Oracle Zero Trust Cloud Adoption

Implement Zero Trust Architecture in Oracle Cloud Infrastructure

Oracle

January, 2024, Version 1.0

Public

Disclaimer

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

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

Table of contents

List of figures

List of tables

Executive Summary

This paper reviews the security features available in the Oracle Cloud applied to the Defense Information Systems Agency (DISA) Zero-Trust Reference Architecture. The DISA Reference Architecture decomposes the implementation of Zero Trust into seven pillars so organizations can prioritize deployment. Oracle has features and services that support each of the pillars, which can speed up implementation time. The seven DISA Pillars are:

1. User
2. Device
3. Application & Workload
4. Data
5. Network & Environment
6. Automation & Orchestration
7. Visibility & Analytics

Though organized around the DISA Zero-Trust Reference Architecture, this paper is meant for all organizations looking to achieve greater security in with the Oracle Cloud. The pillars provide a means to understand the implementation of technology to meet Zero-Trust security.

Implementing a Zero Trust security model is critical to securing workloads in the cloud. Organizations moving to the cloud must implement Zero Trust throughout the enterprise. Oracle Cloud supports Zero Trust adoption and helps you secure your mission-critical data and workloads.

Oracle Zero Trust

Introduction

What is Zero Trust?

Outdated perimeter defense models are failing to secure organizational data. Today, organizational boundaries are no longer limited to on-premises information technology, as organizations can also incorporate devices external to their network perimeter, including remote or mobile devices. The adoption of cloud technologies further expands an organization's security boundary, requiring a multifaceted approach to cybersecurity. As cyberattacks continue to become more complex and impactful, it is crucial for organizations to adopt a more aggressive approach to securing their data. Successful ransomware attacks can cripple a business or enterprise, resulting in the loss of critical functionality and exposing sensitive information.

A Zero-Trust (ZT) approach assumes no device or resource should be trusted without authentication and authorization. This approach presumes breach and therefore focuses on transactional security, constant monitoring, automated responses to confirmed anomalies, and prevention of lateral movement. All assets are protected based on their value, and a defense in depth approach is implemented across the enterprise. In a Zero-Trust environment, resources are queried to provide authorization/authentication at the transaction level. Infrastructure is monitored using advanced analysis to systemically identify anomalous behavior and act immediately to lock down intrusion.

With a Zero-Trust security approach, the organization presumes a hostile environment: there is no place within the enterprise that does not need security. Further, the organization presumes a breach has already occurred with the expectation that threat actors are already operating in the enterprise. A Zero-Trust environment denies by default rather than allowing access after authentication. Resources are accessed only after proper authentication and with the proper authorization. Further, a constant review of permissions should take place to remove unneeded access.

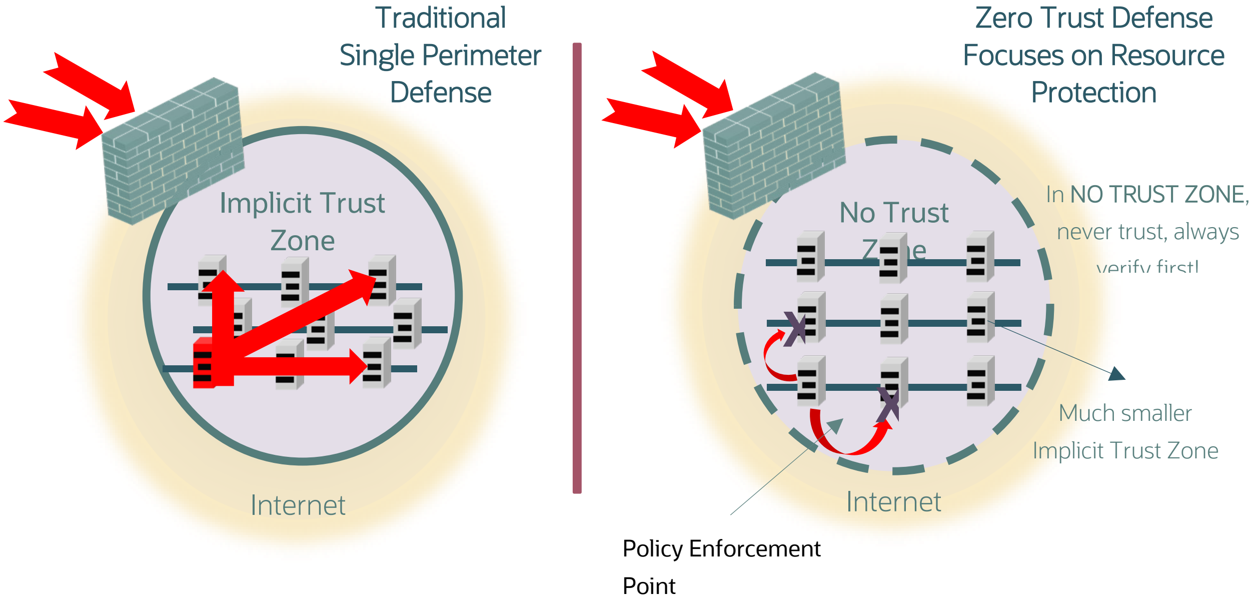
Traditional Single Perimeter Defense
Implicit Trust Zone
Internet
Zero Trust Defense Focuses on Resource Protection
No Trust Zone
In NO TRUST ZONE, never trust, always verify first!
Much smaller Implicit Trust Zone
Internet
Policy Enforcement Point

Figure 1: Zero Trust Defense compared to Traditional Single Perimeter Defense

Integrating Cloud Computing can augment existing enterprise security solutions. Oracle Cloud Infrastructure implements foundational security within the infrastructure at the core and offers a wide range of services and tools for organizations to implement Zero-Trust controls.

Adopting a Zero-Trust architecture can be difficult and challenging. Implementing security technology, though critical, takes time and consideration. This is especially true when an organization does not integrate security during the development phase of their technology solution. Still, organizations must take the time and effort to ensure their workloads and solutions are secure throughout execution.

