

Oracle Cloud Infrastructure Security

The Practice Workshop

Martin Berger
Stefan Oehrli

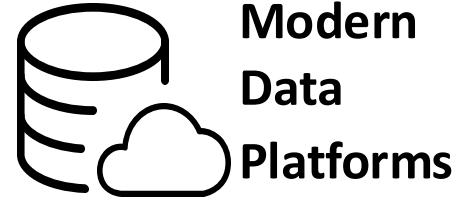
Martin Berger – Modern Data Platforms

stefan.oehrli@accenture.com



Tech Architecture Manager

- Since 1998 working in IT
- More than 22 years of experience in Oracle databases
- Kestenholz / Jurasüdfuss / Switzerland
- 2 Junior-DBAs @ Home (8yrs & 10yrs)
- Firefighter & E-Biker
- Loves his companies' cultural values:
- curiosity, doers, network, space, and together
- Focus: Let's go into the Cloud!
- Co-author of the book The Oracle DBA (Hanser, 2016/07)



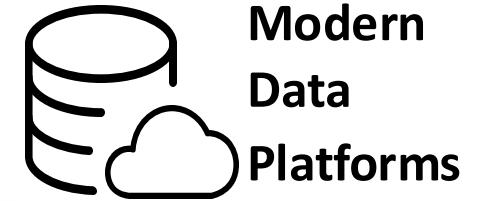
martinberger.com



@martinberger_ch

Stefan Oehrli – Modern Data Platforms

stefan.oehrli@accenture.com



Tech Architecture Manager

- Since 1997 active in various IT areas
- More than 25 years of experience in Oracle databases
- Focus: Protecting data and operating databases securely
 - Security assessments and reviews
 - Database security concepts and their implementation
 - Oracle Backup & Recovery concepts and troubleshooting
 - Oracle Enterprise User and Advanced Security, DB Vault, ...
 - Oracle Directory Services
- Co-author of the book The Oracle DBA (Hanser, 2016/07)





The Oracle ACE Program

400+ technical experts helping peers globally



- The Oracle ACE Program recognizes and rewards community members for their technical and community contributions to the Oracle community
- 3 membership levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com



Modern Data Platforms

VISION & MISSION

WHY? We are the game changer for our client's data platform projects

HOW? Maximum automation, maximum efficiency, maximum quality!

WHAT? We build innovative data platforms based on our blueprints and licensable assets and tools.



3 key benefits

1 Architecture expertise from hands-on projects

2 Delivery of tailor-made data platforms

3 Integrated Teams Like a rowing team, perfect alignment and interaction.



Tools and Blueprints

Key enabler for the implementation of modern data platforms at a high speed and quality.

Continuous Optimization

Tools and Blueprints are continuously optimized to the customer and project's needs.

Expertise & Light Towers

Expert group for modern data platforms from technical implementation to project management and organization

OCI Security

Hands-On Practice Workshop

- 1 Introduction
- 2 Basic OCI Security
- 3 Cloud Guard
- 4 Data Safe
- 5 Security Zones / WAF
- 6 Summary

Course Schedule

Session Times and Breaks

from	to	Topic	
09:00	09:15	Welcome	Course Overview and Lab Setup Instructions
09:15	10:30	Basic OCI Security	In-Transit Encryption, Shielded Instances, Key Management
10:30	10:45	Coffee Break	
10:45	12:00	Cloud Guard	Overview, Recipes, CIS Scans, Remediation, Alerts, and Events
12:00	13:00	Lunch	
13:00	14:15	Data Safe	Overview, Setup, Auditing, Data Masking, Assessments,...
14:15	14:45	Coffee Break	
14:45	16:00	Security Zones / WAF	Overview, Zone Management, Rulesets, and CIS Compliance
16:00	16:30	Wrap-Up	Additional Resources, Next Steps, and Farewell

Security Service Products

Detection and Remediation



Cloud Guard



Maximum
Security Zone



Security
Advisor



Vulnerability
Scanning

Data Protection



Vault Key
Management



Vault Secrets
Management



Data Safe



Certificates

OS and Workload Protection



Shielded
Instances



Dedicated
Host



Bastion



OS
Management

IAM



IAM



MFA



Federation



Audit

Infrastructure Protection



DDoS
Protection



Web Application
Firewall

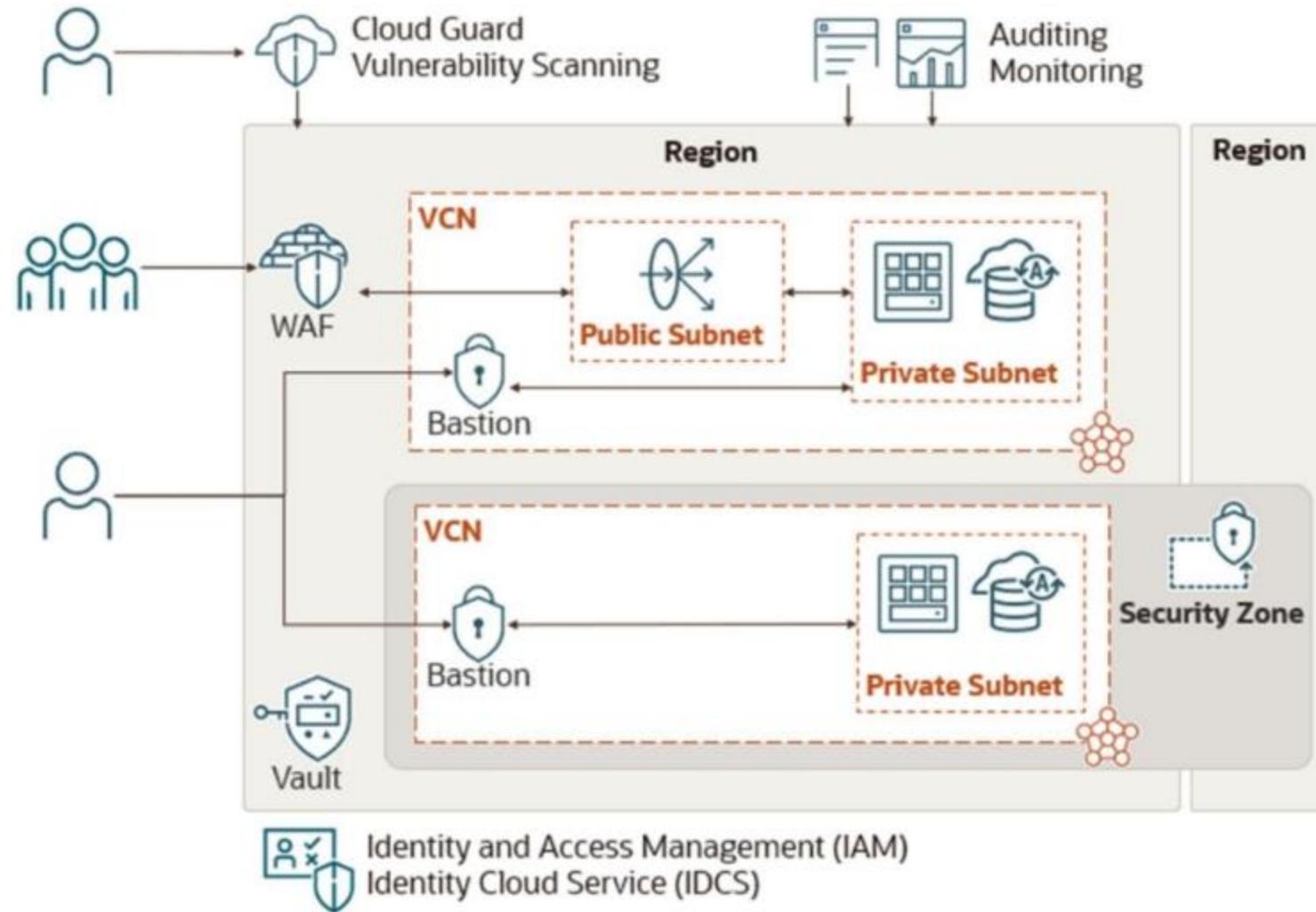


Security
Lists / NSG



Network
Firewall Appliance

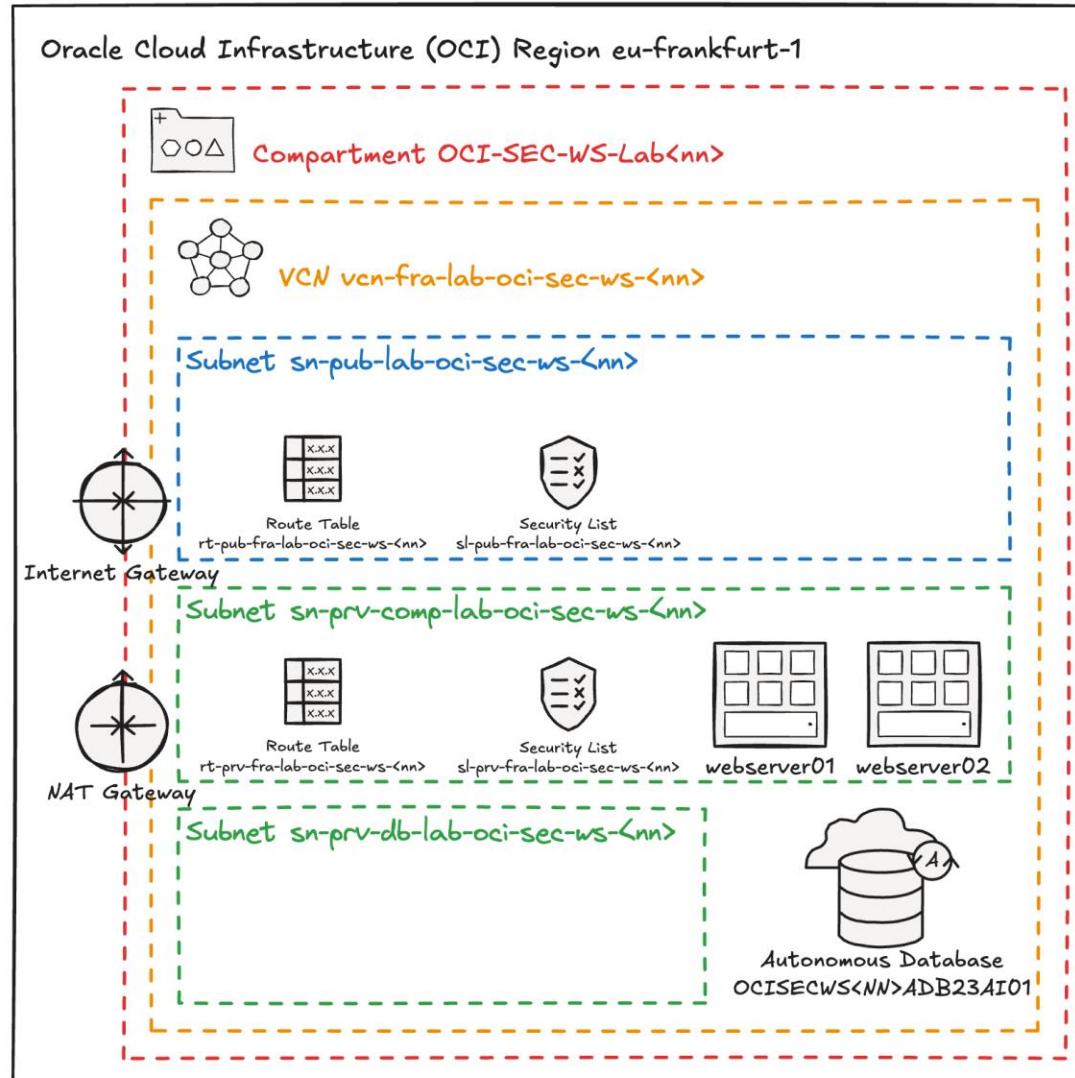
Working Together



Source: oracle.com

OCI Lab Architecture Overview

A High-Level View of the Infrastructure



OCI Access Information

Resources and Cloud Environment Details

The course materials and exercises are available via the GitHub repository/website:

- OCI Walkthrough: <https://code.oradba.ch/oci-sec-ws>
- PDFs and Course Materials: <https://code.oradba.ch/oci-sec-ws/others>

For the workshop, each participant will have access to Oracle Cloud. Accenture is providing an environment with resources for the training day.

- **URL:** <http://cloud.oracle.com>
- **Tenant:** Provided by the instructor
- **User:** *lab-oci-sec-wsNN*
- **Password:** Provided by the instructor
- **Compartment:** *OCI-SEC-WS-LAB-NN*



Oracle Cloud Infrastructure Security

Basics

Martin Berger
Stefan Oehrli

Basics

Security for free.

- 1 Key Management
- 2 OS Management
- 3 Vulnerability Scanning
- 4 Shielded Instances
- 5 Hands-On Labs

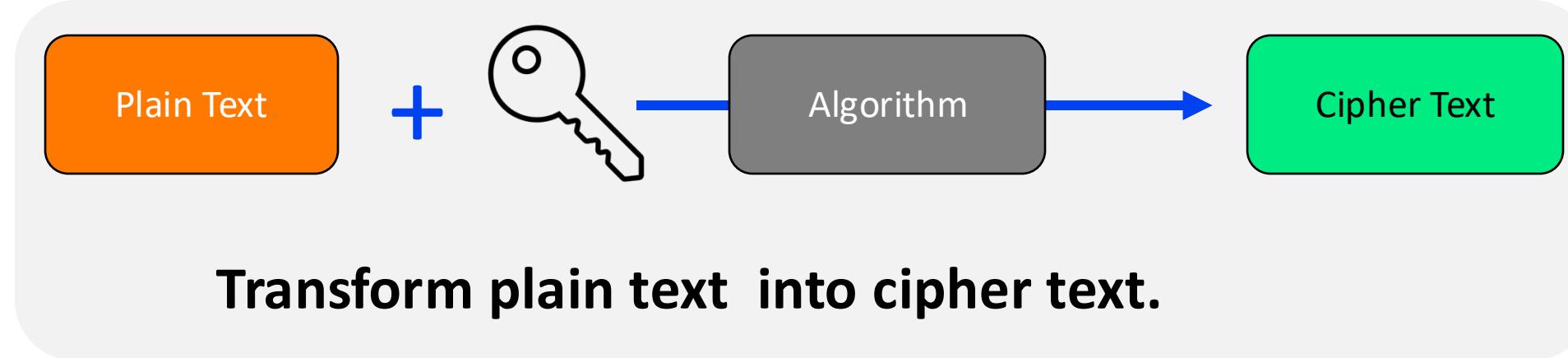
1

Key Management

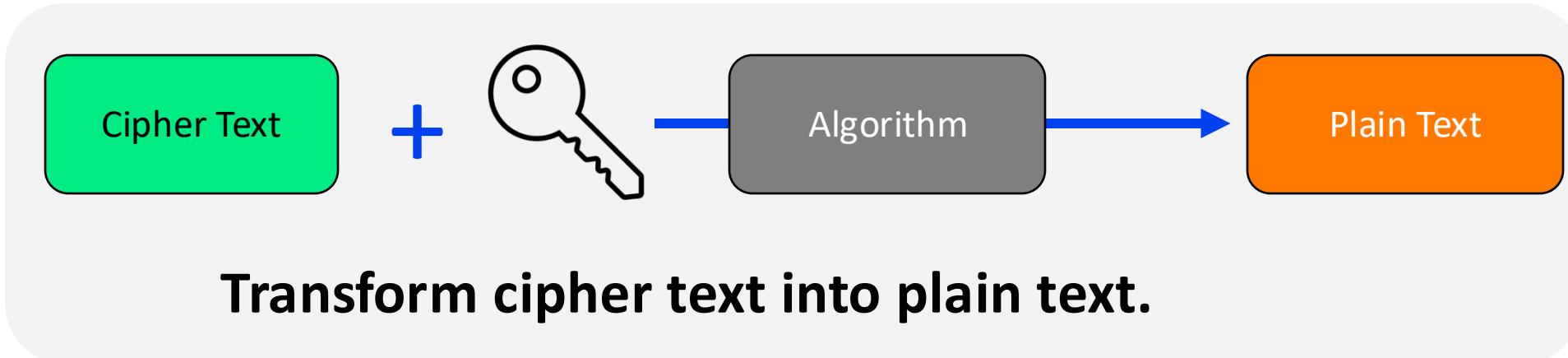
Security for free.

Encryption Basics

ENCRYPTION

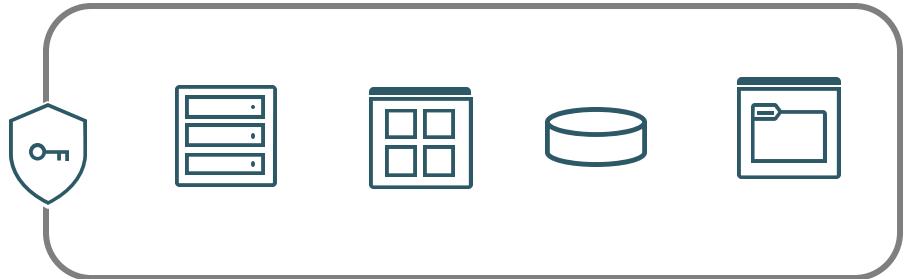


DECRYPTION



Encryption Basics

Encryption at rest



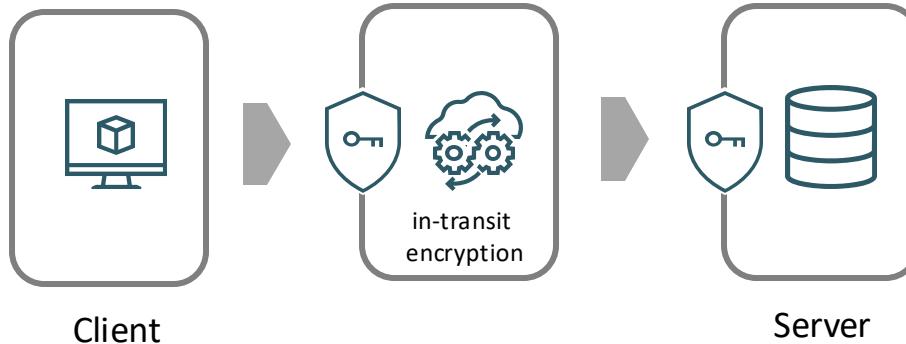
Protect stored, static data

Purpose

Keeps data encrypted until a person or system provides a decryption key to access to the data

How does it work

Encryption in transit



Client

Server

Protect data moving from one location to the other, through a private network.

Encrypts messages before transmission and decrypts upon arrival at the destination

Key Management Service

- The Oracle Cloud Infrastructure (OCI) Key Management Service (KMS) is a cloud-based service that provides **centralized management** and control of encryption keys for data stored in OCI. It simplifies key management by centrally storing and managing encryption keys, protecting data at rest and in transit by supporting various encryption key types, including symmetric and asymmetric keys.
- OCI KMS addresses security and compliance requirements by giving you more control over your encryption keys. You can **bring your own keys** (BYOK) to OCI, **create them within OCI**, or **hold your own keys** (HYOK) externally. Additionally, you can use FIPS 140-2 Level 3-certified hardware security modules (HSMs) to store and protect your encryption keys.

