ORACLE
Cloud Infrastructure

Oracle Cloud Infrastructure Security

ORACLE WHITE PAPER | APRIL 2019

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. 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 for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
April 2, 2019	Added descriptions of new security services.
November 12, 2018	Added descriptions of new security features and services.
August 13, 2018	Added descriptions of new security features and compliance capabilities, and added a new section about high-level security guidelines for security configuration.

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at https://cloud.oracle.com/iaas/technical-resources.

Table of Contents

Oracle Cloud Infrastructure: Next-Generation Enterprise Cloud 5

Security Objectives 5

Shared Security Model 6

Security Services and Features 8

- Regions, Availability Domains, and Fault Domains 8
- Identity and Access Management (IAM) Service 9
- Key Management 13
- Audit Service 15
- Oracle CASB Monitoring 15
- Compute Service 16
- Networking Service 17
- Storage Services 20
- Data Transfer Service 22
- Database Service 22
- Load Balancing Service 23
- Managed Domain Name System Service 23
- Web Application Firewall Service 24
- Email Delivery Service 24
- Container Engine for Kubernetes 25
- Registry 26

High-Level Guidelines for Security Configuration 26

Infrastructure Security 28

- Security Culture 29
- Security Design and Controls 30
- Secure Software Development 31

Personnel Security 32
Physical Security 32
Security Operations 34
Customer Data Protection 34
Data Rights and Ownership 34
Data Privacy 34
Law Enforcement Requests 35
Compliance 35
Conclusion 36

Oracle Cloud Infrastructure: Next-Generation Enterprise Cloud

Enterprises need scalable hybrid cloud solutions that meet all their security, data protection, and compliance requirements. To meet this need, Oracle developed Oracle Cloud Infrastructure, which offers customers a virtual data center in the cloud that allows enterprises to have complete control with unmatched security. Oracle Cloud Infrastructure is a cloud platform designed and architected to support enterprise applications and customers. The platform provides high-performance, secure, and highly available services that scale elastically to handle a wide variety of enterprise workloads. Oracle Cloud Infrastructure offers a variety of cloud services including bare metal compute, virtual machines (VMs), software-defined virtual cloud networks (VCNs), high-performance managed Oracle databases, remote block storage, object storage, audit, identity and access management, managed load balancing, DNS, and other edge services. Oracle Cloud Infrastructure was designed and built to run mission-critical, enterprise workloads while also supporting modern cloud-native workloads.

Primary considerations for enterprise customers who want to leverage a public cloud are data security and the effort involved in migrating existing applications. Given the constraints of traditional public clouds, enterprises normally migrate noncritical applications to the cloud and continue to restrict mission-critical production applications and data to their on-premises data centers. Oracle built Oracle Cloud Infrastructure to enable enterprises to maximize the number of mission-critical workloads that they can migrate to the cloud while continuing to maintain a strong security posture and reduce the overhead of building and operating data-center infrastructure. With Oracle Cloud Infrastructure, enterprise customers get the same control and transparency into their workloads as they have on-premises.

For customers who need a fully isolated and controlled environment, Oracle Cloud Infrastructure offers bare metal instances that are completely managed by the customer without any Oracle software running on the instance. This offering is a result of significant innovation by Oracle Cloud Infrastructure and provides greater control, transparency, and software flexibility alongside traditional benefits of cloud, such as automated provisioning and elasticity of infrastructure.

Security Objectives

Oracle's mission is to build cloud infrastructure and platform services where Oracle customers have effective and manageable security to run their mission-critical workloads and store their data with confidence.

Oracle Cloud Infrastructure's security approach is based on seven core pillars. Each pillar has multiple solutions designed to maximize the security and compliance of the platform.

- **Customer isolation:** Allow customers to deploy their application and data assets in an environment that commits full isolation from other tenants and Oracle's staff.
- **Data encryption:** Protect customer data at-rest and in-transit in a way that allows customers to meet their security and compliance requirements with respect to cryptographic algorithms and key management.
- **Security controls:** Offer customers effective and easy-to-use application, platform, and network security solutions that allow them to protect their workloads, have a secure application delivery using a global edge network, constrain access to their services, and segregate operational responsibilities to reduce the risk associated with malicious and accidental user actions.
- **Visibility:** Offer customers comprehensive log data and security analytics that they can use to audit and monitor actions on their resources, allowing them to meet their audit requirements and reduce security and operational risk.
- **Secure hybrid cloud:** Enable customers to use their existing security assets, such as user accounts and policies, as well as third-party security solutions when accessing their cloud resources and securing their data and application assets in the cloud.
- **High availability:** Offer fault-independent data centers that enable high availability scale-out architectures and are resilient against network attacks, ensuring constant uptime in the face of disaster and security attack.
- **Verifiably secure infrastructure:** Follow rigorous processes and use effective security controls in all phases of cloud service development and operation. Demonstrate adherence to Oracle's strict security standards through third-party audits, certifications, and attestations. Help customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors, and regulators.

Additionally, Oracle employs some of the world's foremost security experts in information, database, application, infrastructure, and network security. By using Oracle Cloud Infrastructure, our customers directly benefit from Oracle's deep expertise and continuous investments in security.

Shared Security Model

Oracle Cloud Infrastructure offers best-in-class security technology and operational processes to secure its enterprise cloud services. However, for customers to securely run their workloads in Oracle Cloud Infrastructure, they must be aware of their security and compliance responsibilities. By design, Oracle provides security of cloud infrastructure and operations (cloud operator access controls, infrastructure security patching, and so on), and customers are responsible for securely

configuring their cloud resources. Security in the cloud is a shared responsibility between the customer and Oracle.

In a shared, multi-tenant compute environment, Oracle is responsible for the security of the underlying cloud infrastructure (such as data-center facilities, and hardware and software systems) and customers are responsible for securing their workloads and configuring their services (such as compute, network, storage, and database) securely.

In a fully isolated, single-tenant, bare-metal server with no Oracle software on it, the customers' responsibility increases as they bring the entire software stack (operating systems and above) on which they deploy their applications. In this environment, customers are responsible for securing their workloads, and configuring their services (compute, network, storage, database) securely, and ensuring that the software components that they run on the bare metal servers are configured, deployed, and managed securely.

More specifically, customer and Oracle responsibilities can be divided into the following areas:

- **Identity and access management (IAM):** As with all Oracle Cloud services, customers should protect their cloud access credentials and set up individual user accounts. Customers are responsible for managing and reviewing access for their own employee accounts and for all activities that occur under their tenancy. Oracle is responsible for providing effective IAM services such as identity management, authentication, authorization, and auditing.
- **Workload security:** Customers are responsible for protecting and securing the operating system and application layers of their compute instances from attacks and compromises. This protection includes patching applications and operating systems, operating system configuration, and protection against malware and network attacks. Oracle is responsible for providing secure images that are hardened and have the latest patches. Also, Oracle makes it simple for customers to bring the same third-party security solutions that they use today.
- **Data classification and compliance:** Customers are responsible for correctly classifying and labeling their data and meeting any compliance obligations. Also, customers are responsible for auditing their solutions to ensure that they meet their compliance obligations.
- **Host infrastructure security:** Customers are responsible for securely configuring and managing their compute (virtual hosts, containers), storage (object, local storage, block volumes), and platform (database configuration) services. Oracle has a shared responsibility with customers to ensure that the service is optimally configured and secured. This responsibility includes hypervisor security and the configuration of the permissions and network access controls required to ensure that hosts can communicate correctly and that devices are able to attach or mount the correct storage devices.

- **Network security:** Customers are responsible for securely configuring network elements such as virtual networking, load balancing, DNS, and gateways. Oracle is responsible for providing a secure network infrastructure.
- **Client and end-point protection:** Customers use various hardware and software systems, such as mobile devices and browsers, to access their cloud resources. Customers are responsible for securing all clients and endpoints that they use to access Oracle Cloud Infrastructure services.
- **Physical security:** Oracle is responsible for protecting the global infrastructure that runs all of the services offered in Oracle Cloud Infrastructure. This infrastructure consists of the hardware, software, networking, and facilities that run Oracle Cloud Infrastructure services.

Security Services and Features

A key objective of Oracle Cloud Infrastructure has been to allow our customers to create a logical extension of their on-premises infrastructure and data centers in Oracle Cloud Infrastructure. Our customers should be able to gain the benefits of a modern public cloud without having to compromise or reinvent their security posture. This idea was central to the design of all our infrastructure and services.