US Department of Defense Zero Trust Reference Architecture

The topic of Zero Trust is a major focus on the US Department of Defense (DoD) and the US Government. In May of 2021, the White House issued Executive Order 14028 which directs federal agencies to protect and secure their computer systems by adopting security best practices and advancing toward Zero Trust Architecture which is a major tool toward accomplishing this security strategy.

There are several models or frameworks available to help develop a Zero-Trust architecture. The National Institute of Standards and Technology (NIST) has devised a 5-tenant model, published in Special Publication 800-207, to help organize the implementation of a Zero-Trust environment. The Cybersecurity and Infrastructure Security Agency (CISA) recently published a Zero Trust Maturity Model version 2, which is comprised of 5 domains.

Finally, the Defense Information Security Agency (DISA) published a reference architecture aligning enterprise technology with 7 pillars.

All these approaches aim to assist organizations with the implementation of Zero-Trust. These models and their associated architecture bring structure and help to scope the effort needed to successfully deploy a secure defense solution. In this paper, we will use the DoD Zero Trust Reference Architecture published by the DISA to structure our discussion.

In the DoD ZT Reference Architecture (RA), enterprise resources are assigned to specific functional pillars. These pillars can then be used to review and assess the enterprise and the technology solutions being implemented. The DoD ZT RA seven pillars are:

1. Users
2. Devices
3. Workloads
4. Data
5. Network/Environment
6. Automation & Orchestration
7. Visibility & Analytics
8. Data

Oracle Cloud Zero Trust

Oracle Cloud is built with integrated security, that applies network segregation within the infrastructure. This approach reduces the risk from hypervisor-based attacks and increases tenant isolation. Oracle integrates another layer of security control with bare metal compute that provides you isolation and control with dedicated physical server access.

Oracle implements encryption by default with data at-rest and in-transit. Oracle provides TLS 1.2 encryption in-transit. Oracle provides keys for encryption, but recommends you bring your own keys for additional security. You can keep and manage your keys using Oracle Private Virtual Vault to ensure data is protected throughout its lifecycle. For protecting data at-rest within the database, Oracle Cloud uses Transparent Data Encryption (TDE). TDE ensures data is encrypted within the Database Management System and within the backup mechanism so you can be certain their data is safe from prying eyes.

Oracle Cloud is built on a deny-by-default paradigm. All actions within a customer tenancy must be explicitly allowed. A customer tenancy is provided a single administrative account for initial access and setup, then the customer then sets up their administrative structure as needed. The cloud tenancy will require explicit policies to allow new groups and users to accomplish all tasks. You have fine-grained control of resources within the Oracle Cloud.

Oracle Cloud segregates the network layer which eliminates network noise and improves both security and efficiency. This segregation prevents lateral movement and separates the network and tenant environment.

Oracle customers are isolated from each other, isolated from the cloud infrastructure support team members, can isolate within their own lines of business, and can isolate from external actors. This security posture prevents exposure and encapsulates organizational data to avoid spillage.

Oracle designs, develops, and securely sources its hardware. Oracle directs all hardware manufacturing and is the only cloud service provider that also designs and sells x86 hardware. Controlling the supply chain ensures availability of required hardware and confirms that the hardware has not been tampered with prior to installation.

Shared Security Model

Oracle Cloud has a wide variety of tools and services that align with the 7 pillars, enabling the implementation of a secure Zero-Trust environment. Customers are responsible for deciding which security services to implement. This paper will discuss fundamental implementations of a Zero-Trust reference architecture, foundational capabilities to secure the cloud, and services available for customer implementation. Customers are primarily responsible for securing their organizational data. The data, controls, and features implemented to protect enterprise resources are solely within the purview of the customer. Oracle provides the tools; the customer must implement them. Failure to implement security measures will leave the tenancy open to attack.

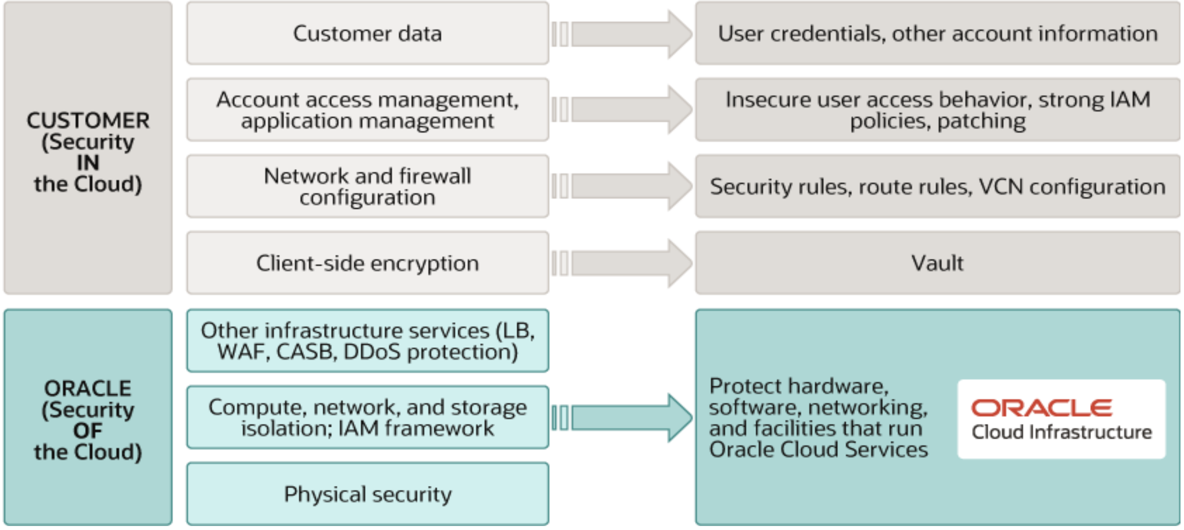
CUSTOMER (Security IN the Cloud)
Customer data
User credentials, other account information
Account access management, application management
Insecure user access behavior, strong IAM policies, patching
Network and firewall configuration
Security rules, route rules, VCN configuration
Client-side encryption
Vault
ORACLE (Security OF the Cloud)
Other infrastructure services (LB, WAF, CASB, DDoS protection)
Compute, network, and storage isolation; IAM framework
Physical security
Protect hardware, software, networking, and facilities that run Oracle Cloud Services
ORACLE Cloud Infrastructure

Figure 2: Shared Security Model

Identity and Access Management

Identity and Access Management (IAM) is a foundational function necessary to secure the tenancy. Control of a tenancy rests on the proper implementation of IAM. When a customer is provisioned, a single administrator is created in an administrator group. This account is used to perform the preliminary configuration of the tenancy and is then reserved for break-glass support.