Example Use Case:
Block Volume Encryption



Key and Secret Management Concepts

- **OCI Vault**
 - A customer-managed encryption service that enables you to control the keys that are hosted in Oracle Cloud Infrastructure (OCI) hardware security modules (HSMs) while Oracle administers the Hardware Security Module HSM.
- **OCI Dedicated KMS**
 - A single-tenant HSM partition as a service that provides a fully isolated environment for storing and managing encryption keys. You can control and claim ownership of the HSM partitions and use standard interfaces, such as PKCS#11, to perform cryptographic operations.
- **OCI External KMS**
 - Enables you to use your own third-party key management system to protect data in OCI services. You control the keys and HSMs outside OCI, and you're responsible for the administration and manageability of those HSMs.

HSM: The OCI Vault Hardware Security Module (HSM) provides secure key management and cryptographic operations by using dedicated hardware devices to protect sensitive data and encryption keys.

Vault

- A managed service in Oracle Cloud Infrastructure that provides secure key management
- There are two different types available: **Virtual private vault** and **Vault in a shared Partition**.
- **Virtual private vault:**
 - creates the vault as a dedicated partition on the HSM
 - pricing based on the maximum usage against key limits
 - isolated cryptographic resources and enhanced security controls
 - greater performance
- **Vault in a shared partition:**
 - free for use
 - cryptographic resources are shared among multiple tenants

Create Vault

Vaults provide your growing data an
to thousands of keys to support you

Create in Compartment

comp-oci-bootcamp-33

acnaobg (root)/OCI-Bootcamp-2024/comp-oci

Name

comp33-private-vault

Make it a virtual private vault

Master Encryption Key

- The **Master Encryption Key** in OCI Vault is the primary key used to encrypt and protect other keys and secrets, ensuring their secure management and storage within Oracle Cloud Infrastructure.

Protection Mode i

Software

Name

mek-vault-comp-33

Key Shape: Algorithm i

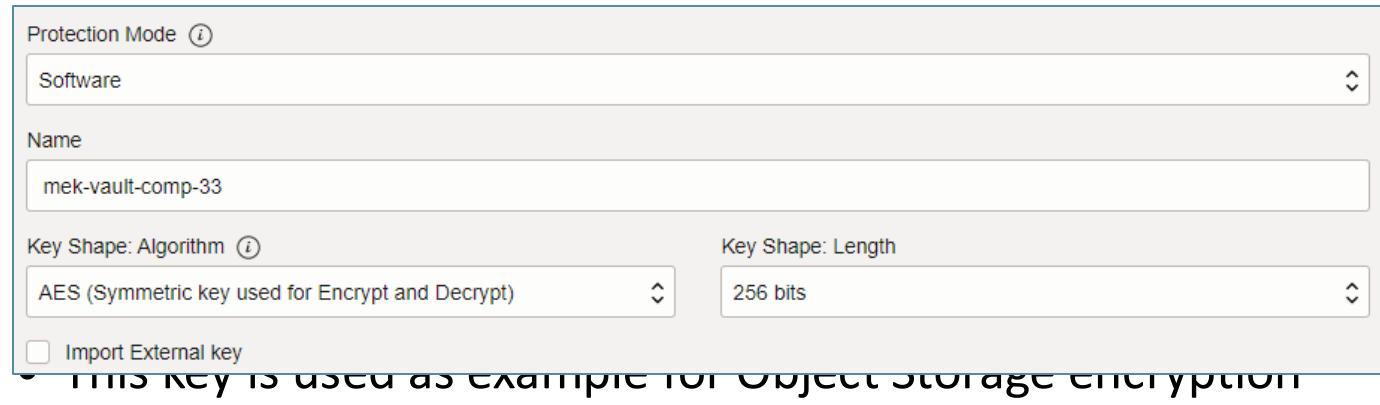
AES (Symmetric key used for Encrypt and Decrypt)

Key Shape: Length

256 bits

Import External key

THIS KEY IS USED AS EXAMPLE FOR OBJECT STORAGE ENCRYPTION



You can choose between **Software** and **HSM** protection mode, with different costs.

Encrypt using customer-managed keys
Requires a valid key from a vault that you have access to. [Learn more](#)

Vault in **comp-oci-bootcamp-33** [\(Change compartment\)](#)

vault-comp-33

Master Encryption Key in **comp-oci-bootcamp-33** [\(Change compartment\)](#)

mek-vault-comp-33



CIS – Center of Internet Security OCI Benchmark

5.2.1 Ensure Block Volumes are encrypted with Customer Managed Keys (CMK). (Automated)

Description:

Oracle Cloud Infrastructure Block Volume service lets you dynamically provision and manage block storage volumes. By default, the Oracle service manages the keys that encrypt block volumes. Block Volumes can also be encrypted using a customer managed key.

Terminated Block Volumes cannot be recovered and any data on a terminated volume is permanently lost. However, Block Volumes can exist in a terminated state within the OCI Portal and CLI for some time after deleting. As such, any Block Volumes in this state should not be considered when assessing this policy.

Rationale:

Encryption of block volumes provides an additional level of security for your data. Management of encryption keys is critical to protecting and accessing protected data. Customers should identify block volumes encrypted with Oracle service managed keys in order to determine if they want to manage the keys for certain volumes and then apply their own key lifecycle management to the selected block volumes.

Impact:

Encrypting with a Customer Managed Key requires a Vault and a Customer Master Key. In addition, you must authorize the Block Volume service to use the keys you create.
Required IAM Policy:

```
Allow service blockstorage to use keys in compartment <compartment-id> where  
target.key.id = '<key_ocid>'
```

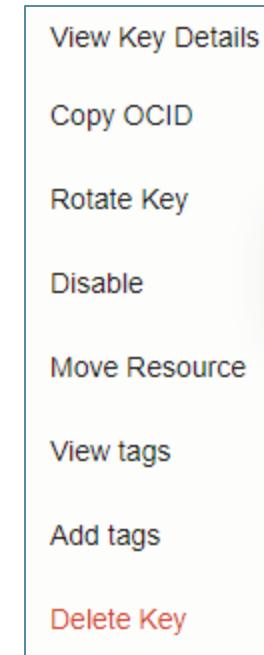
Can I rotate my keys?

Yes. You can regularly rotate your keys in alignment with your security governance and regulatory compliance needs or do it ad hoc in case of a security incident.

Regularly rotating your keys (for example, every 90 days) by using the console, API, or CLI, limits the amount of data protected by a single key.

Note: Rotating a key does not automatically re-encrypt data that was previously encrypted with the old key version; this data is re-encrypted the next time it's modified by the customer.

If you suspect that a key has been compromised, you should re-encrypt all data protected by that key and disable the prior key version.



Backup and Replicate Vault and Keys

Backup:

- Backing up a private vault ensures that cryptographic keys and sensitive data can be restored in case of accidental deletion, corruption, or system failure.
- Regular backups help meet regulatory requirements for data protection and enable thorough audits of key management practices.
- Maintaining backups supports uninterrupted operations by allowing quick recovery of essential cryptographic resources, minimizing downtime in the event of an incident.

Replication:

- Replicate virtual private vaults across regions to meet compliance requirements or improve latency.
- Cross-region replication automatically syncs creation, deletion, updates, or moves of keys and key versions between source and destination vaults.
- The originating vault is called the source vault, and the receiving vault in the destination region is known as the vault replica.



Minimum Level: Private Vault

Secrets

- OCI Vault Secrets provides a secure location to store sensitive information such as passwords, API keys, and confidential data.
- It ensures that secrets are accessible only to authorized applications and users through fine-grained access policies.
- It facilitates automated secret management, including versioning and rotation, to enhance security and compliance.
- Example: Store the database credentials as a secret in OCI Vault. The application can securely retrieve these credentials at runtime, ensuring that sensitive information is not exposed in the codebase or configuration files.

```
curl -s -X GET \
-H "Authorization: Bearer <your_auth_token>" \
-H "Content-Type: application/json" \
"https://<region>.secrets.vaults.<domain>/20190301/secretBundles/<secret_ocid>" | jq -r
'.secret-bundle-content.content' | base64 --decode
```

Secret Creation

- Based on Master Encryption Key
- Different secret types like passphrase, SSH key etc.
- Auto-generation or manual input

Secrets *in* comp-oci-bootcamp-33 Compartment

Create Secret

Name	Status	Created	Auto generation
secret-database-oci-bootcamp	Active	Wed, May 29, 2024, 18:38:28 UTC	On

Secret rules govern the use and management of secrets. For more information about secret rules,

Rule Type Configuration

Secret Expiry Rule Version expiry interval: days

Block content retrieval on expiry Aug 31, 2024 12:00 AM

View Secret Contents

Show decoded Base64 digit

Secret Read-only

```
bTzKNiljZ1MpOFFTRXU=
```

Deleting a Vault

- When you delete a vault, the vault and all its associated keys go into a pending deletion state until the waiting period expires.
- By default, the waiting period is set to 30 days, but it can be adjusted from a minimum of 7 days to a maximum of 30 days.
- When a vault is deleted, all its associated keys are also deleted.
- If replication is configured, deleting a vault in the source region also deletes the vault and any keys in the vault in the destination region.



Vault and the keys contained within are scheduled for deletion on Wed, Oct 30, 2024, 17:30:00 UTC. Anything encrypted by the keys contained within this vault will be unusable or irretrievable immediately, and is permanently unusable or irretrievable after the key has been deleted.

Dismiss

2

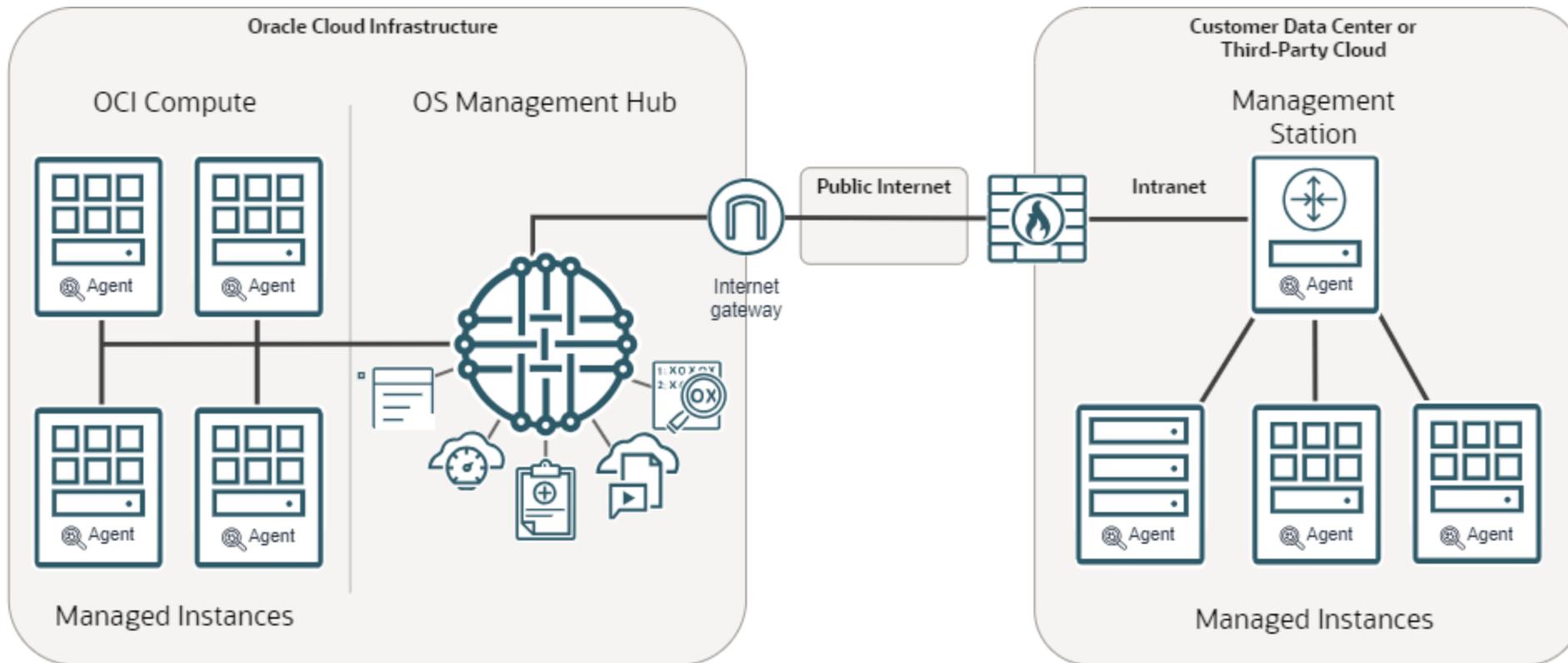
OS Management

Security for free.

OS Management Hub

- Next generation of OS management functionality
- OS Management Hub uses an agent plugin for managing and applying updates.
- Simplified OS Management:
 - Oracle OS Management Hub streamlines the management and monitoring of OS updates across on-premises, OCI, and supported third-party clouds.
- Inclusive Service:
 - OS Management Hub is included with Oracle Linux Support and OCI Compute subscriptions, providing comprehensive OS management at no additional cost.
- Auto-Patch capable:
 - Keep your OS up to date

OS Management Hub Architecture



Source: oracle.com

OS Management Workflow 1/2

1. Adding Vendor Software Sources (create in root compartment first for later usage)
2. Create custom Software Source on compartment level
3. Create Service Profile
4. Verify OS Management Hub plugin is running on target instances

Associated resources

Name	Description
ol8_addons-x86_64	Oracle Linux 8 Addons (x86_64)
ol8_appstream-x86_64	Oracle Linux 8 Application Stream (x86_64)
ol8_appstream_developer-x86_64	Oracle Linux 8 Application Stream Developer(x86_64)

! A policy error was detected

Before using OS Management Hub, you need to enable the service in your compartment.

OS Management Hub Agent i ● Stopped -

OS Management Workflow 2/2

5. Wait 10 mins..
6. (optional) create group with custom software source, attach instances

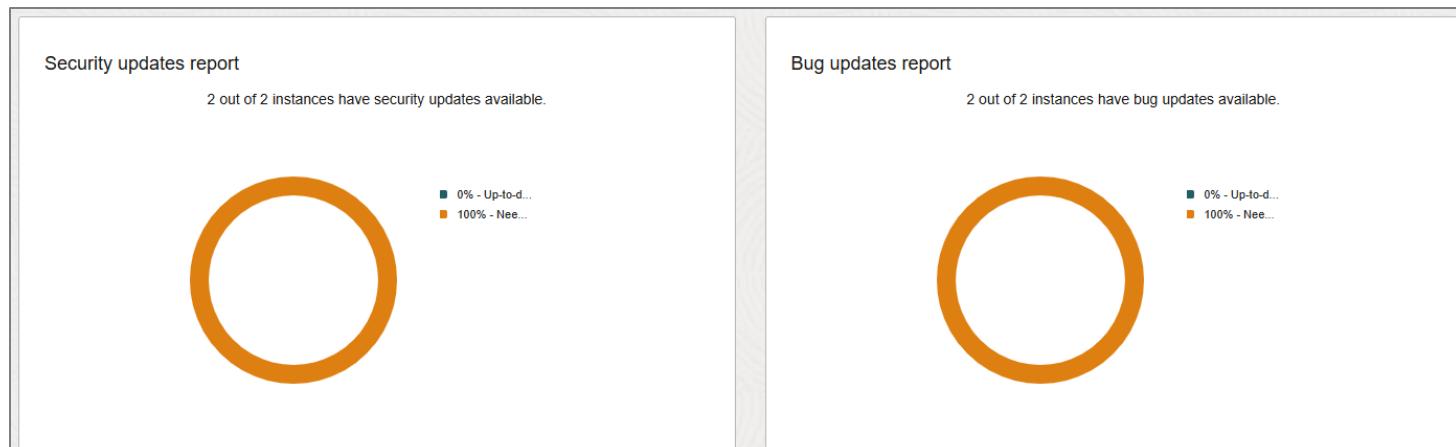
Groups *in* comp-doag-high-sec *compartment*

Create groups to unify and standardize content across the instances within the group.

<input type="checkbox"/>	Name	Description	Location	Instances	OS version	Architecture
<input type="checkbox"/>	high-sec-app-srv		Oracle Cloud Infrastructure	2	Oracle Linux 8	x86_64

0 selected Showing 1 item

7. Verify Dashboard and Reports



Verify OS Management & Categories

- On target hosts, any DNF/YUM command shows the enabled service

```
[opc@compute-high-sec-public ~]$ sudo dnf update
This system is receiving updates from OSMH.
Last metadata expiration check: 0:01:54 ago on Thu 17 Oct 2024 07:25:37 AM GMT.
Dependencies resolved.
```

OS Management Hub Category	Description
Security	An update that addresses security vulnerabilities found during development, testing, or reported by users. Security fixes usually have one or more associated CVE (Common Vulnerabilities and Exposure) names to identify the vulnerabilities.
Ksplice	An update used by Ksplice for installing zero-downtime security patches. The update job can include only Ksplice kernel updates, only Ksplice userspace updates, or both. See Using Ksplice for Oracle Linux for how to configure an instance to receive Ksplice updates.
Bug Fix	An update that fixes issues reported by users or discovered during development or testing.
Enhancement	An update that introduces new features, improved functionality, or enhanced performance in the package's software.
Other	An update that's not associated with any errata.