Regions, Availability Domains, and Fault Domains

To provide data availability and durability, Oracle Cloud Infrastructure enables customers to select from infrastructure with distinct geographic and threat profiles.

A *region* is the top-level component of the infrastructure. Each region is a separate geographic area with multiple, fault-isolated locations called *availability domains*.

Availability domains are designed to be independent and highly reliable. Each one is built with fully independent infrastructure: buildings, power generators, cooling equipment, and network connectivity. Physical separation provides protection against natural and other disasters. Availability domains within the same region are connected by a secure, high-speed, low-latency network, which allows customers to build and run highly reliable applications and workloads with minimum impact to application latency and performance. All links between availability domains are encrypted. Each region has one or more availability domains, allowing customers to deploy highly available applications.

Each availability domain has three *fault domains*. Fault domains enable customers to ensure anti-affinity by distributing instances so that they are not on the same physical hardware within a single availability domain. A hardware failure or compute hardware maintenance update that affects instances in one fault domain does not affect instances in other fault domains.

Identity and Access Management (IAM) Service

The Oracle Cloud Infrastructure Identity and Access Management (IAM) service is built to meet the requirements of enterprises, and it provides authentication and authorization for all their Oracle Cloud Infrastructure resources and services. An enterprise can use a single tenancy shared by various business units, teams, and individuals while maintaining security, isolation, and governance.

When a customer joins Oracle Cloud Infrastructure, a *tenancy* is created. A tenancy is a virtual construct that contains all of the Oracle Cloud Infrastructure resources that belong to the customer. The administrator of the tenancy can create *users* and *group*s and assign them least-privileged access to resources that are partitioned into *compartments*. A compartment is a group of resources that can be managed as a single logical unit, providing a streamlined way to manage large infrastructure. For example, a customer can create a compartment—say HR-Compartment—to host a specific set of cloud network, compute instances, and storage volumes necessary to host its HR applications.

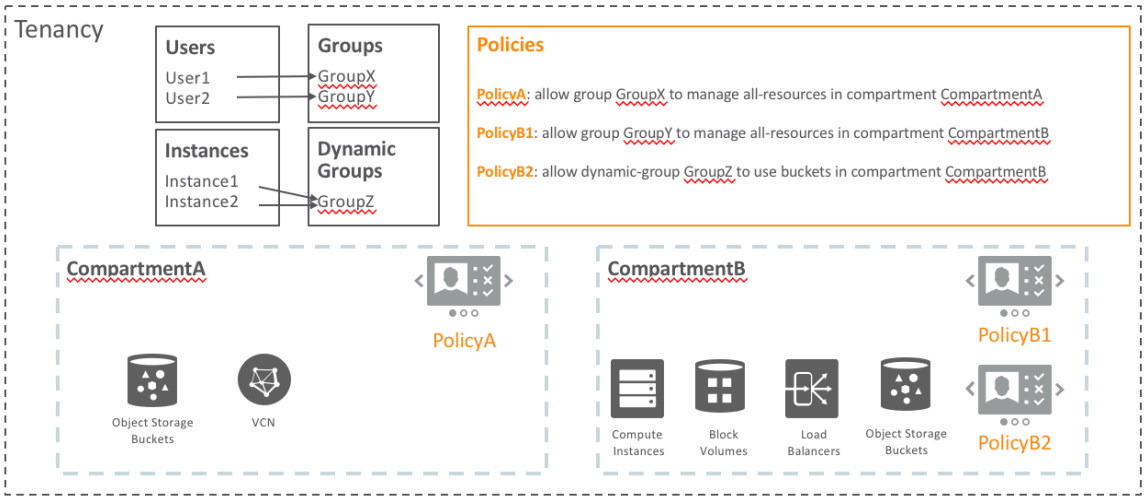
Compartments are a fundamental component of Oracle Cloud Infrastructure for organizing and isolating cloud resources. Customers use them to clearly separate resources for the purposes of isolation (separating the resources for one project or business unit from another). A common approach is to create a compartment for each major part of an organization. You can create subcompartments inside of compartments to create hierarchies that are six levels deep.

Unlike most Oracle Cloud Infrastructure services that are regionally scoped, Identity is global. Customers can have a single tenancy across multiple regions.

Following are key IAM primitives:

- **Resource:** A cloud object that a company's employees create and use when interacting with Oracle Cloud Infrastructure services, for example, compute instances, block storage volumes, virtual cloud networks (VCNs), subnets, and route tables.
- **Policy:** A set of authorization rules that define access to resources within a tenancy.
- **Compartment:** A heterogeneous collection of resources for the purposes of security isolation and access control.
- **Tenancy:** The root compartment that contains all of an organization's resources. Within a tenancy, administrators can create one or more compartments, create additional users and groups, and assign policies that grant groups the ability to use resources within a compartment.

- **User:** A human being or system that needs access to manage their resources. Users must be added to groups in order to access resources. Users have one or more credentials that must be used to authenticate to Oracle Cloud Infrastructure services. Federated users are also supported.
- **Group:** A collection of users who share a similar set of access privileges. Administrators can grant access policies that authorize a group to consume or manage resources within a tenancy. All users in a group inherit the same set of privileges.
- **Dynamic group:** A collection of instances as principal actors, similar to user groups. Administrators can create policies to permit instances in dynamic groups to make API calls against Oracle Cloud Infrastructure services.
- **Matching rule:** A set of criteria that defines membership in a dynamic group. Resources that match the rule criteria are members of the dynamic group.
- **Instance principals:** Instances themselves are a new principal type in IAM. Each Compute instance has its own identity, and it authenticates by using certificates that are added to the instance by the instance principals capability. These certificates are automatically created, assigned to instances, and rotated.
- **Identity provider and federation:** A trust relationship with a federated identity provider. Federated users who attempt to authenticate to the Oracle Cloud Infrastructure graphical administration console are redirected to the configured identity provider, after which they can manage Oracle Cloud Infrastructure resources in the console just like a native IAM user. Users who are federated with Okta and Oracle Identity Cloud Service (IDCS) can directly access the Oracle Cloud Infrastructure SDK and CLI. Oracle Cloud Infrastructure also allows token-based authentication for the CLI for customers using an identity provider that doesn't support the Simple Cloud Identity Management (SCIM). Currently, Oracle Cloud Infrastructure supports the Oracle Identity Cloud Service, Microsoft Active Directory Federation Service (ADFS), and any SAML 2.0 compliant identity provider. Federated groups can be mapped to native IAM groups to define what policy should apply to a federated user.



Policies

All customer calls to access Oracle Cloud Infrastructure resources are first authenticated by the IAM service and then authorized based on IAM policies. A customer can create a policy that gives a specific set of users permission to access the infrastructure resources (network, compute, storage, and so on) within a compartment in the tenancy. These policies are flexible and are written in a human-readable form that is easy to understand and audit. A policy contains one or more policy statements that follow this syntax:

```
Allow group <group_name> to <verb> <resource-type> in compartment
<compartment_name>
```

The IAM service also allows administrators to authorize their instances to make API calls in Oracle Cloud Infrastructure services. Instances themselves are a principal type in IAM. Each Compute instance has its own identity, and it authenticates by using certificates. Administrators can use policies to permit Compute instances to make API calls. IAM dynamic groups are used to authorize Compute instances to access Oracle Cloud Infrastructure APIs. Customers create dynamic groups, which include instances as members, and authorize access to their tenancy resources using IAM security policies. Administrators can add instances to dynamic groups by using resource identifiers and resource tags. A policy that authorizes the members of a dynamic group to access IAM-protected APIs has the following syntax:

```
Allow dynamic-group <group_name> to <verb> <resource-type> in compartment
<compartment_name>
```

A *verb* defines the type of access covered. Oracle defines the following verbs that you can use in your policy statements:

- **inspect:** Provides the ability to list resources, without access to any confidential information or user-specified metadata that might be part of that resource.
- **read:** Includes **inspect** plus the ability to get user-specified metadata and the actual resource itself.
- **use**: Includes **read** plus the ability to work with existing resources (the actions vary by resource type). Includes the ability to update the resource, except for resource types where the **update** operation has the same effective impact as the **create** operation (for example, UpdatePolicy and UpdateSecurityList). In such cases, the **update** ability is available only with the **manage** verb. In general, this verb does not include the ability to create or delete that type of resource.
- **manage**: Includes all permissions for the resource.

