Approaching Zero Trust Security with Oracle Cloud Infrastructure

How Oracle Cloud Infrastructure can help organizations adopt a zero trust security model as recommended by the UK National Cyber Security Centre's eight principles

Paul Toal
Krithiga Gopalan

July, 2024, Version 1.3
Copyright © 2024, Oracle and/or its affiliates
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.

Copyright © 2024, Oracle and/or its affiliates / Public

ORACLE

Table of Contents

Copyright © 2024, Oracle and/or its affiliates / Public

Executive Summary

This paper explores how Oracle Cloud Infrastructure (OCI) can help accelerate deploying a zero trust architecture. The paper uses the UK National Cyber Security Centre (NCSC)'s eight zero trust principles as a framework for discussing OCI controls. The list includes the following zero trust principles:

- Know your architecture, including users, devices, services, and data.
- Know your user, service, and device identities.
- Assess user behaviour, service, and device health.
- Use policies to authorize requests.
- Authenticate and authorize everywhere.
- Focus your monitoring on users, devices, and services.
- Don't trust any network, including your own.
- Choose services which have been designed for zero trust.

Although the NCSC is UK-based and focuses on protecting the most critical organizations in the UK, the guidance isn't specific to UK companies and has applicability to organizations globally.

Copyright © 2024, Oracle and/or its affiliates / Public

Introduction

Cyber security and IT professionals are likely familiar with the phrase zero trust security. Zero trust security assumes low levels of trust for users and devices connected to an organization's network, and it considers the design and deployment of appropriate security controls to establish and to maintain trust. The idea behind zero trust security has grown over the last decade based on several factors, including the growth of public cloud and the threats coming from insiders, not just external attackers.

Adopting a zero trust approach requires significant time and effort. It involves committing to incremental advances towards adopting a technical architecture and business processes that establish and maintain trust throughout the organization. Oracle can help organizations in their zero trust initiative through Oracle Cloud Infrastructure (OCI), which has been designed to provide customers with built-in security features to help quickly and effectively secure their workload in the cloud.

Many organizations want to be more agile as they transform their businesses by using a public cloud to deliver cost-effective infrastructure, platforms, and software services. Oracle designed OCI to be a next-generation cloud. It delivers high-performance computing (HPC) power to run cloud native and enterprise IT workloads in Oracle Cloud data centers or at a customer site through Cloud@Customer deployments. OCI provides real-time elasticity for enterprise applications by combining Oracle autonomous services, integrated security, and serverless compute. One of OCI's core design principles is a security-first approach, ensuring that security is built into the platform from the ground up and not bolted on as an afterthought. Oracle pursues the following tenets to assist customers in securing their cloud:

- **Simple and effortless**: Designing security controls that are easy to use, deploy, and operate.
- **Complete control**: Enabling organizations to have control over their applications and data, regardless of where they reside.
- **Deeply integrated**: Providing built-in and integrated security across infrastructure-, platform-, software-as-a-service (Iaas, PaaS, and SaaS), and distributed cloud (hybrid and multicloud), reducing manual security tasks and human error.

Before exploring the NCSC's eight principles, we must establish that IT departments and their cloud providers have respective roles to play in managing cloud security.

From a security management perspective, cloud is fundamentally different from on-premises. Though IT departments maintain full control of technology infrastructure on-premises, such as physical control of the hardware and full control over the technology stack in production, the cloud uses components under the control of the cloud service provider. As a result, the management of security in the cloud is shared, as shown in Figure 1.

Copyright © 2024, Oracle and/or its affiliates / Public

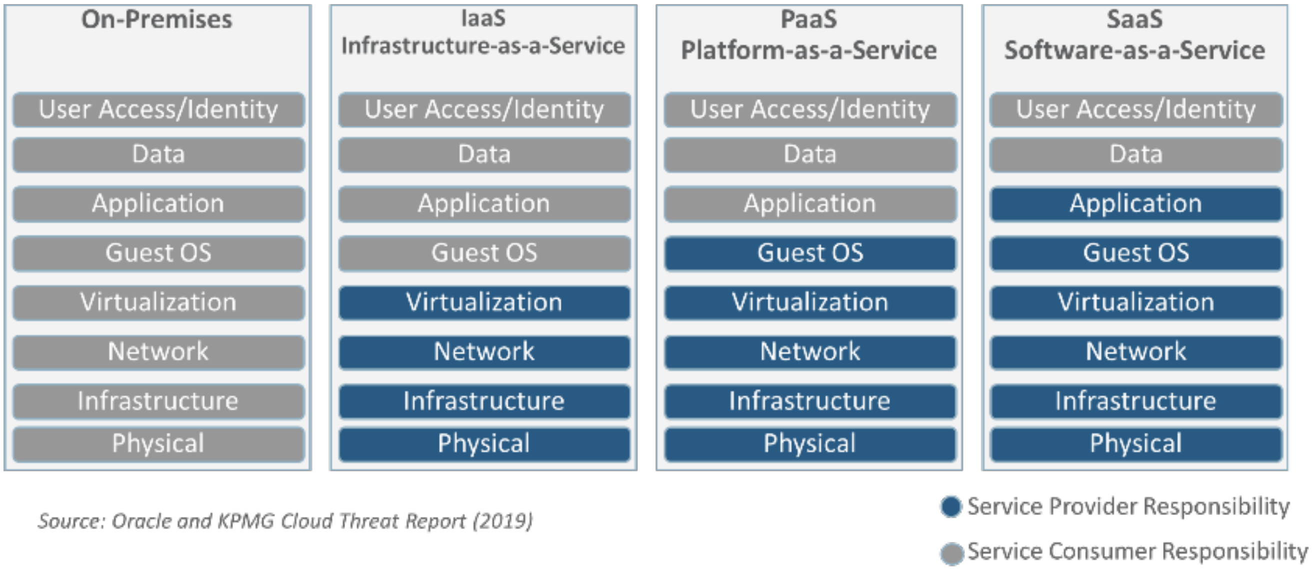


Figure 1: Conceptual representation of the various security management responsibilities between customers and cloud providers

The security-first design principles of OCI, along with the strong set of security capabilities available to OCI customers, can help organizations implement a zero trust security architecture.

To help organizations work toward a zero trust architecture within their deployment, this paper provides a mapping between the OCI security controls and the OCI Center for Internet Security (CIS) secure landing zone. This landing zone template deploys a standardized environment in an OCI tenancy that helps organizations to comply with the CIS OCI Foundations Benchmark v2.0. Though the CIS secure landing zone has been used for mapping in this paper, other OCI landing zones are available, such as the OCI open landing zone and the Oracle Enterprise landing zone. Organizations should evaluate the most appropriate landing zone based on the required workloads being deployed on OCI.

Copyright © 2024, Oracle and/or its affiliates / Public

Principle 1: Know Your Architecture, Including Users, Devices, Services, and Data

Designing a security architecture requires having a good understanding of existing assets, including the data that needs protection. The first three principles from NCSC focus on discovery, with the first principle looking at knowing internal architecture, including users, devices, services, and data.

As highlighted by NCSC, undertaking an asset discovery activity most likely isn't a purely technical exercise, but instead involves tasks, such as reviewing project documentation, procurement records, and conversations with colleagues. Getting to know the architecture can be difficult because of different departments and lines of business implementing their own solutions. This issue is commonly referred to as "shadow IT," which, according to Gartner, refers to "IT devices, software, and services outside the ownership or control of IT organizations."

OCI offers numerous tools and services that expedite the asset discovery phase by helping to identify and understand what's already deployed, as summarized in Table 1.

Table 1. Principle 1 controls and OCI tools to help with asset discovery.

OCI Component	Description	Discovery Provided
Representational state transfer application programming interface (REST API)	OCI provides REST APIs for accessing and managing the OCI tenancy. They also offer SDKs for various languages and a CLI, all of which you can use for programmatic access to an OCI tenancy.	You can write scripts to enumerate all resources that have been created within the OCI tenancy. For examples of scripting using the OCI CLI, see the documentation.
Command-line interface (CLI) **Software development kit (SDK)**	OCI resource tagging allows you to define and associate keys and values with resources.	Organizations can use resource tags to organize and list resources used for specific projects or systems.
Terraform	Oracle delivers an OCI provider for Terraform to enable OCI deployment to be implemented through infrastructure-as-code (IaC).	You can use Terraform Discovery to build IaC scripts based on the existing deployed footprint and document the existing OCI deployment.
Auditing	OCI provides the Audit service, which automatically records calls to all supported OCI public API endpoints as log events, including calls made by the Console, API, SDK, and CLI, custom clients, other OCI services.	You can use auditing within OCI to understand which services are being called, who is making these calls, which calls are successful, and which are unauthorized.
VCN Flow Logs	Virtual cloud network (VCN) flow logs within OCI provide visibility into connection information for traffic within, to, and from a VCN.	You can use VCN flow logs to understand what traffic is flowing between services over which ports. This information can be extremely helpful in understanding data flows as part of the discovery phase.
Existing Platform Services	OCI includes a comprehensive set of PaaS services, covering a wide range of capabilities,	You can use Platform services to understand the existing deployments, including the following examples:

Copyright © 2024, Oracle and/or its affiliates / Public

	including integration, governance, identity, security, data management, and analytics.	• **OCI Identity and Access Management (IAM) and Oracle Access Governance**: Discover users, their roles, and their access privileges. • **Oracle Integration Cloud** and **Oracle API Gateway**: Identify existing data flows. • **Oracle Data Safe**: Identify sensitive data within Oracle Databases, whether running on-premises or in the cloud. • **Oracle Data Catalog**: Manage data and data governance and provide an invaluable repository of existing data assets. • **Oracle Container Registry**: List the published applications and services for DevOps deployments. • **Oracle Container Engine for Kubernetes (OKE)** and **Oracle Resource Manager**: Identify the applications and services that are running.
OCI CIS landing zone compliance checking script *CIS Secure Landing Zone*	The script checks a tenancy's configuration against the CIS OCI Foundations Benchmark. In addition to CIS checks, it can also check for alignment to OCI best practices.	You can use the script to check the security baseline configuration of a tenancy against industry best practices, such as those from CIS.