Reports

- You can apply the patches, fixes automatically or manually

Security updates report

<input type="button" value="Apply update"/> <input type="button" value="Download report"/> <input type="text" value="Search by instance"/>							
<input type="checkbox"/>	Instance	Up-to-date	Advisories/Updates <small>(i)</small>	Group	Lifecycle environment	OS version	Location
<input type="checkbox"/>	compute-high-sec-private-a	● No	6	high-sec-app-srv	-	Oracle Linux 8	Oracle Cloud Infrastructure <small>▼</small>
<input checked="" type="checkbox"/>	compute-high-sec-public	● No	6	high-sec-app-srv	-	Oracle Linux 8	Oracle Cloud Infrastructure <small>▼</small>
1 selected						Showing 2 items	< Page 1 >

Bug updates report

<input type="button" value="Apply update"/> <input type="button" value="Download report"/> <input type="text" value="Search by instance"/>							
<input type="checkbox"/>	Instance	Up-to-date	Advisories/Updates <small>(i)</small>	Group	Lifecycle environment	OS version	Location
<input type="checkbox"/>	compute-high-sec-private-a	● No	23	high-sec-app-srv	-	Oracle Linux 8	Oracle Cloud Infrastructure <small>▼</small>
<input type="checkbox"/>	compute-high-sec-public	● No	23	high-sec-app-srv	-	Oracle Linux 8	Oracle Cloud Infrastructure <small>▼</small>
0 selected						Showing 2 items	< Page 1 >

Update Schedule

- If you want to apply the patches and fixes automated and recurring, a job is required.
 - Can run once
 - Or scheduled, as example every Monday

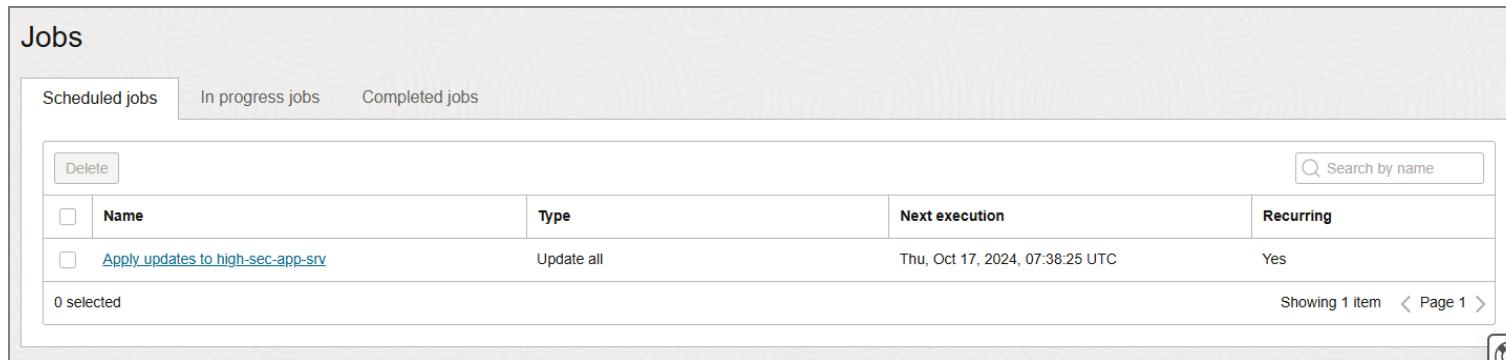
Jobs

Scheduled jobs In progress jobs Completed jobs

<input type="checkbox"/>	Name	Type	Next execution	Recurring
<input type="checkbox"/>	Apply updates to high-sec-app-srv	Update all	Thu, Oct 17, 2024, 07:38:25 UTC	Yes

0 selected

Showing 1 item < Page 1 >



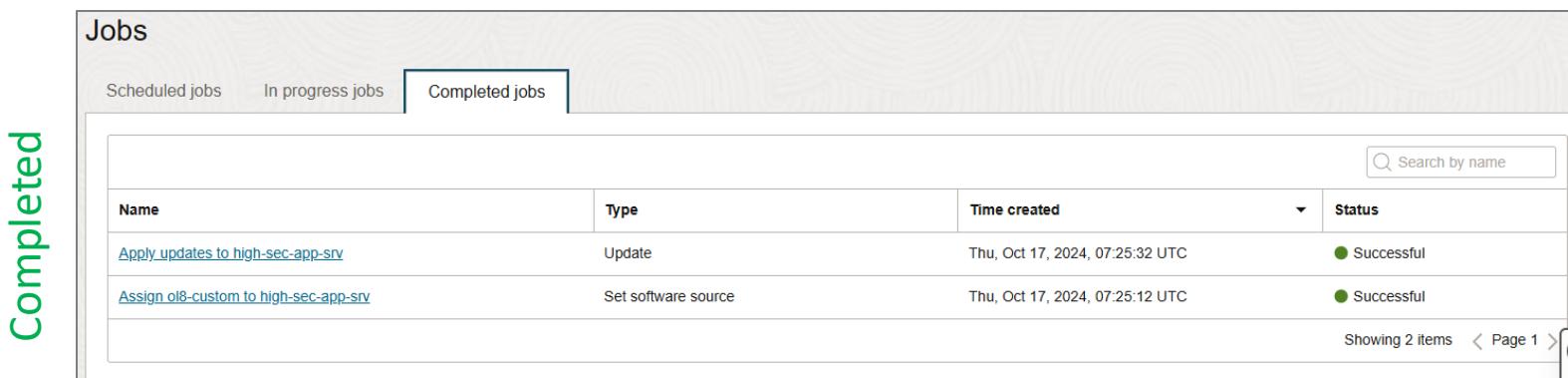
Scheduled

Jobs

Scheduled jobs In progress jobs **Completed jobs**

Name	Type	Time created	Status
Apply_updates_to_high-sec-app-srv	Update	Thu, Oct 17, 2024, 07:25:32 UTC	● Successful
Assign_ol8-custom_to_high-sec-app-srv	Set software source	Thu, Oct 17, 2024, 07:25:12 UTC	● Successful

Showing 2 items < Page 1 >



Completed

Create update job

2 instances will be updated.

Job name

Apply updates to 2 instances

Description Optional

Update all issues

Updates to apply ⓘ

All

Security

Ksplice kernel

Ksplice userspace

Bug fix

Enhancement

Other

Schedule

Run immediately Schedule

Date and time

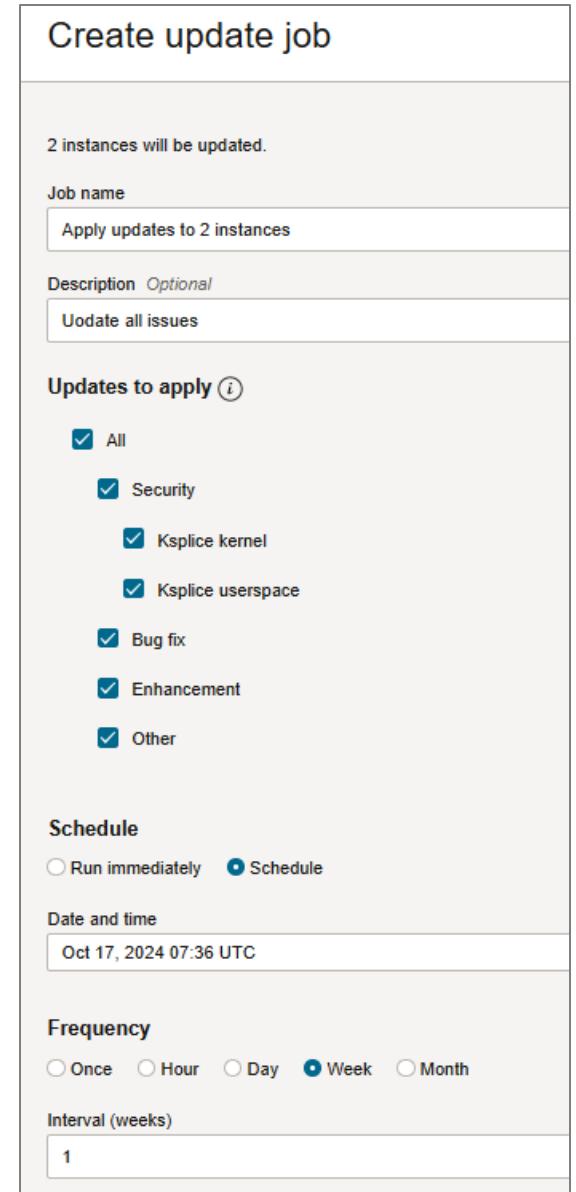
Oct 17, 2024 07:36 UTC

Frequency

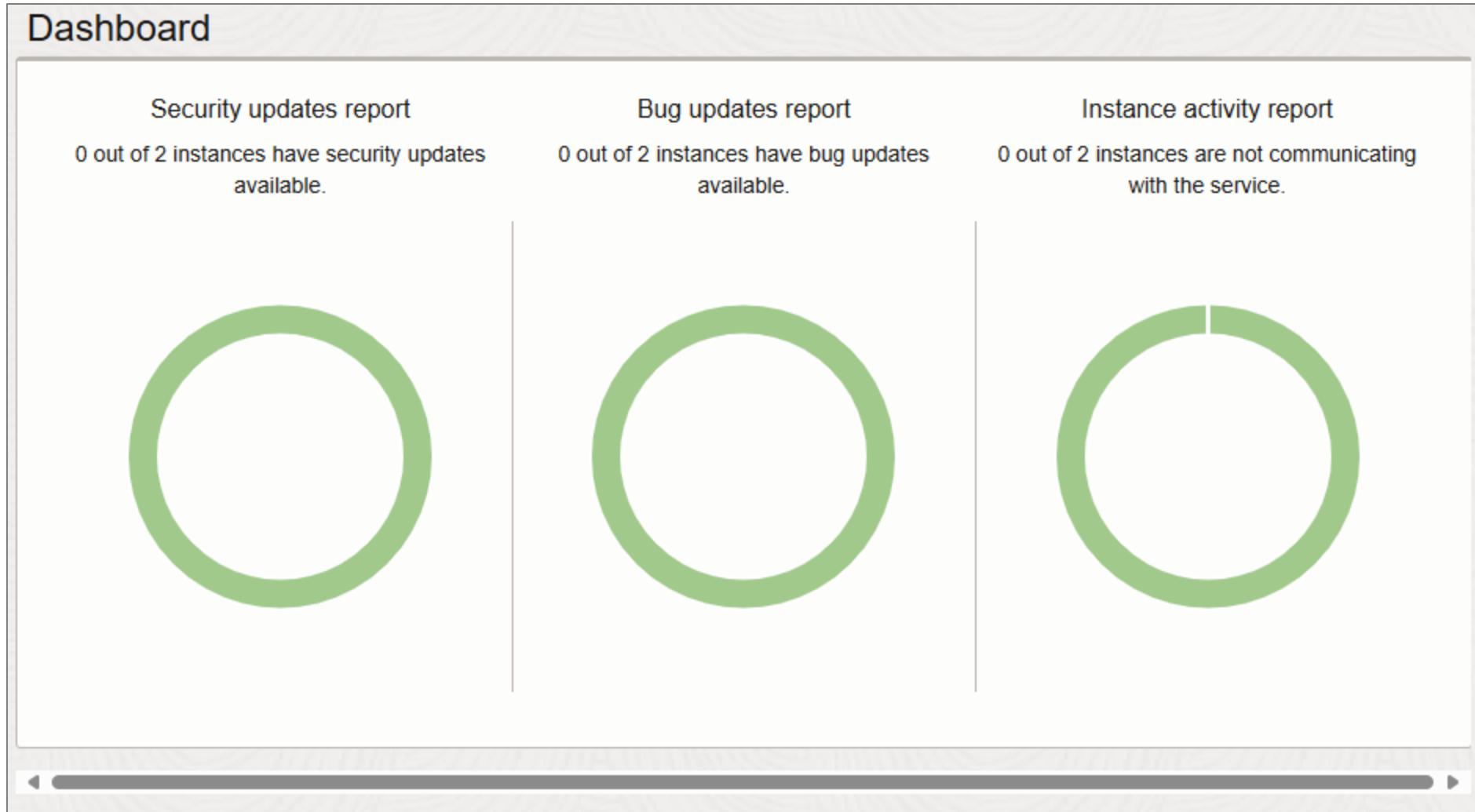
Once Hour Day Week Month

Interval (weeks)

1



Finally

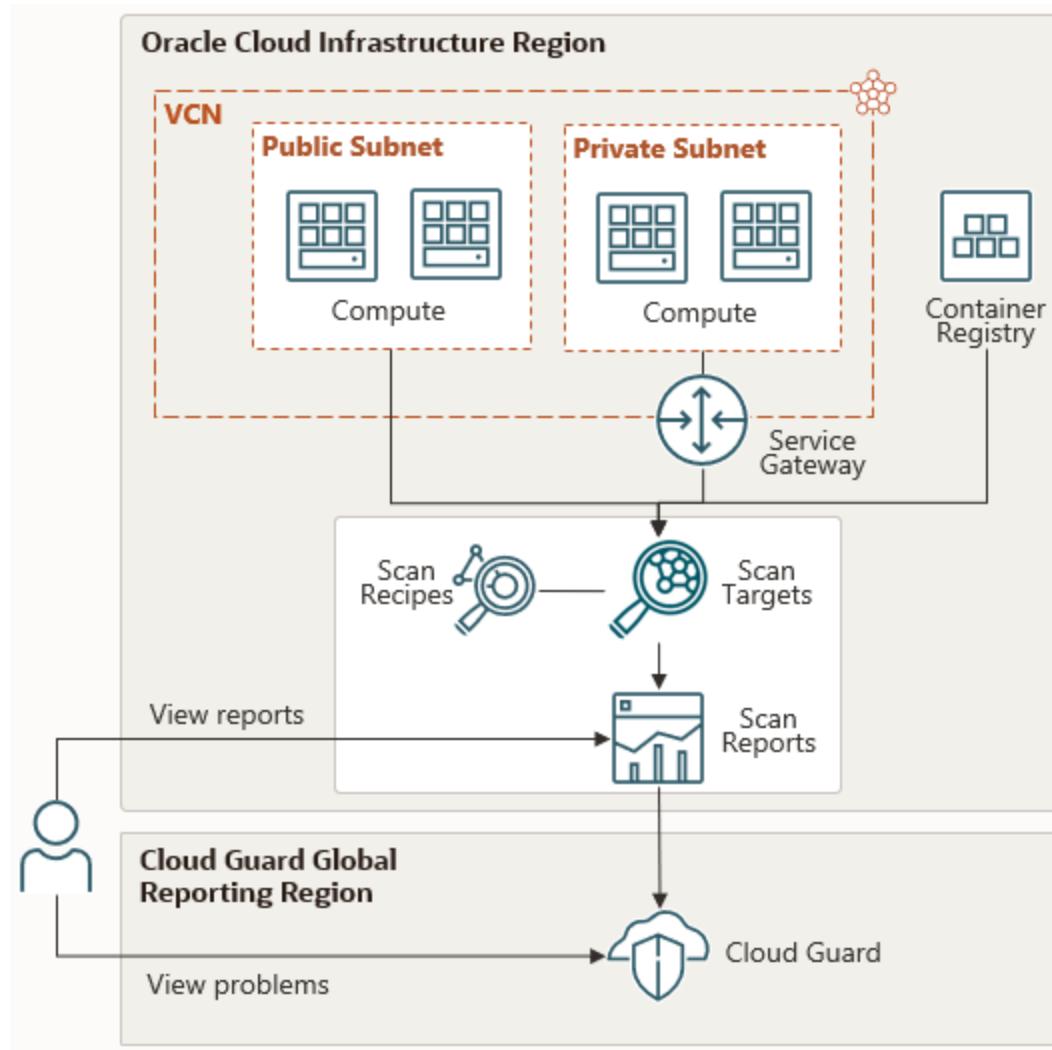


3

Vulnerability Scanning

Security for free.

Vulnerability Scanning Service



Source: oracle.com

Reports

Scanning

Vulnerability Reports

Scanning reports

Hosts

Ports

Container images

Targets

Hosts

Container images

Scan Recipes

Hosts

Container images

List scope

Compartment

comp-doag-high-sec

trivadisbdsxp (root)/Projects_Internal/comp-doag-high-sec

Filters

Risk level

All

Qualys BYOL option now available. See the agent option in host [scan recipe](#)

Export CSV

Search by issue title

CVE ID	Risk level	CVE description	Last detected	First detected	Resources impacted
CVE-2024-45491	Critical	...SIZE_MAX). Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-45490	Critical	...rseBuffer. Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-45492	Critical	...SIZE_MAX). Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-41071	High	...?id=218810 Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-42225	High	...lized data Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-42159	High	...e allowed. Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	2
CVE-2022-48866	High	...nted number Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2023-6040	High	...ds access. Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-42228	High	...Christian) Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1
CVE-2024-39471	High	...n -EINVAL. Show Copy	Thu, Oct 17, 2024, 07:09:59 UTC	Thu, Oct 17, 2024, 07:08:13 UTC	1

Showing 10 items < Page 1 >

Vulnerability Sources

- The Vulnerability Scanning service detects vulnerabilities in the following platforms and using the following vulnerability sources.

Platform	National Vulnerability Database (NVD)	Open Vulnerability and Assessment Language (OVAL)	Center for Internet Security (CIS)
Oracle Linux	Yes	Yes	Yes
CentOS	Yes	Yes	Yes
Ubuntu	Yes	Yes	Yes
Windows	Yes	No	No

- Targets: Compute Instances and images with a Container Registry repository

Vulnerability Scanning

- Free or BYOL by Qualys

Agent to use	
OCI	
Oracle Cloud infrastructure - Free agent	✓
Qualys	
	Premier offering Agents and Dashboard Price - BYOL

- Based on targets according Cloud Guard
- Pre-defined or adapted recipes
- Cloud Guard integration

Export CSV			
Name	Risk level	Issues found	Operating system
ci-useast-test-grafana-001	● High	8	Oracle Linux Server_8.9

Recipes

- A CIS benchmark profile and OS folders can be selected
- Linux and Windows

Scan Recipes *in comp-doag-high-sec Compartiment*

Create a recipe to control how resources are scanned. After creating a recipe, assign it to targets. [Learn more](#)



Qualys BYOL option now available. See the agent option in host [scan recipe](#)

Create

Name	Status	Created	⋮
vss-recipe-high-sec	● Active	Thu, Oct 17, 2024, 06:47:30 UTC	⋮

Showing 1 item < Page 1 >

Targets

- Select all or defined Compute Instances only

Targets *i*

All compute instances in the selected target compartment and its subcompartments
 Selected compute instances in the selected target compartment

[Show advanced options](#)

Targets *in* comp-doag-high-sec Compartment

Create a target to enable scanning for resources in a compartment.

(i) Qualys BYOL option now available. See the agent documentation.

Compute instances

(i) All instances in the compartment comp-doag-high-sec and its subcompartments are scanned

Name	State	Target compartment	Scan recipe	Created	⋮
vss-tgt-recipe-high-sec	● Active	comp-doag-high-sec	vss-recipe-high-sec	Thu, Oct 17, 2024, 06:49:20 UTC	⋮

Showing 1 item < Page 1 >

4

Shielded Instances

Security for free.

A combination of Secure Boot, Measured Boot, and the Trusted Platform Module

Functions:

- Enhanced Security: Oracle Shielded Instances provide an additional layer of security by protecting against unauthorized access and tampering.
- Secure Boot: Ensures that only trusted software is loaded during the boot process, preventing malicious code from running.
- Trusted Platform Module (TPM): Utilizes TPM to securely store cryptographic keys and other sensitive data, enhancing overall security.

Benefits:

- Protection Against Ransomware: Shielded Instances help protect against ransomware attacks by preventing unauthorized changes to system configurations and data.
- Compliance and Regulatory Standards: Meet compliance requirements and regulatory standards with enhanced security features provided by Shielded Instances.
- Integration with OCI Services: Seamlessly integrate with other OCI services such as monitoring, notifications, and identity management for comprehensive security management.