For example, a policy that enables the GroupAdmins group to create, update, or delete any groups would be written as follows:

```
Allow group GroupAdmins to manage groups in tenancy
```

Another policy that allows instances in the dynamic group ImageProcessorApps to read buckets from Object Storage would be written as follows:

```
Allow dynamic-group ImageProcessorApps to read buckets in compartment
ProductImages
```

Credentials

Each user has one or more of the following credentials to authenticate themselves to Oracle Cloud Infrastructure. Users can generate and rotate their own credentials. In addition, a tenancy security administrator can reset credentials for any user within their tenancy.

- **Console password:** Used to authenticate a user to the Oracle Cloud Infrastructure Console. Customers can customize the console password settings including password length and complexity rules. Also, Console users can automatically reset their own passwords using the IAM account recovery mechanism.
- **Time-based one-time password (TOTP):** Used to perform multi-factor authentication (MFA) when users access the Oracle Cloud Infrastructure Console.
- **API key:** All API calls are signed using a user-specific 2048-bit RSA private key. The user creates a public key pair, and uploads the public key in the Console.

- **Swift password:** Used by Recovery Manager (RMAN) to access the Object Storage service for database backups. To ensure sufficient complexity, the password is created by the IAM service and cannot be provided by a customer.
- **Customer secret key:** Used by Amazon S3 clients to access the Object Storage service's S3-compatible API. To ensure sufficient complexity, the password is created by the IAM service and cannot be provided by a customer.
- **SMTP credential:** Simple Mail Transfer Protocol (SMTP) credentials are necessary to send email through Email Delivery. A credential is a composed of a user name and password that can be generated in the Console.

Key Management

All of the data that customers store with any of the Oracle Cloud Infrastructure data services (Block Volumes including Boot Volumes, Object Storage, and File Storage) is protected by encryption keys that are securely stored and controlled by Oracle.

For customers, especially those operating in regulated industries, who need to verify that their company-specific security governance policies and regulatory compliance requirements are implemented in their cloud deployments, Oracle provides a Key Management service in all Oracle Cloud Infrastructure regions.

Oracle Cloud Infrastructure Key Management is a managed service that enables you to encrypt your data by using keys that you control. Key Management provides you with centralized key management capabilities; highly available, durable, and secure key storage using per-customer isolated partitions in FIPS 140-2 Level 3 certified hardware security modules (HSMs); and integration with select Oracle Cloud Infrastructure services.

Vaults and Keys

When you work with Key Management, you work with two types of resources: vaults and keys.

- Vaults are logical entities where Key Management creates and durably stores your keys. Vaults are backed by highly available, per-customer, isolated partitions on HSMs.
- Keys are logical entities that reference one or more key versions that contain the cryptographic material that you use to protect your data. Each key has a minimum of one key version, and the maximum number of versions is limited only by the total number of keys that you can store in a vault. You can choose a key shape that indicates the key length and the algorithm used with it. Currently, all keys are Advanced Encryption Standard (AES) keys used in Galois Counter Mode (GCM), and you can choose from three key lengths: AES-128, AES-192, and AES-256.

When you request the service to create a key on your behalf, Key Management stores the key and all subsequent key versions in vaults. All vaults that contain your keys are replicated multiple times within a region to ensure the durability and availability of the keys.

Plaintext key material can never be viewed or exported from the vault. Only users, groups, or services that you authorize via an IAM policy can use the keys by invoking Key Management to encrypt or decrypt data.

Implementation

You can use Key Management directly in your application or through Oracle Cloud Infrastructure services that integrate with Key Management.

When you use Key Management directly in your application to encrypt data, you can use a method known as *envelope encryption*. Envelope encryption encrypts plaintext data with a data encryption key (DEK) and then encrypts the DEK with a master encryption key (MEK). When you use envelope encryption in your application, you don't have to worry about where to store the encrypted data key because it is always encrypted using the master key. It is safe to store your encrypted data key alongside your encrypted data, thereby reducing the need for sending large payloads of data for encryption or decryption over the network and impacting performance. Additionally, envelope encryption allows you to encrypt the same data by using multiple key versions of the master key without the need for time-consuming decrypt and encrypt operations because you re-encrypt only the data key that protects your data. This enables frequent key rotations with negligible operational and performance impact.

When you use Key Management through Oracle Cloud Infrastructure services that integrate with Key Management, you can assign a key from Key Management to a new resource, add a key assignment to an existing resource, change the key assignment for an existing resource, and remove the key assignment from the resource. When you remove a key assignment from an existing resource, your data is never stored unprotected; Oracle Cloud Infrastructure data services default to protecting your data via encryption keys that are securely stored and controlled by Oracle.

Integration

Oracle Key Management integrates with the Oracle Cloud Infrastructure IAM and Audit services.

Integration with IAM gives customers fine-grained control to perform the following actions:

- Define which Oracle Cloud Infrastructure IAM users or groups can manage keys and key vaults
- Define which IAM users, groups, or services can use keys to encrypt and decrypt data

- Define which IAM users or groups can associate keys with other Oracle Cloud Infrastructure resources (for example, block volumes or buckets)

Integration with Audit helps you monitor the key lifecycle.

To learn more about Oracle Cloud Infrastructure Key Management, visit https://cloud.oracle.com/en_US/cloud-security/kms/faq.

Audit Service

The Oracle Cloud Infrastructure Audit service records all API calls to resources in a customer's tenancy as well as login activity from the graphical management console. Using the Audit service, customers can achieve their own security and compliance goals by monitoring all user activity within their tenancy. Because all Console, SDK, and command-line interface (CLI) calls go through our APIs, all activity from those sources is included. Audit records are available through an authenticated, filterable query API or can be retrieved as batched files from Oracle Cloud Infrastructure Object Storage. Audit log contents include what activity occurred, the user that initiated it, the date and time of the request, as well as source IP address, user agent, and HTTP headers of the request. By default, audit logs are retained for 90 days, but customers can configure log retention for up to 365 days.

Oracle CASB Monitoring

Oracle Cloud Access Security Broker (CASB) monitors the security of Oracle Cloud Infrastructure deployments through a combination of predefined, Oracle Cloud Infrastructure–specific security controls and policies, customer-configurable security controls and policies, and advanced security analytics using machine learning for detecting anomalies. Oracle CASB security functionality includes monitoring security misconfiguration of Oracle Cloud Infrastructure resources, monitoring credentials and privileges, user behavior analysis (UBA) for anomalous user actions, and threat analytics for identifying risk events.

To enable CASB monitoring of Oracle Cloud Infrastructure, you create an Oracle Cloud Infrastructure application instance with Oracle CASB, and provision it with the API key credentials of a least-privilege IAM user who is authorized to get configuration information and audit logs from your Oracle Cloud Infrastructure tenancy. Oracle CASB periodically obtains the tenancy configuration information and audit logs to perform the security analytics, and generates alerts for any deviations from the security baseline.

To learn more about Oracle CASB monitoring of Oracle Cloud Infrastructure, see the documentation located at https://docs.oracle.com/en/cloud/paas/casb-cloud/index.html.

Compute Service

Compute is a core component of Oracle Cloud Infrastructure and provides on-demand and elastic compute capabilities with enterprise-grade security and unrivaled performance. Customers can provision thousands of compute instances and scale them up or down through an easy-to-use web-based management console. Programmatic support to do the same is available through feature-rich SDKs and command-line interfaces (CLIs). All compute instances are hosted in Oracle enterprise-grade data centers.

Compute instances are based on high-performance server hardware that uses latest-generation, multi-core server CPUs, large amounts of memory and high-throughput NVMe local storage. Oracle Cloud Infrastructure provides bare metal and virtual machine (VM) instances, which allows customers to choose instances that fit their performance, cost, and software flexibility requirements.

