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.
# Table of Contents

- Oracle Cloud Infrastructure: Next-Generation Enterprise Cloud .............................................................. 1
- Security Objectives ............................................................................................................................................. 1
- Shared Security Model ........................................................................................................................................ 2
- Security Services and Features .......................................................................................................................... 3
  - Regions and Availability Domains .................................................................................................................. 3
  - Identity and Access Management (IAM) Service ............................................................................................ 3
  - Audit Service .................................................................................................................................................. 5
  - Compute Service ............................................................................................................................................ 5
  - Networking Service ......................................................................................................................................... 6
  - Storage Services ............................................................................................................................................. 7
  - Database Service ........................................................................................................................................... 8
  - Load Balancing Service ................................................................................................................................. 9
  - Managed Domain Name Servers (DNS) Service ........................................................................................... 9
- Infrastructure Security ......................................................................................................................................... 9
  - Security Culture ............................................................................................................................................... 9
  - Security Design and Controls .......................................................................................................................... 10
  - Secure Software Development ......................................................................................................................... 11
  - Personnel Security .......................................................................................................................................... 12
  - Physical Security ............................................................................................................................................ 12
  - Security Operations ....................................................................................................................................... 13
- Customer Data Protection .................................................................................................................................. 13
  - Data Rights and Ownership .............................................................................................................................. 13
  - Data Privacy ................................................................................................................................................... 14
  - Law Enforcement Requests ............................................................................................................................ 14
  - Compliance ..................................................................................................................................................... 14
- Conclusion .......................................................................................................................................................... 14
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 the 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 (BM) 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 non-critical 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 security management solutions that allow them to constrain access to their services and segregate operational responsibilities to reduce 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 the 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 and Availability 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. An Availability Domain is the sub-component of a region and is designed to be independent and highly reliable. Each Availability Domain is built with fully independent infrastructure: buildings, power generators, cooling equipment, and network connectivity. With physical separation comes 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 at least three Availability Domains, which allows customers to deploy highly available applications.

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 groups 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. 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.

- **Identity Provider**: 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. Currently Oracle Cloud Infrastructure supports the Oracle Identity Cloud Service and Microsoft Active Directory Federation Service (ADFS) as identity providers. Federated groups can be mapped to native IAM groups in order to define what policy should apply to a federated user.

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 easy-to-understand syntax:

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

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.

- **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.

**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 (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, user agent, and HTTP headers of the request.

**Compute Service**

Compute is a core component of the 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 (BM) and virtual machine (VM) instances, which allows customers to choose instances that fit their performance, cost, and software flexibility requirements.

» **Bare metal (BM) instances:** In BM 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. All network virtualization is performed off-box and only the Oracle Integrated Lights Out Manager (ILOM) is accessible to the infrastructure (required in order to remotely reboot or reprovision instances). These BM instances offer consistent high performance and are immune to any noisy-neighbor issues. Customers have OS-level administrative privileges to the BM instance. After a customer terminates their BM 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 BM 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 requirements of enterprise customers and their workloads. Oracle Cloud Infrastructure regions have been built with a state-of-the-art, non-blocking Clos network that is not over-subscribed 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 (DRG). 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.

- **Internet Gateway**: Provides public internet connectivity from a VCN. By default, a newly created VCN has no internet connectivity.

- **Dynamic Routing Gateway**: 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.

- **Routing tables**: Virtual routing 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 BM 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.

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**: 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**: 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 customers may 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.

**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 Volumes**: 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.
The Oracle Cloud Infrastructure Block Volumes 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 automated backup and snapshot capabilities. Volumes and their backups are accessible only from within a customer’s VCN and are encrypted at rest using unique keys. For additional security, iSCSI CHAP authentication can be required on a per-volume basis.

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, Oracle highly 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.

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 (LBs) can be created as public (accepting traffic from the internet and directing it to private instances) or private (directing traffic between private instances). LBs can be configured for SSL termination using customer-provided certificates; end-to-end SSL, whereby the LB 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 Servers (DNS) Service

The Oracle Cloud Infrastructure 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 Services (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.

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 our core security components of Security Culture, Security Design and Controls, Secure Software Development, Personnel Security, Physical Security, and Security Operations that we use to protect and secure our customers and business.

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 distributed denial of service (DDoS) attacks and maintain high availability.

» **Control-plane security:** Oracle Cloud Infrastructure back-end (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 back-end hosts. Only authenticated and authorized software agents can successfully interact with Oracle Cloud Infrastructure back-end hosts. For back-end hosts, pre-production environments (for example, dev, test, and integ) 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. When the underlying hardware has reached end-of-life, it is securely destroyed. Before leaving our data centers, drives are rendered unusable by using industry-leading media destruction devices.

**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 housing 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://safeharbor.export.gov/swisslist.aspx.

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. We operate under practices aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which we have identified a comprehensive set of security controls that apply to our business. Oracle Cloud Infrastructure is still a new product line, and we must operate for a period of time in order for these security controls and our operations to undergo external audit. As an enterprise cloud, we plan to pursue a broad suite of industry and government certifications, audits, and regulatory programs.

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 use 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.