, isolated tenancies with unique communications profiles. To access the Core service enclave, Oracle personnel must have explicit user privileges granted by authorized persons. This access is subject to regular auditing and review. Service enclaves are local to a region, so any necessary traffic between them goes through the same security mechanisms as internet traffic, including inbound SSH bastion hosts and outbound HTTPS proxies.

The overlay enclave hosts customer virtual networks, Compute instances, and many other OCI services that are built using the same IaaS and platform-as-a-service (PaaS) foundational services that customers consume. Communication from the overlay to core is limited by narrow ACLs.

ILOM is used to power cycle Compute hosts, invoke root-of-trust card actions, and configure network virtualization. Direct communication with other hosts is prohibited. The ILOM network accepts command messages only from the core services enclave.

Communication between segments is tightly controlled at the physical layer both for human access and services communicating across segments. Oracle personnel who need to access the region to make service updates require explicit user privileges granted by authorized persons. This access is subject to regular auditing and review.

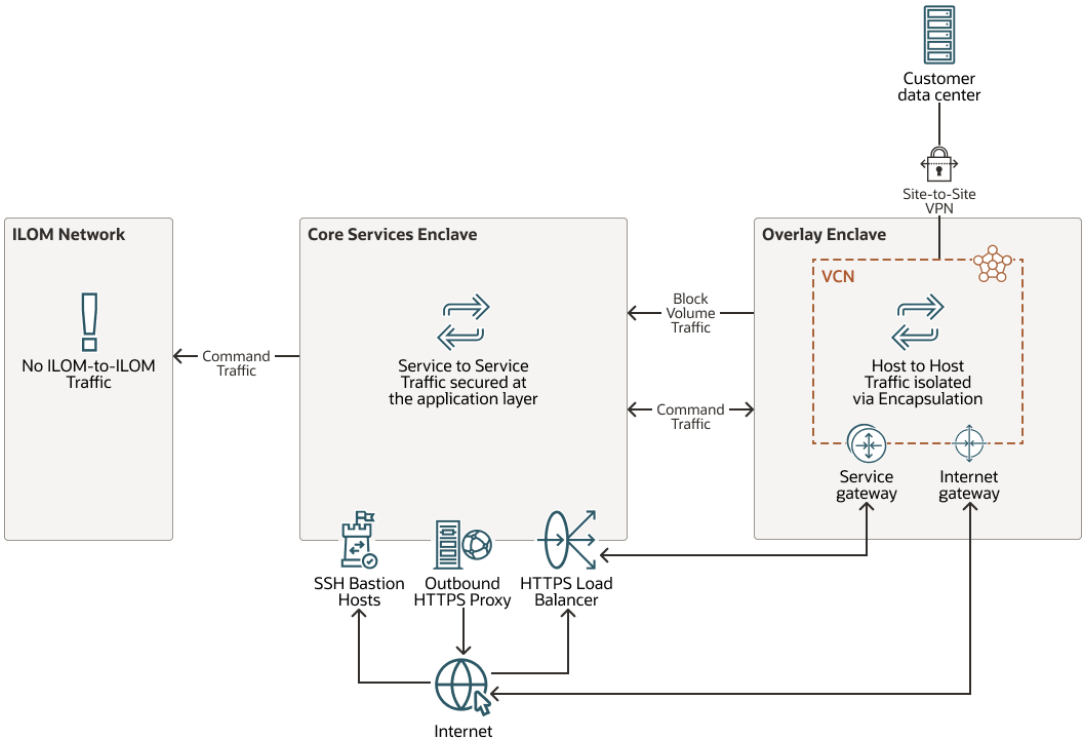

Figure 3: Network Segmentation Isolates Customer Resources and Services

Physical Security

OCI undergoes a risk assessment process to evaluate potential data centers and provider locations. This process considers factors such as environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions, and geopolitical considerations.

Data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow an N2 redundancy methodology for critical equipment operation. Data centers that house OCI services are required to use redundant power sources and maintain generator backups. Oracle monitors server rooms closely for air temperature and humidity and ensures that fire suppression systems are in place. Oracle trains data center staff in event handling, incident response, and escalation procedures to address security or availability events.