In addition to the OCI components in table 1, Oracle also provides an OCI document template with a framework for the discovery, assessment, and planning of an OCI project.

Copyright © 2024, Oracle and/or its affiliates / Public

ORACLE

Principle 2: Know Your User, Service, and Device Identities

The gradual movement to cloud has accelerated the erosion of the traditional network perimeter. With that, identity has been recognized as the new perimeter. Oracle provides an enterprise-class Identity-as-a-Service (IDaaS) platform called OCI Identity and Access Management (IAM), which uses the concept of identity domains. OCI IAM domains have merged the capabilities of OCI IAM and Oracle Identity Cloud service into a combined service. OCI IAM works with the Oracle Access Governance service, which is an OCI cloud native service that provides enterprise-wide visibility to govern access to cloud and on-premises environments for identities.

The OCI IAM service serves as both the front door into Oracle cloud services and a standalone IDaaS platform for both enterprise users and consumers. This provides key identity management capabilities for applications and services running in OCI, third-party clouds, and internal data centers.

Identity is the core tenet of NCSC's second principle, and OCI IAM and Oracle Access Governance can help to deliver on this principle.

User Identity

OCI utilizes the following main types of user identities:

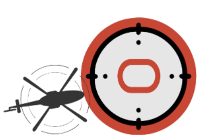
- Administrative users who are accessing OCI to perform functions within the OCI platform itself, such as creating networks, backing up Compute instances, and managing encryption keys.
- End-users who access applications that might be running within OCI, such as in Oracle Analytics Cloud, or outside OCI.

For both user types, OCI IAM provides the capabilities to manage the user identities, attributes, and access privileges.

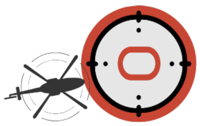
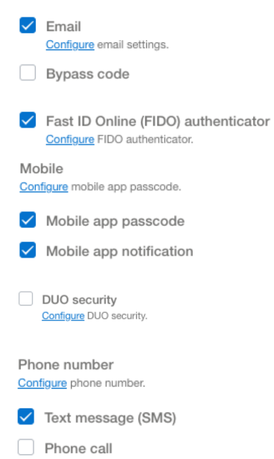
Although Oracle identity services can serve as a main identity repository, many organizations have multiple identity management systems in place, especially for employees. In these cases, OCI can integrate with those existing services, and in some use cases, extend their capabilities.

Table 2 shows how OCI IAM and Oracle Access Governance maps against the capabilities that NCSC states an identity service should be able to do.

Table 2. Principle 2 controls providing a rich set of identity capabilities in OCI IAM.

Identity Service Feature	Description
Create groups  *CIS Secure Landing Zone*	OCI IAM provides the ability to create and manage groups within identity domains. After creation, identities can be assigned to and revoked from groups. You can manage group using one of the following methods: • **Web-based console**: The service provides a feature rich web-based console for administration and self-service. • **System for cross-domain identity management (SCIM) -based REST API**: Administration can be run through the SCIM REST API, or through one of the API derivatives, such as SDKs. **Synchronization**: Numerous ready-to-use connectors enable identities, including groups and group memberships, to be synchronized directly from a source system. For example, an Active Directory bridge is available, as are connectors for popular human capital management (HCM) cloud services and on-premises repositories.

Copyright © 2024, Oracle and/or its affiliates / Public

Define roles that have been configured to be least-privilege  *CIS Secure Landing Zone*	OCI IAM denies access by default, within OCI. Administrators can't access any resources until they're assigned to at least one group that has OCI privileges granted to it. All authorization within OCI is through IAM policies, which provide a simple-to-use policy syntax for creating access policies. For example: `Allow group OCIDBAdmins to manage database-family in tenancy` These policies are then assigned to groups and members of those groups inherit those privileges. When accessing applications that are integrated with OCI IAM, users are typically assigned to groups. A group has no permissions to access any services until that group has been mapped to one or more applications, or application roles. When a group has been mapped to an application or application roles, end-users assigned to that group then have the appropriate access. From a user administration perspective, several predefined administrative roles provide different levels of admin access. So, only the required minimum administrative privileges are granted to any administrator. Oracle Access Governance further strengthens the security of roles by providing insights into access permissions and OCI policy reviews, identifying anomalies, and remediating security risks. It helps implement dynamic identity collections and access bundles for attribute-, policy-, and role-based access control and provides actionable insights into potential security violations that enable rapid remediation of identity and access challenges. These capabilities enable users to have only the necessary permissions necessary to do their job.
Support strong, modern authentication methods	OCI IAM supports a wide range of authentication factors, including multifactor authentication (MFA), passwordless authentication, and risk-based authentication, as shown on the right.  Supported multifactor methods include time-based one-time passcodes (TOTP), push-based notifications, phone calls, SMS, email, security questions, bypass codes, duo security tokens, and X.509 certificates. It also supports passwordless authentication through the FIDO2 industry open standard, enabling support for compliant authentication methods, such as Yubikey, TouchID, FaceID, and Windows Hello. Risk-based authentication within OCI IAM enables the context of the user's request to be examined and evaluated against several risk factors to determine whether to allow the request, block it, or challenge it for an extra authentication factor, such as one of the factors mentioned.

Copyright © 2024, Oracle and/or its affiliates / Public

Securely provision credentials to users	How credentials are provisioned to users securely depend on how the user is created, such as the following methods: • **Self-registration**: For users who self-register, the user can create their own password (subject to the configurable password policy) at registration time. • **Administrative action**: If an administrator creates the user's identity record, a time-bound link is emailed to the users, where they can set their own password. Similarly, an administrative password reset follows the same flow. • **Synchronization**: In many cases, synchronized users don't authenticate to OCI IAM directly, but instead authenticate through federated single sign-on (SSO), such as using the security assertion markup language (SAML). For these users, Oracle doesn't store or maintain a password for the user. Instead, identity records (without user passwords) are synchronized between the two federated providers. • **Delegated authentication**: OCI IAM supports authentication using a user's Active Directory credentials. In this scenario, the service doesn't manage user passwords.
Authenticate to services	Oracle supports industry open standards for federated authentication, including: SAML 2.0, OAuth 2.0, and OpenID Connect. You can use these standards to authenticate to the service or facilitate SSO to connected applications. In scenarios where a target application doesn't support open standards, you can use App Gateway as a reverse-proxy bridge between Oracle and the application, converting the open standards token into a format the protected application can understand, such as header variables.
Manage user identities in external services	OCI IAM supports the SCIM 2.0 open standard. Many application templates are provided to accelerate integration with common, popular target applications and services. SCIM templates are also provided. The service can both produce SCIM messages for managing identities in target application and consume SCIM messages from authoritative sources. Oracle Access Governance supports the provisioning of identities across a range of external systems using several prebuilt and standards-based connectors.
Support Joiner, Mover, Leaver (JML) processes	Oracle supports joiner, mover, leaver (JML) processes through either the SCIM interfaces discussed or one of the other synchronization methods available. The service can consume JML messages from external identity services and can produce JML messages for target applications and services. When consuming JML messages, you can use the feed as an authoritative or nonauthoritative source, meaning that the source can either create the identity record where it doesn't already exist or create an account record, representing an account in a target system, which it links back to the identity record.

Copyright © 2024, Oracle and/or its affiliates / Public

	When producing JML messages, OCI provides control over which message events are produced. In both cases, application templates are available for popular source and target applications.
Support third party federated ID	OCI supports federated identities, both for SSO through standards including SAML, OAuth, and OpenID Connect, and for user management through SCIM and other immediately available synchronization capabilities.

As discussed by NCSC in principle 2, user consent is a key element of an identity system. OCI IAM supports consent management in the following areas:

- The terms of use agreement capability within OCI IAM allows the customers to present disclaimers and acceptable use policies to their users.
- Support for OAuth allows users to specify the scope of access.
- The principle of using end-user tokens allows the applications to prove consent to back-end resources.