- **Bare metal instances:** In bare metal instances, physical servers are dedicated to a single customer who has complete control over the server. There is no Oracle-managed hypervisor, and Oracle personnel have no access to memory or local (NVMe) storage while the instance is running. Off-box virtualization is used to implement network virtualization. Standard remote management mechanisms are used at boot time to provision the instances. These bare metal instances offer consistent high performance and are extremely resilient to noisy-neighbor issues. After instance launch, only customers have OS-level administrative privileges to the instance. After a customer terminates their instance, the server undergoes an automated disk and firmware-level wipe process to ensure isolation between customers.
- **Virtual machine (VM) instances:** Customers with flexibility requirements or those who don't need a dedicate bare metal instance can opt for VMs. Multi-tenant customer VMs in Oracle Cloud Infrastructure are managed by a security-hardened hypervisor which provides strong isolation between customers.

Oracle Cloud Infrastructure instances use key-based SSH by default. Customers provide the SSH public keys to Oracle Cloud Infrastructure and securely use the SSH private keys for accessing the instances. Oracle highly recommends using key-based SSH to access Oracle Cloud Infrastructure instances. Password-based SSH could be susceptible to brute-forcing attacks, and are not recommended.

Oracle Linux images hardened with the latest security updates are available for customers to run on Oracle Cloud Infrastructure instances. Oracle Linux images run the Unbreakable Enterprise Kernel (UEK) and support advanced security features such as Ksplice to apply security patches without booting, which allows enterprises to live-update their instances without any disruption. In addition to Oracle Linux, Oracle Cloud Infrastructure makes a growing list of other OS images available, including CentOS, Ubuntu, and Windows Server. Customers may also bring their own

custom images. All Oracle-provided images come with secure defaults including OS-level firewalls turned on by default.

Networking Service

High-throughput and reliable networking is fundamental to public-cloud infrastructure that delivers compute and storage services at scale. As a result, we invested significant innovation in Oracle Cloud Infrastructure Networking to support the requirements of enterprise customers and their workloads. Oracle Cloud Infrastructure regions have been built with a state-of-the-art, nonblocking Clos network that is not oversubscribed and provides customers with a predictable, high-bandwidth, low-latency network. The data centers in a region are networked to be highly available and have low-latency connectivity between them.

The Oracle Cloud Infrastructure Networking service offers a customizable private network (a VCN, or virtual cloud network) to customers, which enforces logical isolation of customer Oracle Cloud Infrastructure resources. As with their on-premises network in their data centers, customers can set up a VCN with hosts with private IP addresses, subnets, route tables and gateways using VCN. The VCN can be configured for internet connectivity, or connected to the customer's private data center through an IPSec VPN gateway or FastConnect. FastConnect offers a private connection between an existing network's edge router and dynamic routing gateways (DRGs). Traffic does not traverse the internet.

The Networking service also supports bi-directional stateful and stateless firewalls that allow customers to initialize network security access controls. Firewalls and ACLs specified for a customer VCN are propagated throughout the network topology and control plane, ensuring a multi-tiered and defense-in-depth implementation. Each tenant (customer) can create multiple VCNs to implement logical grouping of their resources.

Following are key Networking service primitives associated with a VCN:

- **Subnets:** The primary subdivision of a VCN. Subnets are specific to an availability domain and can be marked as private upon creation, which prevents instances launched in that subnet from having public IP addresses.
- **Route tables:** Virtual route tables that give the subnets access to the VCN’s gateways (internet gateway and dynamic routing gateway). Routes can also use private IPs as a target to implement network functionality such as NAT, firewalls, IDS, and so on.
- **Primary VNICs:** Subnets contain virtual network interface cards (VNICs), which attach to instances. The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each instance has a primary VNIC that is created during instance launch and cannot be removed. During instance launch, the Networking service also assigns a

public IP address. Customers can override that behavior during instance launch and request to have no public IP address assigned.

- **Secondary VNICs:** VNICs with public and private IP addresses that can be attached to an instance. In a Bring Your Own Hypervisor (BYOH) scenario where customers can run their hypervisor on a bare metal instance, a secondary VNIC can be assigned to a VM, to allow VCN networking for the VM. This is very useful for running virtual security appliances in a VCN.
- **IPSec VPN connection:** A secure VPN connection between a VCN and a data center.
- **Security lists:** Virtual firewall rules that define allowed ingress and egress to an instance at the packet level. Individual rules can be defined to be stateful or stateless.
- **Internet gateway:** Provides public internet connectivity from a VCN. By default, a newly created VCN has no internet connectivity.
- **Dynamic routing gateway (DRG):** A virtual router that provides a path for private traffic between a VCN and a data center's network. It is used with an IPSec VPN or Oracle Cloud Infrastructure FastConnect connection to establish private connectivity between a VCN and an on-premises or other cloud network.
- **Service gateway:** A virtual router that provides a path for private network traffic between a VCN and a public Oracle Cloud Infrastructure service such as Object Storage.
- **Local peering gateway (LPG):** A virtual router that provides a path for private network traffic between two VCNs in the same region. The VCNs can belong to the same tenancy or different tenancies.
- **Remote peering connection (RPC):** A component that you can add to a DRG to establish a path for private network traffic between two VCNs that reside in different regions.

Firewalls and Security Lists

Virtual firewalls are implemented by using VCN security lists. Customers can specify a set of firewall rules and associate them with one or more subnets. Associating a security list with a subnet applies those firewall rules to all instances running inside the subnet, at the packet level. There are two types of firewall rules:

- **Ingress rules** specify the *source* (IP CIDR and port range), destination port range, and protocol to match on, and are applied to ingress network connections.
- **Egress rules** specify the *destination* (IP CIDR and port range), source port range, and protocol to match on, and are applied to egress network connections.

Every VCN has a default security list that customers can optionally use that allows only SSH and certain types of important ICMP ingress traffic, and all egress traffic. Customers can associate multiple security lists with a subnet. The subnet uses the default security list if the customer doesn't specify another list for the subnet to use.

VCN Peering

VCN peering is the process of securely connecting multiple VCNs. The two types of VCN peering are local VCN peering and remote VCN peering.

- Local VCN peering is the process of connecting two VCNs in the same region so that their resources can communicate using private IP addresses without routing the traffic over the internet or through your on-premises network. The VCNs can be in the same tenancy or different ones. Without peering, a given VCN would need an internet gateway and public IP addresses for the instances that need to communicate with another VCN.

  Peering involves two VCNs that might be owned by the same party or two different ones. The two parties might both be in your company but in different departments, or the two parties might be in entirely different companies (for example, in a service-provider model). Peering between two VCNs requires explicit agreement from both parties in the form of IAM policies that each party implements for its own VCN's compartment or tenancy. If the VCNs are in different tenancies, each administrator must provide their tenancy OCID and put in place special policy statements to enable the peering.

- Remote VCN peering is the process of connecting two VCNs in *different* regions but the *same* tenancy. The peering allows the VCNs' resources to communicate using private IP addresses without routing the traffic over the internet or through your on-premises network. Without peering, a given VCN would need an internet gateway and public IP addresses for the instances that need to communicate with another VCN in a different region.

  Peering involves two VCNs in the same tenancy that might be administered by the same party or two different ones. The two parties might both be in your company but in different departments. Peering between two VCNs requires explicit agreement from both parties in the form of IAM policies that each party implements for its own VCN's compartment.

Service Gateway

A service gateway enables your VCN to access public Oracle Cloud Infrastructure services such as Object Storage without exposing the VCN to the public internet. No internet gateway is required. The resources in the VCN can be in a private subnet and use only private IP addresses. The traffic from the VCN to Object Storage travels over the Oracle Cloud Infrastructure network fabric and never traverses the internet. If you're using a service gateway, you can protect an Object Storage bucket by allowing only requests from an authorized VCN or CIDR block.

Storage Services

Oracle Cloud Infrastructure offers multiple storage solutions to meet the performance and durability requirements of customers:

- **Local Storage**: NVMe-backed storage on compute instances, offering extremely high IOPS.
- **Block Volume**: Network-attached storage volumes, attachable to compute instances.
- **Object Storage**: Regional service for storing large amounts of data as objects, providing strong consistency and durability.
- **Archive Storage**: A storage service for storing data that is accessed infrequently and requires long retention periods.
- **File Storage**: A durable, scalable, distributed, enterprise-grade network file system.

Block Volume

The Oracle Cloud Infrastructure Block Volume service provides persistent storage that can be attached to compute instances using the iSCSI protocol. The volumes are stored in high-performance network storage and support deep disk-to-disk cloning, and manual and policy-based automated scheduled backup capabilities. Volumes, their clones, and their backups are accessible only from within a customer's VCN and are encrypted at rest using unique keys.