Oracle's layered approach to the physical security of data centers starts with the building itself. The company builds and works with partners to build data center facilities durably with steel, concrete, or comparable materials, and that are designed to withstand impact from light-vehicle strikes.

The data centers use perimeter barriers to secure site exteriors, and security guards and cameras monitor vehicle checks. Every person who enters a data center must pass through security checkpoints at the site entrances. Anyone who doesn't have a site-specific security badge must present government-issued identification and have an approved request that grants them access to the building. All employees and visitors must always wear visible official identification badges. All sites are staffed with security guards.

Extra security layers between the site entrance and the server rooms vary depending on the building and risk profile. Server rooms themselves are required to have more security layers, including cameras, two-factor access control, and intrusion-detection mechanisms. Physical barriers that span from the floor to the ceiling create isolated security zones around server and networking racks. These barriers extend below the raised floor and above the ceiling tiles, where applicable. All access to server rooms must be approved by authorized personnel and is granted only for the necessary time. Access is audited, and access provisioned within the system is reviewed periodically and updated as required.

Secure Connectivity

Oracle controls and protects connectivity to resources within OCI and between OCI and customers' on-premises data centers.

Least-Privilege Access

Unnecessary permissions can pose a significant risk. Attackers can gain access to credentials and then use them to move throughout a system. To help guarding against overprivileged permission, Oracle uses the principle of *least-privilege access* when granting access to production systems. Access in integrated into Oracle's corporate access control systems. Oracle periodically reviews the approved lists of service team members, and revokes access if there is no justifiable need for access.

Access to production systems requires multifactor authentication (MFA). The security team grants MFA tokens and disables the tokens of inactive members. Oracle logs all access to production systems, and the logs are kept for security analysis.

Multiple Authentication Layers

Weak account credentials also pose a significant threat to cloud environments. To strengthen authentication, Oracle uses several layers of advanced access control to limit access to network devices and the servers that support them. One of those layers is compulsory virtual private network (VPN) connectivity to the production network. This VPN requires high password diversity and the use of Universal 2nd Factor (U2F) authentication, an open standard for strengthening and simplifying two-factor authentication by using a hardware key. All administrative access is logged, and all access permissions are audited for least privilege. By using multiple factors for authentication, Oracle helps prevent an attacker from accessing the administrative network with weak or breached passwords.

Internal Connectivity

OCI availability domains and regions help to protect data privacy for cloud network traffic transiting to other OCI data centers. This protection is enabled by private, dedicated wide-area network (WAN) fiber-optic connections that are protected further by MACsec (IEEE 802.1AE) encryption.

External Connectivity

Customers often require connectivity from their OCI tenancy to their campus, private data center, or other clouds. Oracle provides the following methods to securely connect OCI to private VCNs and non-VCN networks:

- **Site-to-Site VPN**: A dedicated, encrypted tunnel that can be routed over the public internet.
- **FastConnect**: A private, dedicated, high-speed WAN connection with an optional IPsec VPN tunnel.

Operational Security

Oracle maintains a large workforce of security professionals, who are dedicated to ensuring the security of OCI. Within the workforce, several teams are responsible for securely developing, monitoring, testing, and seeks to assure compliance with regulations and certification programs.

