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 8 principles

Paul Toal
Krithiga Gopalan

July 2022, Version 1.2
Copyright © 2022, Oracle and/or its affiliates
Public
Table of contents

Executive Summary 4
Introduction 5
Principle 1 – Know your architecture, including users, devices, services, and data 7
Principle 2 – Know your user, service, and device identities 9
  User Identity 9
  Service Identity 12
  Device Identity 13
Principle 3 – Assess user behaviour, service, and device health 14
  Device Health 14
  Service Health 15
  User Health 16
Principle 4 – Use policies to authorize requests 18
Principle 5 – Authenticate and authorize everywhere 22
Principle 6 – Focus your monitoring on users, devices, and services 24
  Service Monitoring 24
  User Monitoring 26
  Device Monitoring 26
  Network Monitoring 27
Principle 7 – Don’t trust any network, including your own 28
Principle 8 – Choose services which have been designed for zero trust 32
Conclusion 34
List of images

Figure 1 - Conceptual representation of the various security management responsibilities between customers and cloud providers 6

Figure 2 – Using different factors to determine an identity's risk level 13

Figure 3 – Ensuring device compliance with Oracle Mobile Authenticator 14

Figure 4 – Evaluating multiple signals during authentication 17

Figure 5 – OCI services currently supported by OCI KMS 20

Figure 6 – Security Lists and Network Security Groups work at different levels of granularity 21

Figure 7 – Using Oracle as an enterprise identity hub 22

Figure 8 – OCI Monitoring & Notifications 25

Figure 9 – OCI Least Trust Design – Assumption of Compromise 32

List of tables

Table 1. Principle 1 controls - These OCI tools can help with asset discovery. 8

Table 2. Principle 2 controls – Providing a rich set of identity capabilities in OCI IAM 11

Table 3. Principle 3 controls – OCI provides capabilities for monitoring health 16

Table 4. Principle 4 controls – Policy-based authentication and authorization controls 20

Table 5. Service monitoring within OCI 25

Table 6. Some of the OCI security-first design principles 30

Table 7. Networking controls within an OCI tenancy 31
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’s¹ (NCSC) 8 Zero Trust principles² as a framework for discussing OCI controls. The 8 Zero Trust principles are as follows:

1. Know your architecture, including users, devices, services, and data
2. Know your user, service, and device identities
3. Assess user behaviour, service, and device health
4. Use policies to authorize requests
5. Authenticate and authorize everywhere
6. Focus your monitoring on users, devices, and services
7. Don’t trust any network, including your own
8. 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 is not specific to UK companies and has applicability to organizations globally.

¹ https://www.ncsc.gov.uk/
² https://www.ncsc.gov.uk/collection/zero-trust-architecture
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 a number of 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 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 leveraging 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 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 three tenets to assist customers in securing their cloud:

- **Simple**—Designing security controls that are easy to use, deploy, and operate.
- **Prescriptive**—Providing prescriptive guardrails reflecting Oracle’s expertise, enabling organizations to more easily achieve a stronger security posture.
- **Integrated**—Providing built-in and integrated security across infrastructure-, platform-, and software-as-a-service, reducing manual security tasks and human error.

Before exploring the NCSC’s eight principles, it is critical to establish that IT departments and their cloud providers have respective roles to play in managing cloud security.

---

1 Gartner®, Hype Cycle™ for Cloud Security, 2021, Tom Croll, Jay Heiser, 27 July 2021. GARTNER and HYPE CYCLE are registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

5 Whitepaper - Approaching Zero Trust Security with Oracle Cloud Infrastructure / Version 1.2
From a security management perspective, cloud is fundamentally different from on-premises. This is because, though IT departments maintain full control of technology infrastructure on-premises (e.g., physical control of the hardware and full control over the technology stack in production), the cloud leverages 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.

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.
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 will most likely not be a purely technical exercise, but instead involve tasks such as reviewing project documentation, procurement records, and conversations with colleagues. Getting to know the architecture can be difficult due to different departments and lines of business implementing their own solutions. This 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 a number of tools and services that expedite the asset discovery phase by helping to identify and understand what is already deployed. Table 1 summarizes this below.