When you launch a virtual machine (VM) or bare metal instance based on an Oracle-provided image or custom image, a new boot volume for the instance is created in the same compartment. That boot volume is associated with that instance until you terminate the instance. When you terminate the instance, you can preserve the boot volume and its data. This feature gives you more control and management options for your compute instance boot volumes. Boot volumes are encrypted by default. For additional security, iSCSI CHAP authentication can be required on a per-volume basis.

Object Storage

The Oracle Cloud Infrastructure Object Storage service provides highly scalable, strongly consistent, and durable storage for objects. API calls over HTTPS provide high-throughput access to data. All objects are encrypted at rest using unique keys. Objects are organized by bucket and, by default, access to buckets and objects within them requires authentication. Users can use IAM security policies to grant users and groups access privileges to buckets. To allow bucket access by users who do not have IAM credentials, the bucket owner (or a user with necessary privileges) can create pre-authenticated requests that allow authorized actions on buckets or objects for a specified duration. Alternately, buckets can be made public, which allows unauthenticated and

anonymous access. Given the security risk of inadvertent information disclosure, however, Oracle recommends carefully considering the business case for making buckets public.

Object Storage enables you to verify that an object was not unintentionally corrupted by allowing an MD5 hash to be sent with the object (or with each part, in the case of multipart uploads) and returned upon successful upload. This hash can be used to validate the integrity of the object.

In addition to its native API, the Object Storage service supports Amazon S3 compatible APIs. Using the Amazon S3 Compatibility API, customers can continue to use the existing S3 tools (for example, SDK clients), and partners can modify their applications to work with Object Storage, with minimal changes to their applications. Their native API can co-exist with the Amazon S3 Compatibility API, which supports CRUD operations. Before customers can use the Amazon S3 Compatibility API, they must create an S3 Compatibility API key. After they've generated the necessary key, they can use the Amazon S3 Compatibility API to access Object Storage in Oracle Cloud Infrastructure.

If you're using a service gateway in your VCN, you can protect an Object Storage bucket by allowing only requests from an authorized VCN or CIDR block. Service gateway is a virtual router that provides a path for private network traffic between a VCN and a public Oracle Cloud Infrastructure service such as Object Storage. The traffic from the VCN to Object Storage public endpoints travels over the Oracle Cloud Infrastructure network fabric and never traverses the internet.

Archive Storage

Archive Storage is ideal for storing data that is accessed infrequently and requires long retention periods. Archive Storage is more cost effective than Object Storage for preserving cold data for compliance and audit mandates. You can achieve Write Once Read Many (WORM) compliance with Archive Storage by applying IAM policy permissions so that data once written can't be overwritten.

File Storage

The Oracle Cloud Infrastructure File Storage service provides a durable, scalable, distributed, enterprise-grade network file system. You can connect to a File Storage file system from any bare metal, virtual machine, or container instance in your VCN. You can also access a file system from outside the VCN by using Oracle Cloud Infrastructure FastConnect and an Internet Protocol security (IPSec) virtual private network (VPN). All files are encrypted at rest by default.

There are four distinct and separate layers of security to consider when using File Storage. Each layer has its own authorization entities and methods that are separate from the other layers.

- The Oracle Cloud Infrastructure Policy layer uses policies to control what users can do within Oracle Cloud Infrastructure, such as creating instances, a VCN and its security rules, mount targets, and file systems.
- The Network Security layer controls which instance IP addresses or CIDR blocks can connect to a host file system. It uses VCN security list rules to allow or deny traffic to the mount target, and therefore access to any associated file system.
- The NFS Export Option layer is a method of applying access control per file system export based on a source IP address that bridges the Network Security layer and the NFS v.3 UNIX layer.
- The NFS v.3 UNIX layer controls what users can do on the instance, such as installing applications, creating directories, mounting external file systems to a local mount point, and reading and writing files.

Data Transfer Service

The Oracle Cloud Infrastructure Data Transfer service is an offline data transfer solution that lets you migrate large volumes of data to Oracle Cloud Infrastructure. Moving a large amount of data over the wire is not always feasible because of poor or unreliable network connectivity or the length of time it would take to move the data into the cloud. The Data Transfer service is a simple and secure solution that overcomes these challenges. You can transfer hundreds of terabytes of data on commodity hard disk drives (HDDs) and ship these drives to an Oracle transfer site.

The Data Transfer Utility is the software that Oracle provides for you to prepare transfer devices for shipment to Oracle. The Data Transfer Utility uses the standard Linux dm-crypt and LUKS utilities to encrypt block devices. All network communication between the Data Transfer Utility and Oracle Cloud Infrastructure is encrypted in transit by using Transport Layer Security (TLS).

Database Service

Oracle Cloud Infrastructure makes it easy to run, scale, and secure your Oracle databases (DBs) in the cloud. The Oracle Cloud Infrastructure Database service offers three types of DB systems:

- **Bare metal:** Comprising 1-node DB and 2-node Real Application Cluster (RAC) systems, providing exceptional performance at cost-effective pricing
- **Exadata:** Proven industry-leading Exadata DB systems in quarter, half, and full rack configurations
- **Virtual machine:** Allows customers to create full featured Oracle databases on VM shapes with various cores

DB systems are accessible only from a customer's VCN, and customers can configure VCN security lists to control network access to their databases. The Database service is integrated with Oracle Cloud Infrastructure IAM for controlling which users can launch and manage DB systems. By default, data is encrypted at rest using Oracle TDE with master keys stored in an Oracle Wallet on each DB system. RMAN backups of DB systems are encrypted and stored in customer-owned buckets in the Object Storage service. Customers need to create a bucket for DB backups and configure the Oracle Database Cloud Backup module with the Swift password and IAM permissions to access the bucket. Alternately, DB backups can be made to local NVMe storage on the DB system. Each user automatically has the ability to create, update, and delete their own Swift passwords in the Console or the API. An administrator does not need to create a policy to give a user those abilities. Administrators (or anyone with permission to the tenancy) also have the ability to manage Swift passwords for other users. Any user of a Swift client that integrates with Object Storage needs permission to work with the service.

Load Balancing Service

Oracle Cloud Infrastructure Load Balancing provides automated traffic distribution to compute instances in a customer's VCN. Load balancers can be created as public (accepting traffic from the internet and directing it to private instances) or private (directing traffic between private instances). Load balancers can be configured for SSL termination using customer-provided certificates; end-to-end SSL, whereby the load balancer terminates the SSL connection and creates a new SSL connection to the backend; or SSL tunneling, in which the SSL connection is passed through to the backend (TCP load balances only). The Load Balancing service supports TLS 1.2 by default, and prioritizes the following forward-secrecy ciphers in the TLS cipher-suite:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256

Managed Domain Name System Service

The Oracle Cloud Infrastructure Domain Name System (DNS) service provides dynamic, static, and recursive DNS solutions for enterprise customers. The service connects visitors to customer websites and applications with fast and secure services. The DNS service operates on a

global anycast network with 18 points of presence (PoPs) on five continents and offers fully redundant DNS constellations and multiple Tier 1 transit providers per PoP. The solution provides a DNS-based distributed denial-of-service (DDoS) protection and in-house security expertise that leverages a vast sensor network that collects and analyzes over 240 billion data points per day. The DNS service also fully supports the secondary DNS features to complement the customer's existing DNS service, providing resiliency at the DNS layer.

Web Application Firewall Service

Oracle Cloud Infrastructure Web Application Firewall (WAF) is a managed service that lets you apply Open Web Application Security Project (OWASP) core rule sets, including cross-site scripting and SQL injection, for internet-facing web applications. The WAF aggregates open source and commercial threat intelligence feeds of known blacklisted IP addresses, with daily updates. The WAF protects against layer 7 DDoS attacks.

Administrators can add their own access controls based on geolocation, whitelisted and blacklisted IP addresses, and HTTP URL and Header characteristics. Bot management provides a more advanced set of challenges and features, including JavaScript acceptance, CAPTCHA, device fingerprinting, and human interaction algorithms.

Oracle Cloud Infrastructure WAF acts as a reverse proxy that inspects all traffic flows or requests before they arrive at the origin web application. It also inspects any request going from the web application server to the end user. This powerful service enables you to control data leakage from your application servers and to protect your servers from outside threats.