Oracle IAM requires the customer to develop the proper groups and users to support the tenancy. Users are assigned to groups and policy statements are executed to allow groups to perform functions within the tenancy. Unless specifically allowed by a policy, users and groups are denied access to perform any function. Users can be administrators and support that have direct access to cloud resources or external users that are part of the enterprise, but do not need increased permissions. Oracle Domains supports segregating these users and helps manage their permissions and access to keep the tenancy secure.

Another functional tool available for you is the compartment. A compartment is a logical grouping of Oracle Cloud resources, which can be used to limit and control access within the tenancy. Policies can be assigned within the compartment and applied to resources, providing fine-grain control of tenancy resources. Compartments can also be used to track costs. Compartments are a foundational mechanism that helps logically separate the enterprise solution, allowing for fine-grained control and access. This tool adds another layer of security for cloud security.

Oracle Secure Landing Zones

Oracle Cloud Landing Zones are prebuilt, curated templates that automate tenancy setup and resource provisioning for various use cases. Landing Zones provide prescriptive optimal design and hardened configurations—including for security, compliance, networking, identity, and more—that are based on industry best practices and Oracle's expertise. Based on open frameworks—Terraform—Landing Zones enable customers to manage their infrastructure deployments in a safe, secure, and predictable fashion. This well-architected foundation enables customers to accelerate cloud onboarding, simplify future operations at scale, and ensure your environment is secure, performant, and cost-effective. Oracle's Landing Zones deploy the needed Oracle Cloud resources that are pre-configured with the services and controls required to support security and Zero-Trust best practices related to:

- IAM (Identity & Access Management)
- Networking
- Keys
- Cloud Guard
- Logging
- Vulnerability Scanning
- Bastion
- Events
- Alarms
- Notifications
- Object Storage
- Budgets
- Security Zone
- Other required workloads

Landing Zones provide a secure foundation and starting point to support Zero-Trust requirements. For example, Oracle Center for Internet Security (CIS) Landing Zone is based on the CIS Foundations Benchmark. It provides a strong foundation for tenancy security. The landing zone implements resource segmentation, a core set of identity policies, and can be customized to meet your infrastructure requirements. The CIS Landing Zone is available from the GitHub repository. [1]

Oracle Enterprise Landing Zone[2] (OELZ) is another starting point for building a secure foundation with a multi-environment architecture that includes production and non-production compartments. OELZ supports multicloud and deploys a hub and spoke architecture that accommodates most enterprise network requirements. You can optionally integrate with Microsoft Active Directory for identity management. OELZ is fully modular and extensible so you can add the specific technology stack you need.

Oracle landing zone solutions help reduce your time-to-production, while maintaining a flexible implementation to support your needs. Customers can modify the Terraform templates to meet specific needs, including support for private vaults and network firewall placement. You can deploy the Landing Zone in a test environment to ensure it meets your requirements and then promote it to a production environment. Oracle uses Terraform templates for

[1] https://github.com/oracle-quickstart/oci-cis-landingzone-quickstart/tree/main

[2] https://docs.oracle.com/en-us/iaas/Content/cloud-adoption-framework/landing-zone-v2.htm

Infrastructure as Code, which allows you to use Oracle Resource Management to manage the Terraform code and deployments. The use of repeatable and reviewable code increases the security posture of the enterprise by automating the deployment process. With Oracle Resource Manager, you can also lock down tenancy configurations and ensure a repeatable outcome each time resources need to be deployed.

NIST Tenets and Oracle Cloud

The NIST special publication 800-207 lists seven tenets of a Zero Trust Architecture. These are:

1. All data sources and computing resources are considered resources.
2. All communications are secured regardless of network location.
3. Access to individual enterprise resources is granted on a per session basis.
4. Access to resource is determined by dynamic policy.
5. The Enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets.

Access to every element of the Oracle Cloud requires explicit policies to allow use. This means each component is considered a resource within the Oracle Cloud and access must be explicitly granted. All communications within the Oracle Cloud is encrypted by default with Oracle-provided keys. Prior to access to any resource, access is checked against existing policies, and policies can be structured to grant extremely fine-grained control and access for each resource to include implementing dynamic access. The Oracle Cloud implements monitoring and auditing on cloud resources, allowing you to use existing object storage to conduct analysis or use an existing Security Information and Event Management (SIEM) tool of choice to appropriately monitor the enterprise. Our Cloud Guard solution provides automated responses to triggered events to speed up reaction time to potential threat actions. Oracle technology provides tools to support the implementation of Zero Trust principals and tenets.

The DoD Pillars

As discussed in the DoD Zero Trust Reference Architecture, the seven pillars are areas of focus for implementing controls and technology to meet security standards. Additionally, the pillars provide a means to visualize the scope of implementing a Zero Trust solution and apply increasingly secure technologies to deploy in depth access controls. We use these pillars to align our technology with implementation strategies. It should be noted that one technology or service can meet a variety of requirements in different pillars. Organizations should develop their Zero Trust security adoption implementation strategy based on their identified security requirements. Zero Trust implementation in a mature enterprise can take a long time while teams ensure mission functionality. Identifying the technology available to implement security can improve implementation timelines and speed up the deployment process.

In the following sections, we will discuss the available technology based on the pillar it supports. Organizations should consider which technology meets their security needs and plan the deployment within their tenancy to implement a Zero Trust architecture.

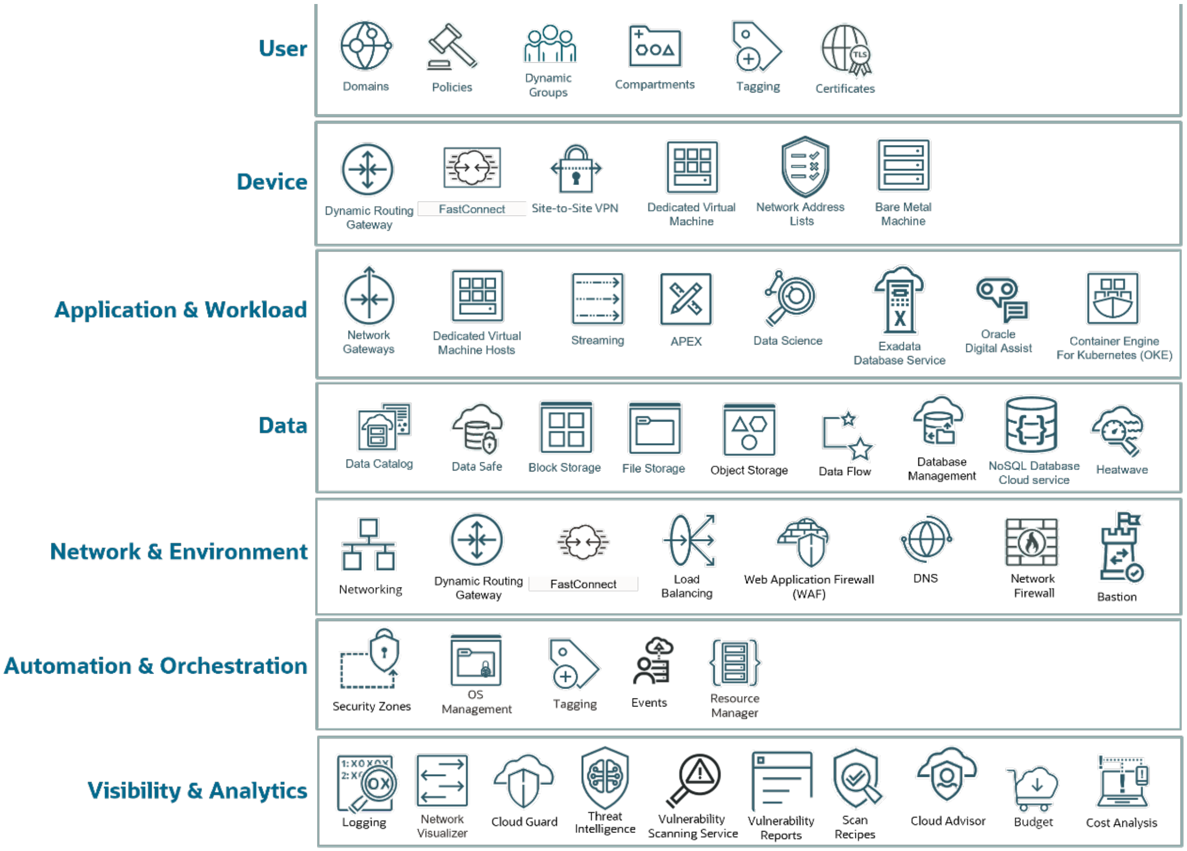

Figure 3: Services by Pillar

Pillar 1: User

The users of the information system represent the people accessing the environment and the people performing administration. Many of the services supporting users and access control can be found in the Identity and Access Management functional domain of the Oracle Cloud environment.

As explained in the DoD ZT RA, the user pillar will secure, limit, and enforce both person and non-person access to the Data, Assets, Applications & Services (DAAS). Access controls must be implemented for the protected resources. There are several services that work in tandem to control and maintain access for the users. Table 1 summarizes the tools available.

Oracle Cloud Component	Description	Zero Trust Applicability
Identity Domains	Identity Domains are an identity solution that creates the ability to group users with their own settings and configurations. Identity Domains enables federation with external identity providers. A user population is defined by the Identity Domain, which provides overarching access control for the user base.	Defining and controlling access to resources is a prime function and focus of Zero Trust. Identity Domains provide an easy means to segregate the user population and apply access to users based on their function and purpose.
Policies	Policies are statements that enable access to resources. Oracle Cloud is deny by default. In order to perform any action on an Oracle Cloud resource, a policy statement is required.	Policies allow for fine-grained access control to Oracle Cloud resources and are the means to allow any activity to take place. Oracle Cloud is deny by default. Policies are the mechanism to explicitly allow access.

Oracle Cloud Component	Description	Zero Trust Applicability
Dynamic Groups	Dynamic groups allow you to group compute instances and other resources as "principal" actors (similar to user groups). You can then create policies to permit the resources to make API calls against services.	Dynamic groups allow for non-user principals to be included in policy statements which in turn allows for Oracle Cloud resources to securely make API calls against other Oracle Cloud resources.
Compartments	Compartments are logical groupings of resources within a tenancy. They provide a means to control access to resources, track budget, and logically group resources.	Compartments make resource segmentation possible. An Oracle Cloud customer can restrict access to resources by referencing compartments in identity policies.
Tagging	Oracle Cloud Infrastructure Tagging allows you to add metadata to resources, which enables you to define keys and values, then associate them with resources.	Tagging extends policy by allowing a customer to tag resources and then reference tags in identity policies. This is what Oracle Cloud refers to as Tag Based Access Control (TBAC) which is related to Attribute Based Access Control (ABAC). This is another mechanism to control access to cloud resources.
Certificates	Certificates provides organizations with certificate issuance, storage, and management capabilities, including revocation and automatic renewal. If you have a third-party certificate authority (CA) that you already use, you can import certificates issued by that CA for use in an Oracle Cloud tenancy. Integration with Oracle Cloud Load Balancer allows you seamlessly associate a TLS certificate issued or managed by Certificates with resources that need certificates. The Certificates Service lets you create and manage Certificate authorities (CAs), Certificates, and CA Bundles.	By controlling the certificates, you can ensure resources are approved to authorize access and connect to cloud resources. Oracle Certificates enables you to seamlessly integrate with existing certificate stores and include the same security controls within the cloud.