<table>
<thead>
<tr>
<th>OCI COMPONENT</th>
<th>DESCRIPTION</th>
<th>DISCOVERY PROVIDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Representational State Transfer Application Programming Interface (REST API)</td>
<td>OCI provides REST APIs for accessing and managing the OCI tenancy. There is also an SDK for various languages as well as a CLI, all of which can be used for programmatic access to an OCI tenancy. OCI Resource Tagging allows keys and values to be defined and associated with resources.</td>
<td>Scripts can be written to enumerate all resources that have been created within the OCI tenancy. Examples of scripting using the OCI CLI are provided. Resource tags can be used by organizations to organize and list resources used for specific projects or systems.</td>
</tr>
<tr>
<td>Command Line Interface (CLI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development Kit (SDK)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terraform</td>
<td>Oracle delivers an OCI provider for Terraform to enable OCI deployment to be implemented through Infrastructure-as-Code (IaC). Terraform Discovery can be used to build IaC scripts based on the existing deployed footprint and therefore, could be used to document the existing OCI deployment.</td>
<td></td>
</tr>
<tr>
<td>Auditing</td>
<td>OCI provides an Audit service that automatically records calls to all supported OCI public API endpoints as log events. This includes calls made by the console, API, SDK, and CLI, custom clients, other OCI services. Auditing within OCI can be used to understand which services are being called, who is making these calls, which calls are successful, and which are unauthorized.</td>
<td></td>
</tr>
</tbody>
</table>

As highlighted by NCSC, undertaking an asset discovery activity will most likely not be a purely technical exercise, but instead involve reviewing project documentation, procurement records, and conversations with colleagues.

---


5 https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/cliusing.htm
### VCN Flow Logs

VCN flow logs within OCI provide visibility into connection information for traffic within and to-and-from a virtual cloud network (VCN).

VCN flow logs can be used to understand what traffic is flowing between services over which ports. This 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, including integration, governance, identity, security, data management, analytics, etc.

Platform Services can be used to understand the existing deployments. For example:

- **OCI Identity and Access Management (IAM)** can be used to discover users, their roles, and their access privileges.
- **Oracle Integration Cloud and Oracle API Gateway** can be used to identify existing data flows.
- **Oracle Data Safe** can be used to identify sensitive data within Oracle Databases, whether running on-premises or in the cloud.
- **Oracle Data Catalog** can be used for managing data and data governance and can provide an invaluable repository of existing data assets.
- **Oracle Container Registry** can be used to list the published applications and services for DevOps deployments.
- **Oracle Container Engine for Kubernetes** and **Oracle Resource Manager** can be used to identify the applications and/or services that are running.

<table>
<thead>
<tr>
<th>Table 1. Principle 1 controls - These OCI tools can help with asset discovery.</th>
</tr>
</thead>
</table>

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. The template can be found here:

Principle 2 – Know your user, service, and device identities

The IT industry has recognized that the gradual movement to cloud has accelerated the erosion of the traditional network perimeter. With that, identity has been recognized as the new perimeter for some time⁶. Oracle provides an enterprise-class Identity-as-a-Service (IDaaS) platform called OCI Identity and Access Management (IAM), which uses the concept of domains⁷.

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

Identity is the core tenet of NCSC’s second principle, and OCI IAM can help to deliver upon this principle.

User Identity

OCI utilizes two main types of user identities:

- Administrative users who are accessing OCI to perform functions within the OCI platform itself (e.g., creating networks, backing up compute instances, and managing encryption keys).
- End users who access applications. These applications may be running within (e.g., Oracle Analytics Cloud Service) or outside of OCI.

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

Although the identity service can serve as a main identity repository, many organizations will 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 below shows how OCI IAM maps against the capabilities that NCSC states an identity service should be able to do.