Components

Shielded Instances

Harden the firmware security on bare metal hosts and virtual machines (VMs) to defend against malicious boot level software.

Secure Boot

Unified Extensible Firmware Interface (UEFI) feature that prevents unauthorized boot loaders and operating systems from booting.

Measured Boot

Measured Boot enhances boot security by taking and storing measurements of boot components, such as bootloaders, drivers, and operating systems. Bare metal instances do not support Measured Boot.

Trusted Platform Module

The Trusted Platform Module (TPM) is used to securely store boot measurements.

Security

[Collapse](#)



Uncompromised Boot Security

- No live migration or reboot migration support.
- If you enable the hardware TPM on a bare metal instance, the instance cannot be migrated, because the hardware TPM is not migratable.
- Custom images are not supported.
- Confidential computing is not supported.



The current instance settings prevent you from enabling confidential computing.

You can enable either shielded instances or confidential computing but not both, simultaneously.

To enable confidential computing, you must update the instance settings to compatible values. [Learn more](#)

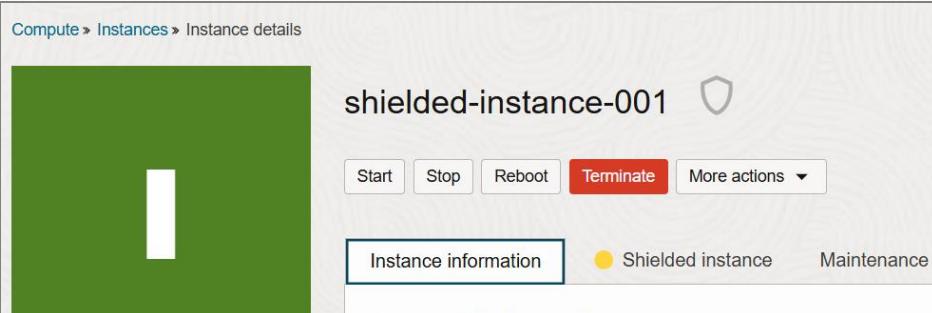
[View incompatibilities](#)

General information

Maintenance reboot: -

Live migration: Disabled [View incompatibilities](#) [Change](#)

Platform Configuration Register



The screenshot shows the 'Compute > Instances > Instance details' section for a shielded instance. The instance name is 'shielded-instance-001'. It includes standard actions like Start, Stop, Reboot, Terminate, and More actions. Below these are tabs for Instance information, Shielded instance (which is selected), and Maintenance.

Reset golden measurements

Do you want to reset the golden measurements? The current baseline values will be replaced with new values.

[Reset](#) [Cancel](#)

Platform Configuration Register (PCR)

Reset golden measurements			Copy PCR values
Index	Hash algorithm	Value	Status
PCR0	sha1	9ec8a29fb32ff0aff53771ad5c9d7c1cb02474e	✓
PCR0	sha256	21a59414a7ecc85bf0932c9eb4b51c5b73721605c36934d03f8d53c281e781f	✓
PCR0	sha384	af176b0ab08ba51218ee9653222041d3ebc2ab58bbaa955566fb6e608ce2222918b4c6aa2ecec09ef00b22fb84b997ea	✓

A PCR is an internal memory slot within a Trusted Platform Module (TPM) that attests to the current system configuration or any alterations thereof. PCRs are used to store measurements of software and hardware states, which can then be used to verify the integrity of the system. This ensures that the system has not been tampered with and is running trusted software.

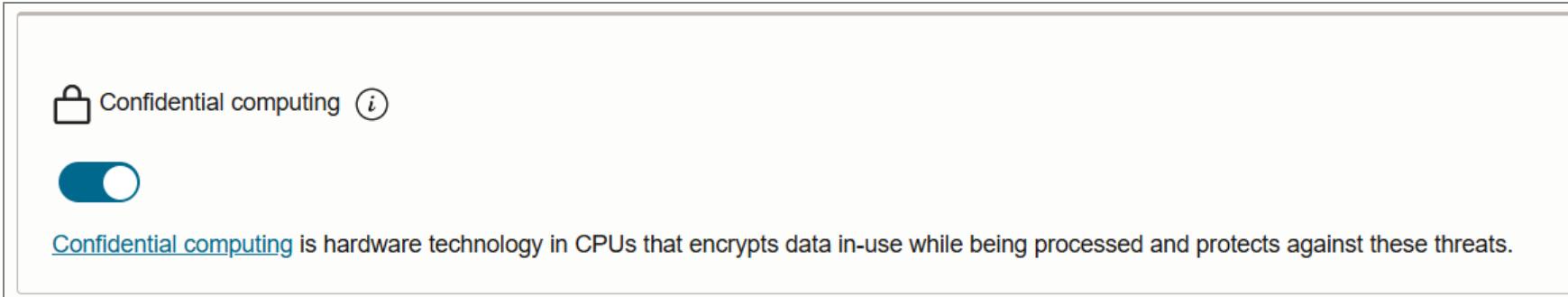
Confidential Computing - AMD EPYC™ Processors

- **Real-time Encryption:** OCI Confidential Computing provides real-time CPU encryption, ensuring that data is encrypted while it is being processed. This helps protect sensitive information from unauthorized access¹.
- **Secure Key Management:** The encryption keys used in OCI Confidential Computing reside only in the AMD Secure Processor, making them inaccessible to any user, including administrators¹.
- **Enhanced Data Privacy:** By encrypting data in use, OCI Confidential Computing enhances data privacy and security, making it suitable for workloads that require high levels of confidentiality

Virtual Machine Compute Shapes (on Oracle Linux 7.x or 8.x platform images)	Bare Metal Instance Compute Shapes (on any platform image)
VM.Standard.E4.Flex	BM.DenseIO.E4.128
VM.Standard.E3.Flex	BM.Standard.E4.128
	BM.Standard.E3.128

Create Instance

- Create instance, enable confidential computing without additional costs.



- Select shape – watch for shield icon



Instance with confidential computing enabled can be live migrated. No code change and a minimal performance impact.

Launch options

NIC attachment type: PARAVIRTUALIZED

Remote data volume: PARAVIRTUALIZED

Firmware: UEFI_64

Boot volume type: PARAVIRTUALIZED

In-transit encryption: Disabled

Secure Boot: Disabled

Measured Boot: Disabled

Trusted Platform Module: Disabled

Confidential computing: Enabled

5

Hands-On Labs

What about the
Database Security?

Hands-On Labs

List of Hands-On Labs

- **Key Management** – Create and manage encryption keys within a customer-managed key vault.

Oracle Cloud Infrastructure Security

Cloud Guard

Martin Berger
Stefan Oehrli

Cloud Guard

Security for free.

- 1** Understanding Cloud Guard
- 2** Hands-On Labs

1

Understanding Cloud Guard

Security for free.

What is Cloud Guard?

Oracle Cloud Guard is a cloud-native service designed to help customers monitor, identify, and maintain a strong security posture on Oracle Cloud Infrastructure. It continuously examines OCI resources for security weaknesses related to configuration and user activities

Real-Time Threat Detection

Cloud Guard provides real-time monitoring and threat detection by continuously scanning OCI resources for misconfigurations, vulnerabilities, and anomalous activities. This ensures that potential security issues are identified and addressed promptly

Automated Risk Assessment

Cloud Guard automatically assesses security risks based on predefined security policies and industry standards, such as the CIS Benchmark. It offers actionable recommendations for addressing detected risks, allowing for quick remediation and enhancing overall security

Customizable Security Policies

Users can configure custom policies and rules to align monitoring with their specific security requirements. Cloud Guard integrates seamlessly with other OCI tools, providing a comprehensive and flexible security solution.

Overview

Security score rating ⓘ

Excellent

Security score 83

Risk score ⓘ

1396

Security recommendations ⓘ

- Resolve **VCN Security list allows traffic to restricted port** problems i...
- Resolve **VCN Security list allows traffic to restricted port** problems i...

[View recommendations](#)

The Concept

- **Detector Rules** provide a class of resources with specific actions or configurations that can cause a detector to report a problem.
- **Detector Recipes** provide the baselines for examining the resources and activities in the target.

Detector rules

<input type="checkbox"/>	Detector rule	Risk level	Status	Settings configured
<input type="checkbox"/>	Write Log access disabled for bucket	Low	Disabled	Not allowed
<input type="checkbox"/>	VNIC without associated network security group	Minor	Enabled	Not allowed
<input type="checkbox"/>	VCN has no inbound Security List	Medium	Disabled	Not allowed
<input type="checkbox"/>	VCN has Local Peering Gateway attached	Low	Enabled	Not allowed
<input type="checkbox"/>	VCN has no IP ACL applied	Low	Enabled	Not allowed

Input setting

Restricted Protocol: Ports List

TCP:[11,17-19,21,23-25,43,49,53,70-74,79-81,88,111,123,389,636,445,500,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888], UDP:[11,17-19,49,69,80,82,83-85,

Key Components of Cloud Guard



Targets

Targets define the scope of what Cloud Guard is to check. This scope is tied to the compartment where the target is defined and all the child compartments from that point until another target is encountered. Compute Instances, Object Storage etc.



Detectors

Detectors perform checks and identify potential security problems based on their type and configuration.



Responder Recipes

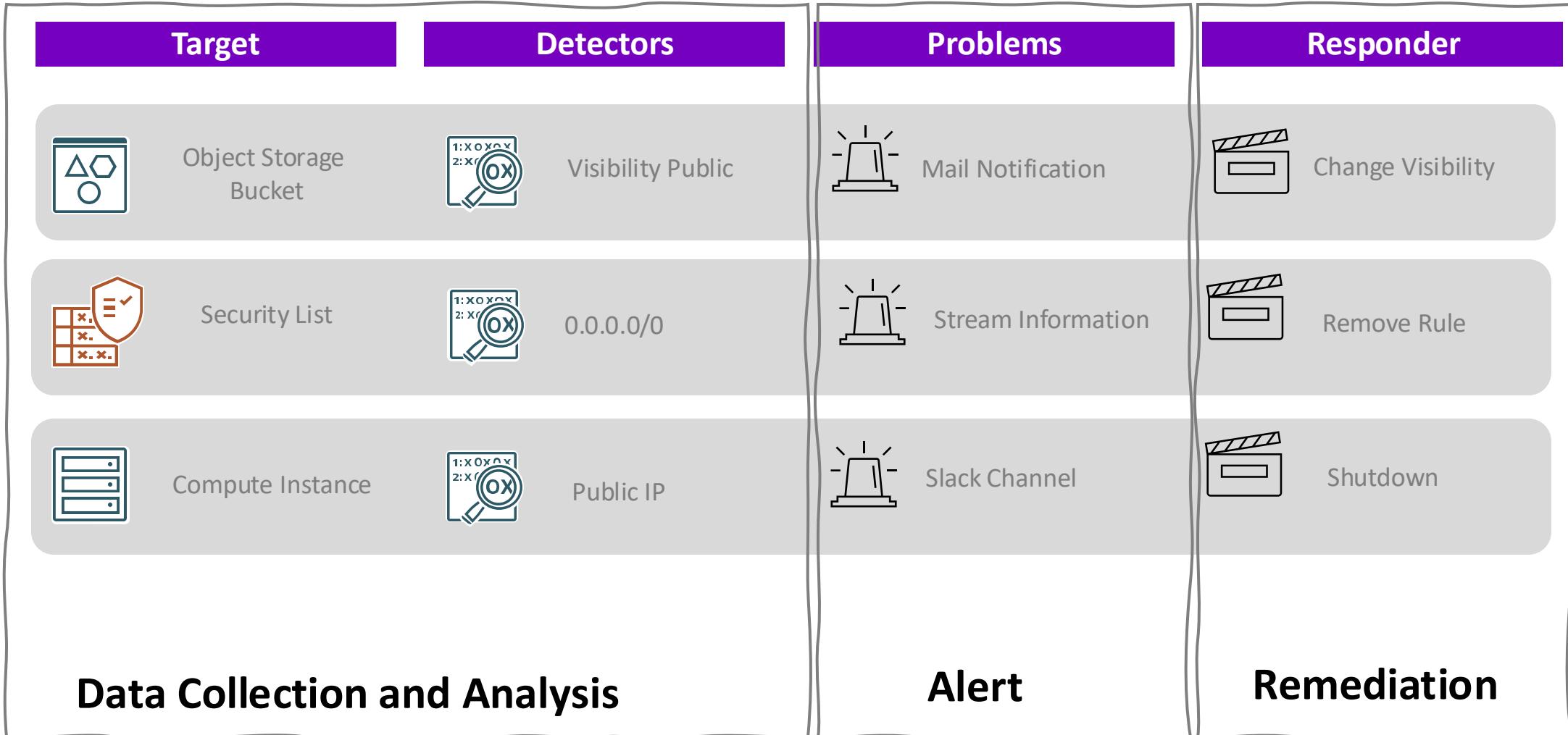
These provide the baselines for examining the resources and activities in the target. Oracle-managed detector recipes allow setting only the scope of resources for which a rule triggers a problem, while user-managed detector recipes allow more customization.



Detector Recipes

Responder recipes define the actions to be taken when a problem is detected. They can be configured to automatically remediate security issues or to notify administrators for manual intervention.

How Cloud Guard works



Enable Cloud Guard

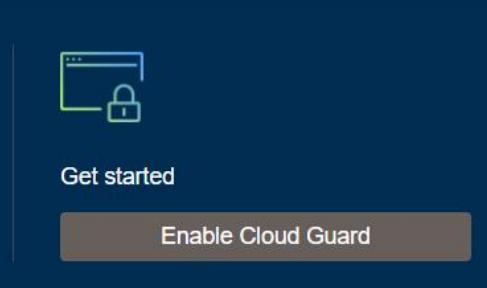
The prerequisites for enabling Oracle Cloud Guard:

- Having a paid Oracle Cloud Infrastructure tenancy, as Cloud Guard is not available for free tenancies.
- Users must create a user group with administrator privileges to work with Cloud Guard, and this group should be restricted to a limited audience.
- Additionally, specific policy statements must be added to enable the Cloud Guard users group to manage Cloud Guard resources.

Cloud Guard

Automatically identify and remediate security problems.

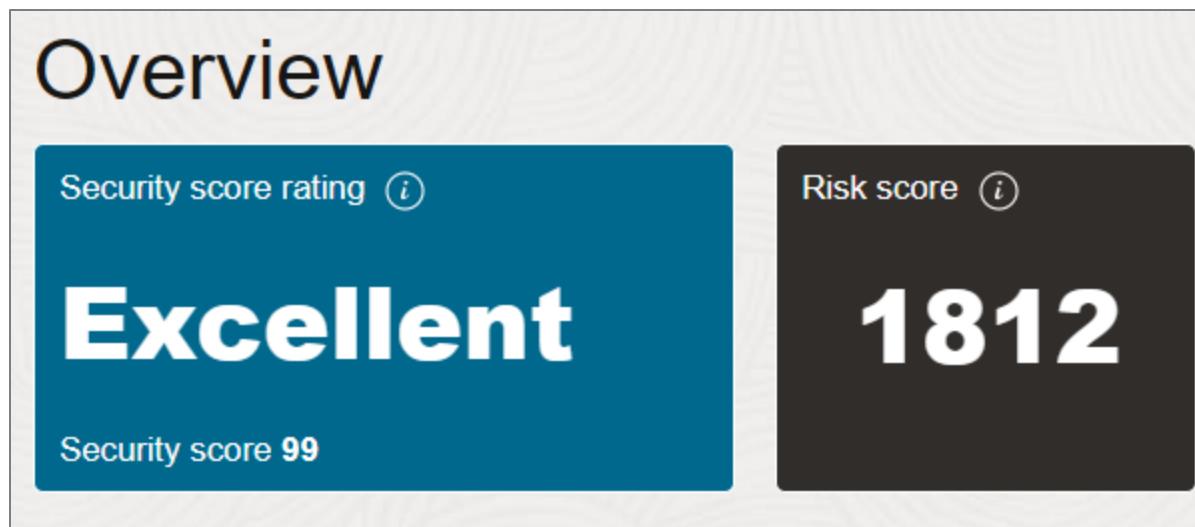
Cloud Guard is a centralized infrastructure security console that enables IT security and risk management teams to monitor the aggregated security posture for applications, workloads and databases running on Oracle cloud.



Scores

Security Score: A higher security score is better. A security score of 100 would mean that no problems were detected for any resources. Reflects monitoring for past 30 days.

Risk Score: Related to the number and severity of problems. In general, organizations with many more resources are likely to have more problems, and thus a higher risk score. The risk score is closely related to the "potential surface area" of risk. Updated every 15 Minutes.



About Compartments – Important Notes

All compartments of a target inherit that target's configuration.

- Detector and responder rule settings for a target apply to:
 - The top-level compartment assigned to that target.
 - Any subordinate compartments below it in the hierarchy.

Target defined within an existing target overrides inherited configuration.

- If you want to exclude some compartments from monitoring, create targets below the root level and do not include the root compartment in any target.

Setting Up Cloud Guard Targets

- Defines the resources where Cloud Guard is enabled.
- Setting up more targets allows more specific monitoring
- OCI Cloud Guard service targets are logical objects inspected by Cloud like Compute Instance, Object Storage Bucket, Security Lists etc.
- Rules to detect and resolve issues are applied to targets.

Cloud Guard > Configuration

Configuration Targets

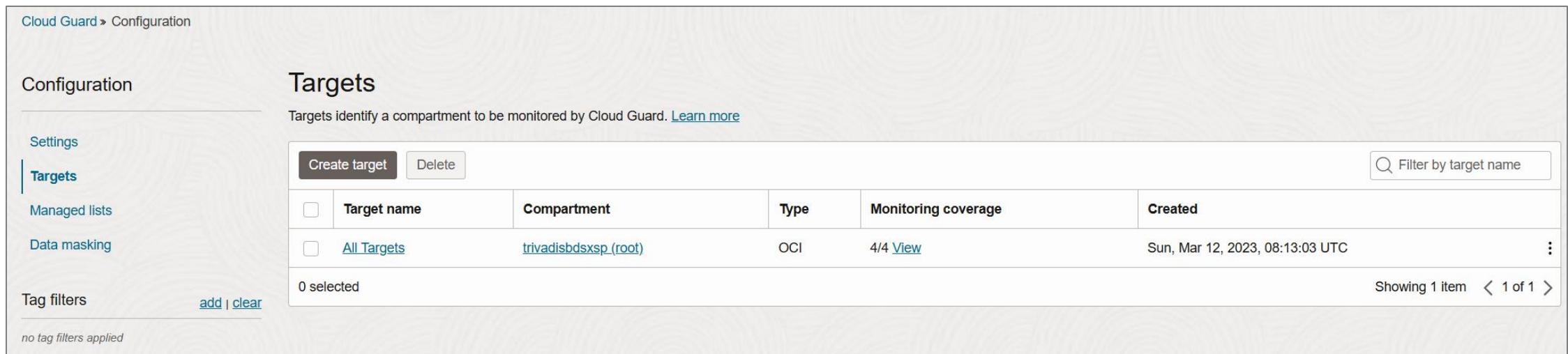
Targets identify a compartment to be monitored by Cloud Guard. [Learn more](#)

Settings Targets Managed lists Data masking Tag filters [add | clear](#) no tag filters applied

Create target Delete Filter by target name

<input type="checkbox"/>	Target name	Compartment	Type	Monitoring coverage	Created	⋮
<input type="checkbox"/>	All Targets	trivadisbdsxsp (root)	OCI	4/4 View	Sun, Mar 12, 2023, 08:13:03 UTC	⋮

0 selected Showing 1 item < 1 of 1 >



Targets Inside

You don't see the new created target for a compartment in the configuration list? Search it via **Tenacy Explorer** or **Search Bar**.