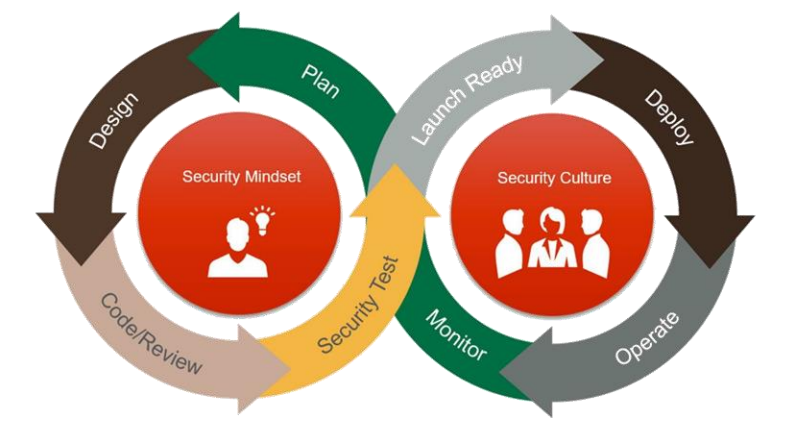

Figure 4: Operational Security Flow in OCI

Defensive Security

In all computing environments, daily attacks can occur against networking and compute infrastructure. At OCI, a dedicated team of defensive experts and analysts—the *defensive security team*—monitors and responds to these events. The members of this team are the first responders of cloud security. They work proactively and continuously to spot potential threats within OCI, and they shut down exploit paths within the OCI service enclaves. When the team detects incidents, they work to remediate them promptly by using modern security operations methodologies and developer security operations (DevSecOps)-enabled configuration and tooling.

This team doesn't monitor threats within the customer's tenancy. Customers are responsible for monitoring their tenancies for indicators of compromise and addressing their security events.

Offensive Security

After new capabilities of OCI security architecture are developed or modified, the *offensive security team* verifies that they meet security benchmarks. This team works to understand and emulate the methods used by attackers, including sophisticated bad actors and nation-states. This work involves research, penetration testing, and simulating advanced threats against Oracle hardware and software. This team informs secure development, secure architecture, and defensive capabilities.

Security Assurance

Oracle develops and implements security plans with high-security standards that tends to align with existing Oracle and industry standards. To assure the security of the cloud platform, the *security assurance group* works collaboratively with service teams and security and risk stakeholders throughout Oracle to develop and deploy security controls, technologies, processes, and guidance for the teams that build and operate OCI and the teams that build *on* OCI.

Data and Application Protection

Oracle designed the OCI data handling and management practices to help customers configure their data and provide the tools to help them protect their data and applications from outside threats.

Data Access

In its interactions with customers, Oracle defines the following categories of data:

- **Data about customers**: The contact and related information needed to operate an OCI account and bill for services. The use of any personal information that Oracle gathers for purposes of account management is governed by the Oracle General Privacy Policy.
- **Data stored by customers**: The data that customers store in OCI, such as files, documents, and databases. Oracle's handling of this data is described by the Oracle Services Privacy Policy and the Data Processing Agreement for Oracle Services.

Data Destruction

Oracle uses physical destruction and logical data erasure processes so that data doesn't persist in decommissioned hardware.

Storage Media Destruction

Oracle Asset Management requirements explicitly prohibit the removal of storage media that contains customer data from the data hall in which it's stored. Each data hall in a data center contains a secure media disposal bin. When a hard disk or other storage media is faulty or removed from production for disposal, it's placed in this secure bin for storage until it's degaussed and shredded.

Data Erasure

When a customer releases a VM instance, an API call starts the workflow to delete the instance. When a new bare metal Compute instance is added to the service or is released by a customer or service, the hardware goes through the provisioning workflow before it's released to inventory for reassignment. This automated workflow discovers the physical media connected to the host. Then, the workflow initiates secure erasure by running the applicable erasure command for the media type.

Hosts intended for customer use also have a network-attached disk that's used to cache the customer's storage volume. This disk is erased using the AT Attachment (ATA) security erase command. When the erasure process is complete, the workflow starts a process to flash the BIOS, update drivers, and return the hardware to a known good state. The workflow also tests the hardware for faults. If the workflow fails or detects a fault, it flags the host for further investigation.

When a customer terminates a block storage volume, the key is irrevocably deleted, which renders the data permanently inaccessible.

Data Encryption

OCI has a "ubiquitous encryption" program that requires teams encrypt all data at rest and in transit, including customer tenant data. Oracle uses encryption at rest and in transit. The Block Volume and Object Storage services enable at-rest data encryption by default by using the Advanced Encryption Standard (AES) algorithm with 256-bit encryption. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later.

API Security

In modern cloud environments, APIs are critical to application function. However, they also can create broader attack surfaces. Oracle recognizes the importance of API security for applications in cloud environments and has developed the API Gateway service to provide that security.