---


⁷ OCI IAM domains has merged the capabilities of OCI IAM and Oracle Identity Cloud Service into a combined service
<table>
<thead>
<tr>
<th>IDENTITY SERVICE FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Create groups | OCI IAM provides the ability to create and manage groups within identity domains. Once created, identities can be assigned to, and revoked from groups. Group management can be done in one of several ways:  
  - **Web-based console** – The service provides a feature rich web-based console for administration and self-service.  
  - **SCIM-based REST API** – Administration can be executed through the SCIM REST API, or through one of the API derivatives such as SDKs.  
  - **Synchronization** – Numerous out-of-the-box 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. |
| Define roles that have been configured to be ‘least privilege’ | OCI IAM denies access with administrative privileges by default, within OCI. Administrators cannot access any resources until they are 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:  
  ```bash  
  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. Once a group has been mapped to either an application or application roles, end-users assigned to that group will then have the appropriate access.  
  From a user administration perspective, there are a number of pre-defined administrative roles which provide differing levels of admin access. Therefore, only the minimum administrative privileges that are required are granted to any particular administrator. |
| Support strong, modern authentication methods | OCI IAM supports a wide range of authentication factors, including multi-factor authentication (MFA), passwordless authentication, and risk-based authentication.  
  Supported multi-factor 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, Windows Hello, etc.  
  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 for an additional authentication factor, such as one of the factors mentioned above. |

---


**Different MFA factors can be enabled/disabled in OCI IAM as required**

- Email
- Bypass code
- FIDO2 Online (FIDO) authenticator
- Mobile
  - Mobile app password
- Mobile app notification
- Duo security
- Text message (SMS)
- Phone call
| Securely provision credentials to users | How credentials are provisioned to users securely will depend on how the user was created:  
| • Self-registration – For users who self-register, the user can create their own password (subjected to the configurable password policy) at registration time.  
| • Administrative action – If an administrator creates the user’s identity record, then a time-bound link will be emailed to the users, from where they can set their own password. Similarly, an administrative password reset follows the same flow.  
| • Synchronization – In many cases, synchronized users will not authenticate to OCI IAM directly, but will instead authenticate through federated single sign-on (SSO) (e.g., using the Security Assertion Markup Language or SAML). For these users, Oracle does not 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 does not manage user passwords. |

| Authenticate to services | Oracle supports industry open standards for federated authentication, including: SAML 2.0, OAuth 2.0, and OpenID Connect. These can be used to authenticate to the service, or to facilitate SSO to connected applications.  
In scenarios where a target application doesn’t support open standards, App Gateway can be used as a reverse-proxy bridge between Oracle and the application, converting the open standards token into a format the protected application can understand (e.g., header variables). |

| Manage user identities in external services | OCI IAM supports the SCIM 2.0 open standard. A large number of application templates are provided out-of-the-box to accelerate integration with common, popular target applications and services. In addition, generic SCIM templates are also provided.  
The service can both produce SCIM messages for managing identities in target applications, as well as consume SCIM messages from authoritative sources. |

| Support Joiner, Mover, Leaver (JML) processes | OCI supports joiner, mover, leaver (JML) processes through either the SCIM interfaces discussed above, or via 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, the feed can be used as an authoritative or non-authoritative source, meaning that the source can either create the identity record (where it does not already exist) or create an account record, representing an account in a target system, which it links back to the identity record.  
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 | As discussed above, OCI supports federated identities, both for SSO through standards including SAML, OAuth, and OpenID Connect, as well as for user management through SCIM and other out-of-the-box synchronization capabilities. |

Oracle supports industry open standards such as SAML, OAuth, OpenID Connect and SCIM for both user as well as service requests.

OCI helps customers and partners to avoid cloud vendor lock-in by supporting such open standards and creating an open-ecosystem.

Table 2. Principle 2 controls – Providing a rich set of identity capabilities in OCI IAM
As discussed by NCSC in principle 2, user consent is a key element of an identity system. Consent management is supported by the identity service in several different areas:

- ‘Terms of use’ agreement 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. OCI built the cloud-native identity service using a microservices approach, with each microservice authenticating to each other’s microservice using secure protocols. This design does not require inherent trust among these microservices.

Though OCI provides a consistent repository for different types of identities, additional capabilities exist to help achieve Zero Trust security.

In addition to user identities, OCI provides identities for compute instances, called instance principals. A compute instance may often need to access other OCI services, such as storage, databases, networking, etc. The traditional approach to achieving authenticated access to these resources would be to embed credentials for those resources within the compute instance. However, this approach adds management overhead as there is a responsibility to ensure that those credentials are 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 very similar to instance principals, but used for resources that are not 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 those written for user identities), thus ensuring the authorization policies are defined centrally within OCI IAM for user identities as well as instance and resource principals.

Certificates are used as the credentials for instance and resource principals and these are managed by OCI automatically, including creation, assignment, and rotation.
Furthermore, OCI Administrators write IAM policies that determine the privileges that an instance/resource principal can execute. 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. A sample instance principal policy is below:

Allow dynamic-group AppServersProd to inspect objects in compartment images

For situations where an application/system running on a compute instance may need credentials to access an endpoint (e.g., API endpoint, database, etc.), OCI provides OCI Vault. OCI Vault can securely store and retrieve secrets encrypted using customer-managed master encryption keys stored in FIPS 140-2 Level 3 Hardware Security Modules (HSMs). The identity referenced by these secrets can be stored and mastered in the identity service.

OCI Vault offers two main capabilities: OCI Key Management Service (KMS) and OCI Secrets Management Service. The remainder of this document refers to the specific service to meet the principle being addressed.

Device Identity

OCI does not 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, then the user’s risk score can be increased accordingly and appropriate action taken, such as challenging for stronger authentication, or denying the authentication attempt. Figure 2 shows the risk factors available as part of the risk-based authentication.

Figure 2 – Using different factors to determine an identity’s risk level
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

Device health can be monitored as part of MFA. When using either time-based one-time password (OTP) or push notification factors for MFA, the Oracle Mobile Authenticator can be used. As part of the MFA configuration, a compliance policy can be set to enforce certain device configuration settings (OS version check, rooted devices check, etc.) as shown in the figure below.

- Compliance policy

  Mobile authenticator app version check
  - Require latest updates
  - Block users from using an outdated app.

  Minimum OS version check
  - Restrict access from devices with outdated OS versions
  - Block users from using the app on a device that has an outdated operating system. Users won’t receive push notification requests and won’t be able to generate passcodes.

  Rooted devices check (iOS and Android only)
  - Block users from using the app on a device that is rooted or where rooted status is unknown. Users won’t receive push notification requests and won’t be able to generate passcodes.
  - Restrict access from rooted devices
  - Restrict access from devices where rooted status is unknown

Device screen lock check

- Block users from using the app on a device that doesn’t have a screen lock or where the screen lock status is unknown. Users won’t receive push notification requests and won’t be able to generate passcodes.
- Restrict access from devices without a screen lock
- Restrict access from devices where screen lock status is unknown

Figure 3 – 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. This includes the OCI Hardware Root of Trust\(^9\), 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.

## Service Health

OCI implements a number of capabilities to establish the health of services.

<table>
<thead>
<tr>
<th>OCI CAPABILITY</th>
<th>DESCRIPTION</th>
<th>HEALTH INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Autonomous Services</strong></td>
<td><strong>Autonomous Linux</strong> minimizes complexity and human error to increase security and availability by providing core security capabilities including zero downtime, automatic patching, as well as known exploit detection.</td>
<td>Autonomous Linux and Autonomous Database can be utilized to improve the health of services through automation and machine learning.</td>
</tr>
<tr>
<td></td>
<td><strong>Autonomous Database</strong> protects sensitive and regulated data automatically through self-securing capabilities including automated patching, enforced separation of duties, encryption at rest and in motion by default.</td>
<td></td>
</tr>
<tr>
<td><strong>OS Management</strong></td>
<td><strong>OS Management Service</strong> enables management of updates and patches for the operating system environment on OCI instances that are not running Autonomous Linux.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Auditing and Logging</strong></td>
<td>The <strong>OCI Logging Service</strong> provides access to all the logs from OCI resources in a tenancy, including OCI Audit Service, Service logs, and custom logs. Furthermore, <strong>OCI Logging Analytics</strong> provides the capability to capture and analyze all log data from applications and system infrastructure either on cloud, or on-premises.</td>
<td>Log and audit data can be generated across an OCI tenancy as well as 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.</td>
</tr>
<tr>
<td><strong>Vulnerability Scanning</strong></td>
<td><strong>OCI Vulnerability Scanning Service (VSS)</strong> scans installed packages and artifacts looking for the existence of known vulnerabilities on customer’s compute instances and in container images from their Oracle Cloud Infrastructure Container Registry (OCIR) repositories. The service also scans for publicly and privately open ports on an instance and reviews the configuration of each instance against specific OS CIS benchmarks.</td>
<td>These findings from VSS can be used to enable customers to know what packages should get patched or what security hardening steps should be taken by them. VSS is integrated by default with Cloud Guard to provide users a unified view of their vulnerability status of their instances and container images.</td>
</tr>
</tbody>
</table>
### Events

OCI services emit industry standard CloudEvent 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.
- **Functions** – executing a serverless function, based on the industry standard Fn project.
- **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.

### Operational Insights

**Operational Insights** provides a 360-degree insight into the resource utilization and capacity of Oracle Autonomous Database.

**Operational Insights** can be used 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.

**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**.

### 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**, that enable visibility and insight across cloud native and traditional technology, whether deployed in multi-cloud or on-premises environments, with broad, standards-based ecosystem support.

**Service Connector Hub** can be used to provide 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 can be utilized to provide cross technology, cross-cloud, full stack visibility with unified telemetry, data exchange and applied machine learning.

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

<table>
<thead>
<tr>
<th><strong>User Health</strong></th>
</tr>
</thead>
</table>

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 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 has not previously registered a second factor, then enrollment can be made mandatory if required.
Sign-on policies can also consider additional signals from users, such as where they are coming from, their group membership, and which application they are accessing. These factors, including the user’s risk score can be considered when making an authentication decision. In the example shown in figure 4, a user who is authenticating through the Google Identity Provider, and is a member of the Federated Users group, will be prompted for an additional factor whenever they try to access the application associated with this sign-on policy.

### Conditions

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticating identity provider</td>
<td>Optional</td>
</tr>
<tr>
<td>Group membership</td>
<td>Optional</td>
</tr>
</tbody>
</table>

- **Authenticating identity provider**: Google Login
- **Group membership**: Federated Users

#### Adaptive security conditions

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk provider</td>
<td>Select</td>
</tr>
<tr>
<td>Risk score</td>
<td>&gt;</td>
</tr>
</tbody>
</table>

**Actions**

- Allow access
- Deny access
- Prompt for reauthentication
- Prompt for an additional factor
- Any factor
- Specified factors only

**FIDO Authentication**

[Image of FIDO Authentication]

**Figure 4** – 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.

---

10 https://fidoalliance.org/fido2/
Principle 4 – Use policies to authorize requests

Authorization has long been a challenge for many organizations. The subject can split be into two 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 will often result in changes being needed in off-the-shelf applications, or changes to software development approaches, where custom software is being developed.

As a result, it is common for an organization to implement coarse-grained authorization within a central SSO platform, while leaving each target application/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 below summarizes the key controls for this principle.

<table>
<thead>
<tr>
<th>OCI CAPABILITY</th>
<th>DESCRIPTION</th>
<th>APPLICABLE CONTROLS</th>
</tr>
</thead>
</table>
| OCI Identity and Access Management (IAM) | OCI IAM provides centralized authentication and coarse-grained authorization services for any integrated, protected applications. The service examines a number of 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/entitlements that help manage authorization within target applications. | OCI IAM can be used to deliver a core set of identity capabilities including:  
  • Single sign-on  
  • Risk-based, adaptive authentication  
  • Multi-factor authentication  
  • Role-based access control  
 Different applications can be protected by different sign-on policies. Authorization to an application can be controlled through mapping of roles. |
<table>
<thead>
<tr>
<th>OCI IAM provides the central, fine-grained authorization policy engine for all OCI services. This 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. 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 (i.e., inspect, read, use, and manage). OCI IAM can be used 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).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OCI Compartments</strong></td>
</tr>
<tr>
<td><strong>OCI Platform Services</strong></td>
</tr>
<tr>
<td><strong>Security Zones and Security Advisor</strong></td>
</tr>
</tbody>
</table>
**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 virtual cloud network.

**WAF** can be configured with access control rules that can be used to ensure requests are coming from authorized requesters.

Also, **WAF** can be used to provide additional layer of security onto legacy applications that may not support the latest security standards such as TLS.

---

**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 the OCI load balancer or API gateway.

OCI Certificates service can be used by organizations to avoid error-prone manual certificate management processes and instead automatically monitor and renew the certificates.

In a flexible Certificate Authority (CA) hierarchy, OCI Certificates service helps create private CAs to provide granular security controls for each CA.

---

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

In addition to the above 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\(^\text{11}\). This includes data at rest for the services shown in figure 5, as well as Database Cloud Service running on both virtual machine DB and bare metal DB. Encryption of data at rest is not something that a tenant administrator needs to enable; it is enabled as a standard across OCI.

Furthermore, customers can use **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. The OCI services shown in figure 5 all support KMS.

---

OCI implements “ubiquitous encryption” with the goal of encrypting all data, everywhere, always.

---

\(^{11}\) With the exception of local NVMe temporary storage on bare metal servers

---

20  Whitepaper - Approaching Zero Trust Security with Oracle Cloud Infrastructure / Version 1.2

Copyright © 2022, Oracle and/or its affiliates / Public
KMS also enables generating and securing the storage of asymmetric keys, which can be used with the KMS endpoints for signing and encrypting, ensuring the integrity of payloads.

For encryption in transit, OCI provides TLS 1.2-encrypted connections for all endpoints published by Oracle such as API endpoints, OCI 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.

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, for example limiting traffic between different applications and services.

OCI provides both Security Lists and Network Security Groups (NSG) 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, whereas Network Security Groups are applied to grouped set of resources, as shown in figure 6. A combination of security lists and network security groups can be used to help address the organization’s requirements.

![Security Lists and Network Security Groups diagram](image-url)

Figure 6 – 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, emergency access could be granted as required. For example, a common approach is to have local, highly privileged accounts, where the credential is not known to any single person and the credentials are kept secure (e.g., in a safe) and only accessed under controlled circumstances when needed. In these situations, there must be a process to rotate those credentials after every use. Alternatively, the use of a Privileged Access Management (PAM) tool is common for securely storing credentials of highly privileged user accounts. These can then be allocated to users under break-glass situations as needed. In addition, auditing, logging, and monitoring within OCI can be used to provide additional levels of scrutiny for necessary emergency access.
**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 provided a summary of the main capabilities of those controls, which ensure that all user and service requests are authenticated and authorized, whether they are an end user accessing applications and services, a power user/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, as well as delivering adaptive, risk-based authentication utilizing a range of signals contained in the request, including location, group membership, and authentication method (as shown previously in figure 4). Support for industry open standards such as SAML, OAuth, and OpenID Connect are also discussed, along with how they can be used for both user as well as 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 re-enter their credentials, not all applications support open standards. However, OCI IAM can deliver SSO for web applications that do not support those industry open standards, using the App Gateway.

Figure 7 demonstrates how OCI provides support for these open standards and how OCI IAM can be used to provide 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 IdP and then has SSO access to authorized applications, which may or may not support industry open standards.
Within principle 2, the subject of service-to-service communication was also discussed, including:

- How OCI instance principals and resource principals are used as secure mechanisms of authenticating OCI compute instance and serverless functions to other OCI resources, and
- How the OCI IAM policy is used to authorize access control for resources (i.e., services) within OCI.
Principle 6 – Focus your monitoring on users, devices, and services

In a Zero Trust environment, it is essential to carry out effective and efficient monitoring to know what is happening in the platform and applications. As suggested under NCSC principle 6, logging and monitoring will help identify patterns of activity on networks, which in turn can provide indicators of compromise. Furthermore, 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 some abnormal activities happen, or when there is a deviation from the defined security baseline.

Service Monitoring

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

<table>
<thead>
<tr>
<th>OCI CAPABILITY</th>
<th>DESCRIPTION</th>
<th>HEALTH INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Guard</td>
<td>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 out-of-the-box security recipes to scale the security operations center effectively. Cloud Guard for detecting and remediating OCI problems is provided at no additional cost for OCI customers. Cloud Guard can be used to help ensure that the security posture of services has not been weakened through misconfiguration or activity within an OCI tenancy. Cloud Guard Threat Detector can be used to continuously monitor cloud environments using targeted behavior models aligned with the MITRE ATT&amp;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 Fusion Applications Detectors, for Oracle Cloud HCM and Oracle Cloud ERP, can be used to provide organizations a consistent way to secure their applications, providing a unified view of the security posture across IaaS and SaaS.</td>
<td></td>
</tr>
<tr>
<td>Threat Intelligence Service</td>
<td>OCI Threat Intelligence Service 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. Threat Intelligence Service can be started just by enabling Cloud Guard in the tenancy. This service will then begin to correlate the logs against known malicious IPs and support detection such as suspicious IP activity by default.</td>
<td></td>
</tr>
</tbody>
</table>
This 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 such as CrowdStrike, a cybersecurity company that correlates trillions of security events per day to deliver actionable insights to secure endpoints, workloads, identities, and data.

**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.

Data Safe can be used to monitor a database’s security posture, thereby allowing organizations to mitigate the risk of a configuration change weakening that posture. User assessment can be utilized to allow regular review of database user accounts, removing unnecessary privileges, or users who present a critical risk to a database.

Table 5. Service monitoring within OCI

In addition, a number of 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. Custom metrics can also be published to the OCI Monitoring service using the API. The Monitoring Service then uses these metrics to monitor the resources and the OCI Notification service sends notifications when these metrics meet alarm-specified triggers, as shown in figure 8.

Figure 8 – OCI Monitoring & 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, etc. 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 a variety of 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 in an attempt 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 offered by Oracle for continuous device monitoring. However, risk-based authentication can be performed based on the device footprint collected by the identity service. OCI also supports creating monitoring-enabled compute instances using the Console or API.

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 can be interrogated either interactively through the console, or programmatically through the API to analyze the data.

Threats to a cloud deployment can be detected, and responded by setting up efficient SIEM for analyzing logs generated by the OCI Logging and Audit service. OCI Functions can fetch these audit events through API, then process and export audit data to a SIEM such as Splunk and QRadar, for example, through a HTTP event collector. There is also an OCI plugin13 for Splunk to 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, suspicious and/or malicious activity identified by Cloud Guard Threat Detector can easily be ported into an organization’s SIEM or Security Orchestration, Automation and Response (SOAR) system.

---

13 https://splunkbase.splunk.com/app/5289/
Network Monitoring

Performing continuous network monitoring is good cyber hygiene to improve visibility into connection information for traffic within as well as 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. This information can be used for network monitoring, troubleshooting, and compliance. Through native-cloud integration with the logging service, log files can be viewed, searched, exported, or streamed to an on-premises SIEM.

Although the network is untrusted and assumed hostile in Zero Trust security, network monitoring is still important to ensure good performance and cyber hygiene.
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>
<thead>
<tr>
<th>OCI SECURITY CONSTRUCT</th>
<th>DESCRIPTION</th>
<th>BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware-based Root of Trust</td>
<td>A primary design principle of OCI is protecting tenants from firmware-based attacks. This entails not trusting the server and, more specifically, the firmware that resides on it. This 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.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Hypervisor</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Isolated Network Virtualization</td>
<td>The underlying design principle of <strong>Isolated Network Virtualization</strong> is removing network control from the hypervisor and placing it in a separate physical SmartNIC installed in every server within OCI. This off-box virtualization provides maximum isolation and protection, thereby limiting the blast radius.</td>
<td><strong>Isolated Network Virtualization</strong> helps prevent hypervisor breakouts or hyper jacking. The hardened, &quot;isolated&quot; network virtualization layer helps to ensure that any threat is contained within that server. The design prevents lateral movement in the event of a machine compromise, ensuring that an attacker cannot 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.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyper Segmentation</td>
<td>The OCI 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.</td>
<td><strong>Hyper Segmentation</strong> 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 hyper-segmented enclaves within the OCI substrate.</td>
</tr>
</tbody>
</table>

One of the OCI 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 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 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.

<table>
<thead>
<tr>
<th>Network</th>
<th>WAN encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSI implements layer-2 MACSec encryption on the private backbone between availability domains, as well as between regions. Region-to-region traffic is authenticated using unique key pairs between regions, preventing a bad actor from traversing regions simply by stealing a secret key.</td>
<td>WAN Encryption prevents network sniffing and enables removing a region from the trust if necessary.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>TLS public endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Oracle-provided endpoints are encrypted using TLS 1.2.</td>
<td>TLS public endpoints remove the chance of man-in-the-middle attacks or network sniffing.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>DDoS Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSI 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. 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 not already using it.</td>
<td>Layer 3/4 DDoS protection helps to mitigate customer workloads from the risk of a volumetric DDoS attack. This service is provided as 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 may be eligible for credits due to excessive consumption due to a DDoS attack.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>OCI Network Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCI Network Firewall provides a cloud-native, managed firewall service that is 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.</td>
<td>OCI Network Firewall enables flexible policy enforcement, thereby allowing organizations to easily apply granular security rules on inbound (north-south), outbound, and lateral (east-west) traffic to their application and network workloads.</td>
</tr>
</tbody>
</table>
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 additional security infrastructure.

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.

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 is 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.

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

All of 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>
<thead>
<tr>
<th>OCI CAPABILITY</th>
<th>DESCRIPTION</th>
<th>APPLICABLE CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCI DNS</td>
<td>OCI provides a global anycast, fully managed DNS service that can be used as a primary or secondary DNS service. Security lists and network security groups provide the ability to control traffic flow within and across subnets and VCNs within a tenancy.</td>
<td>OCI DNS provides both public and private DNS resolvers. The capability provides built-in layer 3 and 4 protection against DDoS. Security lists and network security groups limit traffic flows across a VCN within OCI through configurable rules and policies.</td>
</tr>
<tr>
<td>Security Lists and Network Security Groups</td>
<td>Security lists and network security groups provide the ability to control traffic flow within and across subnets and VCNs within a tenancy.</td>
<td>Security lists and network security groups limit traffic flows across a VCN within OCI through configurable rules and policies.</td>
</tr>
<tr>
<td>OCI Bastion</td>
<td>OCI Bastion provides secure and time-limited Secure Shell (SSH) access and port forwarding communication to customers’ private Oracle Compute resources, such as virtual machines and Kubernetes clusters and to databases.</td>
<td>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, execute access using time-bound SSH sessions, and audit access centrally using OCI Logging.</td>
</tr>
<tr>
<td>Gateways, including:</td>
<td>Gateways enable communication with destinations outside of the VCN.</td>
<td>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.</td>
</tr>
</tbody>
</table>

- Internet
- NAT
- Dynamic routing
- Service
- Local peering
<table>
<thead>
<tr>
<th>Private Endpoints</th>
<th>Private endpoints control how traffic is routed from a VCN’s subnet to destinations outside the VCN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCI IAM</td>
<td><strong>OCI IAM</strong> provides control over specific access and actions permitted by IAM groups to resources in a tenancy.</td>
</tr>
<tr>
<td>Private and Public Subnets</td>
<td>Private and public subnets enable segregation of resources into different subnets that can be marked as private or public.</td>
</tr>
</tbody>
</table>

**Private endpoints** ensure that traffic can be configured to flow as designated.

For example, routing service-to-service traffic over a private link vs the internet.

**OCI IAM** limits the ability for any unauthorized users to view and/or change any networking configuration within a tenancy.

**Private and public subnets** provide a way to compartmentalize resources into subnets that cannot be connected to the internet directly.

Table 7. Networking controls within an OCI tenancy

In addition to the above 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.
**Principle 8 – Choose services which have been designed for zero trust**

As suggested under principle 7, given that the network is not trusted under a Zero Trust architecture, services need to 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. There are four dimensions of the isolation property:

1. Isolation from other tenants
2. Isolation from the cloud provider's staff
3. Ability to configure isolation between lines of businesses in tenancies
4. Ability to configure isolation from external threat actors

OCI built these security capabilities in the architecture to help enforce isolation from these four threat actors, as shown in figure 9. One such example of this isolation is the use of OCI Compartments as first-class resources within OCI. As discussed in table 4, these are logical containers of OCI resource to which access controls policies can be applied, allowing policy-driven isolation within a tenancy.

![Figure 9 – OCI Least Trust Design – Assumption of Compromise](image)

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 they can be used for both user as well as service requests.

OCI is architected on least-trust principles, based on the assumption of compromise, which culminates in a Zero Trust architecture.
Previous sections also explained that an identity service is provided with the support for these open standards. Consequently, this identity service is used not just for OCI, but for any web-based applications hosted in OCI, in a third-party cloud provider, or on-premises. Through the use of the App Gateway, SSO can be enabled for web applications that do not support open standards, as discussed in this paper. Furthermore, delegated authentication is possible for organizations that want to standardize on Active Directory for authentication.
Conclusion

Zero Trust security is not 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, it is important to choose a cloud provider who aligns to a Zero Trust security strategy and can provide the necessary controls to help accelerate a Zero Trust program.

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 hyper-segmentation. All of the principles are designed with a least trust approach for critical components of the cloud infrastructure such as servers, hypervisors, and networks. Further information on the OCI security-first approach can be found in the OCI Security Architecture whitepaper14.

In addition, 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 is not 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.