Targets

Targets identify a compartment to be monitored by Cloud Guard. [Learn more](#)

<input type="checkbox"/>	Target name	Compartment	Type	Monitoring coverage	Created
0 selected					

[Create target](#) [Delete](#) Filter by target name

Cloud Guard > Configuration > Targets > Target details

tgt-compartment-high-sec
Cloud Guard Settings for High Sec Compartment

Add tags [Delete](#)

Cloud Guard target information [Tags](#)

OCID: ...2sa2rlrmq [Show](#) [Copy](#)
Target type: Local
Created: Wed, Oct 16, 2024, 12:07:00 UTC
Compartment: [comp-doag-high-sec](#)

Resources Configuration

[Configuration](#) Compartments [comp-doag-high-sec](#)

[Detector recipes](#)

[Responder recipe](#)

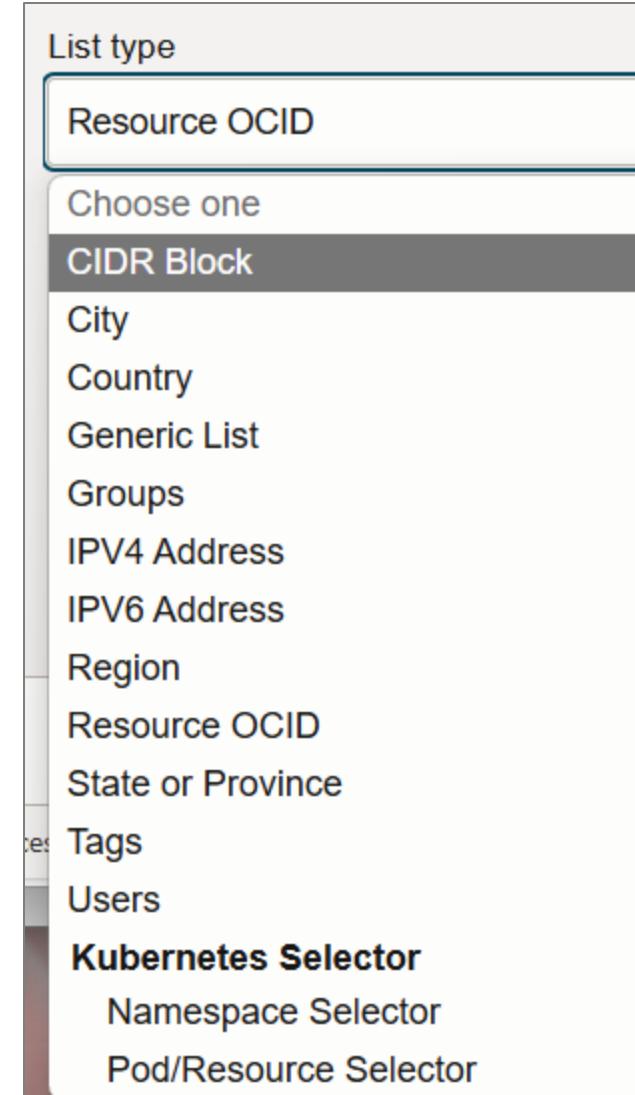
Managed Lists

A managed list is a reusable set of target parameters that simplifies setting the scope for detector and responder rules. It can be used to apply specific configurations to detectors.

- For example, a predefined "**Trusted Oracle IP address space**" list includes all Oracle IP addresses you want to consider trusted when defining rules for detectors and responders.
- Cloud Guard also allows you to create your own managed lists as needed, such as lists of states or provinces, zip or postal codes, OCIDs, or any other criteria you require.

Here are some specific use cases for custom managed lists:

- **Trusted IP addresses:** Exempt listed IP addresses from triggering alerts that should only be triggered by untrusted IP addresses.
- **Resources that should be public:** Exempt listed resources from all detectors related to identifying public configurations.



Detection or Responding

Detector Recipes

- These recipes are used to identify potential security issues by continuously monitoring resources for misconfigurations, vulnerabilities, and anomalous activities.
- Detector recipes contain rules that define what constitutes a problem. When these rules are triggered, Cloud Guard creates a problem.

Responder Recipes

- These recipes define the actions to be taken when a problem is detected by a detector recipe.
- Responder recipes contain rules that specify the actions to remediate, resolve, or dismiss the identified problems.

Oracle provides a set of recipes (3+1) – you can clone them for adaption according to your security needs.



Detector Recipes

OCI Configuration Detector Recipe

- Designed to detect resource configuration settings that could pose a security problem.
- Helps identify misconfigured resources to ensure compliance with security policies.

OCI Instance Security Recipe

- Monitors compute hosts for suspicious activity, providing runtime security for workloads in Compute virtual and bare metal hosts.
- Collects important security information such as security alerts, vulnerabilities, and open ports to provide actionable guidance for detection and prevention.

OCI Activity Detector Recipe

- Detects actions on resources that could pose a security problem.
- Monitors activities to identify potential security issues based on resource actions.

OCI Threat Detector Recipe

- Designed to detect subtle patterns of activity that could be building up to pose a security problem.
- Continuously monitors OCI audit events for malicious activity using machine learning-based behavioral attack models.

OCI Configuration Detector Recipe – Center of Internet Security

The **Configuration Detector** recipe follows the CIS – *Center of Internet Security* – guidelines in version 1.0 ,1.1 or 2.0.

Problems

A problem is any action or setting on a resource that could potentially cause a security threat. All list scope and filter settings are persistent and will remain in place until they are cleared or reset. [Learn more](#)

First detected start time	First detected end time	Last detected start time	Last detected end time			
<input type="text"/>	<input type="text"/>	Sep 16, 2024 19:11 UTC	Oct 16, 2024 19:11 UTC			
Filters						
Labels = CIS_OCI_V1.0_NETWORK <input type="text"/> Enter search filters		Reset all				
Manage columns Mark as resolved Dismiss						
<input type="checkbox"/> Problem name	Risk level ▲	Detector type	Resource	Target	Regions	Labels
<input type="checkbox"/> Instance has a public IP address		Configuration	...high-sec-public	...rtment-high-sec	Switzerland North (Zurich)	CIS_OCI_V1.0_NETWORK,COMPUTE,CIS_OCI_V1.1_NETWORK
0 selected				Showing 1 item		

Responder Recipes

Recipes

Detector recipes

Responder recipes

- Define actions to be taken when a problem is detected by a detector recipe.
- Can be configured for automatic remediation or to notify administrators for manual intervention.
- Contain multiple responder rules specifying actions to address identified problems.
- Can use Oracle-managed recipes with default rules or customized user-managed recipes.

Responder recipes

To create your own recipe, clone an existing Oracle managed recipe from the root compartment [Learn more](#)

Responder recipes		
Recipe name	Oracle managed	Created
OCI Responder Recipe - HIGH SEC	No	Wed, Oct 16, 2024, 12:06:14 UTC

Auto-Resolve

- This is configured on level targets according the **Responder** rules.
- Requires an IAM policy to allow Cloud Guard the action.

**Allow service clouguard to manage buckets in compartment
comp-doag-high-sec**

- The Detector and Responder rule must be enabled.

<input type="checkbox"/> Bucket is public	● Critical	Enabled	Not allowed	No	⋮	^
Description: Object Storage supports anonymous, unauthenticated access to a bucket. A public bucket that has read access enabled for anonymous users allows anyone to obtain object metadata, download bucket objects, and optionally list bucket contents.						
Associated responders: Make Bucket Private						
Conditional group: None						

How to enable Auto-Resolve

1. Search **Cloud Guard Target Group**
2. Select **Responder Recipe - Responder Rule** – click on three dots / edit
3. Change **Setting** and enable **checkbox** for confirmation

Make Bucket Private	REMEDIATION	Enabled	No	<button>Edit</button> :
Rotate Vault Key	REMEDIATION	Enabled	No	⋮
Stop Compute Instance	REMEDIATION	Enabled	No	⋮

Setting

Rule trigger

Ask me before executing rule

Execute automatically
Responder executes automatically when Make Bucket Private is prompted in compartment comp-doag-high-sec.

! Selecting **execute automatically** grants the responder permissions to modify all resources, **without further confirmation**, to correct the rule violation as soon as it is detected. To limit the scope of this action to a subset of the resources, add one or more conditional group statements.

You must select the checkbox below to confirm this selection.

Confirm execute automatically

Conditional Execution

Key points about the **conditional execution** of a responder recipe:

- Specify conditions under which a responder rule will be executed.
- Define conditional groups with parameters like region, resource type, or tags.
- The rule is enforced only if all conditions in the group are met.
- Helps create precise, context-aware security responses, reducing unnecessary actions.

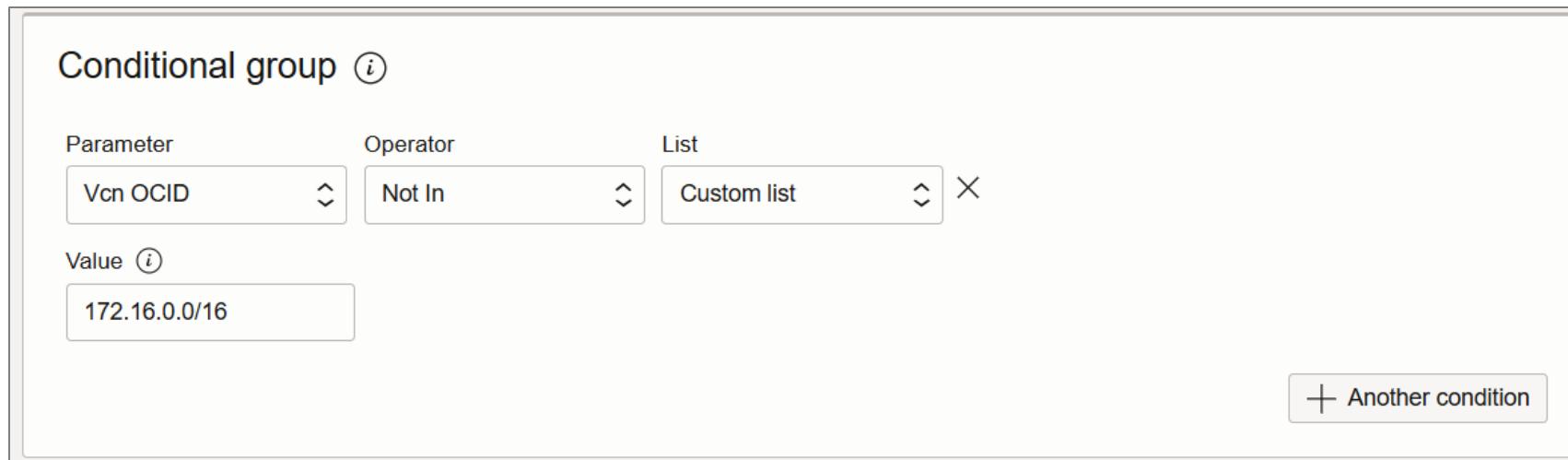
Conditional group *i*

Parameter	Operator	List
Vcn OCID	Not In	Custom list

Value *i*

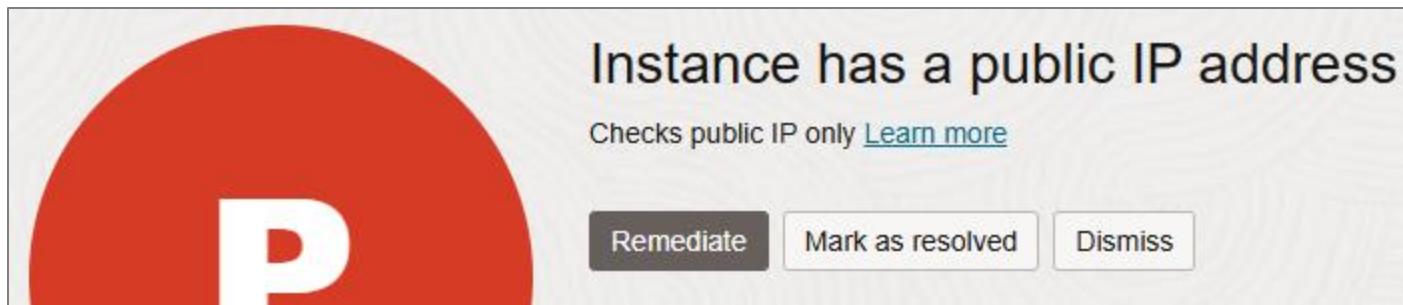
172.16.0.0/16

+ Another condition



Problem solving

- **Remediate:** When you click the "Remediate" button, you are instructing Cloud Guard to take action to fix the identified problem. This typically involves executing a responder rule that addresses the issue, such as changing a configuration setting or applying a security patch. The goal is to resolve the problem so that it does not occur again.
- **Mark As Resolved:** Used to indicate that a problem has been addressed and resolved. When you mark a problem as resolved, you are telling Cloud Guard that the issue was indeed a problem, but you have taken the necessary actions to handle it.
- **Dismiss:** Clicking the "Dismiss" button indicates that you have reviewed the alert and decided that no action is necessary. This could be because the alert is a false positive, or the issue is not relevant or critical. Dismissing an alert will close it without taking any corrective action.



Processing Problems

- If not auto-resolved, see what you have to do for remediation.
- Remediated: Fixed by Cloud Guard Responder
- Resolved: Fixed by other processes
- Dismissed: Ignored / closed

Cloud Guard > Alerts > Problems > Problem details

P Instance has a public IP address

Checks public IP only [Learn more](#)

[Remediate](#) [Mark as resolved](#) [Dismiss](#)

[Details](#)

General information

Problem OCID: ...2l7arpeaaa [Show](#) [Copy](#)
Resource ID: ...7dbgsbbr4q [Show](#) [Copy](#)
Detector type: Configuration
Resource name: [compute-high-sec-public](#)
Managed: Local
Risk level: ● High

Additional details

vnicDetails: [{"vnicAttachmentId": "ocid1.vnicattachment.oc1.eu-zurich-1.an5heljrsijhdmqc43g4cdlzb6wzabxsb15b4ywqmjni7kmfigxgesoso23a", "vnicAttachmentDisplayName": null, "vnicId": "ocid1.vnic.oc1.eu-zurich-1.ab5heljrq7q6rcivrsgrwf2xaeeixeab5owcuhdaehe6to2hu4fp3mu637q", "vnicDisplayName": "compute-high-sec-public", "vnicPublicIcp": "140.238.174.154"}]

Subnet Access Type and Public IPs: [{"subnetAccessType": "Public", "vnicPublicIcp": "140.238.174.154"}]

Notification

- Be informed whenever Cloud Guard has detected or auto-resolved the problem by definig Rules.

Rule Conditions

Limit the events that trigger actions by defining conditions based on event types, attributes, and filter tags. [Learn more](#)

Condition	Service Name	Event Type
Event Type	: Cloud Guard	Detected - Problem Problem Threshold Reached Remediated - Problem

[+ Another Condition](#)

Rule Logic

```
MATCH event WHERE (
  eventType EQUALS ANY OF (
    com.oraclecloud.cloudguard.problemdetected,
    com.oraclecloud.cloudguard.problemthresholdreached,
    com.oraclecloud.cloudguard.problemremediated
  )
)
```

[View example events \(.JSON\)](#)

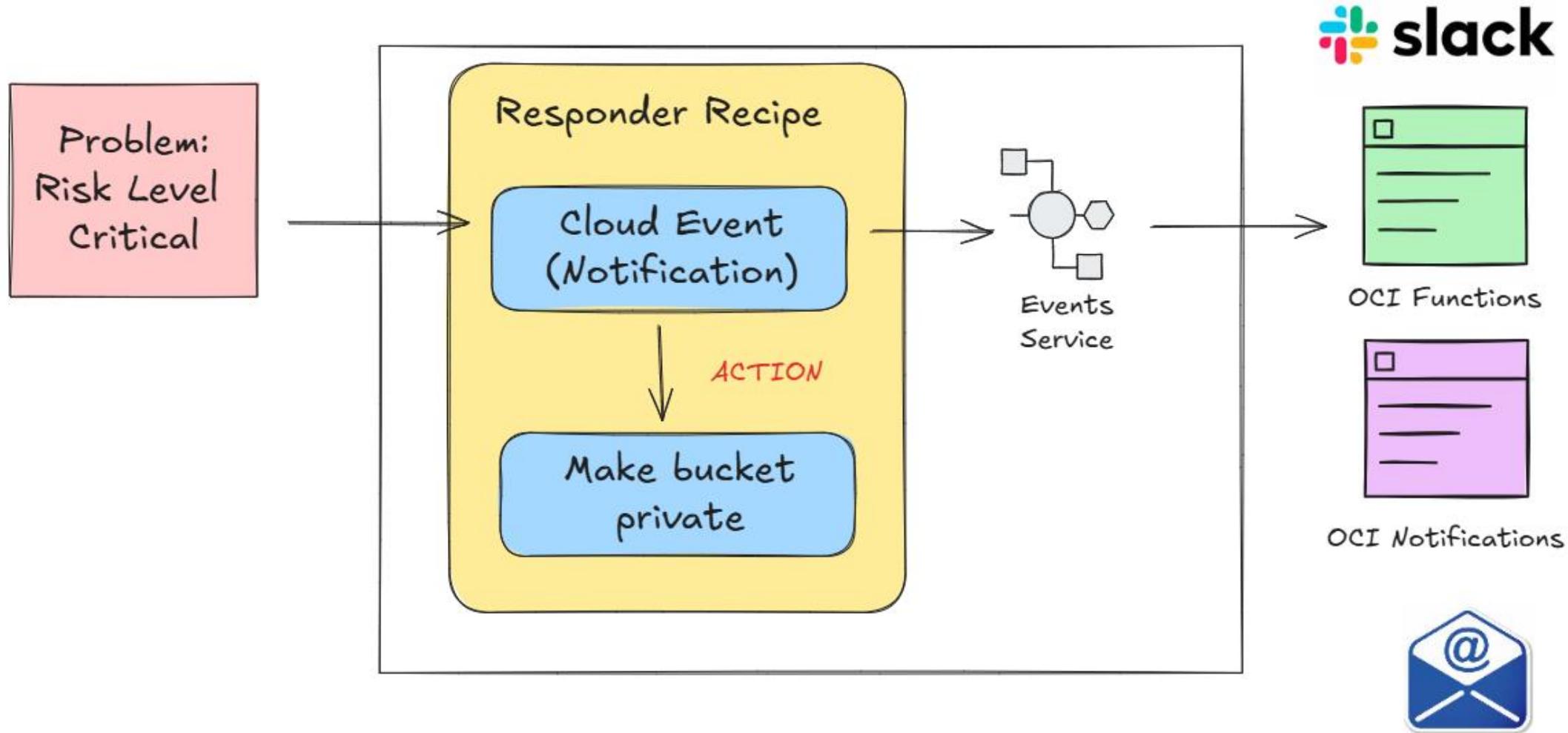
[External] OCI Event Notification :com.oraclecloud.cloudguard.problemremediated

 noreply@notification.eu-zurich-1.oci.oraclecloud.com
An ● Berger, Martin

External email. Inspect before opening any links or attachments.

{
 "eventType" : "com.oraclecloud.cloudguard.problemremediated",

Notification



Queries – Verify Instances

- Use queries to get critical information about the current state of your compute instances via **OS Agent** plugin.
- Instance Security uses **Osquery**, which leverages a relational data model to describe an instance.
- A little bit tricky to configure (IAM & Firewall)

Run query

Use queries to get critical information about the current state of your compute instances.

Instance Security

Scope

Targets

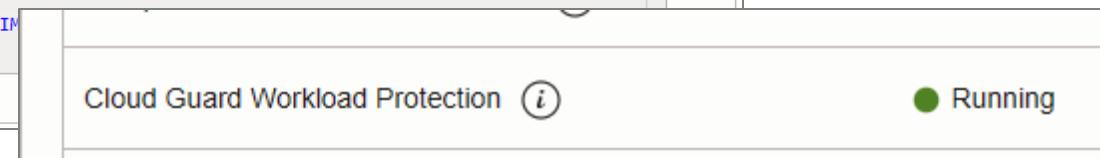
All targets
 Choose target

SQL Query

```
1 -- Provide an osquery
2 SELECT pid, name, ROUND((total_size * '10e-7'), 2) AS memory_used FROM processes ORDER BY total_size DESC LIMIT 10
```

Cloud Guard Workload Protection ⓘ

Running



A screenshot of the Cloud Guard Workload Protection interface. At the top, it says "Run query" and "Use queries to get critical information about the current state of your compute instances." Below this is a section titled "Instance Security" with a "Scope" dropdown set to "Targets". Under "Targets", there are two options: "All targets" (which is selected) and "Choose target". In the "SQL Query" section, there is a code block containing the following SQL:1 -- Provide an osquery
2 SELECT pid, name, ROUND((total_size * '10e-7'), 2) AS memory_used FROM processes ORDER BY total_size DESC LIMIT 10

At the bottom right, there is a status indicator for "Cloud Guard Workload Protection" which shows a green circle and the word "Running".

Queries – Results

Results

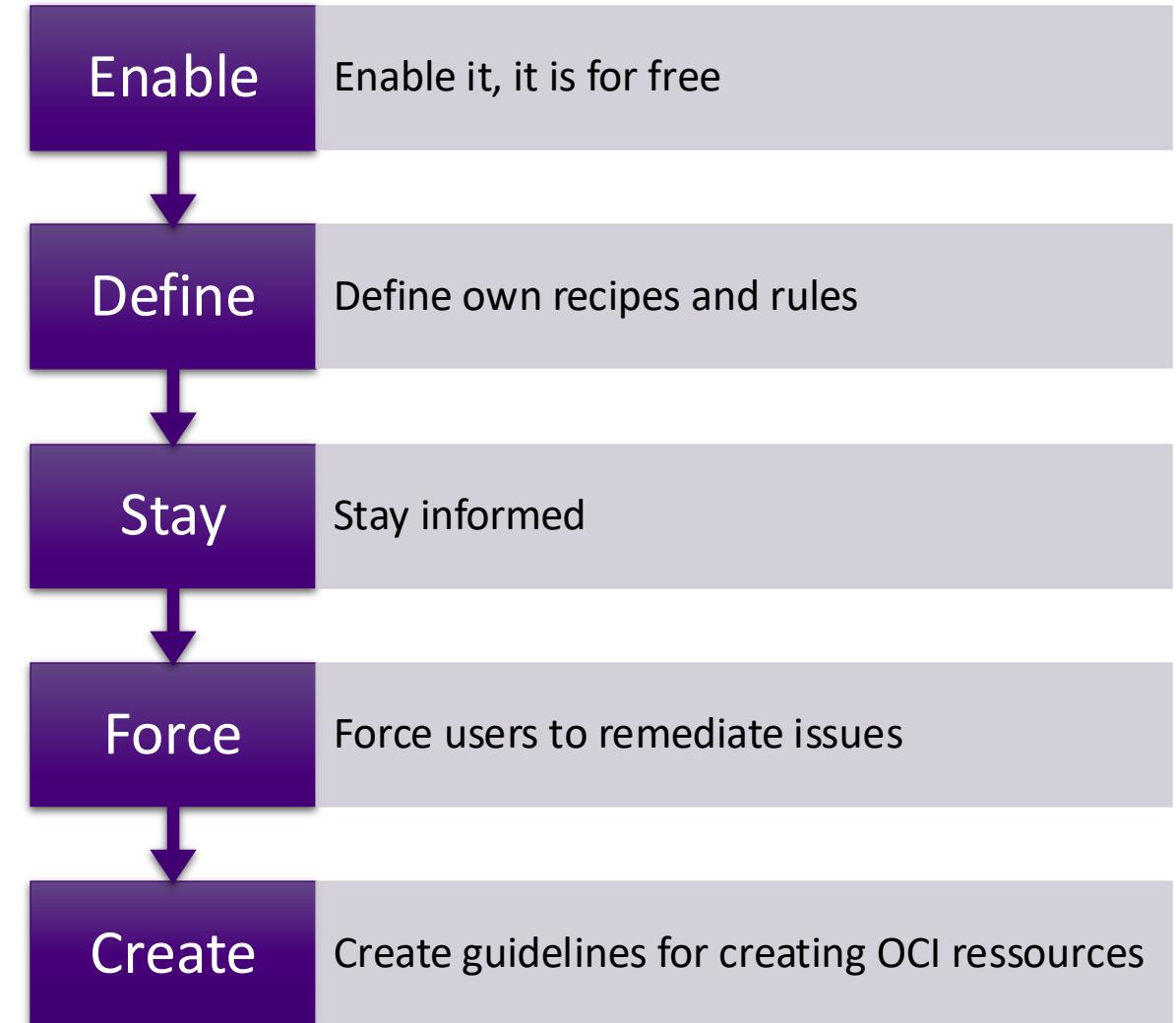
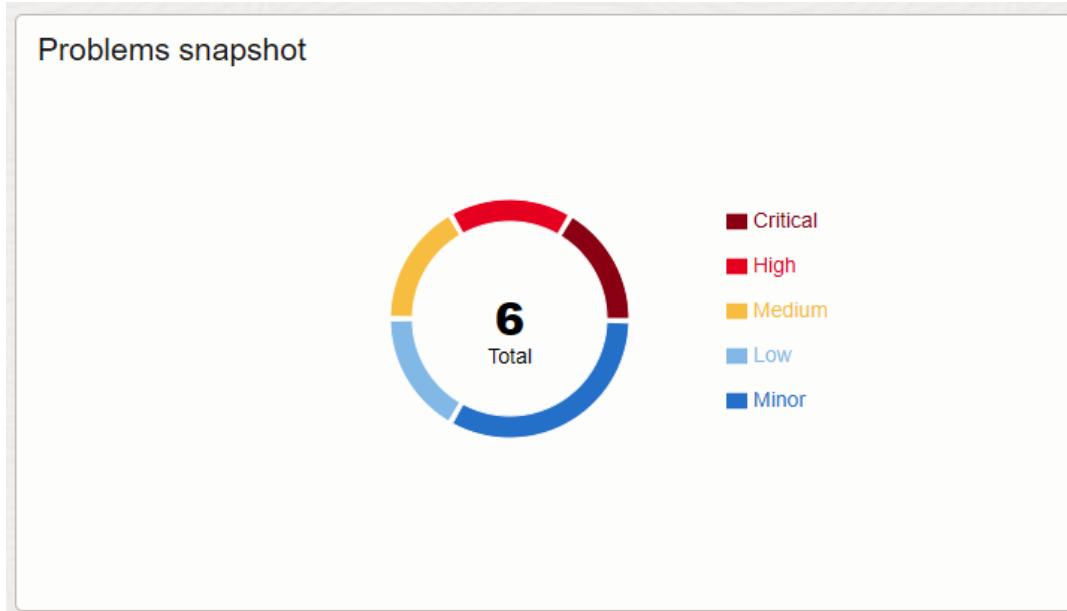
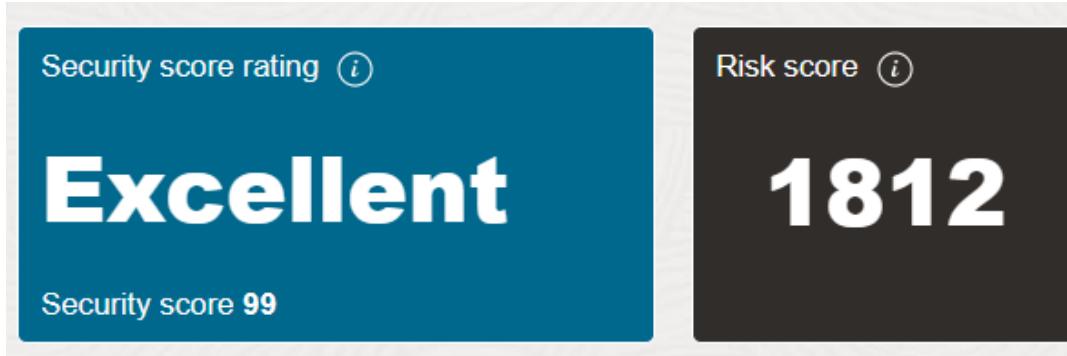
Running query

1 of 1 instances completed

Showing 1 result.

Instance OCID	Status	Region	Time submitted
...7dbgsbbr4q	● Completed	Switzerland North (Zurich)	Wed, Oct 16, 2024, 19:04:06 UTC
memory_used		name	pid
1768.89000000000001		oci-wlp	2378
1764.0		runcommand	5043
1763.53		oci-vulnerabili	2333
1763.28		gomon	4901
1762.559999999999		agent	2196
		Sh	

Best Practices for Using OCI Cloud Guard



2

Hands-On Labs

What about the
Database Security?

Hands-On Labs

List of Hands-On Labs

- **Manual Remediation** – Configure manual remediation for detected security risks.
- **Auto Remediation** – Automate responses to detected security vulnerabilities
- **Notification Setup** – Set up notifications to monitor and alert on security-related events.

Oracle Cloud Infrastructure Security

Data Safe

Martin Berger
Stefan Oehrli

Data Safe

A short Introduction

- 1** Overview
- 2** Security Assessment
- 3** User Assessment
- 4** Database Audit
- 5** SQL Firewall
- 6** Sensitive Data Discovery
- 7** Data Masking
- 8** Hands-On Labs

1

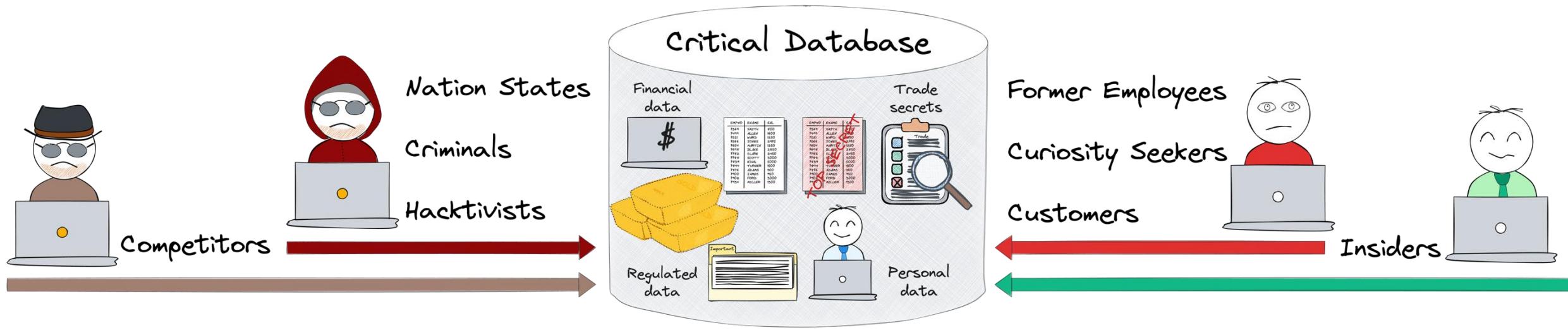
Overview

Data Safe in a Nutshell

Data: The Crown Jewel of Your Organization

Protecting Data to Prevent Liability

- **Data is a Key Asset:** While data holds immense value, it can quickly turn into a major liability if not adequately protected.
- **Rising Cybercrime:** Cybercrime is expected to cause \$8 trillion in global damages in 2023, with databases being prime targets due to their concentration of valuable information.
- **Increasing Regulations:** New and expanding data protection laws demand stricter security and accountability.



Why Oracle Data Safe?

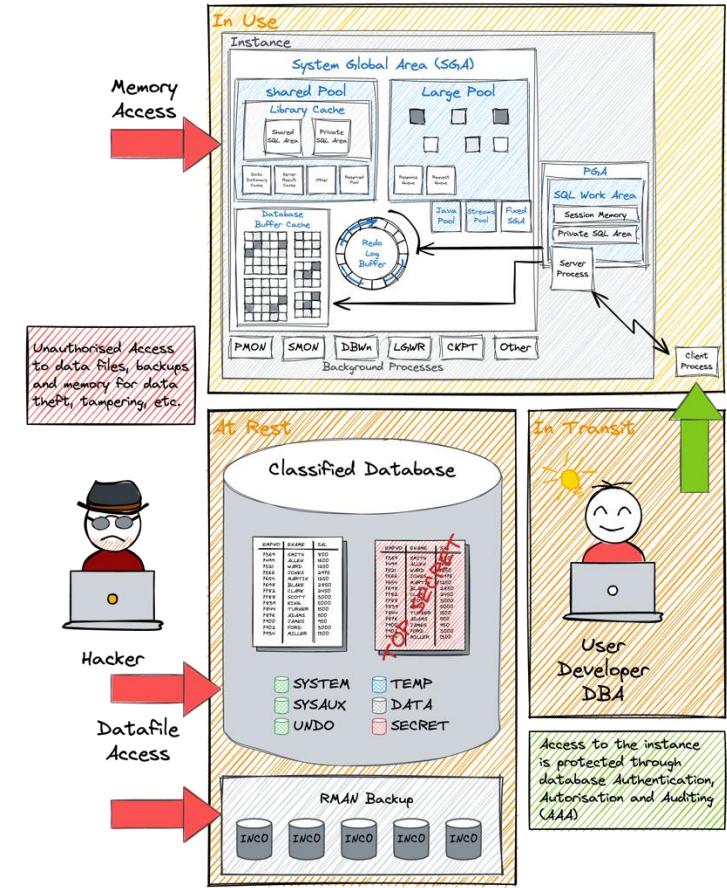
Beyond Encryption and Patching – Comprehensive Database Security

More Than Basic Security – Encryption and patching are crucial but incomplete.

Key Security Focus Areas:

- **Configuration Compliance** – Is the database securely configured?
- **User Risk & Monitoring** – Who are the highest-risk users, and what actions are they performing?
- **Audit & Compliance** – Which activities should be audited, and how do we manage and protect the audit logs effectively?
- **Sensitive Data Control** – What sensitive data is stored, and can exposure be minimized?

***Holistic Security Management** – Oracle Data Safe offers centralized tools to address these areas, enhancing control, visibility, and compliance.*



Oracle Data Safe Overview

Centralized Security for Cloud and On-Premises DBs

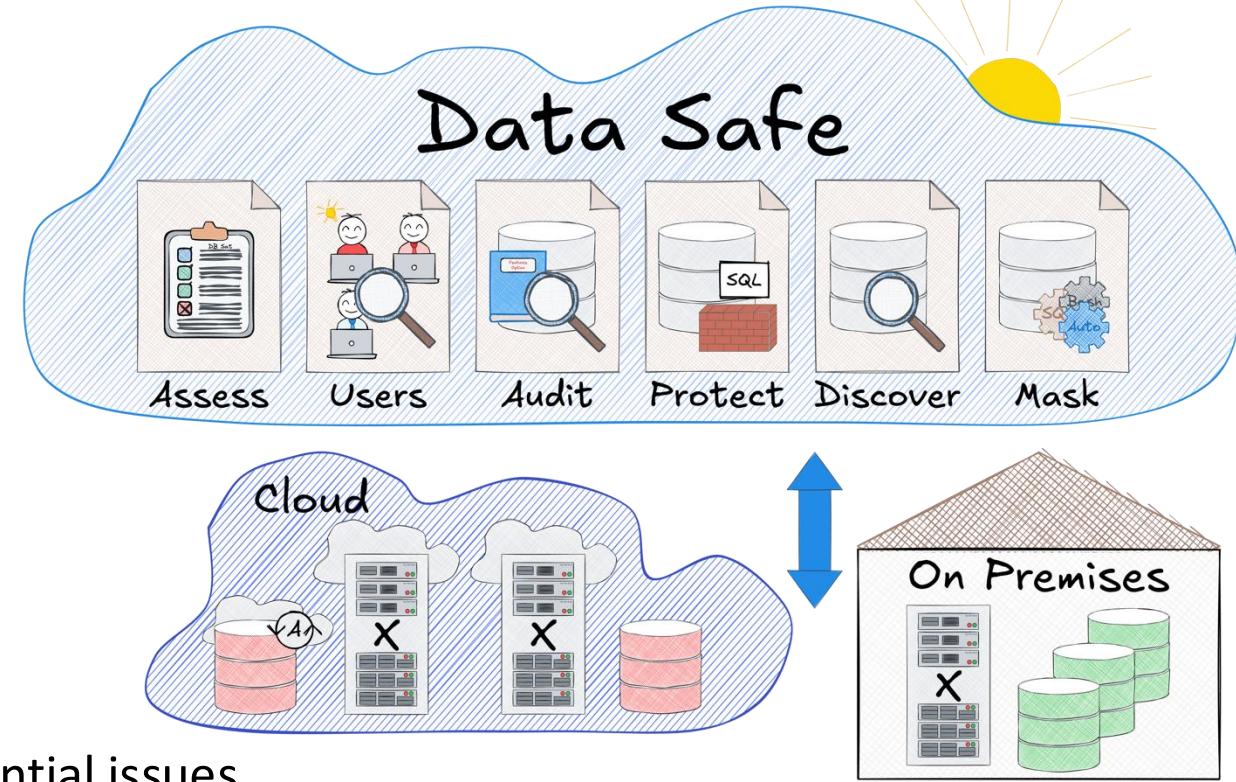
Unified Security Center – Manage and monitor security for cloud and on-premises databases.

Core Capabilities

- **Risk Dashboard:** Visualizes risk across users, data and configurations.
- **User Monitoring:** Audits user activities to detect potential issues.
- **Data Masking:** Protects sensitive data in test environments.
- **Future-Ready:** Regular updates add new security features.

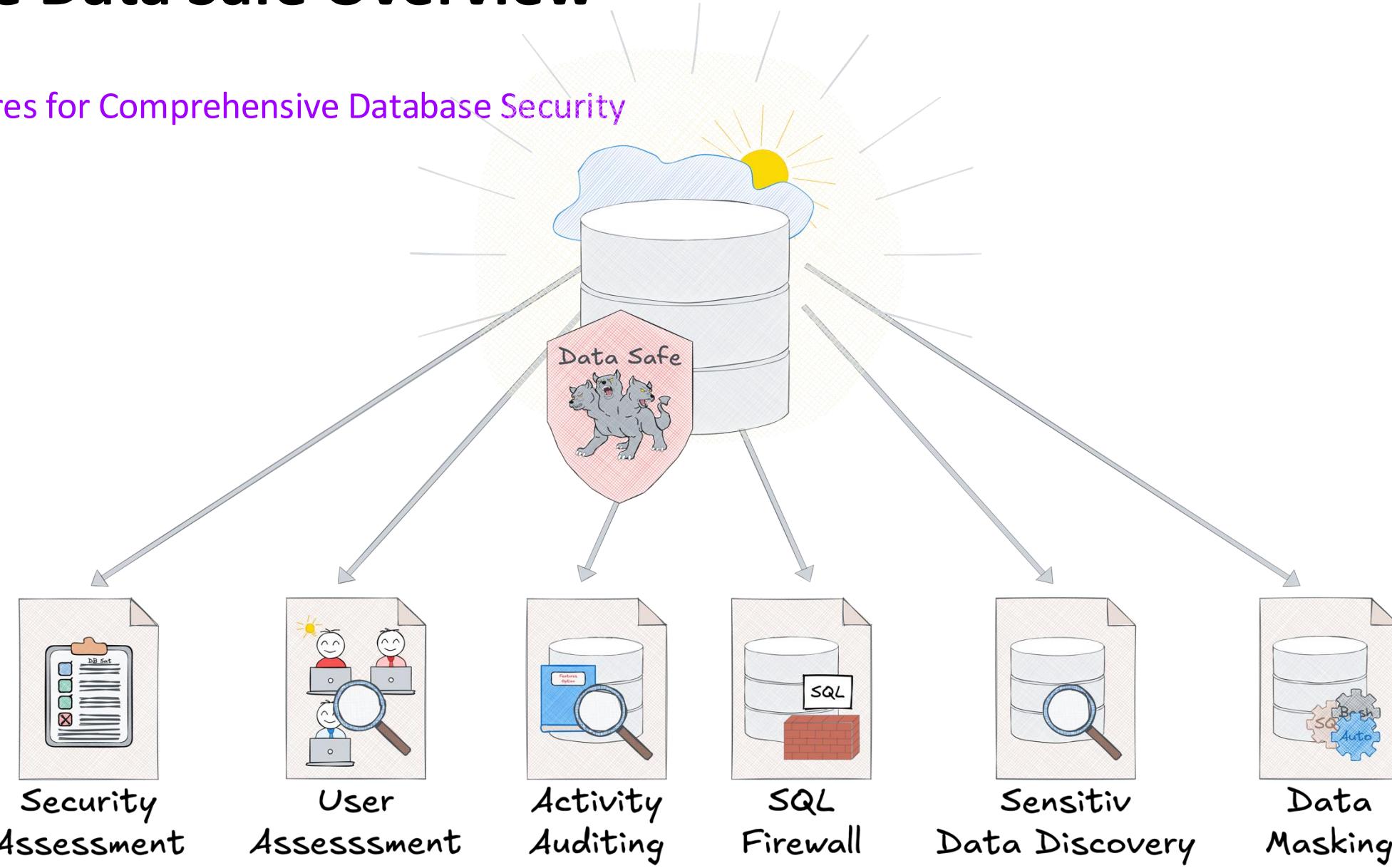
Key Benefits

- **Easy & Efficient:** No special expertise required—quick setup and automated security.
- **Risk Mitigation:** Saves time and reduces exposure to threats.
- **Comprehensive Protection:** Defense-in-depth security for all Oracle databases.



Oracle Data Safe Overview

Key Features for Comprehensive Database Security

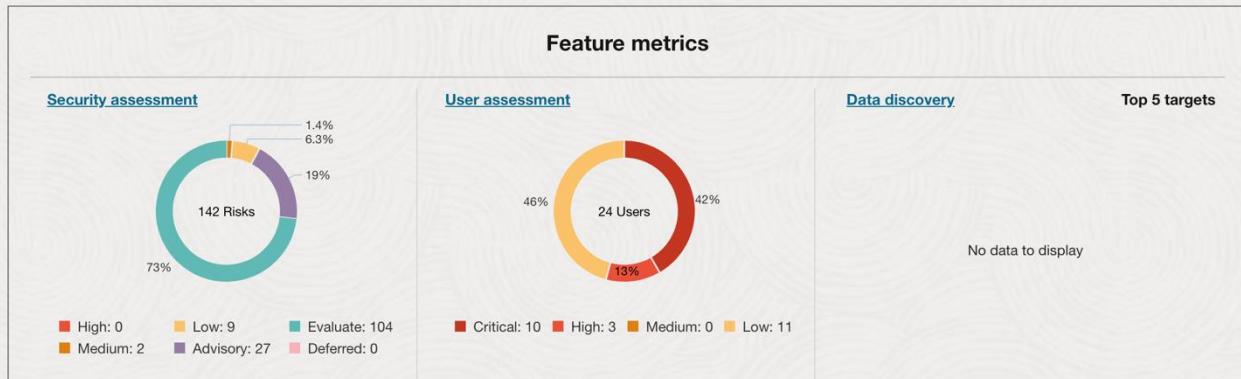


Data Safe Dashboard

Key Security Indicators at a Glance

Dashboard

Key security indicators for all the registered target databases



2

Security Assessment

Database Security
Assessment

Database Security Assessment

Comprehensive Assessment

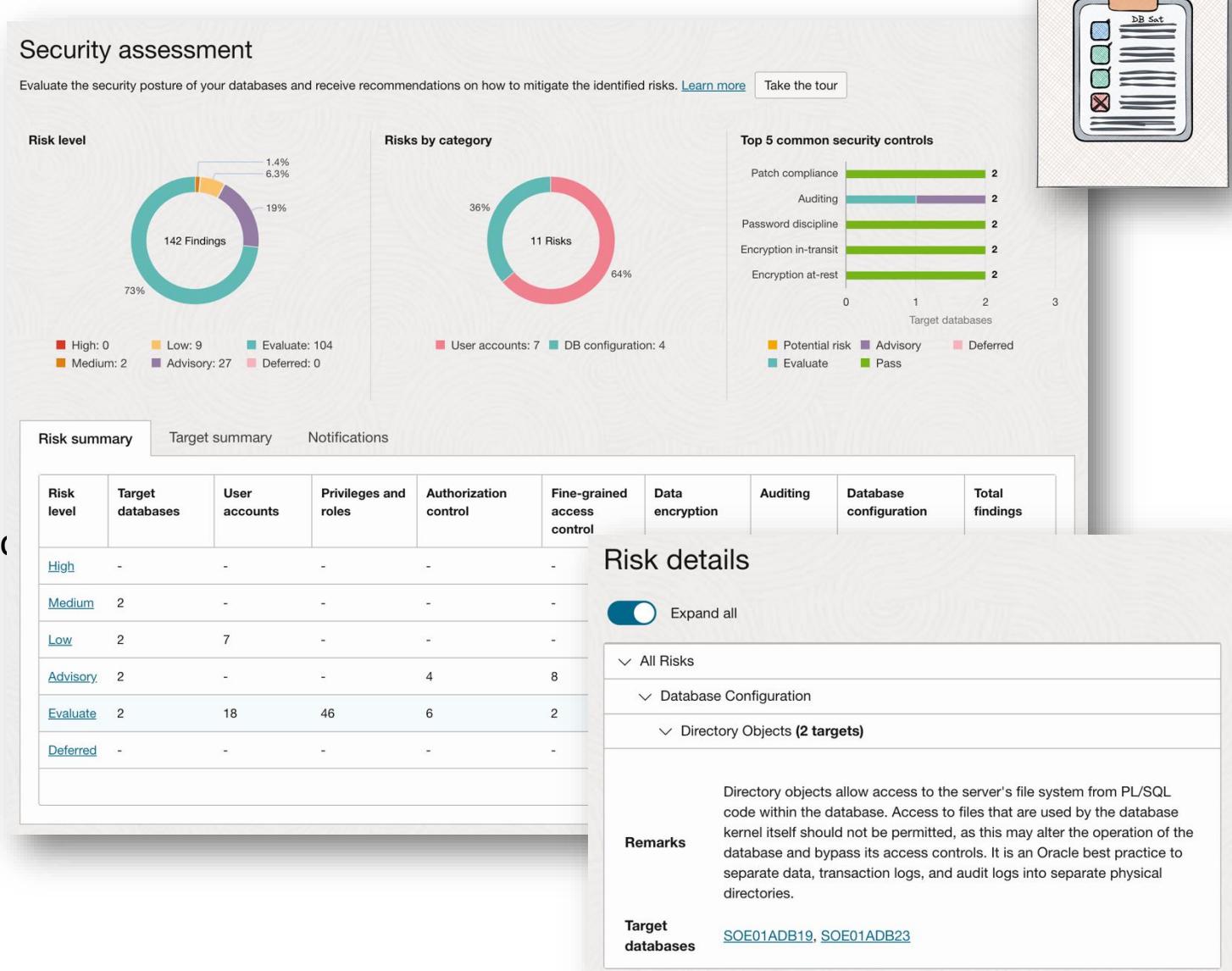
- Security parameters
- Security controls in use
- User roles and privileges

Landscape-Wide Risk Overview

- Identified risks with actionable recommendations

Compliance Mappings

- Aligns with GDPR, STIG, CIS standards



Database Security Assessment



Detecting Configuration Drifts

Establish a Security Baseline

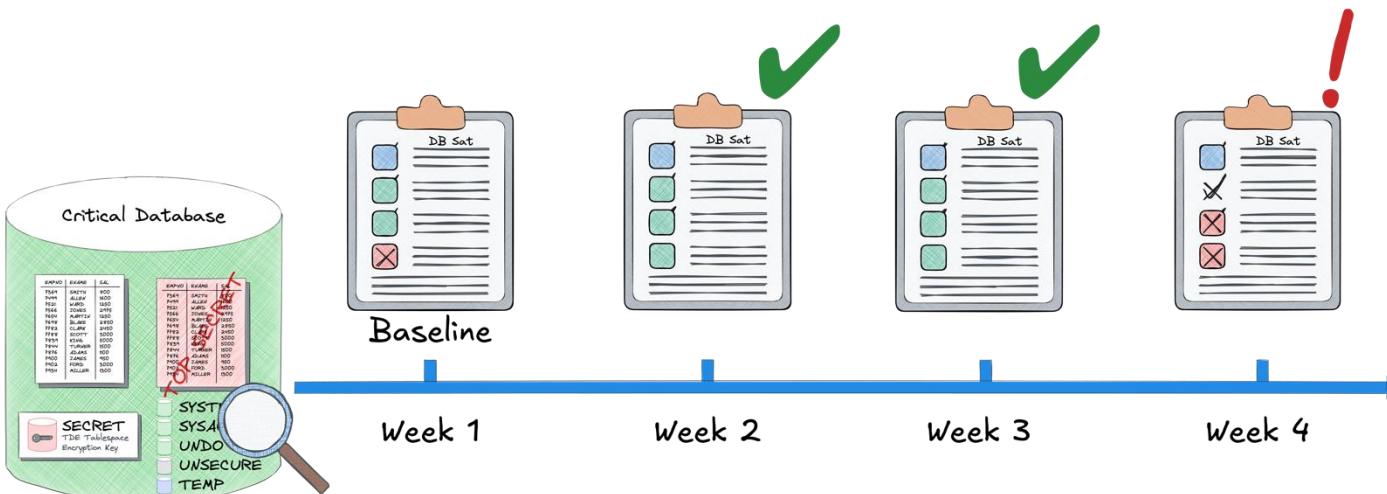
- Define a baseline configuration for secure operations.

Automatic Comparisons

- New assessments are automatically checked against the baseline.

Notifications for Drift

- Receive alerts and review any deviations from the baseline to address potential risks.



3

User Assessment

User Security
Assessment

User Risk Assessment



Reducing Risk Through Role and Privilege Management

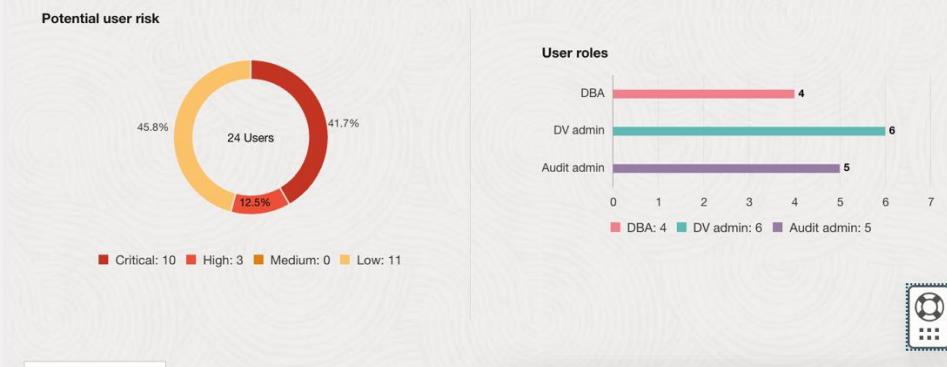
User assessment

Identify potential risk inherent in database accounts. Assess the potential risk a compromised or misused account would pose. [Learn more](#) [Take the tour](#)

Info New authorization required
To view the available schema access details of the user you will need permissions on the data-safe-security-policy-reports resource in the compartment of the target database.

- Allow group <user-group> to read data-safe-security-policy-reports in compartment <compartment-name>
- Allow group <user-group> to inspect data-safe-security-policy-reports in compartment <compartment-name>

Please re-run the privilege script for non-ADB databases [Learn more](#)



Risk summary Target summary Notifications

Manage columns

Potential risk	Target databases	Users	Privileges	User name	Target database	User type	DBA	DV admin	Audit admin	Potential risk	Status	Last login time	User profile	Audit records
Critical	2	10	10	ADBSNMP	SOE01ADB23	PRIVILEGED, SCHEMA	-	✓	-	HIGH	LOCKED	-	ORA_PROTECTED_PROFILE	View activity
High	2	3	3	ADBSNMP	SOE01ADB19	PRIVILEGED, SCHEMA	-	✓	-	HIGH	LOCKED	-	ORA_PROTECTED_PROFILE	View activity
Medium	-	-	-	SCOTT	SOE01ADB23	PRIVILEGED	-	-	-	HIGH	OPEN	Tue, 24 Sep 2024 11:38:01 UTC	DEFAULT	View activity
Low	2	11	-											

Displaying 3 users < 1 of 1 >

Identify High-Risk Users

- Pinpoint users with elevated privileges who may pose security risks.

Review Roles and Privileges

- Analyze assigned roles, object access, and system privileges.

Evaluate User Details

- Check user details like last login, password change history, and recent database activity.

User Risk Assessment



Detecting User and Entitlement Changes

Periodic User Assessments

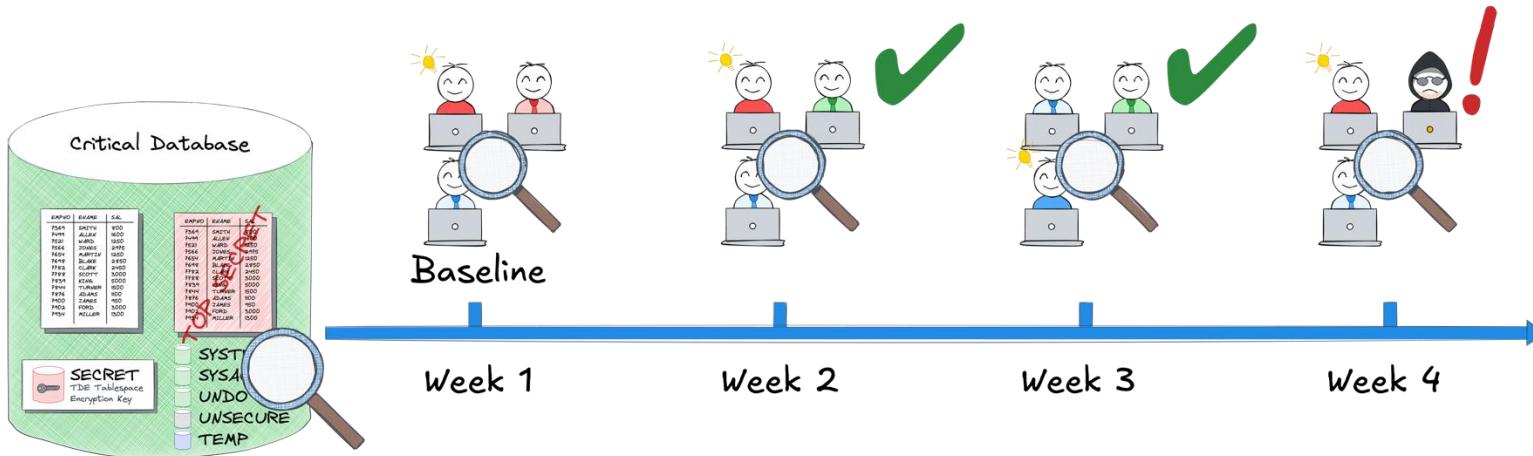
- Regularly evaluate user accounts and privileges.

Compare with Previous Results

- Identify changes by comparing new assessments with prior ones.