Service Identity

Zero trust security is a key design principle of OCI, and identity is no different. Oracle built our cloud native identity services using a microservices approach, with each microservice authenticating to each other's microservice using secure protocols. This design doesn't require inherent trust among these microservices.

Though OCI provides a consistent repository for different types of identities, other capabilities exist to help achieve zero-trust security.

With user identities, OCI provides identities for Compute instances, called instance principals. A Compute instance often needs to access other OCI services, such as storage, databases, and networking. The traditional approach to achieving authenticated access to these resources embeds credentials for those resources within the Compute instance. However, this approach adds management overhead because those credentials must be responsibly managed and rotated on a regular basis. Through OCI instance principals, embedding credentials within the Compute instance is no longer necessary. OCI handles the complexity of continuously rotating credentials for those Compute instances.

The concept of resource principals is similar to instance principals but used for resources that aren't instances, such as serverless functions, enabling them to access other OCI resources.

OCI IAM uses instance principals and resource principals to enable access control in a more secure manner than embedding long-term credentials. IAM policies are written against those principals, similar to policies written for user identities, ensuring that the authorization policies are defined centrally within OCI IAM for user identities and instance and resource principals.

Certificates are used as the credentials for instance and resource principals, which OCI manages automatically, including creation, assignment, and rotation.

Furthermore, OCI administrators write IAM policies that determine the privileges that an instance or resource principal can run. Compute instances are grouped together in dynamic groups, based on group membership rules, and any Compute instance that matches the membership rules inherits the OCI privileges assigned to those dynamic groups. Consider the following sample instance principal:

```
Allow dynamic-group AppServersProd to inspect objects in compartment images
```

For situations where an application or system running on a Compute instance needs credentials to access an endpoint, such as an API endpoint or database, OCI provides Secrets Management. This service can securely store and retrieve secrets encrypted using customer-managed master encryption keys stored in FIPS 140-2 Level 3

Copyright © 2024, Oracle and/or its affiliates / Public

hardware security modules (HSMs). The identity referenced by these secrets can be stored and mastered in the identity service.

Device Identity

OCI doesn't provide endpoint security or enterprise mobility management for managing device identity. However, OCI IAM can utilize device information as part of a risk-based authentication approach, based on a device fingerprint collected during authentication. For example, if a user is attempting to authenticate from a new device, the user's risk score can be increased accordingly and appropriate action taken, such as challenging for stronger authentication or denying the authentication attempt. Risk factors include too many failed sign-in attempts and access from a suspicious IP address.

Copyright © 2024, Oracle and/or its affiliates / Public

Principle 3: Assess User Behaviour, Service, and Device Health

Principle 3: Assess User Behaviour, Service, and Device Health

For principle 2, OCI IAM was recognized as a key security control within OCI. The same service is used when monitoring the health of users, devices, and services.

Device Health

You can monitor device health as part of MFA. When using either time-based one-time password (OTP) or push notification factors for MFA, you can use the Oracle Mobile Authenticator. As part of the MFA configuration, you can set a compliance policy to enforce certain device configuration settings, such as OS version check or rooted devices check, as shown in the following figure.

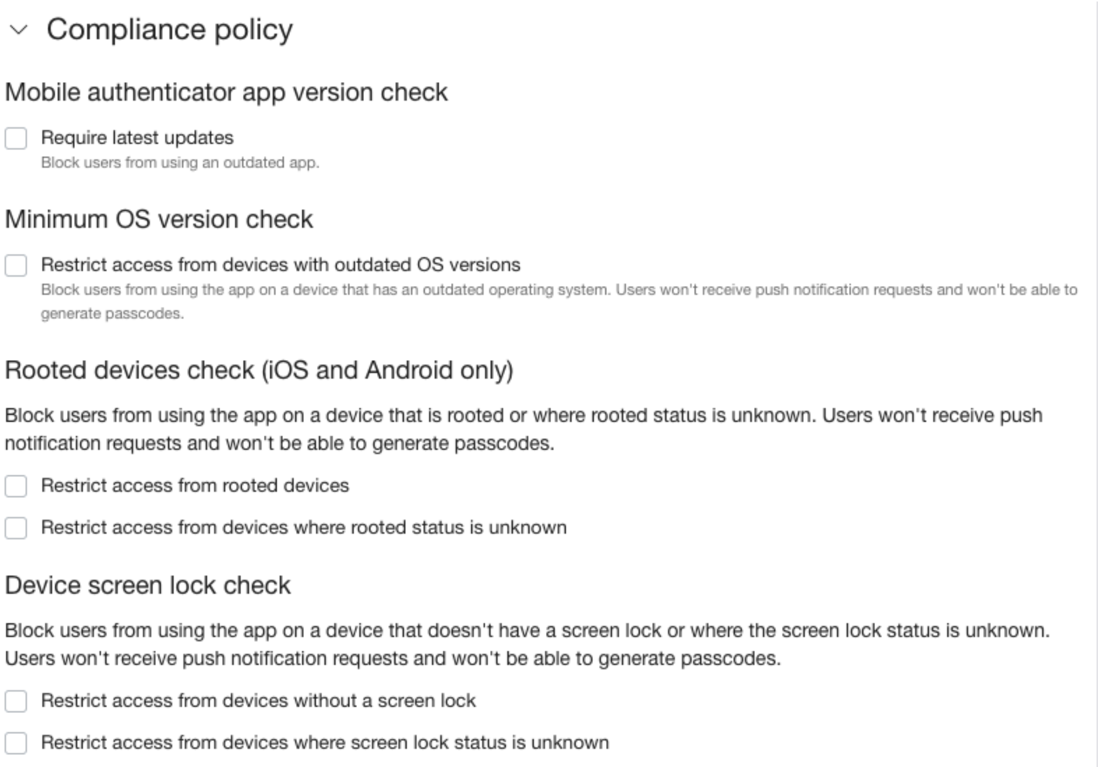


Figure 2: Ensuring device compliance with Oracle Mobile Authenticator

Another consideration when examining device health is the state of any Compute instances used when running IaaS. Within OCI, lowering the trust level of various infrastructure components, including servers and hypervisors, is a key tenet and design principle. As a result, a number of security controls are in place across OCI, including the OCI Hardware Root of Trust, which, through the use of hardware-based Root of Trust technology, can reduce the risk of firmware-based attacks against OCI customer tenants. This technology is designed to wipe and reinstall the firmware every time a new server is provisioned, or a new customer tenancy is established. Furthermore, shielded instances can help to protect the firmware security on a Compute instance against malicious boot-level software, using a combination of secure boot, measured boot, and the trusted platform module (TPM).

Service Health

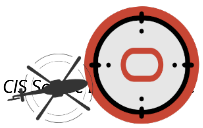
OCI implements several capabilities to establish the health of services, as outlined in the following table:

Copyright © 2024, Oracle and/or its affiliates / Public

Table 3. Principle 3 controls – OCI provides capabilities for monitoring health

OCI Capability	Description	Health Information
Autonomous Services	Autonomous Linux minimizes complexity and human error to increase security and availability by providing core security capabilities, including zero downtime, automatic patching, and known exploit detection. Autonomous Database protects sensitive and regulated data automatically through self-securing capabilities, including automated patching, enforced separation of duties, and encryption at rest and in motion by default.	Use Autonomous Linux and Autonomous Database to improve the health of services through automation and machine learning (ML).
OS Management	OS Management enables management of updates and patches for the operating system environment on OCI instances that aren't running Autonomous Linux.	Use OS Management to check that the operating systems running applications and services are kept up to date with the latest patches, helping to reduce the risk of a known vulnerability in the OS being exploited.
Auditing and Logging *CIS Secure Landing Zone*	The OCI Logging service provides access to all the logs from OCI resources in a tenancy, including OCI Audit, service logs, and custom logs. Furthermore, OCI 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 an OCI tenancy, applications, and services running on a tenancy and can be interrogated either interactively through the Console or programmatically through the API to analyze the data.
Vulnerability Scanning *CIS Secure Landing Zone*	The OCI Vulnerability Scanning service scans installed packages and artifacts looking for the existence of known vulnerabilities on customers' Compute instances and in container images from their OCI Container Registry (OCIR) repositories. Vulnerability Scanning has been partially replaced by Cloud Guard Instance Security for host scanning. You can use Vulnerability Scanning and Cloud Guard Instance Security currently for host scanning, while Vulnerability Scanning can still be used for container image scanning. The service also scans for publicly and privately open ports on an instance and reviews the	You can use these findings from Vulnerability Scanning to know what packages should get patched or what security hardening steps to take. Vulnerability Scanning is integrated by default with Cloud Guard to provide users a unified view of their vulnerability status of their instances and container images.

Copyright © 2024, Oracle and/or its affiliates / Public

	configuration of each instance against specific OS CIS benchmarks.	
Events  *CIS Secure Landing Zone*	OCI services emit industry-standard CloudEvent format events, which can indicate change in resources. Actions can be taken on the back of these events, including the following examples: • **Notifications**: Sending emails and SMS notifications • **Functions**: Running a serverless function, based on the industry standard Fn project. • **Streaming**: Publishing an event to a stream	You can use events to indicate a change in a resource and identify potential changes to the health of a service.
Operational Insights	Operational Insights provides a 360-degree insight into the resource utilization and capacity of Oracle Autonomous Database.	You can use Operational Insights to identify security issues by monitoring the CPU usage and storage resources and looking for anomalous behavior.
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.	You can use Cloud Advisor to help maximize the efficiency of a tenancy by identifying where you can achieve cost savings and where to improve security in areas that Cloud Guard identifies with security posture weaknesses.
Observability and Management Platform	The Oracle Cloud Observability and Management Platform consists of a set of OCI services, including Logging, Log Analytics, and Service Connector Hub, which enable visibility and insight across cloud native and traditional technology, whether deployed in multicloud or on-premises environments, with broad, standards-based ecosystem support.	Service Connector Hub provides a single pane of glass for administrators to manage and monitor data movements across their services within and from OCI to third-party observability tools, taking near-real-time actions. The combined platform provides cross-technology, cross-cloud, full stack visibility with unified telemetry, data exchange and applied machine learning.
Container Image Scanning, Signing & Verification	OCI Vulnerability Scanning scans images in the repository for security vulnerabilities. To ensure that images aren't modified after being published, images in OCI Registry can be signed using master encryption keys stored in OCI Vault.	View and verify image signatures, ensuring that the integrity of the image hasn't been compromised. After successful verification, you can deploy the image to the Kubernetes cluster.

Copyright © 2024, Oracle and/or its affiliates / Public

User Health

OCI IAM provides the capabilities for monitoring the risk or security posture of users. Based on the risk provider settings configured by the customer, an adaptive risk engine evaluates risk for users and maintains a risk score for each user. This score is evaluated at every authentication and can be used as part of the authentication process to determine whether to allow access, deny access, or challenge for a further level of authentication. If a user hasn't previously registered a second factor, then enrollment can be made mandatory.

Sign-on policies can also consider extra signals from users, such as where they're coming from, their group membership, and which application they're accessing. Consider these factors, including the user's risk score, when making an authentication decision. In the example shown in figure 3, a user who is authenticating through the Google Identity Provider and is a member of the Federated Users group, is prompted for another factor whenever they try to access the application associated with this sign-on policy.

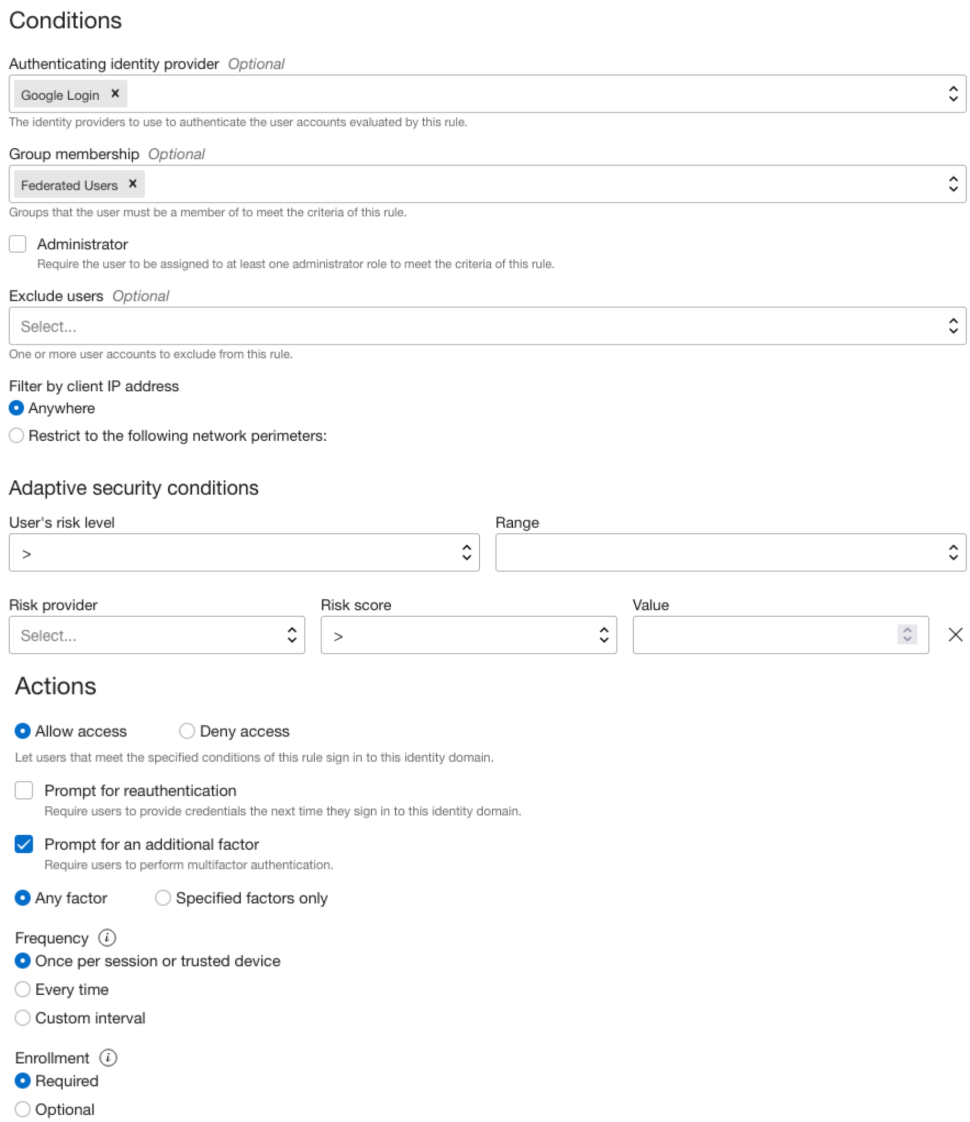


Figure 3: Evaluating multiple signals during authentication.

NCSC's principle 3 suggests passwordless authentication through the FIDO2 standard as the ideal authentication type. OCI supports passwordless authentication through the FIDO2 standard.

Copyright © 2024, Oracle and/or its affiliates / Public

Principle 4: Use Policies to Authorize Requests

Authorization has long been a challenge for many organizations. The subject can split be into the following areas:

- **Coarse-grained authorization** looks at a macro-level authorization policy and usually answers the question, "Does the user have access to this application?"
- **Fine-grained authorization** determines what a user is authorized to do within an application or service.

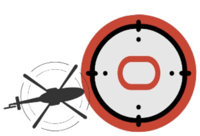
Implementation of centralized, coarse-grained authorization is commonplace within many organizations. Using technologies such as single sign-on and role-based access control, it can be easier to control which applications or services an identity can access.

However, enterprise-scale, fine-grained authorization is much more of a challenge. Each individual application or service normally manages their own fine-grained authorization. Technology is available to centralize fine-grained authorization using industry open standards, including extensible access control markup language (XACML). Wide adoption of these technologies often results in changes needed in off-the-shelf applications or changes to software development approaches, where custom software is being developed.

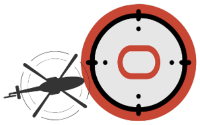
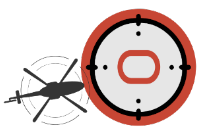
As a result, an organization often implements coarse-grained authorization within a central SSO platform, while leaving each target application or service to manage its own fine-grained authorization.

Within OCI, all access to resources is denied until required privileges are assigned. Many of the capabilities for delivering these functionalities have been discussed in the previous principles. Table 4 summarizes the key controls for this principle.

Table 4. Principle 3 controls – Policy-based authentication and authorization controls

OCI Capability	Description	Applicable Controls
OCI Identity and Access Management (IAM)  *CIS Secure Landing Zone*	OCI IAM provides centralized authentication and coarse-grained authorization services for any integrated, protected applications. The service examines several signals associated with a request to determine the level of authentication. The service applies policies globally or to specific applications. OCI IAM allows mapping of enterprise roles to application roles and entitlements that help manage authorization within target applications. OCI IAM provides the central, fine-grained authorization policy engine for all OCI services. This control allows a tenant administrator to determine exactly what level of access an identity has within OCI, for accessing and managing OCI resources. The permissions allow fine-grained authorization policies to be defined that control the ability to perform operations on resources.	Use OCI IAM to deliver the following core set of identity capabilities: • Single sign-on • Risk-based, adaptive authentication • Multifactor authentication • Role-based access control Protect different applications with different sign-on policies. Control authorization to an application through mapping of roles. Use OCI IAM to define role-based, fine-grained authorization policies, utilizing a deny-by-default approach. All access to any resources in OCI must be explicitly authorized through IAM policies, including users and resources through instance principals and resource principals.

Copyright © 2024, Oracle and/or its affiliates / Public

	In a policy statement, OCI allows using conditions combined with permissions or API operations to reduce the scope of access granted by a particular verb, such as inspect, read, use, and manage.	
OCI Compartments  *CIS Secure Landing Zone*	OCI compartments provide logical groupings of resources to enable defining both coarse and fine-grained authorization policies against them.	You can use OCI compartments to allow scoping of OCI IAM policies to specific sets of resources, under specific conditions.
OCI Platform services	With OCI Platform services**,** each platform service provides its own fine-grained authorization, typically through application-level roles, mapping to privileges within the service.	You can map application roles to roles within OCI IAM, so that role-based access control flows all the way from user authentication into the target applications.
Security zones and Security Advisor  *CIS Secure Landing Zone*	A security zone enables highly secure and restrictive compartments in which to deploy sensitive OCI resources. Restrictive policies can help you from configuring a weak security posture. Security zone policies provide prescriptive guardrails to help prevent human errors and help guard highly sensitive data and resources. Organizations determine which policies are appropriate for their needs by defining custom security zone policy sets. Security Advisor works closely with Maximum Security Zones and guides customers through efficiently creating secure resources in OCI correctly from the outset by providing a guide-driven interface.	You can configure security zones to help ensure that even the most sensitive resources can't be exposed to the internet or other weakened security posture through misconfiguration. Use Security Advisor to help implement recommended security practice for OCI resources created, including object storage, Compute instances, file systems, and block volumes. Security zones and Security Advisor are provided at no extra cost for OCI customers within the service limits.
Web application firewall (WAF)	WAF delivers a cloud native, web application firewall, designed to help protect applications from malicious requests and requesters. WAF provides two modes of protection. Edge policies are customer-managed policies that are deployed on Oracle-managed edge nodes, enabling layer 7 protection for web applications published on the internet. Load balancer policies are customer-managed policies that are applied to OCI public or private load balancers that are deployed by a customer within their VCN.	Configure WAF with access control rules that can be used to ensure that requests are coming from authorized requesters. You can also use WAF to provide an extra layer of security for legacy applications that don't support the latest security standards, such as TLS.

Copyright © 2024, Oracle and/or its affiliates / Public

OCI Certificates	OCI Certificates service enables customers to easily create, deploy, and manage Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates. Using OCI Certificates service, organizations can automatically deploy SSL/TLS certificates to integrated services, such as OCI load balancers or API Gateway.	Organizations can use the OCI Certificates service to avoid error-prone manual certificate management processes and instead automatically monitor and renew the certificates. In a flexible certificate authority (CA) hierarchy, the OCI Certificates service helps create private CAs to provide granular security controls for each CA.
Confidential Computing	OCI Confidential Computing encrypts and protects data that's in use, while in RAM, and during computations in Compute instances.	This setup improves isolation using real-time encryption without requiring any change to the application. The encryption keys are safeguarded at the hardware level by the secure processor.

With policy controls for authorization, principle 4 discusses the encryption of data at rest and in transit. Within OCI, all data at rest is encrypted by default, except for local NVMe temporary storage on bare metal servers. Encrypted data includes data at rest for the services such as block storage, boot volumes, object storage, file storage service, and the various Oracle Database cloud services. Encryption of data at rest isn't something that a tenant administrator needs to enable. It's enabled as a standard across OCI.

Furthermore, customers can use OCI Key Management Service (KMS) to manage their organization's own master encryption keys for data at rest encryption. This service uses a FIPS 140-2 Level 3 certified HSM to store key material. Virtual vault, private vault and external KMS within OCI KMS support integration with OCI storage, database, and Fusion SaaS.

KMS also enables generating and securing the storage of asymmetric keys, which you can use with the KMS endpoints for signing and encrypting, ensuring the integrity of payloads. Customers can choose virtual or private vaults within KMS for storing and managing their keys within OCI.

Furthermore, OCI External KMS enables customers to use encryption keys that are stored and managed outside OCI. External KMS can be useful for customers who have regulatory requirements to store encryption keys on-premises or outside OCI or who want to have more control over their encryption keys.

While vaults within OCI KMS store customer-managed keys in single- or multitenant HSMs that are Oracle-managed, OCI Dedicated KMS is a HSM solution in OCI that provides single-tenant HSM partitions that are customer-managed. This fully managed service lets customers gain exclusive control over their encryption keys and the HSM partitions that store them, providing a direct PKCS#11 interface to the HSM.

For encryption in transit, OCI provides TLS 1.2-encrypted connections for all endpoints published by Oracle, such as API endpoints and the Oracle Cloud Console. You can also encrypt traffic between Compute instances, boot volumes, and block volumes through configuration during the creation of Compute instances.

The final consideration when looking at authorization policy is at the network level. As part of a zero trust strategy, the network is an untrusted component. Controls must still be implemented at the network layer, such as limiting traffic between different applications and services.

Copyright © 2024, Oracle and/or its affiliates / Public

OCI provides both security lists and network security groups (NSGs) for enforcing network ingress and egress traffic. Security lists are defined at the subnet level and enforced on the virtual network interfaces (VNICs) of each Compute instance, while NSGs are applied to grouped set of resources, as shown in figure 4. You can use a combination of security lists and NSGs to help address your organization's requirements.

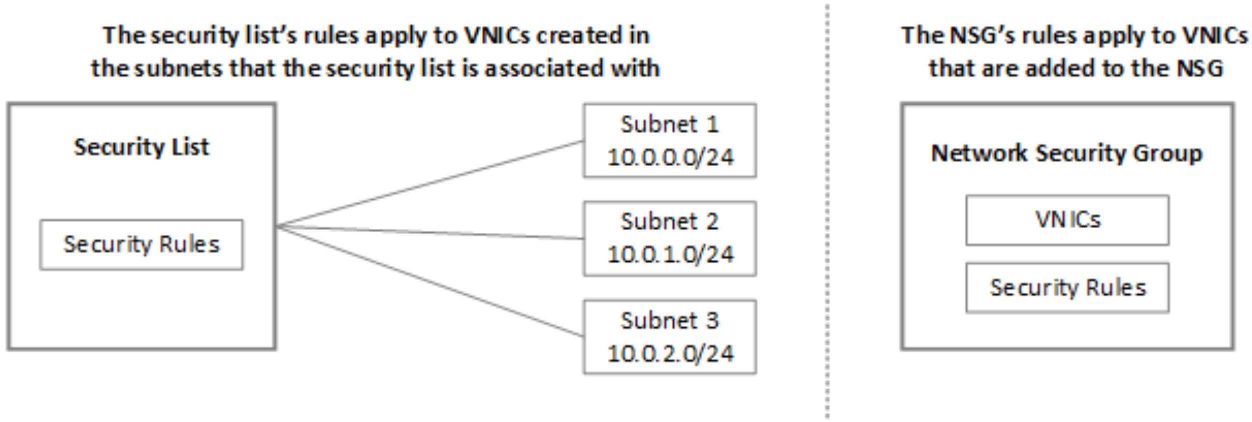


Figure 4: Security lists and network security groups work at different levels of granularity.

Principle 4 also discusses the need for break-glass access. Through appropriate design of IAM policies, you can grant emergency access as required. For example, a common approach is to have local, highly privileged accounts, where the credential isn't known to any single person and the credentials are kept secure, such as in a safe, and only accessed under controlled circumstances when needed. In these situations, a process to rotate those credentials after every use must be in place. Alternatively, the use of a privileged access management (PAM) tool is common for securely storing credentials of highly privileged user accounts. You can then allocate these accounts to users under break-glass situations as needed. You can use auditing, logging, and monitoring within OCI to provide extra levels of scrutiny for necessary emergency access.

Copyright © 2024, Oracle and/or its affiliates / Public

Principle 5: Authenticate and Authorize Everywhere

As discussed in detail in the previous principles, OCI provides the core controls to meet principle 5 through its identity capabilities. Table 4 provides a summary of the main capabilities of those controls, which ensure that all user and service requests are authenticated and authorized, whether they're an end-user accessing applications and services, a power user or administrator accessing OCI, or a service accessing another service.

The mappings against the previous principles cover the use of OCI IAM to provide MFA using a range of configurable factors, including FIDO2-based passwordless authentication, and delivering adaptive, risk-based authentication that uses a range of signals contained in the request, including location, group membership, and authentication method, as shown in Figure 4. Support for industry open standards, such as SAML, OAuth, and OpenID Connect, are also discussed, along with how to use then for both user and service requests.

Though open standards are commonly used to enable SSO for users, to authenticate once and seamlessly access other authorized applications without the need to reenter their credentials, not all applications support open standards. However, OCI IAM can deliver SSO for web applications that don't support those industry open standards using App Gateway.

Figure 5 demonstrates how OCI provides support for these open standards and how OCI IAM provides an identity service, not just for OCI, but for any web-based applications, whether hosted in OCI, in a third-party cloud provider, or on-premises. In this figure, a user authenticates to OCI IAM, either directly or through an existing identity provider (IdP), and then has SSO access to authorized applications, which might or might not support industry open standards.

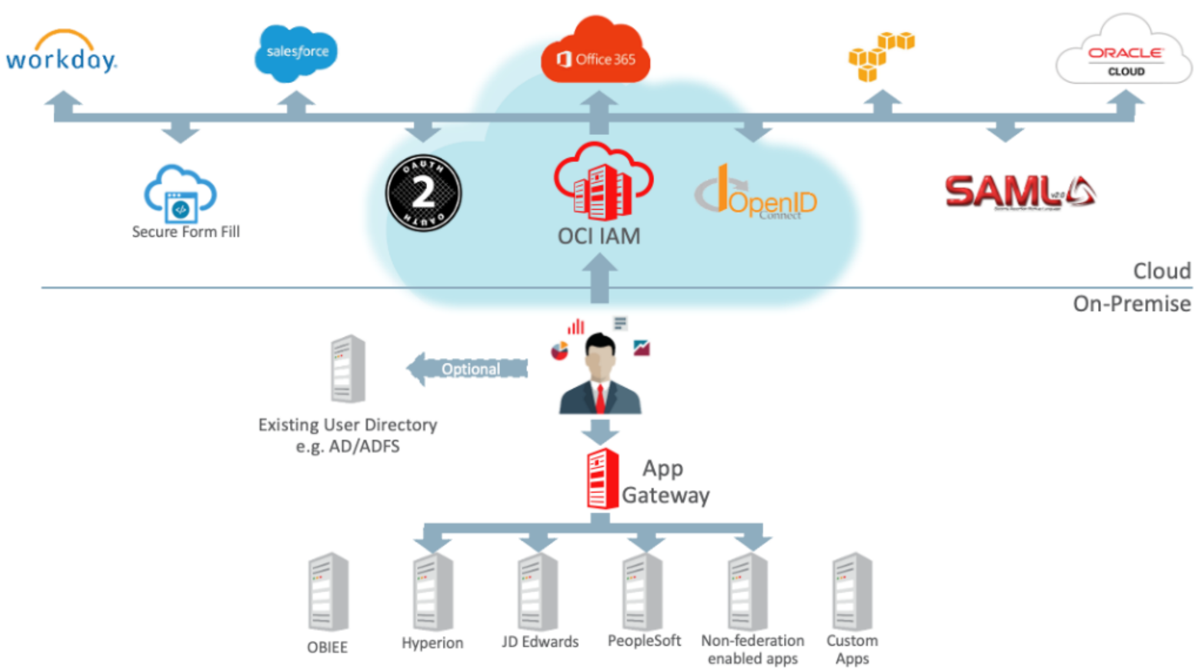


Figure 5: Using Oracle IAM as an enterprise identity hub.

Principle 2 also discussed the subject of service-to-service communication, including the following concepts:

- How OCI instance principals and resource principals are used as secure mechanisms of authenticating OCI Compute instance and serverless functions to other OCI resources
- How the OCI IAM policy is used to authorize access control for resources and services within OCI.

Copyright © 2024, Oracle and/or its affiliates / Public

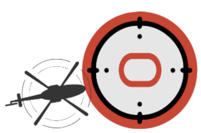
Principle 6: Focus Your Monitoring on Users, Devices, and Services

In a zero trust environment, carrying out effective and efficient monitoring to know what's happening in the platform and applications is essential. As suggested under NCSC principle 6, logging and monitoring help identify patterns of activity on networks, which can provide indicators of compromise. In the event of incidents, logging data can identify the source and the extent of compromise more effectively. For this purpose, it becomes necessary to collect key metrics from various resources continuously and trigger automated alarms and remediations when abnormal activities happen or when there's a deviation from the defined security baseline.

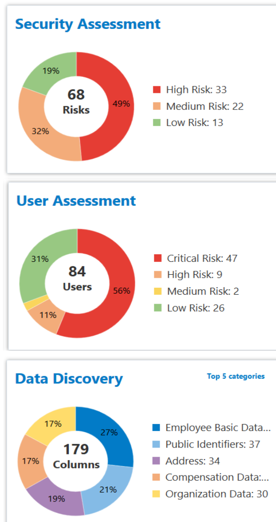
Service Monitoring

OCI enables continuous and comprehensive monitoring of resources and services in a tenancy. Table 5 details two key controls for service monitoring within OCI.

Table 5: Service Monitoring within OCI

OCI Component	Description	Health Information
Cloud Guard  *CIS Secure Landing Zone*	Oracle Cloud Guard provides a unified view of cloud security posture management for OCI. Oracle Cloud Guard, including the new Threat Detector, detects misconfigured resources, insecure activity across tenants, and malicious threat activities. It provides security administrators with the visibility to triage and resolve cloud security issues. Security inconsistencies can be remediated automatically with ready-to-use security recipes to scale the security operations center effectively. Cloud Guard Instance Security inspects Compute instances in near-real time and provides MITRE-ATT&CK-aligned runtime security alerts using ready-to-use detectors.	You can use Cloud Guard to help ensure that the security posture of services hasn't been weakened through misconfiguration or activity within an OCI tenancy. Cloud Guard Threat Detector can continuously monitor cloud environments using targeted behavior models aligned with the MITRE ATT&CK framework. It applies data science to help discover compromised environments quickly, so that customers can focus on the most important threat alerts. Cloud Guard Instance Security can provide visibility into the security posture of Compute instances and risks and vulnerabilities associated with them. Instance Security can also provide remote endpoint visibility by enabling remote querying of instances to detect threat and suspicious behavior.
Threat Intelligence service	OCI 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 and other OCI services.	You can start Threat Intelligence by enabling Cloud Guard in the tenancy. This service then begins to correlate the logs against known malicious IPs

Copyright © 2024, Oracle and/or its affiliates / Public

	This service provides insights from Oracle security researchers, our own unique telemetry, and open source feeds, such as abuse.ch and Tor exit relays.	and support detection, such as suspicious IP activity, by default. Threat Intelligence service also provides a searchable database of indicators that security analysts can use to get more contextual information about indicators.
Data Safe	Oracle Data Safe provides security and user risk assessment for Oracle databases, whether running in the cloud or on-premises. As shown on the right, these key findings are presented in a dashboard within Data Safe. 	You can use Data Safe to monitor a database's security posture, allowing organizations to mitigate the risk of a configuration change weakening that posture. You can utilize user assessment to allow regular review of database user accounts, removing unnecessary privileges, or users who present a critical risk to a database.

Many capabilities are listed in tables 3 and 4, highlighting capabilities including Web Application Firewall**,** which acts as a reverse proxy that monitors and inspects all traffic flows or requests from the internet, before they arrive at the web application. This powerful service enables control over data to application servers while helping to protect servers from outside threats.

Furthermore, metrics are published by all OCI services about the health, capacity, and performance of the resources. You can also publish custom metrics to the OCI Monitoring service using the API. OCI Monitoring then uses these metrics to monitor the resources, and OCI Notification sends notifications when these metrics meet alarm-specified triggers, as shown in figure 6.

Copyright © 2024, Oracle and/or its affiliates / Public

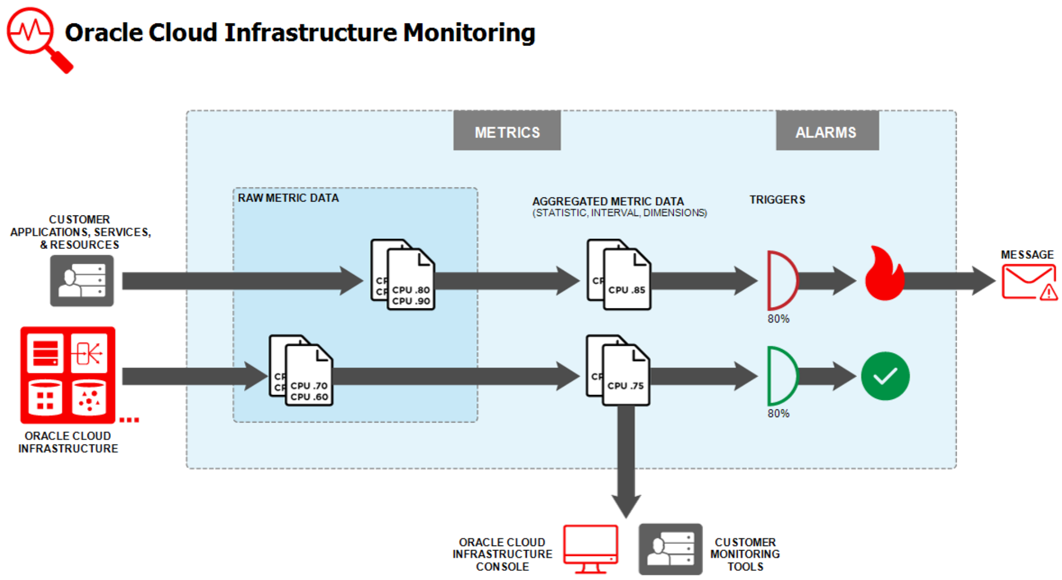


Figure 6: OCI Monitoring and Notifications.

User Monitoring

OCI IAM generates audit data in response to all administrator and end-user operations, such as user login, application access, password reset, user profile update, and operations such as create, read, update, and delete (CRUD) on users, groups, applications, and so on. This audit data is accessible through the SCIM 2.0-compliant REST endpoints. Using these APIs, data can be integrated into an organization's existing security tools. Integrations can include a security information and event management (SIEM) system, which collects logging data from various sources and collates that data to look for security events. Another option is integration with user and entity behavior analytics (UEBA) systems, which collect logging and activity data, build patterns of normal behavior to then spot anomalous behavior in users and other entities, such as devices.

Device Monitoring

Earlier principles covered how endpoint security and enterprise mobility management are beyond the scope of capabilities that Oracle offers for continuous device monitoring. However, you can perform risk-based authentication based on the device footprint collected by the identity service. OCI also supports creating monitoring-enabled Compute instances using the Console or APIs.

Principle 6 underscores the importance of having reliable logging. The extensive auditing and logging capabilities provided by OCI provide insights into activities on the OCI tenancy from the perspective of who did what and when. Log and audit data are available across an OCI tenancy, as well as applications and services running on a tenancy, and you can interrogate this information either interactively through the Console or programmatically through the API to analyze the data.

You can detect and respond to threats to a cloud deployment by setting up efficient SIEM for analyzing logs generated by the OCI Logging and Audit services. OCI Functions can fetch these audit events through API, then process and export audit data to a SIEM, such as Splunk and QRadar, through an HTTP event collector. An OCI plugin for Splunk can ingest logs directly from a stream within OCI Streaming. Administrators can also integrate with other Splunk plugins and data sources, such as threat intel feeds, to augment and enhance alerting from log data.

Furthermore, you can easily port suspicious or malicious activity identified by Cloud Guard Threat Detector into an organization's SIEM or security orchestration, automation, and response (SOAR) system.

Copyright © 2024, Oracle and/or its affiliates / Public

Network Monitoring

Performing continuous network monitoring is good cyber hygiene to improve visibility into connection information for traffic within, to, and from a VCN. VCN flow logs keep detailed metadata records of every flow that passes through a VCN and presents this data for analysis in the OCI Logging service. This data includes information about the source and destination of the traffic, along with the volume of traffic and the accept or reject policy action taken, based on existing network security rules. You can use this information for network monitoring, troubleshooting, and compliance. Through cloud native integration with the Logging service, you can view, search, export, and stream log files to an on-premises SIEM.

Copyright © 2024, Oracle and/or its affiliates / Public

Principle 7: Don't Trust Any Network, Including Your Own

Oracle has considered the trust given to various critical components of a cloud infrastructure, including servers, hypervisors, and networks, and designed a secure architecture to help mitigate threats to these elements from within the underlying infrastructure. To reduce the risk from hypervisor-based attacks and increase tenant isolation, OCI designed the virtualization stack with a security-first architecture, enabling customers to trust OCI with the most critical workloads. Table 6 shows a summary of some of these security design principles.

Table 6: Some of the OCI security-first design principles

OCI Security Construct	Description	Benefits
Server **Hardware-based root of trust**	A primary design principle of OCI is protecting tenants from firmware-based attacks, which entails not trusting the server and, more specifically, the firmware that resides on it. This method requires a process of wiping and reinstalling the gold-state server firmware from trusted source every time a new server is provisioned for a tenant or between tenancies, regardless of the instance type.	OCI hardware root of trust helps reduce the risk from firmware-based attacks, such as a permanent denial of service (PDoS) attack or attempts to embed backdoors in the firmware to steal data or make it otherwise unavailable. The design avoids the risk of a firmware compromise spreading across customers.
Hypervisor **Isolated network virtualization**	The underlying design principle of isolated network virtualization is removing network control from the hypervisor and placing it in a separate physical smartNIC installed in every server within OCI. This ready-to-use virtualization provides maximum isolation and protection, limiting the blast radius.	Isolated network virtualization helps prevent hypervisor breakouts or hyperjacking. The hardened, isolated network virtualization layer helps ensure that any threat is contained within that server. The design prevents lateral movement if a machine is compromised, ensuring that an attacker can't use the compromised machine as a pivot point to move laterally to other machines on the network. It enforces security of network traffic across the OCI network backbone.
Network **Hyper Segmentation**	The OCI physical network is designed for customer and service isolation. It's segmented into enclaves with unique communications profiles. Access into and out of these enclaves is controlled, monitored, and 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	Hypersegmentation separates cloud service workloads running in a service enclave, from customer workloads that run on their own physical network. It enables strict monitoring and control over traffic flows between hypersegmented enclaves within the OCI substrate.

Copyright © 2024, Oracle and/or its affiliates / Public

	security mechanisms as internet traffic such as inbound Secure Shell (SSH) bastion hosts and outbound SSL proxies.	It implements least privileged access for services within the OCI services network by controlling access both in and out of the enclaves.
WAN encryption	OCI implements layer 2 MACSec encryption on the private backbone between availability domain and between regions. Region-to-region traffic is authenticated using unique key pairs between regions, preventing a bad actor from traversing regions by stealing a secret key.	WAN encryption prevents network sniffing and enables removing a region from the trust if necessary.
TLS public endpoints	All Oracle-provided endpoints are encrypted using TLS 1.2.	TLS public endpoints remove the chance of man-in-the-middle attacks or network sniffing.
DDoS Protection	OCI 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 feature is provided by default and is transparent to users. Oracle provides a layer 7 DDoS mitigation service to help mitigate layer 7 DDoS attacks. DDoS mitigation specialists help onboard our customers to WAF if they're not already using it.	Layer 3 and 4 DDOS protection helps to mitigate customer workloads from the risk of a volumetric DDoS attack. This service is provided standard with all OCI accounts, at no extra cost, and requires no configuration or monitoring. Layer 7 DDoS mitigation service has a price insurance program, through which a customer might be eligible for credits because excessive consumption from a DDoS attack.
Governance **Supply Chain Security**	Oracle carries a long history of developing enterprise-class secure hardware. The hardware security team designs and tests the security of the hardware that's used to deliver OCI services. This team works with our supply chain and validates hardware components against our rigorous hardware security standards.	Oracle supply chain risk management practices focus on quality, availability, continuity of supply, and resiliency in Oracle's direct hardware supply chain, and authenticity, and security across Oracle's products and services.

All the controls detailed in table 6 are part of the security provided within the infrastructure design and build. Beyond those design principles, a broad set of controls are provided for customers to use when building out solutions on OCI, as summarized in table 7.

Table 7: Networking controls within an OCI tenancy

OCI Capability	Description	Applicable Controls
OCI DNS	OCI provides a global anycast, fully managed DNS service that you can use as a primary or secondary DNS service.	OCI DNS provides both public and private DNS resolvers. The capability provides built-in layer 3 and 4 protection against DDoS.

Copyright © 2024, Oracle and/or its affiliates / Public

Security lists and NSGs *CIS Secure Landing Zone*	Security lists and network security groups provide the ability to control traffic flow within and across subnets and VCNs within a tenancy.	Security lists and NSGs limit traffic flows across a VCN within OCI through configurable rules and policies.
OCI Bastion *CIS Secure Landing Zone*	OCI Bastion provides secure and time-limited SSH access and port forwarding communication to customers' private Oracle Compute resources, such as VMs and Kubernetes clusters, and databases.	OCI Bastion enables customers to access Oracle Compute resources and databases without requiring those resources to use a public endpoint. Customers authorize access using fine-grained IAM policies, run access using time-bound SSH sessions, and audit access centrally using OCI Logging.
Shielded instances	Shielded instances harden the firmware security on bare metal hosts and VMs to defend against malicious boot level software. Shielded instances use the combination of secure boot, measured boot, and the trusted platform module (TPM) to harden the firmware security on the instances.	While secure boot prevents unauthorized boot loaders and operating systems from booting, measure boot complements it and enhances boot security by storing measurements of boot components to ensure integrity. TPM is a specialized security chip used by measured boot to store the boot measurements.
Gateways • **Internet** • **NAT** • **Dynamic routing** • **Service** • **Local peering**	Gateways enable communication with destinations outside of the VCN.	Gateways provide control over how and where traffic can flow. For example, not configuring an internet gateway ensures that no external traffic can reach a subnet.
Private endpoints	Private endpoints control how traffic is routed from a VCN's subnet to destinations outside the VCN.	Private endpoints ensure that you can configure traffic to flow as designated, such as routing service-to-service traffic over a private link versus the internet.
OCI IAM *CIS Secure Landing Zone*	OCI IAM provides control over specific access and actions permitted by IAM groups to resources in a tenancy.	OCI IAM limits the ability for any unauthorized users to view and change any networking configuration within a tenancy.
Private and public subnets *CIS Secure Landing Zone*	Private and public subnets enable segregation of resources into different subnets that can be private or public.	Private and public subnets provide a way to compartmentalize resources into subnets that can't be connected to the internet directly.

Copyright © 2024, Oracle and/or its affiliates / Public

OCI Network Firewall	OCI Network Firewall provides a cloud native, managed firewall service built using Palo Alto Networks' next-generation firewall technology (NGFW). It offers machine learning-powered firewall capabilities to protect the OCI workloads and is easy to consume on OCI. As an OCI native firewall-as-a-service offering, OCI Network Firewall enables the organizations to begin to take advantage of the firewall features without the need to configure and manage more security infrastructure.	OCI Network Firewall enables flexible policy enforcement, allowing organizations to easily apply granular security rules on inbound (north-south), outbound, and lateral (east-west) traffic to their application and network workloads. It can be transparently inserted in the traffic path using VCN routing rules and configured with other network functions, such as OCI gateways and VCN subnets, for security enforcement in arbitrary network topologies.
Virtual test access point (VTAP)	OCI VTAP is a traffic mirroring service that copies traffic that traverses a specific point in the network and sends the mirrored traffic to a network packet collector or network analytics tool for deep inspection and further analysis later.	OCI VTAP provides comprehensive visibility into network traffic to identify granular anomalies. It also helps adhere to compliance requirements that might mandate monitoring and logging specific traffic by mirroring required traffic to a network monitoring appliance.
Network sources	A network source is a set of defined IP addresses. The IP addresses can be public IP addresses or IP addresses from VCNs within your tenancy. After you create the network source, you can reference it in policy or in your tenancy's authentication settings to control access based on the originating IP address.	Network sources enable further protection of resources based on network location.

In addition to network-specific controls, further controls, including security zones, Cloud Guard, and Web Application Firewall, have already been discussed in detail in previous sections of this paper.

Copyright © 2024, Oracle and/or its affiliates / Public

Principle 8: Choose Services Designed for Zero Trust

As suggested under principle 7, given that the network isn't trusted under a zero trust architecture, services must be designed to protect themselves. Table 6 in the previous section details some of the security design principles in the OCI security-first approach.

OCI is architected on least-trust principles, based on the assumption of compromise, which culminates in a zero trust architecture. The isolation property has the following dimensions:

- Isolation from other tenants
- Isolation from the cloud provider's staff
- Ability to configure isolation between lines of businesses in tenancies
- Ability to configure isolation from external threat actors

OCI built these security capabilities into the architecture to help enforce isolation from these four threat actors, as shown in figure 7. One example of this isolation is the use of OCI compartments as first-class resources within OCI. As discussed in table 4, compartments are logical containers of OCI resource to which you can apply access controls policies, allowing policy-driven isolation within a tenancy.

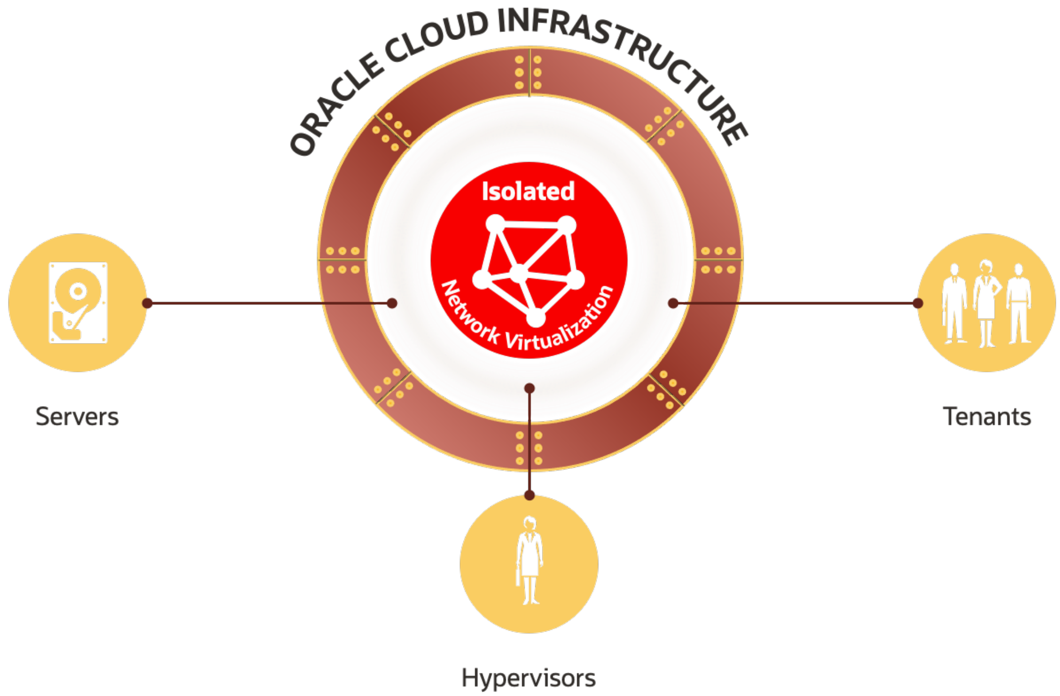


Figure 7: OCI least-trust design with an assumption of compromise.

Principle 8 also highlights the importance of using standards. OCI enables customers and partners to avoid cloud vendor lock-in by following standards for an open ecosystem. The mapping against earlier principles discusses the support for industry open standards, such as SAML, OAuth, OpenID Connect, and SCIM, together with how you can use them for both user and service requests.

Previous sections also explained that an identity service is provided with the support for these open standards. Consequently, you can use this identity service not just for OCI, but for any web-based applications hosted in OCI, in a third-party cloud provider, or on-premises. Using the App Gateway, you can enable SSO for web applications that don't support open standards, as discussed in this paper. Furthermore, delegated authentication is possible for organizations that want to standardize on Active Directory for authentication.

Copyright © 2024, Oracle and/or its affiliates / Public

Mapping the OCI CIS Secure Landing Zone to NCSC Zero Trust Principles

In the following table, empty boxes show that the landing zone isn't applicable or doesn't yet implement controls for this area.

Capability	Description	8 Zero Trust Principles Applicability							
		1	2	3	4	5	6	7	8
OCI Identity and Access Management	The landing zone creates the groups, compartments, and policies to enable least privilege and segregation of duties within a tenancy.	✓	✓	✓	✓	✓	✓	✓	✓
Networking	The landing zone separates different resources across multiple subnets and VCNs and applies the necessary structure to logically separate resources within a tenancy.	✓			✓		✓	✓	✓
Key Management (KMS)	The landing zone creates virtual vaults and keys that any OCI services that integrate with the Vault service can use.		✓		✓				✓
Cloud Guard	The landing zone enables OCI Cloud Guard with all the detectors and responders at the root compartment.						✓	✓	✓
Vulnerability Scanning	The landing zone creates a single Vulnerability Scanning target. The recipe is assigned to all provided targets.								✓
Bastion	The landing zone creates a single instance of Bastion to connect to a target subnet, as defined within the Terraform configuration.							✓	✓
Events (Auditing)	The landing zone creates multiple OCI event rules, such as IAM policy changes, VCN changes, IAM group changes, and IAM user changes.	✓	✓				✓		✓
Notifications	The landing zone creates at least two topics each with a subscription: A security topic and subscription where all IAM related events are sent and a network topic and subscription where all network related events are sent.	✓							
Security Zones	The landing zone creates one recipe for each defined compartment and creates a security zone for each defined compartment with the associated recipe.				✓			✓	✓

Copyright © 2024, Oracle and/or its affiliates / Public

Conclusion

Zero trust security isn't a product or a checkbox to enable something within an application at a given point in time. Zero trust is an approach, not a single action, and takes time, effort, and investment to adopt.

Based on the principles of a compromised network with untrusted devices and users, zero trust security puts the emphasis on understanding an organization's users, services, devices, and data, and then implementing appropriate controls to suitably authenticate requests and authorize them based on multiple signals, while monitoring all access. When deciding where to place workloads, choosing a cloud provider who aligns to a zero trust security strategy and can provide the necessary controls to help accelerate a zero trust program is important.

Oracle built OCI with a security-first design principle, implementing core zero trust security from the ground up, through controls, including Hardware-based Root of Trust, isolated network virtualization, and hypersegmentation. All the principles are designed with a least-trust approach for critical components of the cloud infrastructure, such as servers, hypervisors, and networks. For more information on the OCI security-first approach, see the OCI Security Architecture tech brief.

Oracle has emphasized delivering security controls within OCI that help automate and strengthen security. Oracle enables encryption by default and provides cloud security posture management with the ability to remediate problems automatically. Oracle's strategy is to deliver cost effective solutions that are easy for organizations to implement, helping organizations effectively address their cloud security responsibilities.

Zero trust security isn't a product to buy or a checkbox to enable within an application. Instead, zero trust is an approach that takes time, effort, and investment to adopt.

Choose a cloud provider who aligns to a zero trust security strategy and can provide the necessary controls to help accelerate a program based on zero trust.

Copyright © 2024, Oracle and/or its affiliates / Public

Connect with us

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

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

Copyright © 2024, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.