Oracle Cloud Component	Description	Zero Trust Applicability
Vault	Oracle Cloud Vault is a key management service that stores and manages master encryption keys and secrets for secure access to Oracle Cloud resources. Vault lets you securely store master encryption keys and secrets that you might otherwise store in configuration files or in code. Specifically, depending on the protection mode, vault keys are either stored on the server or they are stored on highly available and durable Hardware Security Modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification. The key encryption algorithms that the Vault service supports includes the Advanced Encryption Standard (AES), the Rivest-Shamir-Adleman (RSA) algorithm, and the elliptic curve digital signature algorithm (ECDSA). You can create and use AES symmetric keys and RSA asymmetric keys for encryption and decryption. You can also use RSA or ECDSA asymmetric keys for signing digital messages.	Oracle Cloud Vault service provides a way for you to securely store and access encryption keys and other secrets. Before a user or a service can access a vault, a policy must be written granting access to the vault. Users can create fine-tuned granular access control policies related to vault access.
Oracle Access Governance	Access Governance is a cloud native identity governance and administration (IGA) service that provides enterprise-wide visibility to govern access to cloud and on-premises environments	Oracle Access Governance provides a number of services to secure your tenancy. This includes creating custom identity attributes, identity marking, Attribute Based Access Control (ABAC), enhanced Role Based Access Control (RBAC), access control tracking and evaluation. These tools help administrators review the administrator access for your tenancy. Understanding access control within the tenancy is a primary goal of Zero-Trust implementation policies.
Key Management	Oracle Cloud Infrastructure Vault is a key management service that stores and manages master encryption keys and secrets for secure access to Oracle Cloud resources. Vault lets you securely store master encryption keys and secrets that you might otherwise store in configuration files or in code. Specifically, depending on the protection mode, vault keys are either stored on the server or they are stored on highly available and durable hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification.	Customer Key Management lets you bring your own encryption keys to the cloud resources, replacing the Oracle provided keys and ensuring you encrypt your data at-rest and in-transit using the same keys throughout the enterprise. Data is encrypted in Oracle Cloud. If you do not bring your own keys, Oracle will provide the keys to encrypt all cloud resources. Oracle strongly recommends you use your own keys to protect your data using the Key Management function.

Table 1: User Pillar Services

Pillar 2: Devices

The second pillar in the DISA Zero Trust Reference Architecture is Devices. In this pillar lies the devices that connect to the enterprise. We also include in this layer specific mechanisms used to directly connect customer devices to the Oracle Cloud.

Oracle Cloud Component	Description	Zero Trust Applicability
Dynamic Routing Gateway 2	The DRG v2 works as a virtual router, sending traffic from the customer on premises environment to the cloud or from existing Virtual Cloud Networks (VCNs) in Oracle Cloud.	The DRG establishes high availability for resources in connected VCNs, while simplifying the connection configuration. DRG V2 are important elements in creating a secure connection between the on-premises environment and the Oracle Cloud.
Fast Connect	FastConnect establishes a secure, direct connection between on premises environments and Oracle Cloud resources.	Provides private access to the cloud resources from a customer facility. A variety of security controls can be implemented to manage the privacy of the connection.
Shielded Instances	Shielded instances harden the firmware security on bare metal hosts and virtual machines (VMs) to defend against malicious boot level software.	By using Secure Boot, Measured Boot and Trusted Platform Module (TPM) support, Oracle Cloud Shielded Instances are protected from attacks such as root kits.
Dedicated Virtual Machines	Deploy Virtual Machines (VM) on dedicated hardware without sharing any underlying infrastructure with another tenant. Meet compliance, regulatory requirements, or meet host-based licensing requirements by using dedicated VMs.	The Dedicated VM ensures the VM is fully segregated from other tenants. You can secure specific workloads and lock down resources on the VM to achieve fine-grained security control.
Network Access Lists	Network Access Lists on the provisioned VM to provide specific port and protocol control in conjunction with the VCN rules.	Using Network Access Lists, you can define specific routes for ports and protocols for specific resources. Specific devices can have specific traffic available while protecting the rest of the network infrastructure.
Bare Metal Machines	With Oracle Cloud Bare Metal Hosting, the customer has complete isolation for a server. Nothing is shared with other tenants.	By taking complete control of the server, the customer can support high compute dedicated workloads, improve performance, and increase security by applying dedicated controls around the device.
OS Management	The OS Management Service supports the patching for certain operating systems (Linux & Windows Server). This Service provides a means to list needed patches and deploy them for collections of systems.	Maintaining the proper patching for client devices is critical to ensuring a proper security environment. A Zero Trust environment requires that devices have the latest software and remain patched to prevent threats from exploiting vulnerabilities.

Table 2: Device Pillar Services

Pillar 3: Application & Workload

The third pillar in the DISA Zero Trust Reference Architecture is Application and Workload. This is a wide spanning pillar that focuses on the workloads and services used in the enterprise. From the computers used to the applications they run; the enterprise customer must secure all resources in a presumed hostile environment. From a cloud perspective, this includes securing the applications hosted in the cloud and the resources in use to host and manage those capabilities.

While securing the enterprise, you should also consider on-premises technology. Adopting a zero-trust paradigm means securing the entire enterprise.

You can leverage the underlying security available with Oracle Cloud to provide your first line of defense, backed by premier Oracle security.