API Gateway is a fully managed regional service that integrates with customers' networks on OCI. API gateways enable customers to publish public or private APIs, process incoming requests from a client, and help to apply policies for security, availability, and validation. API gateways also forward requests to backend services, apply policies to the responses from the backend services, and then forward the responses to the client. API gateways protect and isolate backend services and help customers meter API calls.

Connections from clients to API gateways always use TLS to help preserving the confidentiality and integrity of data. Customers can also configure the connections from API gateways to backend services to use TLS.

Culture of Trust and Compliance

The broader culture of trust and compliance at Oracle informs all practices in OCI.

Development Security

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, test, and maintenance phases of its products, whether they're used on-premises by customers or delivered through OCI. Oracle's goal is to help customers meet their security requirements, while providing a cost-effective ownership experience. The industry-leading standards, technologies, and practices in OSSA have the following goals:

- **Foster security innovations**: Oracle's long tradition of security innovations continues with solutions that help enabling organizations to implement and manage consistent security policies across the hybrid cloud data center. These solutions include database security and identity management, and security monitoring and analytics.
- **Reduce security weaknesses in all Oracle products**: OSSA programs include Oracle's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools.
- **Reduce the impact of security weaknesses in released products**: Oracle has adopted transparent policies for security vulnerability disclosure and remediation. Oracle is committed to treating all customers equally and delivering a positive security patching experience through our Critical Patch Update and Security Alert programs.

Personnel Security

Oracle strives to hire the best candidates and develop its employees. Oracle provides baseline security training for all employees and specialized training opportunities to learn the latest security technologies, exploits, and methodologies. The company provides standard corporate training programs that cover information security and privacy. Oracle also engages with various industry groups and sends employees to specialist conferences to collaborate with other industry experts on emerging challenges. The objectives of Oracle's security training programs are to help employees protect customers and products, to enable employees to learn more about security areas they're interested in and to further the mission to attract and retain the best talent.

Oracle also strives to hire people with strong ethics and good judgment. All employees undergo preemployment screening as permitted by law, including criminal background checks and previous employment validation in accordance with in-country hiring rules. Oracle maintains performance-evaluation processes to recognize good performance and identify opportunities for growth. Oracle uses security as a component of the team-evaluation processes. This approach gives the company visibility into how teams are performing against Oracle's security standards and helps identify best practices and improvement areas for critical security processes.

Supply-Chain Security

Oracle has a long history of developing enterprise-class secure hardware. The Hardware Security team designs and tests the security of the hardware that's used to deliver OCI services. This team works with supply chains and validates hardware components against Oracle's rigorous hardware security standards.

Compliance

Oracle continues to invest in services that help customers more easily address their security and compliance needs. Independent assurance promotes trust and builds confidence in third-party service provider relationships. To gain this trust and confidence, Oracle has many recurring programs that help maintaining compliance with global, regional, and industry-specific certifications and publish reports that attest to that compliance. These reports can play an important role in customers' internal corporate governance, risk management processes, vendor management programs, and regulatory oversight. Further, enabled by cloud native DevOps technologies, Oracle can unify service compliance for regions around the world by using automation for service deployment.

Auditing

Oracle regularly performs penetration testing, vulnerability testing, and security assessments against OCI, platforms, and applications. These tests are intended to validate and improve the overall security of OCI services.

Oracle engages independent auditors and assessors to test and provide opinions about security, confidentiality, and availability controls that are relevant to international data protection laws, regulations, and industry standards.

Oracle also permits customers to conduct their own or third-party testing of their tenancy, as outlined in the Cloud Security Testing Policy.

Conclusion

OCI puts the security of critical workloads at the center of our next-generation public cloud. For customers running security-sensitive workloads, such as financial applications or citizen service applications, OCI provides a security-first architecture that reduces the risk and attack surfaces commonly associated with first-generation clouds. Oracle has built security features and controls into the architecture, data center design, personnel selection, and the processes for provisioning, using, certifying, and maintaining OCI. Oracle Cloud Infrastructure is a modern public cloud built for the world's most critical data with the highest security requirements.

References

- Oracle Corporate Security Practices
- Oracle Cloud Compliance
- Oracle Software Security Assurance (OSSA)
- Oracle Security Testing Policy
- More information about Oracle Cloud Infrastructure Security

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle