Oracle Cloud Infrastructure Security Architecture

March 5, 2020

DISCLAIMER

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, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

REVISION HISTORY

The following revisions have been made to this white paper:

DATE	REVISION
March 5, 2020	Initial publication

TABLE OF CONTENTS

OVERVIEW

Oracle Cloud Infrastructure is a second-generation infrastructure-as-a-service (IaaS) offering architected on security-first design principles. These principles include isolated network virtualization and pristine physical host deployment, which provide superior customer isolation compared to earlier public cloud designs and reduced risk from advanced persistent threats.

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

This paper describes how Oracle Cloud Infrastructure meets the security requirements of enterprises and 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 Oracle Cloud Infrastructure.

SECURITY-FIRST DESIGN

As cloud has become more common, security concerns have become more important. From its inception, Oracle Cloud Infrastructure prioritized solving the security issues that grew out of first-generation clouds.

First-Generation Public Clouds

First-generation public clouds focused on the efficient use of hardware resources enabled by virtualization and use of a hypervisor. These clouds were built on many of the same technologies and principles used in private clouds, which were designed so that expensive hardware resources didn't remain idle. Security sometimes wasn't a foundational principle of this design because private data centers relied on perimeter defenses. As public cloud use became more common, so did concerns about vulnerabilities associated with hypervisor-based attacks. Security is a primary concern for enterprise customers, and the risk associated with the hypervisor design of first-generation public clouds was only growing.

Oracle Cloud Infrastructure—Second-Generation Public Cloud

The founding team of Oracle Cloud Infrastructure was tasked with designing a security-first public cloud that could earn the trust of enterprises and customers with critical workloads. *Security-first* means that we redesigned the virtualization stack to reduce the risk from hypervisor-based attacks and increase tenant isolation. This design helps protect tenants from each other and also from the cloud provider. The result is a second-generation, or *Generation 2*, public cloud design that's a significant improvement over first-generation public clouds. We've implemented this Generation 2 design across Oracle Cloud Infrastructure, in every data center and region.

Oracle Cloud Infrastructure is a complete IaaS platform. It provides the services needed to build and run applications in a highly secure, hosted environment with best-in-class performance and availability. You 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 computing 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 Oracle Cloud Infrastructure protections built in to those layers.

PLATFORM SECURITY

The Oracle Cloud Infrastructure architecture was designed for security of the platform through isolated network virtualization, highly secure firmware installation, a controlled physical network, and network segmentation.

Isolated Network Virtualization

Central to the Oracle Cloud Infrastructure design is *isolated network virtualization*, which greatly reduces the risk from the hypervisor.

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 it to flow between VM instances and between VM instances and physical hosts. This adds considerable complexity and computational overhead in the hypervisor. Proof-of-concept computer security attacks, such as virtual machine escape attacks, 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. The attacker can then access other hosts, sometimes undetected.

Oracle Cloud Infrastructure reduces this risk by decoupling network virtualization from the hypervisor. We’ve implemented network virtualization as a highly customized hardware and software layer that moves cloud control away from the hypervisor and host, and puts it on its own network. This hardened and monitored layer of control is what enables isolated network virtualization.

Isolated network virtualization reduces risk by limiting the attack surface. Even if a malicious actor succeeds with a VM escape attack on a single host, it’s designed so they can’t reach other hosts in the cloud infrastructure. The attack is effectively contained to the one host. Isolated network virtualization is implemented in every data center in every region, which means that all Oracle Cloud Infrastructure tenants benefit from this reduced risk.

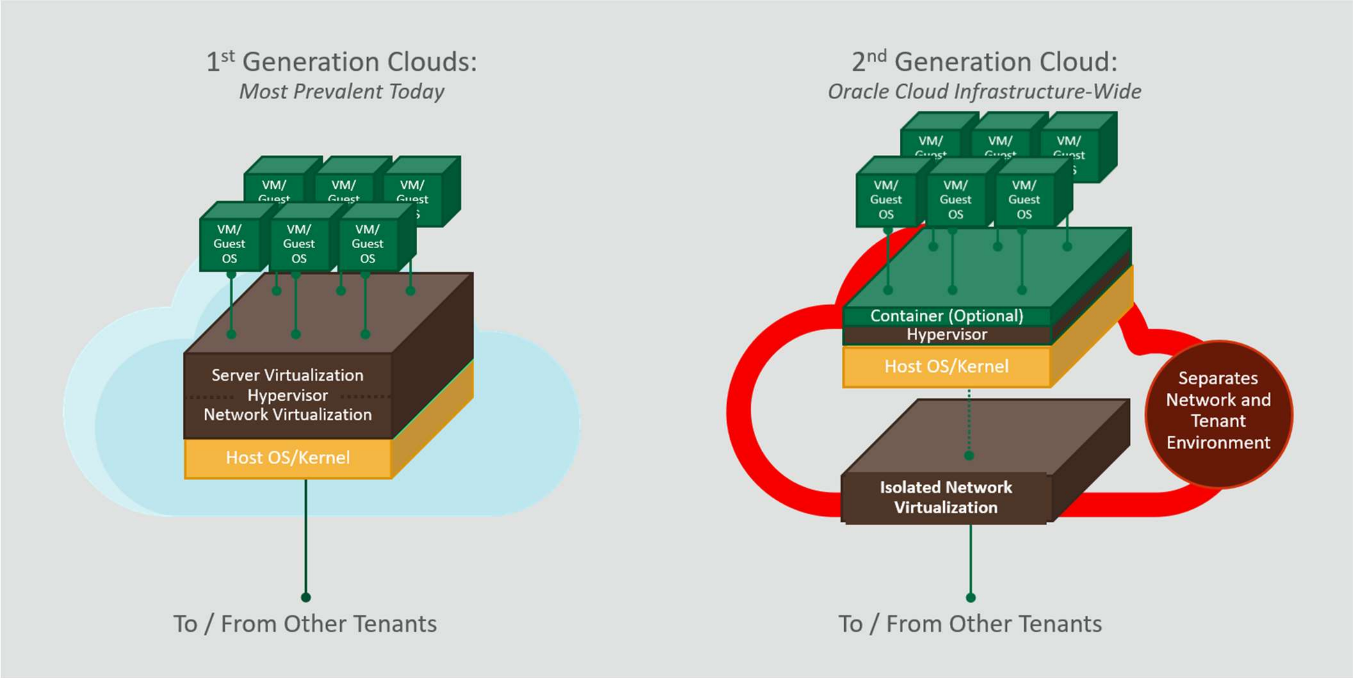

Figure 1. Isolated Network Virtualization Reduces Risk in the Oracle Generation 2 Cloud

Hardware

A primary design principle of Oracle Cloud Infrastructure is protecting tenants from firmware-based attacks. Threats from the firmware level are becoming more common, which raises the potential risks for public cloud providers. So that each server is provisioned with clean firmware, we've implemented a *hardware-based root of trust* for the process of wiping and reinstalling the server firmware. We use this process every time a new server is provisioned for a tenant or between tenancies, regardless of the instance type.

The hardware-based root of trust is a protected hardware component that's manufactured to our specification and inspected visually. 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 performed as expected. This method of firmware installation reduces the risk from 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.

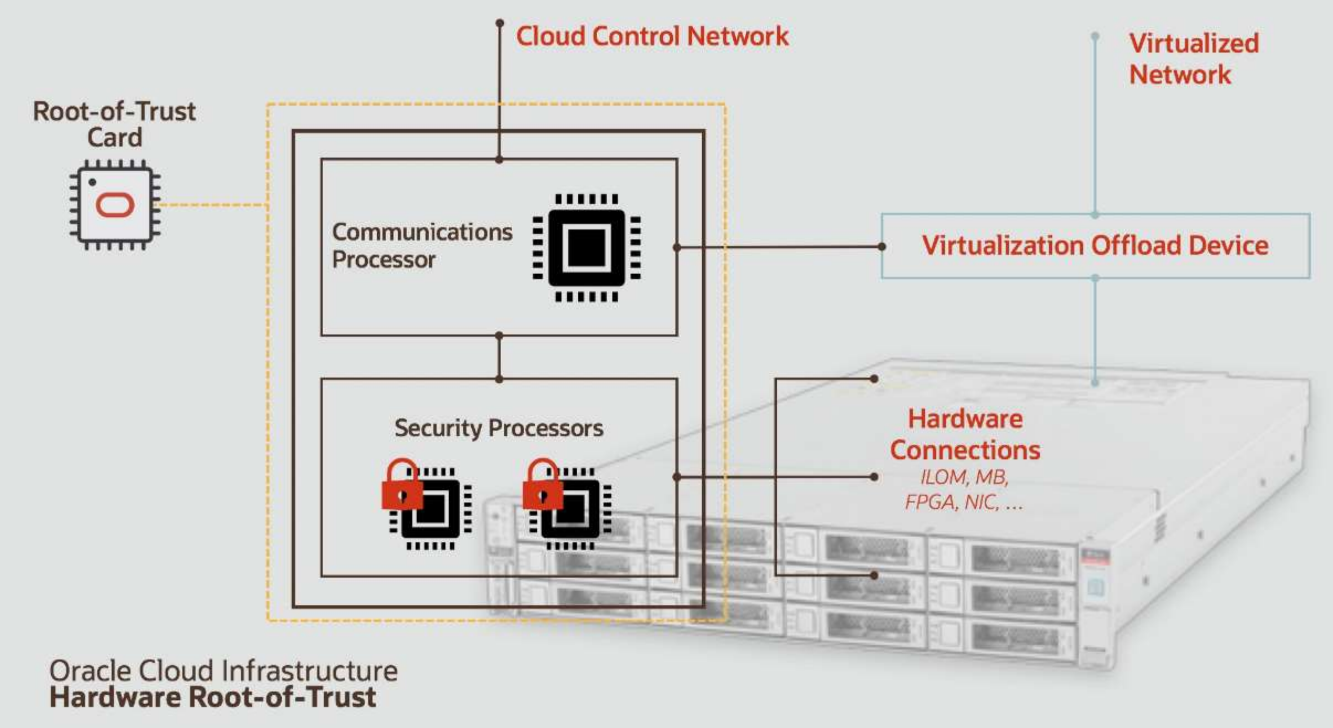

Figure 2. Hardware-Based Root of Trust Design for Firmware Installation

Physical Network

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

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 would occur if an attacker spoofed the virtual source IP address, to pretend to be a legitimate traffic source to reach other tenants. The ACLs are designed to 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. Additionally, the destination device performs a reverse-path check on packets to prevent 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.

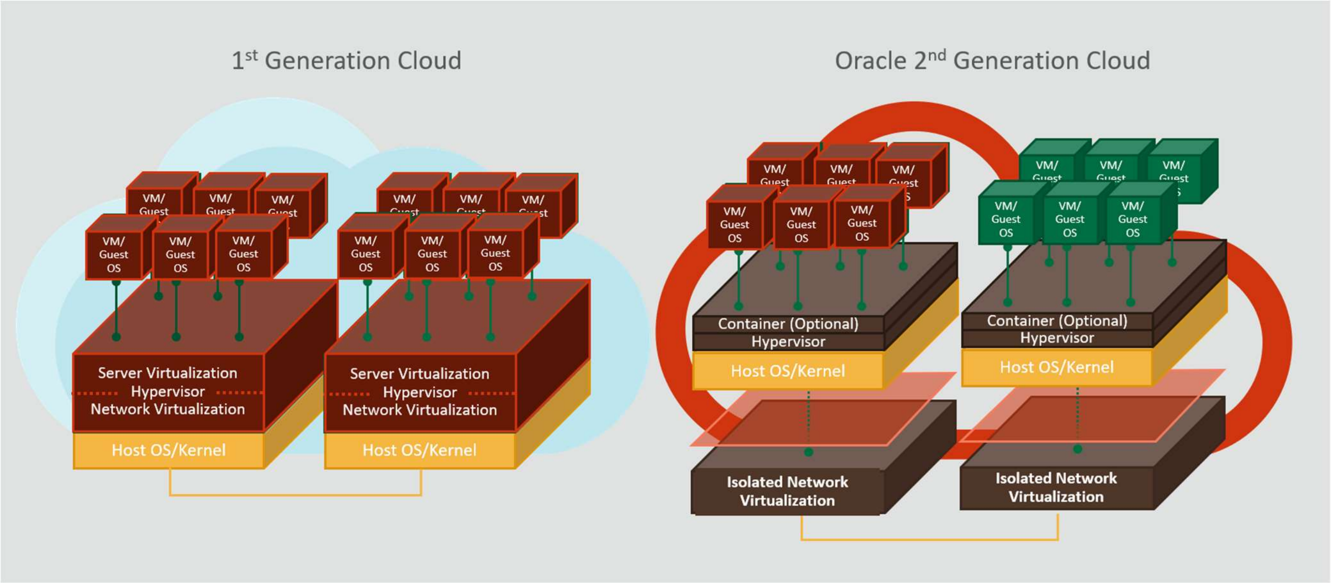

Figure 3: A Simple, Flat Network Design Protects the Generation 2 Cloud

Network Segmentation

Oracle Cloud Infrastructure's physical network is designed for customer and service isolation. It’s segmented into *enclaves* with unique communications profiles. Access into and out of these enclaves is controlled, monitored, and policy driven.

Compute hosts are power-cycled by an Integrated Lights Out Manager (ILOM). Each host has one ILOM, and direct communication with other hosts is prohibited. The ILOM network accepts command messages only from the *services enclave*, which is where the core Oracle Cloud Infrastructure services are provisioned. These services include Networking, Identity & Access Management (IAM), Block Volumes, Load Balancing, and Audit. Oracle personnel must have explicit user privileges, granted by authorized persons, to access the services enclave. 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 (inbound SSH bastion hosts and outbound SSL proxies) as internet traffic.

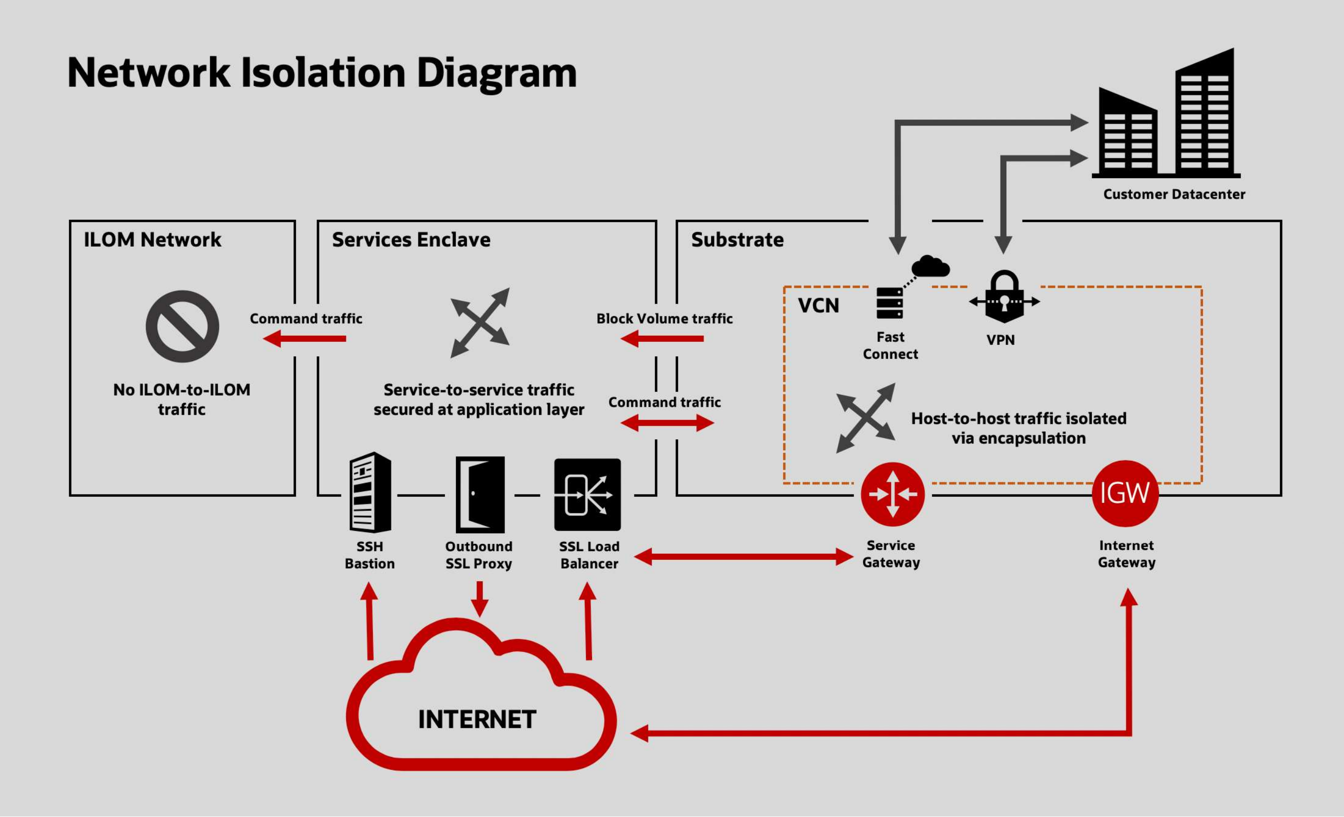

Figure 4. Network Segmentation Isolates Customer Resources and Services

FAULT-TOLERANT INFRASTRUCTURE

Oracle Cloud Infrastructure is organized by regions, which are built within a certain geography and include one or three availability domains. Whether your instances reside in a region with one availability domain or multiple availability domains, numerous layers of redundancy are available for data and service resiliency and backup.

Fault tolerance is implemented in the service architecture and in how data is stored. Services and data span racks of hardware, which themselves include multiple layers of redundancy at the node, server, and hardware component level. Connectivity and edge services link each region with other regions and with peering networks and customer data centers.

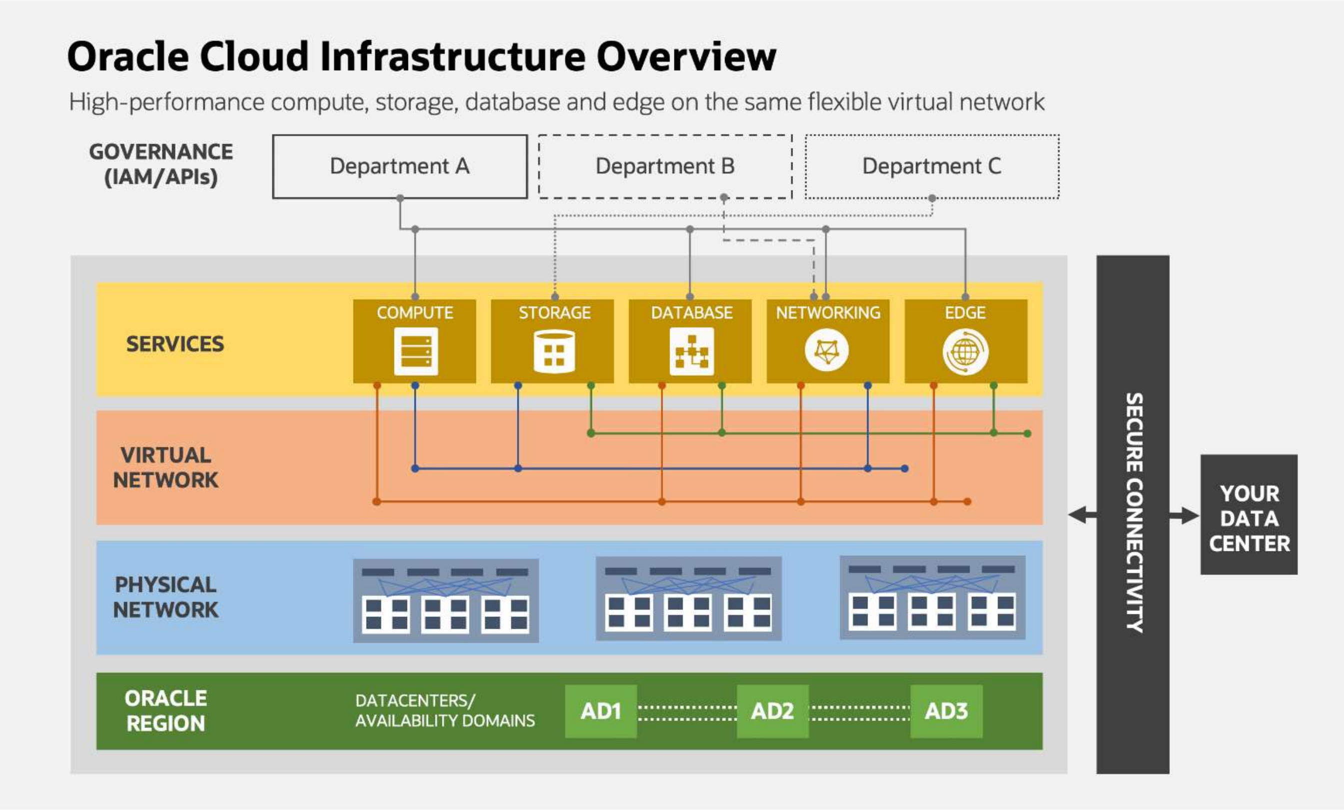

Figure 5. Fault-Tolerant Design Within Oracle Cloud Infrastructure Regions

PHYSICAL SECURITY

Sites that are candidates for Oracle Cloud Infrastructure data centers and provider locations undergo an extensive risk-evaluation process. 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 Oracle Cloud Infrastructure services are required to use redundant power sources and maintain generator backups. Server rooms are closely monitored for air temperature and humidity, and fire suppression systems are in place. Data center staff are trained in incident response and escalation procedures to address any security or availability events.

Our layered approach to the physical security of data centers starts with the building itself. Data center facilities are durably built with steel, concrete, or comparable materials and 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.

Additional 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 period. Access usage is audited, and access provisioned within the system is periodically reviewed and updated as required.

SECURE CONNECTIVITY

Least-Privilege Access

Unnecessary or out-of-date permissions pose a significant threat. Attackers can gain access to them and use them to move throughout a system. To reduce the risk from overly permissioned users or applications, we use the principle of *least-privilege access* when granting access to production systems. We periodically review the approved lists of service team members, and revoke access if no justifiable need for access exists.

Access to production systems requires multifactor authentication (MFA). The Security team grants MFA tokens and disables the tokens of inactive members. All access to production systems is logged, 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, we use several layers of advanced access control to meter access to network devices and the servers that support those resources. 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, we help prevent an attacker from accessing the administrative network with weak or breached passwords.

Internal Connectivity

Oracle Cloud Infrastructure availability domains and regions enable data privacy for cloud network traffic transiting to other Oracle Cloud Infrastructure data centers. This privacy is enabled by private, dedicated wide-area network (WAN) fiber optic connections, which are further protected by MACSec (802.1AE) encryption. MACSec is a high-speed, Layer 2 network encryption protocol that encrypts other non-IP Layer 3 protocol traffic such as DNS and ICMP that might not be covered by traditional Layer 3 encryption.

External Connectivity

Customers often require connectivity from their Oracle Cloud Infrastructure tenancy to their campus, private data center, or other clouds. We provide two ways to securely connect Oracle Cloud Infrastructure to non-VCN networks:

- IPSec VPN, a dedicated encrypted tunnel that can be routed over the general internet
- FastConnect, a private, dedicated high-speed WAN connection, with an optional IPSec VPN tunnel

OPERATIONAL SECURITY

We maintain a large workforce of security professionals who are dedicated to ensuring the security of Oracle Cloud Infrastructure. Within the workforce, several teams are responsible for securely developing, monitoring, testing, and assuring compliance with regulations and certification programs.

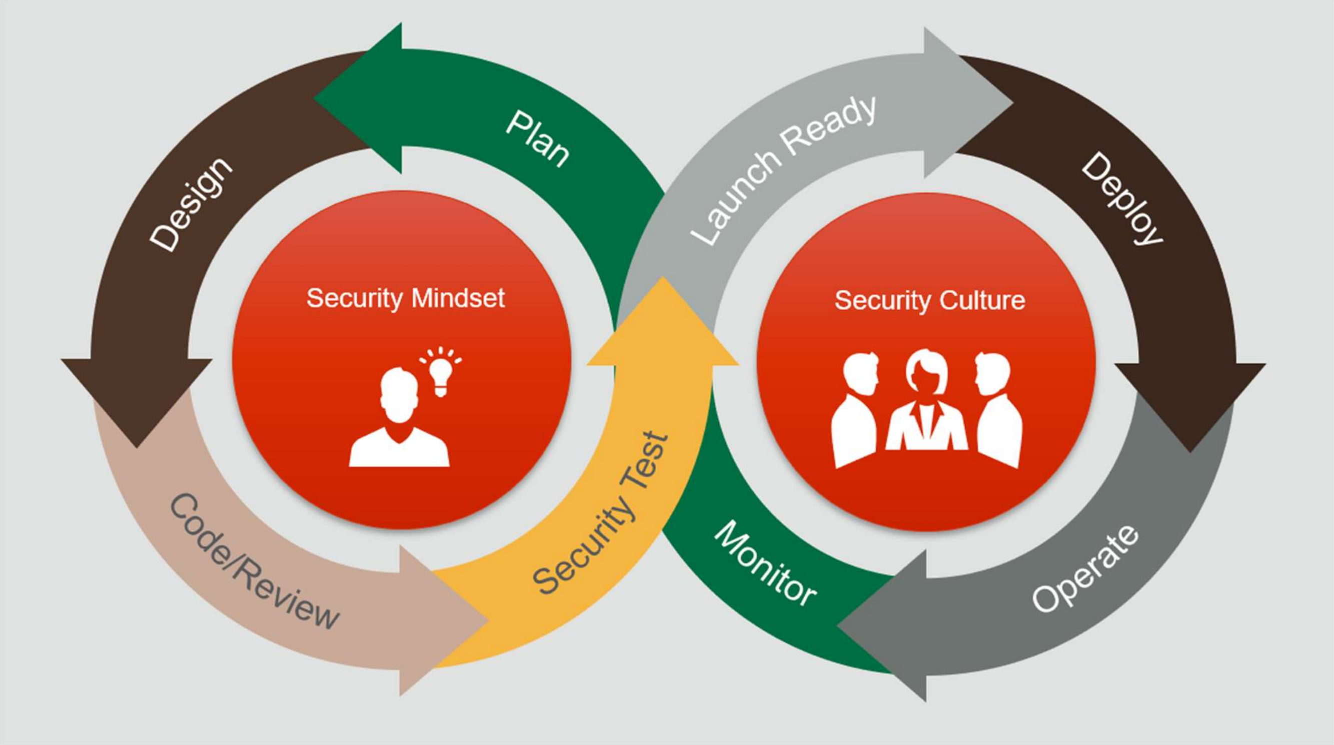

Figure 6. Operational Security Flow in Oracle Cloud Infrastructure

Defensive Security

In all computing environments, daily attacks occur against networking and compute infrastructure. A dedicated team of defensive experts and analysts is required to monitor and respond to these events. At Oracle Cloud Infrastructure, this team is the Defensive Security team. The members of this team are the first responders of cloud security. They work proactively and continuously to spot potential threats and shut down exploit paths. When incidents are detected, they work to remediate them promptly by using modern security operations methodologies and DevSecOps-enabled configuration and tooling.

Offensive Security

After an aspect of Oracle Cloud Infrastructure security architecture is developed or modified, the Offensive Security team verifies that it meets security benchmarks and best practices. 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. The Offensive Security team's work informs secure development, secure architecture, and defensive capabilities.

Security Assurance

We develop and implement security plans with high security standards that align with existing Oracle and industry standards. To assure the security of the cloud platform, the Security Assurance group works collaboratively with the service teams and with security and risk stakeholders throughout Oracle to develop and deploy security controls, technologies, processes, and guidance for teams building on Oracle Cloud Infrastructure.

DATA AND APPLICATION PROTECTION

Oracle Cloud Infrastructure's data handling and management practices are designed to protect your data and applications from outside threats.

Data Access

We define two broad categories of data in our interactions with customers:

- **Data about our customers**: The contact and related information needed to operate an Oracle Cloud Infrastructure account and bill for services. The use of any personal information that we gather for purposes of account management is governed by the Oracle General Privacy Policy.
- **Data stored by our customers**: The data that customers store in Oracle Cloud Infrastructure, such as files, documents, and databases. We don't have insight into the contents of this data. Our handling of this data is described by the Oracle Services Privacy Policy and the Data Processing Agreement for Oracle Services.

Data Destruction

We use physical destruction and logical data erasure processes so that data does not 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 is 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 executing 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 its initial factory 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

We've implemented a "ubiquitous encryption" program with the goal of encrypting all data, everywhere, always. For customer tenant data, we use encryption both at-rest and in-transit. The Block Volumes 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 expose broader attack surfaces. We recognize the importance of API security for applications in cloud environments and have developed the API Gateway service to provide that security.

API Gateway is a fully managed, regional service that integrates with customers' networks on Oracle Cloud Infrastructure. API gateways enable customers to publish public or private APIs, process incoming requests from a client, and 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 preserve the privacy and integrity of data. Customers can also configure the connections from API gateways to backend services to also use TLS.

CULTURE OF TRUST AND COMPLIANCE

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

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 are used on-premises by customers or delivered through Oracle Cloud. Our goal is to help customers meet their security requirements while providing for cost-effective ownership experience. The industry-leading standards, technologies, and practices in OSSA have the following goals:

- **Foster security innovations**: Our long tradition of security innovations continues with solutions that enable 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 our 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**: We've adopted transparent policies for security vulnerability disclosure and remediation. We're committed to treating all customers equally and delivering a positive security patching experience through our Critical Patch Update and Security Alert programs.

Personnel Security

We strive to hire the best candidates, and then invest in and develop our employees. We provide baseline security training for all employees and specialized training opportunities to learn the latest security technologies, exploits, and methodologies. We provide standard, corporate training programs that cover our information security and privacy programs. Additionally, we engage with various industry groups and send employees to specialist conferences to collaborate with other industry experts on emerging challenges. The objectives of Oracle security training programs are to help our employees protect our customers and products, to enable employees to learn more about security areas they are interested in, and to further our mission to attract and retain the best talent.

We also strive to hire people with strong ethics and good judgment. All employees undergo pre-employment screening as permitted by law, including criminal background checks and prior employment validation in accordance with in country hiring rules. We maintain performance-evaluation processes to recognize good performance and identify opportunities for growth. We use security as a component of the team-evaluation processes. This approach gives us visibility into how teams are performing against our security standards and helps identify best practices and improvement areas for critical security processes.

Supply-Chain Security

We have 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 Oracle Cloud Infrastructure services. This team works with our supply chain and validates hardware components against our rigorous hardware security standards.

Compliance

We continue to invest in services that help our customers more easily meet their security and compliance needs. Independent assurance promotes trust and builds confidence in third-party service provider relationships. To gain this trust and confidence, we have many recurring programs that maintain compliance with global, regional, and industry-specific certifications, and that issue reports to attest to that compliance. These reports may 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, we can unify service compliance for regions around the world by using automation for service deployment.

Auditing

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

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

We also permit customers to conduct their own or third-party testing of their tenancy as outlined in the Security Testing Policy.

CONCLUSION

Oracle Cloud Infrastructure puts the security of critical workloads at the center of our Generation 2 public cloud. For customers running security-sensitive workloads, such as financial applications or citizen service applications, Oracle Cloud Infrastructure provides groundbreaking security architecture that reduces the risks and attack surfaces commonly associated with first-generation clouds. We've built security into the architecture, data-center design, personnel selection, and the processes for provisioning, using, certifying, and maintaining Oracle Cloud Infrastructure. It's a modern public cloud built for the world's most security-intense data.

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

Oracle Cloud Infrastructure Security Architecture
March 2020