Oracle Cloud Component	Description	Zero Trust Applicability
Network Gateways	Network Gateways enable communication with destinations outside of the VCN. Network Gateways include Internet, NAT, Dynamic routing, Service, Local peering.	Network Gateways provide control over how and where traffic can flow. For example, not configuring an internet gateway ensures no external traffic can reach a subnet. Network Gateways provide port and protocol level control for cloud resources.
Streaming	The Streaming service provides a fully managed, scalable, and durable solution for ingesting and consuming high-volume data streams in real time. Use Streaming for any use case in which data is produced and processed continually and sequentially in a publish-subscribe messaging model.	Streaming data is encrypted both at-rest and in-transit, ensuring message integrity. You can let Oracle manage encryption or use the Oracle Cloud Vault service to securely store and manage your own encryption keys if you need to meet specific compliance or security standards. Integration with Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who and what services can access which keys and what they can do with those resources. Private endpoints restrict access to a specified VCN within your tenancy so that its streams cannot be accessed through the internet.
APEX	APEX is an integrated platform for developing and running low-code/no-code applications. APEX is readily available in Oracle Database Engine which can be consumed through a web console by the developers and the application users. The applications are developed by the APEX App builder or through APEX enabled Integrated Development Environment (IDE) and deployed to the APEX runtime instance instantly or through export operation.	Oracle APEX comes with a comprehensive set of built-in authentication schemes that make it simple to integrate with Cloud-based authentication providers, your LDAP repository or using the local Oracle APEX workspace repository. Define access to your application, pages and page components with authorization schemes. Use the built-in Application Access Control to manage users and roles. With APEX, you can quickly deploy secure data centered applications for your enterprise.

Oracle Cloud Component	Description	Zero Trust Applicability
Exadata Cloud Service	Exadata Service enables fully featured Oracle Databases to run on the Exadata platform in the cloud environment. Exadata Service instances come pre-configured according to best practices that have been proven at thousands of mission-critical Exadata sites around the world	Databases provisioned on the Exadata Service include all the features of Oracle Database Enterprise Edition, all Oracle Enterprise Manager Packs, and all Database Enterprise Edition Options, such as: Oracle Multi-tenant, Oracle Database In-Memory, Oracle RAC, Oracle Advanced Security, Oracle Active Data Guard. Key security features include: • Data Safe • Identity Management • Transparent Data Encryption • Network Encryption • Database Vault • Audit Vault • Key Vault • Database Firewall • Virtual Private Database • Label Security • Data Redaction • Data Masking & Subsetting
Oracle Digital Assistant	Oracle Digital Assistant is a platform that allows you to create and deploy digital assistants, which are AI-driven interfaces that help users accomplish a variety of tasks in natural language conversations.	Automating and supporting user tasks support the redundant and repeatable nature of security tasks ensuring the same outcome occurs each time a task is executed. Reducing the variability in task execution supports repeatable processes.
Container Engine for Kubernetes (OKE)	Oracle 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. They can use Container Engine for Kubernetes (OKE) when your development team wants to reliably build, deploy, and manage cloud-native applications. This service allows you to focus on deploying and running your containerized applications without having to deploy and maintain your own container orchestration layer.	Kubernetes ships an integrated Role-Based Access Control (RBAC) component that matches an incoming user or group to a set of permissions which are bundled into roles. These permissions combine verbs (get, create, delete) with resources (pods, services, nodes) and can be scoped to a namespace or cluster. A set of preconfigured roles are provided which offer reasonable default separation of responsibility, depending on what actions a client might want to perform.
Zero Trust Packet Networking	Oracle Zero Trust Packet Routing Platform's intent-based security policy helps constrain data movement in and between distributed environments and control user and application interactions with the data. You can use your network devices to track and block threats to your data wherever it is stored, creating a unified layer of security.	Zero Trust Packet Routing Platform helps prevent data leaks and insider threats by restricting attackers' ability to move laterally and enforcing strict access control policies based on the identity and attributes of both the data and the communicating resources.

Oracle Cloud Component	Description	Zero Trust Applicability
Oracle Cloud CIS Foundation Benchmark	Oracle CIS benchmark provides prescriptive guidance for establishing a secure baseline configuration for the Oracle Cloud Infrastructure environment. The scope of this benchmark is to establish a base level of security for anyone utilizing the included Oracle Cloud Infrastructure services. The benchmark is, however, not an exhaustive list of all possible security configurations and architecture.	The CIS Foundation Benchmark is a starting point for an enterprise to customize to meet specific security targets. The baseline is a foundational programmatic deployment. You customize the baseline, incorporate your own specific security requirements, add additional security features, and deploy. This reduces the potential for mistakes and is a repeatable solution.

Table 3: Application and Workload Services

Pillar 4: Data

The fourth pillar in the DISA Zero Trust Reference Architecture is Data. Protecting data is one of the highest priorities for most customers, and Oracle has a variety of tools to protect and secure data. All data is encrypted at-rest within Oracle Cloud and is encrypted in-transit.

Oracle Cloud Component	Description	Zero Trust Applicability
Data Safe	The Oracle Data Safe service empowers you to understand data sensitivity, evaluate data risks, mask sensitive data, implement and monitor security controls, assess user security, and monitor user activity—all in a single, unified console.	Data Safe gives you the power to understand your data models and make the decisions needed to protect that data. Data Safe capabilities help to manage the day-to-day security and compliance requirements of Oracle Databases.
Data-At-Rest Encryption	Encryption of data at-rest is not something that a tenant administrator needs to enable; it is enabled by default for Object, Block, and File storage.	You can use Key Management Service to manage your own master encryption keys for data at-rest encryption.
Data In-Transit Encryption	For encryption in-transit, Oracle Cloud provides TLS 1.2-encrypted connections for all endpoints published by Oracle such as API endpoints and the cloud console, etc. In addition, traffic between compute instances and its boot volumes and block volumes can be encrypted through configuration during the creation of compute instances.	Encryption for data in-transit over the network is automatically configured and enforced by Oracle.
Database Vault	Oracle Database Vault provides controls to prevent unauthorized privileged users from accessing sensitive data and to prevent unauthorized database changes.	Oracle Database Vault realms, command rules, factors, and separation of duty features help reduce the overall security risks addressed by regulation provisions worldwide.
Data Catalog	Data Catalog is a fully managed, self-service, data discovery and data governance solution for the enterprise data. With Data Catalog, you get a single collaborative environment to manage technical, business, and operational metadata.	Oracle data catalog can be used for managing data, data governance, and can provide an invaluable repository of existing data assets.

Oracle Cloud Component	Description	Zero Trust Applicability
Data Flow	Data Flow is a fully managed service for running Apache Spark ™ applications. It allows developers to focus on your applications and provides an easy runtime environment to execute them. It has an easy and simple user interface with API support for integration with applications and workflows. Runtime support includes Apache Spark SQL, Streaming, Machine Learning and Graph.	Private endpoints allow Data Flow to access data sources that are only accessible privately in the Oracle Cloud, or access on-premises data sources using Oracle Site-to-Site VPN or Oracle FastConnect.

Table 4: Data Pillar Services

Pillar 5: Network & Environment

The fifth pillar in the DISA Zero Trust Reference Architecture is Network and Environment. This pillar covers the network layer and all the physical connections that should be isolated and controlled granularly. Micro segmentation should be implemented, and data flows should be understood and controlled.

Oracle Cloud Component	Description	Zero Trust Applicability
Networking	The Oracle Cloud physical network is designed for customer and service isolation. It is segmented into enclaves with unique communications profiles. Access into and out of these enclaves is controlled, monitored, and driven by policy. Oracle personnel must have explicit user privileges, granted by authorized persons, to access the services enclave. This access is subject to regular auditing and review. Service enclaves are local to a region, so any necessary traffic between them goes through the same security mechanisms as internet traffic such as inbound SSH bastion hosts and outbound SSL proxies.	Hyper segmentation separates cloud service workloads running in a service enclave from customer workloads that run on your own physical network. It enables strict monitoring and control over traffic flows between hyper segmented enclaves within the Oracle Cloud substrate. It implements least privileged access for services within the Oracle Cloud services network by controlling access both in and out of the enclaves.
Dynamic Routing Gateway	Dynamic Routing Gateway is an optional virtual router that you can add to your VCN. It provides a path for private network traffic between your VCN and on-premises network. You can use it with other Networking components and a router in your on-premises network to establish a connection by way of Site-to-Site VPN or Oracle Cloud FastConnect. It can also provide a path for private network traffic between your VCN and another VCN in a different region.	Gateways (Internet, Network Address Translation or NAT, Dynamic Routing, Service, etc.) provide control over how and where traffic can flow. Gateway policy is tightly integrated with IAM.
Security Lists and Network Security Groups	Security lists and network security groups provide the ability to control traffic flow within and across subnets and VCNs within a tenancy.	Controlling network access to resources prevents exploitation and reduces the threat environment. Controlling the protocols and ports that are available for exploitation further secures the resources and prevents tampering.

Oracle Cloud Component	Description	Zero Trust Applicability
DDoS Protection	Oracle Cloud provides an always-on detection and mitigation platform for common layer 3 and 4 volumetric DDoS attacks such as SYN floods, UDP floods, ICMP floods, and NTP amplification attacks. This is provided by default and is transparent to users.	DDoS protection helps to mitigate customer workloads from the risk of a volumetric DDoS attack. This service is provided as standard with all Oracle Cloud accounts at no extra cost and requires no configuration or monitoring.
Web Application Firewall	Web Application Firewall (WAF) delivers a cloud native, Oracle-managed web application firewall, designed to help protect applications from malicious requests and requesters. The service enables layer 7 protection for web applications published on the internet.	WAF can be deployed to ensure that any services exposed to the internet have layer 7 protection for the web application itself. Also, it can be used to provide additional layer of security onto legacy applications that may not support the latest security standards such as TLS
Domain Name System (DNS)	Oracle Cloud provides a global anycast, fully managed DNS service that can be used as a primary or secondary DNS service.	Oracle Cloud DNS provides both public and private DNS resolvers. The capability provides built in layer 3 and 4 protection against DDoS.
Network Firewall	Network Firewall is a next-generation managed network firewall and intrusion detection and prevention service for your Oracle Cloud Infrastructure VCN, powered by Palo Alto Networks®. The Network Firewall service offers simple setup and deployment and gives you visibility into traffic entering your cloud environment (north-south network traffic) as well traffic between subnets (east-west network traffic)	Stateful network filtering creates rules that allow or deny network traffic based on source IP (IPv4 and IPv6), destination IP (IPv4 and IPv6), port, and protocol. Custom URL and FQDN filtering restricts ingress and egress traffic to a specified list of fully qualified domain names (FQDNs), including wild cards and custom URLs. The Network Firewall also provides Intrusion Detection and Prevention (IDPS), SSL inspection, and VCN to -VCN subnet traffic inspection.
Bastion	Oracle Infrastructure Bastion provides restricted and time-limited access to target resources that don't have public endpoints. Bastions let authorized users connect from specific IP addresses to target resources using Secure Shell (SSH) sessions. When connected, users can interact with the target resource by using any software or protocol supported by SSH.	Bastions are essential in tenancies with stricter resource controls. For example, you can use a bastion to access compute instances in compartments that are associated with a security zone. Instances in a security zone cannot have public endpoints. Integration with Oracle Cloud Identity and Access Management (IAM) lets you control who can access a bastion or a session and what they can do with those resources.

Table 5: Network and Environment Pillar Services

Pillar 6: Automation & Orchestration

The sixth pillar in the DISA Zero Trust Reference Architecture is Automation and Orchestration. There are significant benefits from automating responses in the cloud as speed and repeatability both increase the security posture. The more you can rely on repeatable processes and automated responses, the more you can focus on other challenges. Oracle Cloud has several services that support repeatable security processes.

Oracle Cloud Component	Description	Zero Trust Applicability
Security Zones	Security Zones let you be confident that your Oracle Cloud resources, including Compute, Networking, Object Storage, and Database, comply with Oracle security principles. Security Zones integrates with Cloud Guard to identify policy violations in existing resources.	A security zone is associated with a compartment and a security zone recipe. When you create and update resources in a security zone, Oracle Cloud validates these operations against the list of policies defined in the security zone recipe. If any security zone policy is violated, then the operation is denied.
OS Management	OS Management Service enables management of updates and patches for the operating system environment on Oracle Cloud instances that are not running Autonomous Linux.	OS Management can be used to check that the operating systems running applications and services are kept up to date with the latest patches, thereby helping to reduce the risk of a known vulnerability in the OS being exploited.
Tagging	Oracle Cloud Resource Tagging allows keys and values to be defined and associated with resources.	Resource tags can be used by organizations to organize and list resources used for specific projects or systems.
Events	Oracle Cloud services emit industry standard Cloud Event format events which can indicate change in resources. Actions can be taken on the back of these events, such as: Notifications – sending emails, SMS etc. notifications Functions – executing a serverless function. Streaming – publishing an event to a stream.	Events can be used to indicate a change in a resource and can therefore be leveraged to identify potential changes to the health of a service.
Resource Manager	Resource Manager automates deployment and operations for all Oracle Cloud resources. Using the infrastructure-as-code (IaC) model, the service is based on Terraform, an open-source industry standard that lets DevOps engineers develop and deploy your infrastructure anywhere. A Terraform configuration codifies your infrastructure in declarative configuration files. Resource Manager allows you to share and manage infrastructure configurations and state files across multiple teams and platforms	The ability to confidently repeat deployment of resources within the cloud is an important part of ensuring the same security technology is present. Resource Manager is the deployment mechanism where Infrastructure as Code can be used to confidently deploy solutions consistently.

Table 6: Automation and Orchestration Pillar Services

Pillar 7: Visibility & Analytics

The seventh pillar in the DISA Zero Trust Reference Architecture is Visibility and Analytics. Observing the enterprise means being aggressively focused on potential problems. In a Zero Trust environment, the enterprise is constantly reviewing telemetry looking for signs of potential attack. The vast amount of data requires automated tools that capture, collect, and interrogate the data to determine if a potential attack is taking place. When necessary, the Zero Trust environment should take the appropriate action for the potential attack. This might be alerting administrators or taking remedial action automatically. Speed of response is a critical factor in responding to attacks.

Oracle Cloud has services and features that either directly support the Visibility and Analytics pillar or augment enterprise tools. In many cases, you may bring your own tool sets to support this effort. Oracle tools adopt an open-source paradigm to integrate with a variety of tools, allowing you to avoid a costly change to new technology. Oracle Cloud telemetry is available for incorporation using Open-Source APIs to help you build the tools to meet your requirements.

Oracle Cloud Component	Description	Zero Trust Applicability
Logging	The Oracle Cloud Logging Service provides access to all the logs from Oracle Cloud resources in a tenancy, including Audit Service, Service logs, and custom logs. Logging Analytics provides the capability to capture and analyze all log data from applications and system infrastructure either on cloud or on-premises.	Log and audit data can be generated across a tenancy as well as applications and services running in a tenancy and can be interrogated either interactively through the console or programmatically through the API to analyze the data.
Network Visualizer	The Network Visualizer provides a diagram of the implemented topology of all VCNs in a selected region and tenancy. It has the ability visualize a concise picture of these entities and their relationships is essential for understanding the design and operation of a virtual network.	A visualization of network topology is critical for the security of the workload to see how they are related and connected through routing that's often complex. These resources can also have complex relationships with other Oracle Cloud services.
Cloud Guard	Oracle Cloud Guard provides cloud security posture management by detecting misconfigured resources and insecure activities across tenants, per a tenancy's defined thresholds. It provides security administrators with the visibility to triage and resolve cloud security issues. Security inconsistencies can be remediated automatically with out-of-the-box security recipes to scale the security operations center effectively.	Cloud Guard can be used to help ensure that the security posture of services has not been weakened through misconfiguration or activity within a tenancy. Oracle Cloud Guard for detecting and remediating problems is provided at no additional cost.
Threat Intelligence	Threat Intelligence aggregates threat intelligence data across many different sources and manages this data to provide actionable guidance for threat detection and prevention in Oracle Cloud Guard.	The threat intelligence service provides insights from Oracle security researchers, our own unique telemetry, open-source feeds such as abuse.ch and Tor exit relays, and third-party partners. Malicious actors often use known techniques to attack target environments. Contextual information about the threats found in your environment, such as associated threat types, threat actors, and geolocations, can help you detect potentially malicious activities, prioritize alerts, and assess your security posture.

Oracle Cloud Component	Description	Zero Trust Applicability
Vulnerability Scanning and Reports	Oracle Vulnerability Scanning Service helps improve your security posture in Oracle Cloud by routinely checking hosts for potential vulnerabilities. The service generates reports with metrics and details about these vulnerabilities.	Vulnerability scanning results are provided so administrators can make reasonable prioritization decisions on which hosts need to be patched and in what order. The vulnerability service identifies gaps in compute resources and easily allows administrators to install required software.
Cloud Advisor	Cloud Advisor finds potential inefficiencies in a tenancy and offers guided solutions that explain how to address them, covering both security and cost management.	Cloud Advisor can be used to help maximize the efficiency of a tenancy by identifying where cost savings can be achieved and where security can be improved in areas with security posture weaknesses identified by Cloud Guard.

Table 7: Visibility and Analytics Pillar Services

Conclusion

Implementing a Zero Trust security architecture is a challenging task for most organizations. You need to carefully design and engineer the Zero Trust deployment to avoid interruptions in mission workloads. Implementing a Zero Trust environment in an existing operational enterprise can cause disruptions unless a careful evaluation takes place. This can take a long time to properly account for all the information technology that has been deployed.

The tools, features, and services Oracle offers can assist you in the implementation of a Zero Trust plan. Oracle services presented in this document, when integrated with a detailed plan, can greatly increase the speed of implementation for security teams. Integration of our managed services, coupled with our underlying secured infrastructure, means you can feel confident when it comes to security.

There are no easy buttons when it comes to security. Security requires consistently applied vigilance to ensure all actors within the enterprise only have access to the data and services they need and no more. Implementing a deny-by-default approach greatly improves the security environment and prevents privilege escalation.

Oracle Cloud provides organizations with the tools they need to deploy a Zero Trust security architecture. Organizations must implement the appropriate services to achieve a truly secure, mission-ready enterprise environment.