The WAF can be integrated across other Oracle Cloud Infrastructure services, such as Oracle Cloud Infrastructure Load Balancing, to provide visibility into traffic from the core to the edge. Changes to WAF policies are written to the same audit destination as other Oracle Cloud Infrastructure services. You can apply tagging to WAF policies for cost tracking, and you can use Identity and Access Management (IAM) to control access to WAF management.

Oracle Cloud Infrastructure WAF is SecDevOps ready, with APIs for the entire control plane and SDKs in various languages.

Email Delivery Service

The Oracle Cloud Infrastructure Email Delivery service is an email sending service that provides a fast and reliable managed solution for sending high-volume emails that need to reach your recipients' inboxes. Email Delivery provides the tools necessary to send application-generated email for mission-critical communications such as receipts, fraud-detection alerts, multi-factor identity verification, and password resets.

The Email Delivery service uses the Sender Policy Framework (SPF), which enables email receivers to detect email spoofing. Using SPF, an email receiver can check if the IP address is explicitly authorized to send for that domain. SPF is implemented by publishing a special TXT record to a domain's DNS records. The TXT record declares which hosts are allowed to send mail on behalf of this domain. Receiving mail servers check the SPF records of sending domains to verify that the email's source IP address is authorized to send from that domain. Without SPF, a spam or phishing email can be "spoofed" to appear that the email comes from a legitimate domain. Domains that implement SPF are more likely to block emails that attempt to spoof your domain.

Users need Simple Mail Transfer Protocol (SMTP) credentials to send email through Email Delivery.

Container Engine for Kubernetes

Oracle Cloud Infrastructure Container Engine for Kubernetes is a fully-managed, scalable, and highly available service that you can use to deploy your containerized applications to the cloud. You can access Container Engine for Kubernetes to define and create Kubernetes clusters using the Console and the REST API.

Container Engine for Kubernetes is integrated with Oracle Cloud Infrastructure IAM, which provides easy authentication with native Oracle Cloud Infrastructure identity functionality. Users' permissions to access clusters come from the IAM groups to which they belong.

In addition to IAM, the Kubernetes RBAC Authorizer can enforce additional fine-grained access control for users on specific clusters via Kubernetes RBAC *roles* and *cluster roles*. A Kubernetes RBAC role is a collection of permissions. For example, a role might include read permission on pods and list permission for pods. A Kubernetes RBAC cluster role is just like a role but can be used anywhere in the cluster. A Kubernetes RBAC *role binding* maps a role to a user or set of users, granting that role's permissions to those users for resources in that namespace. Similarly, a Kubernetes RBAC *cluster role binding* maps a cluster role to a user or set of users, granting that cluster role's permissions to those users across the entire cluster.

IAM and the Kubernetes RBAC Authorizer work together to enable users who have been successfully authorized by at least one of them to complete the requested Kubernetes operation. When a user attempts to perform any operation on a cluster (except for create role and create cluster role operations), IAM first determines whether the group to which the user belongs has the appropriate and sufficient permissions. If so, the operation succeeds. If the attempted operation also requires additional permissions granted via a Kubernetes RBAC role or cluster role, the Kubernetes RBAC Authorizer then determines whether the user has been granted the appropriate Kubernetes role or cluster role. By default, users are not assigned any Kubernetes RBAC roles (or

cluster roles). So before attempting to create a new role (or cluster role), users must be assigned an appropriately privileged role (or cluster role).

Users can connect to worker nodes by using SSH. If you provided a public SSH key when creating the node pool in a cluster, the public key is installed on all worker nodes in the cluster. On UNIX and UNIX-like platforms (including Solaris and Linux), you can then connect through SSH to the worker nodes by using the SSH utility (an SSH client) to perform administrative tasks. Before you can connect to a worker node by using SSH, you must define a security ingress rule in the security list for the worker node subnet to allow SSH access.

Registry

Oracle Cloud Infrastructure Registry is an Oracle-managed registry that enables you to simplify your development-to-production workflow. The Registry makes it easy for developers to store, share, and manage development artifacts like Docker images. Oracle Cloud Infrastructure Registry is integrated with IAM, which provides easy authentication with native Oracle Cloud Infrastructure identity. A user's permissions to access repositories comes from the groups to which they belong. Before developers can push and pull Docker images to and from Oracle Cloud Infrastructure Registry, they must already have an Oracle Cloud Infrastructure username and an auth token.

Repositories can be private or public. Any user with internet access and knowledge of the appropriate URL can pull images from a public repository in Oracle Cloud Infrastructure Registry. If you make a repository private, you (along with users belonging to the tenancy's Administrators group) can perform any operation on the repository. You can use identity policies to allow other users to perform other operations on repositories (both public and private) that you create.

High-Level Guidelines for Security Configuration

Security of an Oracle Cloud Infrastructure tenancy is based on a combination of factors, all of which must be carefully considered and securely configured. From a practical perspective, take a hierarchical view of Oracle Cloud Infrastructure tenancy security configuration, where we start with addressing the foundational security issues. The following steps provide a roadmap of high-level guidelines to follow when configuring the security of a tenancy:

1. **User authentication and authorization:** The initial step in securely configuring a tenancy is to create mechanisms for authenticating users and authorizing users to access tenancy resources in a least-privilege manner. This step comprises the following actions:
    - Creating Oracle Cloud Infrastructure Identity and Access Management (IAM) users
    - Creating IAM groups

- Formulating authentication mechanisms (for example, Console access using a password, API access using API keys, and Object Storage access using an auth token) for the IAM users created
- Grouping customer tenancy resources into logical groups using compartments
- Formulating IAM security policies that authorize access of IAM groups to tenancy or compartment resources

For enterprises, federating their on-premises users and groups to their tenancy is an important consideration. IAM allows you to create users, groups, security polices, and federation mechanisms.

2. **Network security architecture:** After formulating IAM user authentication and authorization, a next step is creating a network security architecture for securely running the customer applications and storing their data in a tenancy. All the customer's compute and storage resources are enclosed in a virtual cloud network (VCN) created for the customer. VCN is a software-defined network, resembling the on-premises physical network used by customers to run their workloads. Formulating a VCN security architecture includes tasks such as the following ones:
   - Creating VCN subnets for network segmentation.
   - Formulating VCN and load balancer firewalls by using VCN security lists.
   - Using load balancing for high availability and TLS.
   - Determining the type of VCN external connectivity: internet, on-premises network, peered VCN, or combination of these.
   - Using virtual network security appliances (for example, next-generation firewalls, IDs).
   - Creating DNS zones and mappings. An important security consideration in load balancers is using customer Transport Layer Security (TLS) certificates to configure TLS connections to the customer's VCN.
3. **Compute instance security configuration:** Within a customer VCN, the customer applications run on compute instances, including bare metal instances, virtual machine (VM) instances, and GPUs. Compute instances are the basic compute building blocks.
   - Bare metal instances have no Oracle-managed software running on them, with the result that the instances and data stored (in memory and local drives) are completely controlled by the customer.
   - VM instances are architected with least-privilege mechanisms, and with corporate industry-leading hypervisor security best practices.

Depending on their security and performance requirements, customers have a choice of using bare metal and VM instances to run their application workloads in their tenancy. It's imperative to securely configure compute instances to maintain the security of the customer applications running on them.

4. **Data storage security configuration:** Depending on the type of data and access required, customers can store data in local drives (attached to compute instances), remote block volumes, object storage buckets, databases, or file storage in their tenancy. To handle these data storage requirements, Oracle Cloud Infrastructure offers multiple data storage services, such as Block Volume, Object Storage, Database, and File Storage. To meet their data security requirements, customers need to formulate an architecture for storing their data in their tenancy, and securely configure the storage services used. Compliance and regulatory requirements are an important factor in determining an appropriate data storage security architecture.

API Audit logs record calls to APIs (for example, through the Console, SDKs, CLIs, and custom clients using the APIs) as log events. The API Audit logs are always on by default and can't be turned off. Information in the API Audit logs show what time API activity occurred, the source of the activity, the target of the activity, what the action was, and what the response was. Oracle recommends that customers periodically review the Oracle Cloud Infrastructure API Audit logs to ensure they are in accordance with actions they took on their tenancy resources.

Detailed guidelines for security configuration are available in the Oracle Cloud Infrastructure Security Guide.

Infrastructure Security

Our security model is built around people, process, tooling, and a common security "platform" of methodologies and approaches from which we build our products. We apply this model to the core security components that we use to protect and secure our customers and business:

- Security Culture
- Security Design and Controls
- Secure Software Development
- Personnel Security
- Physical Security
- Security Operations

Security Culture

We believe that a dynamic security-first culture is vital to building a successful security-minded organization. We have cultivated a holistic approach to security culture in which all our team members internalize the role that security plays in our business and are actively engaged in managing and improving our products security posture. We have also implemented mechanisms that assist us in creating and maintaining a security-aware culture.

- **Security-minded leadership:** Our senior leadership is actively involved in our security planning, monitoring and management. We define and measure ourselves against security metrics and include security as a component of our team evaluation processes.
- **Embedded expertise:** To assist in driving security practices within our team, we have an embedded security-engineering model with security team members sitting and working with our product development teams. This approach enables our security organization to build deep understanding of the product-development processes and system architectures. We are also able to better assist teams in solving security challenges in real time and drive security initiatives more effectively.
- **Common security standards:** We actively work to integrate security into our products and operations. One way we have done this is to establish a security standards baseline. Our objective in creating this baseline is to provide a single security point of reference for business that establishes clear and actionable guidelines. The security baseline is updated frequently to incorporate learned lessons and reflect emerging business factors. We have also created a series of support materials to assist our teams in implementing security controls including reference architectures, implementation guides, and access to security experts.
- **Values of openness, constructive debate, and encouraged escalation:** Security issues can be addressed only when the people who can fix them are aware of them. We believe that openness and transparency, constructive debate, and encouraged escalation make us stronger. We encourage escalation, and we work to create an environment where raising issues early and often is rewarded.
- **Security training awareness:** We maintain robust security and awareness training programs that raise awareness and reinforce our security culture. We require in-depth security training sessions for all new employees as well as annual refresher trainings, and we provide security training that is tailored to our employees' specific job roles. All our software developers undergo a secure development training that establishes baseline security requirements for product development and provides best practices. We also work to provide engaging and innovative forms of security awareness training such as guest speakers and interactive forums (and we're not above providing food, drinks, or swag to drive attendance).

Security Design and Controls

Security is integrated into our products and operations through our Oracle Cloud Infrastructure Security Methodology. This centralized methodology defines our approach for the core security areas that form the security foundation from which we build our products. This approach lends itself to agility and helps us apply best practices and lessons learned from one product across the business, thus raising the security of all our products.

- **User authentication and access control:** Least-privilege access is used to grant access to production systems, and the approved lists of service team members are periodically reviewed to revoke access when there is no justifiable need. Access to production environments requires multi-factor authentication (MFA). The MFA tokens are granted by the security team, and tokens of inactive members are disabled. All access to production systems is logged, and the logs are stored for security analysis.
- **Change management:** Oracle Cloud Infrastructure follows a defined and rigorous change management and deployment process that uses purpose-built proprietary testing and deployment tools. All changes deployed into our production environment follow a testing and approval process prior to release. This process is designed to ensure that changes operate as intended, and can otherwise be rolled back to a previous known good state to recover gracefully from unforeseen bugs or operational issues. We also track the integrity of critical system configurations to ensure that they align with expected state.
- **Vulnerability management:** We use both internal penetration testing teams and external industry experts to help us identify potential vulnerabilities in our products. These exercises help us improve the security of our products, and we work to incorporate the lessons that we learn into our future development work. Oracle Cloud Infrastructure hosts undergo periodic vulnerability scanning using industry-standard scanners. Scan results are triaged to validate that applicability of findings to the Oracle Cloud Infrastructure environment, and applicable findings are patched by our product teams.
- **Incident response:** We have developed strong processes and mechanisms to enable us to respond to and address incidents as they arise. We maintain 24/7 incident response teams ready to detect and respond to events. Our critical staff members carry paging devices that enable us to call on the expertise needed to bring issues to resolution. We have also built process to help us learn from our incidents. We perform root cause analysis through our Corrective Action/Preventative Action (CAPA) process. CAPAs are intended to discover process gaps and changes that should be made by the business after an incident. CAPAs act as a common language that we can use to reflect on an issue and capture concrete steps to improve future operational readiness. CAPAs capture the root cause of an issue, what is required to contain or fix the issue, and what steps we need to take to ensure that the issue does not recur. Our leadership team reviews all CAPAs, looks for cross-organizational applications for learned lessons, and ensures that actions are implemented in a timely manner.

- **Security logging and monitoring:** We have created automated mechanisms to log various security-relevant events (for example, API calls and network events) in the infrastructure, and monitor the logs for anomalous behavior. Alerts generated by monitoring mechanisms are tracked and triaged by the security team.
- **Network security:** By default, customer communications with Oracle Cloud Infrastructure services are done using the latest TLS ciphers and configuration to secure customer data in transit, and hinder any man-in-the-middle attacks. As a further defense in depth, customer commands to the services are digitally signed using public keys, to prevent any tampering. The services also deploy proven, industry-leading tools and mechanisms to mitigate DDoS attacks and maintain high availability.
- **Control-plane security:** Oracle Cloud Infrastructure backend (control plane) hosts are security isolated from customer instances by using network ACLs. Provisioning and management of customer instances is done by software agents that need to interact with the backend hosts. Only authenticated and authorized software agents can successfully interact with Oracle Cloud Infrastructure backend hosts. For backend hosts, preproduction environments (for example, development, test, and integration) are separated from production environments so that any development and test activities do not have any impact on production systems.
- **Server security and media management:** Oracle has a long history of enterprise-class secure hardware development. Our Hardware Security team is responsible for designing and testing the security of the hardware used to deliver Oracle Cloud Infrastructure services. This team works with our supply chain and tests hardware components to validate them against rigorous Oracle Cloud Infrastructure Hardware security standards. This team also works closely with our product development functions to ensure that hardware can be returned to a pristine safe state after being released by customers
- **Secure host wipe and media destruction:** Oracle Cloud Infrastructure instances are securely wiped after hardware is released by customers. This secure wipe restores hardware to a pristine state. We have reengineered the platform with proprietary hardware components that allow us to wipe and reinitialize the hardware in a secure manner. We follow a media destruction process that adheres to NIST SP 800-88r1 and DoD (Emergency Destruction and up to Secret Classification) standards. Decommissioned drives are degaussed and then physically destroyed using mechanical shredders. Drive decommission workflow is tracked using JIRA and handled by data-center technicians who verify the end results of the workflow.

Secure Software Development

Secure product development requires consistently applied methodologies that conform to clear security objectives and principles. We build security practices into every element of our product development life cycle. Oracle employs formal secure product development standards that are a roadmap and guide for developers. These standards discuss general security knowledge areas

such as design principles and common vulnerabilities, and provide specific guidance on topics such as data validation, data privacy, and user management.

Oracle secure product development standards have evolved and expanded over time to address the common issues affecting code, new threats as they are discovered, and new use cases by Oracle customers. The standards incorporate insights and learned lessons; they do not live in a vacuum, nor are they an “after the fact” addendum to software development. They are integral to language-specific standards such as C/C++, Java, PL/SQL, and others, and are a cornerstone to Oracle's secure development programs and processes.

Security assurance analysis and testing verify security qualities of Oracle products against various types of attacks. There are two broad categories of tests employed for testing Oracle products: static and dynamic analysis. These tests fit differently in the product development lifecycle and tend to find different categories of issues, so they are used together by Oracle product teams.

Personnel Security

Our people make our business. We strive to hire the best, and we invest in and continue to develop our employees. We value training, and we require not only baseline security training for all our employees but also specialized training to keep our teams abreast of the latest security technologies, exploits, and methodologies. In addition to standard annual corporate training programs that cover our information security and privacy programs (among many others), we engage with a broad spectrum of industry groups and send our employees to specialist conferences to collaborate with other industry experts on emerging challenges. The objectives of our security training programs are to help our employees better protect our customers and products, to enable employees to grow in their passion areas around security, and to further our mission to attract and retain the best talent.

We work to recruit the best talent for our team as we grow, and we hire people with strong ethics and good judgment. All our employees undergo pre-employment screening as permitted by law, including criminal background checks and prior-employment validation. We also maintain performance evaluation processes to recognize good performance and help our teams and employees identify opportunities for growth. We maintain both team and employee evaluation processes, and we use security as a component of our team evaluation processes. This approach provides our teams and leadership visibility into how our teams are performing against our security standards and enables us to identify best practices and improvement areas for critical security processes.

Physical Security

Oracle Cloud Infrastructure data centers are designed for security and availability of customer data. This approach begins with our site selection process. Candidate build sites and provider

locations undergo an extensive risk evaluation process that considers environmental threats, power availability and stability, vendor reputation and history, neighboring facility functions (for example, high-risk manufacturing or high-threat targets), and geopolitical considerations among other criteria.

Oracle Cloud Infrastructure data centers align with Uptime Institute and Telecommunications Industry Association (TIA) ANSI/TIA-942-A Tier 3 or Tier 4 standards and follow a N2 redundancy methodology for critical equipment operation. Data centers that house Oracle Cloud Infrastructure services use redundant power sources and maintain generator backups in case of widespread electrical outage. 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 security or availability events that may arise.

We take a layered approach to physical security that starts with the site build. Oracle Cloud Infrastructure data-center facilities are durably built with steel, concrete, or comparable materials, and are designed to withstand impact from a light vehicle strike. Our sites are staffed with security guards who are ready to respond to incidents 24 hours a day, 7 days a week, 365 days a year. The exterior of the sites is secured with perimeter barriers and vehicle checks are actively monitored by a guard force and cameras that cover the building perimeter.

All persons entering our data centers must first go through a layer of security at the site entrances, which are staffed with security guards. Persons without site-specific security badges entering the site must present government-issued identification and have an approved access request granting them access to the data-center building. All employees and visitors must wear visible official identification badges at all times. There are additional security layers between the entrance and server rooms that vary depending on the site build and risk profile. Data-center server rooms are built with additional security layers including cameras that cover server rooms, two-factor access control, and intrusion-detection mechanisms. Physical barriers are in place to create isolated security zones around server and networking racks that span from the floor (including below the raised floor where applicable) to the ceiling (including above ceiling tiles where applicable).

Access to Oracle Cloud Infrastructure data centers is carefully controlled and follows a least-privilege access approach. All access to server rooms must be approved by authorized personnel and is granted only for the necessary period. Access usage is audited, and access provisioned within the system is periodically reviewed by data-center leadership. Server rooms are isolated into secure zones that are managed on a zone-by-zone basis, and access is provisioned only for those zones required by personnel.

Security Operations

The Oracle Cloud Infrastructure Security Operations team is responsible for monitoring and securing the unique Oracle Cloud Infrastructure hosting and virtual networking technologies. The team works and trains directly with the Oracle engineers who develop these technologies to leverage the unique security and introspection capabilities they provide.

We monitor emerging internet security threats daily and implement appropriate response and defense plans to address risks to the business. When we determine that urgent changes are recommended that are within the scope of the customers' responsibilities, we issue security alert bulletins to those customers to ensure their protection.

In the case of a detected or reported security issue that affects Oracle Cloud Infrastructure servers or networks, Security Operations staff is available 24/7 to respond, escalate, or take required corrective action. When necessary, we will escalate and coordinate with external parties (including network and hosting service providers, hardware vendors, or law enforcement) to protect Oracle Cloud Infrastructure, our customers, and our network's security and reputation.

All actions performed in response to a security issue by the Security Operations team are done according to our documented process, and are logged in accordance with compliance requirements. Care is always taken to protect the goals of service and data integrity, privacy, and business continuity.

Customer Data Protection

Data Rights and Ownership

Oracle Cloud Infrastructure customers retain all ownership and intellectual property rights in and to their content. Customer data protection is critically important, and we strive to be transparent with our data protection processes as well as law enforcement requests that we might receive.

Data Privacy

Oracle complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Oracle is also responsible for ensuring that third parties who act as an agent on our behalf do the same.

Oracle has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in our privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit https://www.privacyshield.gov/list.

With respect to personal information received or transferred pursuant to the Privacy Shield Framework, Oracle is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

Oracle continues to adhere to the underlying European privacy principles of the U.S.-Swiss Safe Harbor for the processing of Personal Information received from Switzerland. To learn more about the Safe Harbor program, and to view our certification, visit https://2016.export.gov/safeharbor/swiss/.

Law Enforcement Requests

Except as otherwise required by law, Oracle will promptly notify customers of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority that it receives and which relates to the personal data Oracle is processing on the customer's behalf. Upon customer request, Oracle will provide customers with reasonable information in its possession relevant to the law enforcement request and any assistance reasonably required for them to respond to the request in a timely manner.

Compliance

Oracle Cloud Infrastructure is built for Enterprise. Oracle continues to invest to provide services that help our customers more easily meet their security and compliance needs. Oracle successfully completed ISO/IEC 27001 Stage 2 and Service Organization Control (SOC) 1, 2, and 3 audits for Oracle Cloud Infrastructure.

Independent assurance promotes trust and builds confidence in third-party service provider relationships. In particular, Oracle Cloud Infrastructure's ISO 27001:2013 certification, SOC 1 Type 2 and SOC 2 Type 2 attestations, and SOC 3 attestation offer customers the highest forms of independent assurance available with respect to internal control, data protection, and regulatory compliance. These assurance reports play an important role in customers' internal corporate governance, risk management processes, vendor management programs, and regulatory oversight.

Oracle received a Payment Card Industry Data Security Standard (PCI DSS) Attestation of Compliance (AoC) covering Oracle Cloud Infrastructure services. As a PCI Level 1 Service Provider, customers can use these services for workloads that store, process, or transmit cardholder data.

Oracle also received an attestation performed in accordance with American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements (SSAE) 18, AT-C sections 105 and 205, covering controls aligned with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Breach Notification Rule, and the

applicable parts of the Privacy Rule. Oracle Cloud Infrastructure is categorized as a “no-view cloud service provider” and can support customers who are in scope for HIPAA by entering into a Business Associate Agreement (BAA). The BAA is required for identifying and establishing the respective responsibilities of Oracle Cloud Infrastructure and the customer for appropriately safeguarding PHI in accordance with HIPAA and any amending legislation.

The development, deployment, configuration, and management of underlying services, infrastructure, and systems are the responsibility of Oracle Cloud Infrastructure. Customers are responsible for maintaining and managing their PCI DSS and HIPAA compliance with respect to applications and workloads that they run on Oracle Cloud Infrastructure.

You can find the most recent versions of the Oracle Cloud Infrastructure compliance capabilities at https://cloud.oracle.com/iaas-paas-compliance.

Conclusion

Oracle built Oracle Cloud Infrastructure to enable enterprises to maximize the number of mission-critical workloads that they can migrate to the cloud while continuing to maintain their desired security posture and reduce the overhead of building and operating data-center infrastructure. With Oracle Cloud Infrastructure , enterprise customers get unparalleled control and transparency into their applications running on in the cloud, including:

- Customer isolation that allows customers to deploy their application and data assets in an environment that commits full isolation from other tenants and Oracle’s staff as well as between the same tenant’s workloads.
- Always-on encryption that protects customer data at-rest and HTTPS-only public APIs.
- Easy-to-use security policy that allows customers to constrain access to their services and segregate operational responsibilities to reduce risk associated with malicious and accidental user actions.
- Comprehensive log data that allows customers to audit and monitor actions on their resources, helping them to meet their audit requirements while reducing security and operational risk.
- Identity federation that allows customers to user their existing users and groups in the cloud.
- Support for bringing in third-party software solutions for protecting customer data and resources in the cloud.
- Fault-independent data centers that enable high availability scale-out architectures and are resilient against network attacks, ensuring constant uptime in the face of disaster and security attack.

- Rigorous internal processes and use of effective security controls in all phases of cloud service development and operation.
- Adherence to Oracle's strict security standards through third-party audits, certifications, and attestations. Oracle helps customers demonstrate compliance readiness to internal security and compliance teams, their customers, auditors, and regulators.

All of the Oracle Cloud Infrastructure security capabilities have been designed with one goal in mind: allowing customers to run their mission-critical workloads in the cloud with complete control and confidence. Oracle continues to invest in the above areas and more to offer unmatched security and assurance to enterprise customers.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Oracle Cloud Infrastructure Security
April 2019
Author: Oracle Corporation