Alerts for Changes

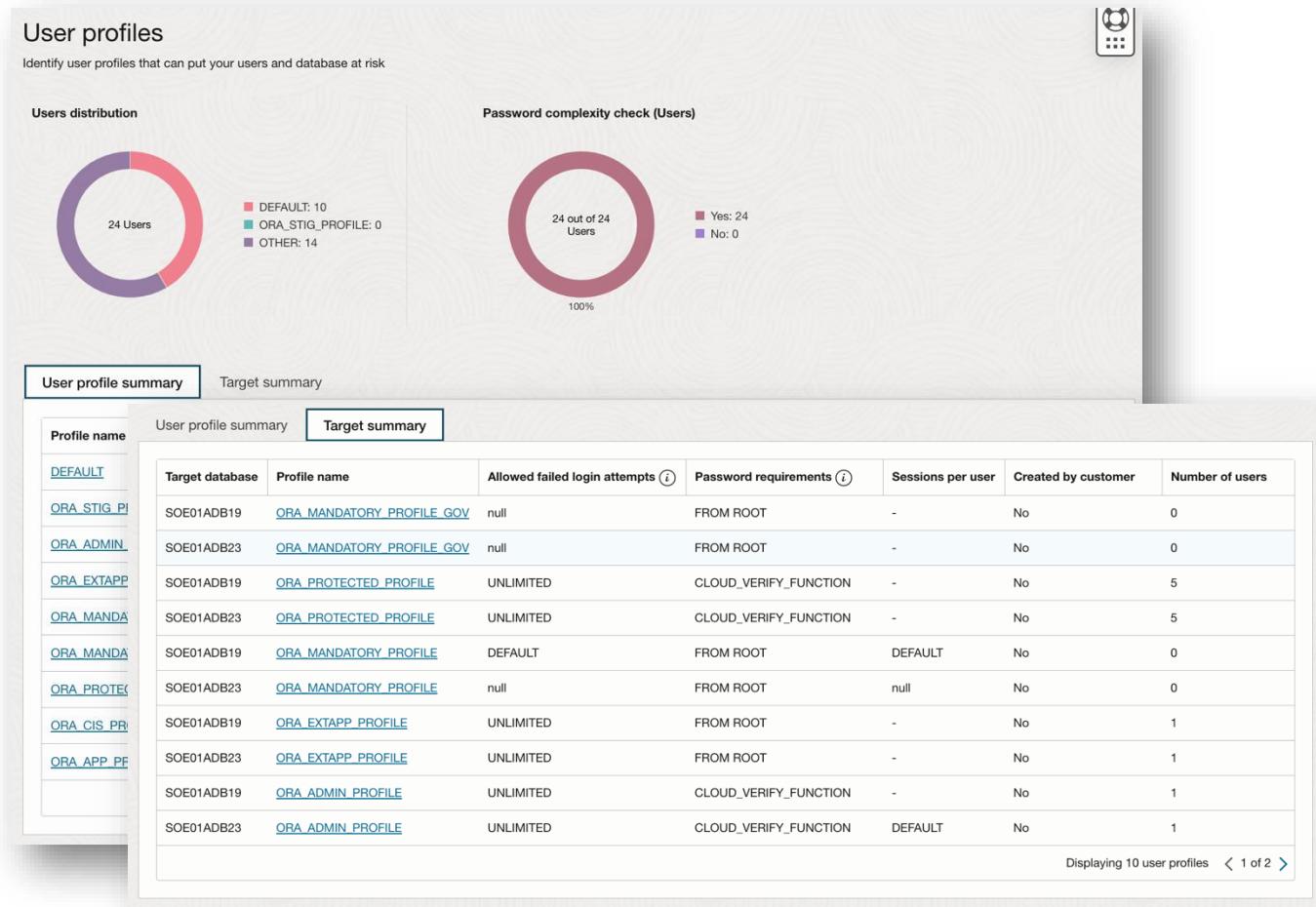
- Receive notifications for newly added users or modifications in user entitlements.



User Profile Insight



Evaluating Password-Related Attributes in User Profiles



Review User Profiles

- Examine existing profiles and their security parameters.

Map Profiles to Users

- Identify which users are assigned to specific profiles.

Detect Weak Profiles

- Easily spot profiles and users lacking password complexity or other security measures.

4

Database Audit

Central Audit
Management and
Reporting

User Activity Auditing



Track User Actions with Comprehensive Auditing and Reporting

Audit and Compliance Policies

- Define policies for auditing, compliance, and alerts.

Data Collection

- Gather audit data from databases, focusing on sensitive operations.

Audit Reports:

- Interactive Reports** – For in-depth forensic analysis.
- Summary & Detailed Reports** – Tailored insights for different auditing needs.
- PDF Compliance Reports** – Ready-made reports for regulatory compliance.

The screenshot shows the Oracle Database Audit Trail configuration and reporting interface. It includes sections for Audit policy information, General information, Policy activity, Target database, Audit trails, Basic auditing, Audit profile, Admin activity auditing, User activity auditing, and Audit compliance standards. A central callout box provides instructions for getting started with activity auditing. Below the interface are three charts: Audit trails, Failed login activity, and Admin activity.

Audit policy information

General information

- Name: AuditPolicy_1725518337750
- Description: Audit policies for target: SOE01ADB23
- OCID: ...hdqttq [Show](#) [Copy](#)
- Compartment: trivadisbdsxsp (root)/Projects_Internal/comp-ocw-dev
- Created time: Thu, 05 Sep 2024 06:38:57 UTC
- Updated time: Thu, 14 Nov 2024 07:42:30 UTC

Policy activity

- Last provisioned time: Thu, 14 Nov 2024 07:42:28 UTC
- Last retrieved time: Thu, 14 Nov 2024 07:42:30 UTC
- Data Safe user activity excluded: Yes

Target database

- Name: SOE01ADB23

Basic auditing

- Database schema changes: Enabled for specific users and/or roles [View details](#)
- Logon events: Enabled for specific users and/or roles [View details](#)
- Critical database activity: Enabled for specific users and/or roles [View details](#)

Audit profile

- Profile name: AuditProfile_1725518338090

User activity auditing

- User activity: Disabled

Audit compliance standards

- Center for Internet Security (CIS) configuration: Disabled

Activity auditing in comp-ocw-dev compartment

Collect and store database audit data from all your target databases centrally in Data Safe and identify anomalous behavior with pre-defined audit policies, alerts and reports. [Learn more](#)

Custom policies

Configure auditing and alerts **Start audit trails**

Audit trails

Status	Trail count
Running	2
Stopped	0
Not started	0
Needs attention	0

Failed login activity

Date	Failed logins
8 Nov 2024	0
9 Nov 2024	0
10 Nov 2024	0
11 Nov 2024	0
12 Nov 2024	0
13 Nov 2024	0
14 Nov 2024	1

Admin activity

Date	Activity
8 Nov 2024	47
9 Nov 2024	0
10 Nov 2024	0
11 Nov 2024	0
12 Nov 2024	0
13 Nov 2024	0
14 Nov 2024	0

Legend

- Audit setting changes
- Failed logins
- User/Role/permissions changes

Audit Insights Dashboard

Fine-Tune Your Audit Policies

Gain Deeper Insights

- Analyze audit data to optimize policies.

High-Volume Policies

- Identify which audit policies generate the most records.

Top Targets

- See which databases produce the highest audit volumes.

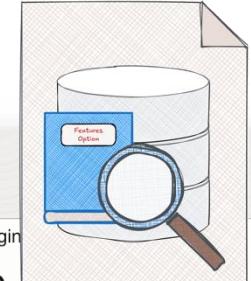
Frequent Access Patterns

- Discover the most-accessed objects and schemas.

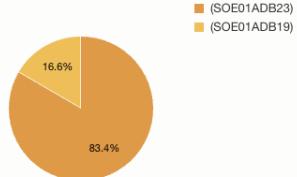
Audit insights in Projects_Internal compartment

Summary of activity audit data for the last 1 week. Use this information to understand and refine your audit policies.

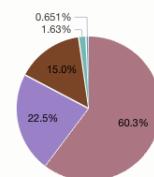
Targets	DB users	Client hosts	DDLS	User/entitlement changes	DMLs	Login
2	3	5	2	2	2	0



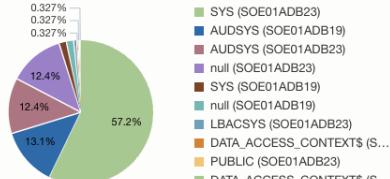
Top 10 targets by audit volume ⓘ



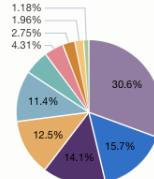
Top 10 audit policies by volume ⓘ



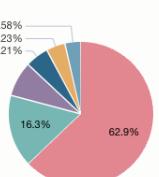
Top 10 schemas by audit volume ⓘ



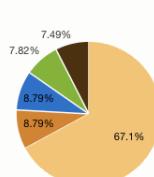
Top 10 objects by audit volume ⓘ



Top 10 database users by audit volume ⓘ



Top 10 client hosts by audit volume ⓘ



Audit Data Retention Management

Ensure Compliance with Retention Policies

Retention Periods

- Store audit data for up to 7 years
- **Online Retention** – Up to 1 year
- **Archive Retention** – Up to an additional 6 years

Configurable Retention

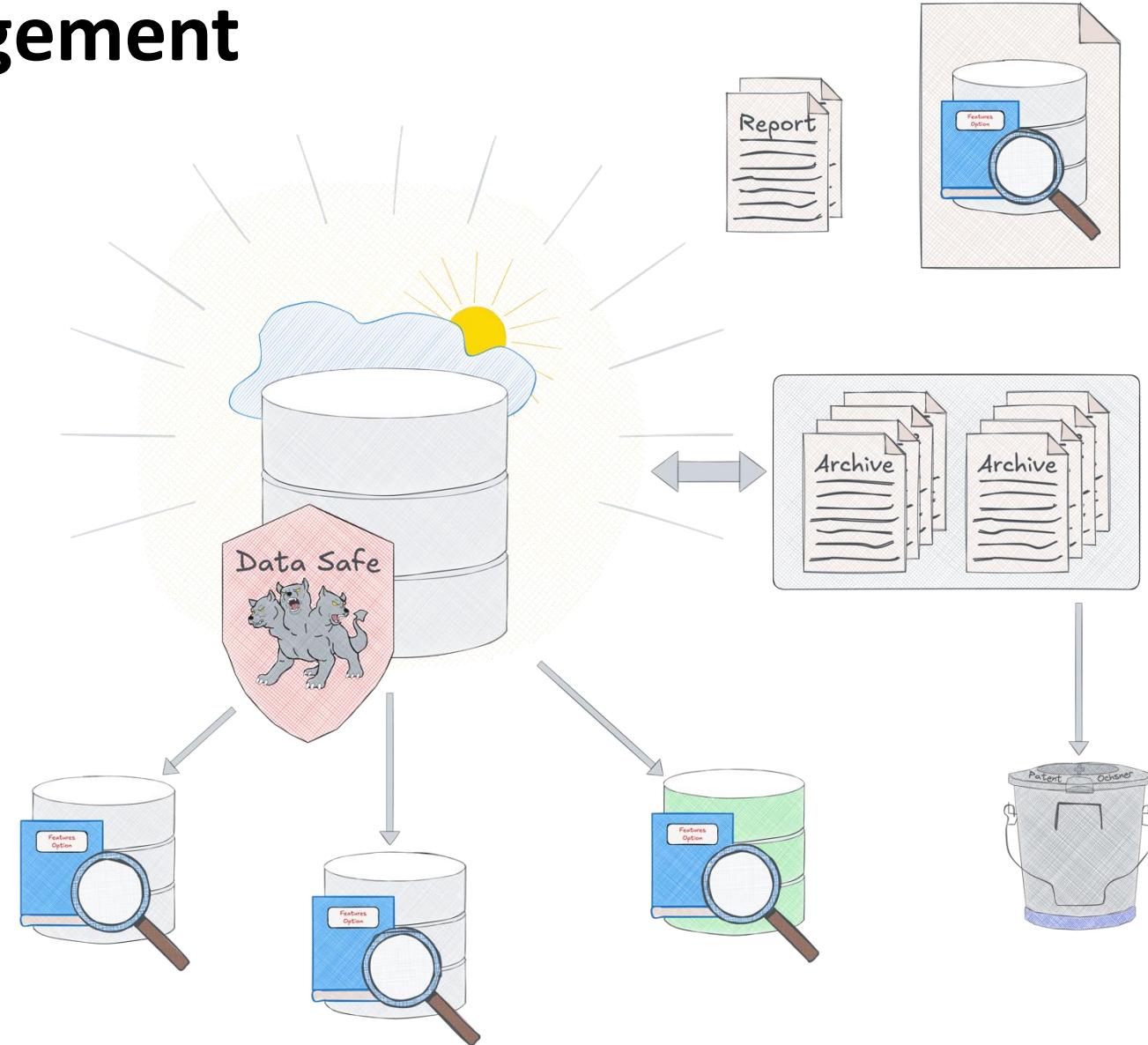
- Set retention periods globally or for specific targets.

Easy Access to Archived Data

- Quickly retrieve audit records as needed.

Fully Managed by Data Safe

- No additional fees for archiving audit data....
... as long as it is not too much data per month



5

SQL Firewall

23ai latest Security
Enhancement

SQL Firewall

Prevent SQL Injection and Unauthorized Access

Real-Time Protection

- Restricts database access to only authorized connections and SQL statements.

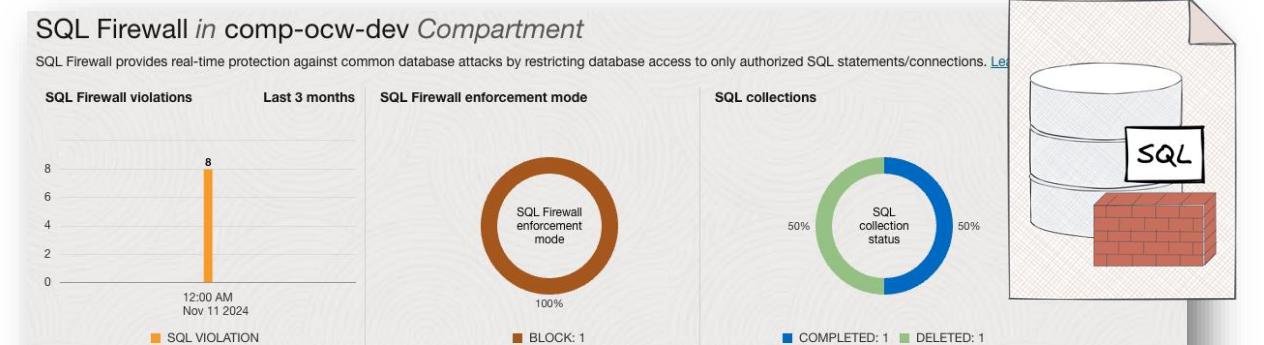
Monitor or Block Violations

- Choose to either monitor or block any access violations.

Risk Mitigation

- Defends against SQL injection, unauthorized access, and credential abuse.

Currently only available in Oracle 23ai



Target summary		Violation summary	Notifications		
Target database	SQL Firewall status	Collecting	Blocked	Observed	
SOE02ADB23	● Enabled	-	-	-	
SOE01ADB23	● Enabled	-	-	-	
SOE01ADB23	● Disabled	-	-	-	

Note: SQL Firewall configuration records are updated every 24 hours

Enforcement information

Status: ● Enabled

SQL collection level: User issued SQL commands

Enforcement scope: SQL statements only

Action on violations: Block and log violations

Audit for violations: Off

Violation reports: [View report](#)

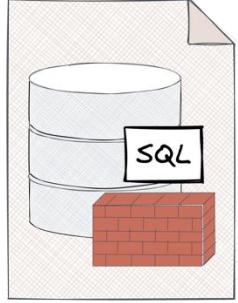
Unique allowed SQL statements

Refresh now Generate report Download report Add from violations

<input type="checkbox"/> SQL text	Version	SQL collection level
<input type="checkbox"/> SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL	1	USER_ISSUED_SQL
<input type="checkbox"/> SELECT * FROM V\$OPTION O,DBMS_DATABASE_COMPATIBLE_LEVEL V WHERE O.PARAMETER=':SYS_B_0' AND O.VALUE=':SYS_B_1' AND V.VALUE LIKE ':SYS_B_2' OR V.VALUE LIKE ':SYS_B_3' OR V.VALUE LIKE ':SYS_B_4' OR V.VALUE LIKE ':SYS_B_5'	1	USER_ISSUED_SQL

Navigating SQL Firewall – Processes

Understanding the Mechanics and Strategies for Optimal Deployment

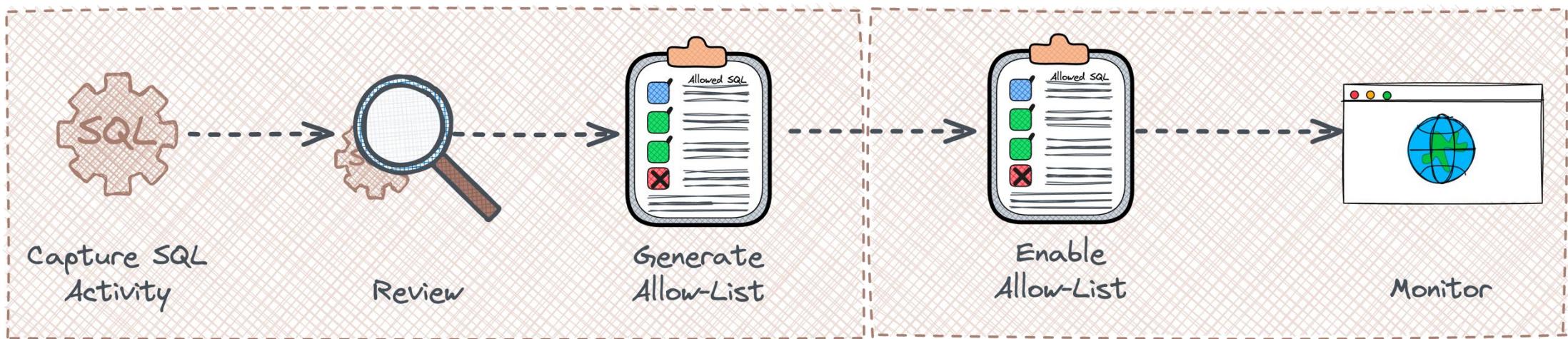


Learning Stage

- **Collect** Enable collection of SQL statements and user connections.
- **Review & Configure** Review collected SQL statements and connections, then define allowed connections as needed.
- **Set Permissions:** Adjust allowed SQL statements and user connections based on security requirements.

Protecting Stage

- **Enable** the allow-list
- **Monitor violations** SQL Firewall raises violation for any unexpected access patterns to ensure compliance



6

Sensitive Data Discovery

Where is my sensitive
Data?

Sensitive Data Discovery

Identify and Classify Sensitive Data to Prioritize Security Efforts

Predefined Sensitive Types

- Detects and classifies over 150 sensitive data types.

Custom Sensitivity Definitions

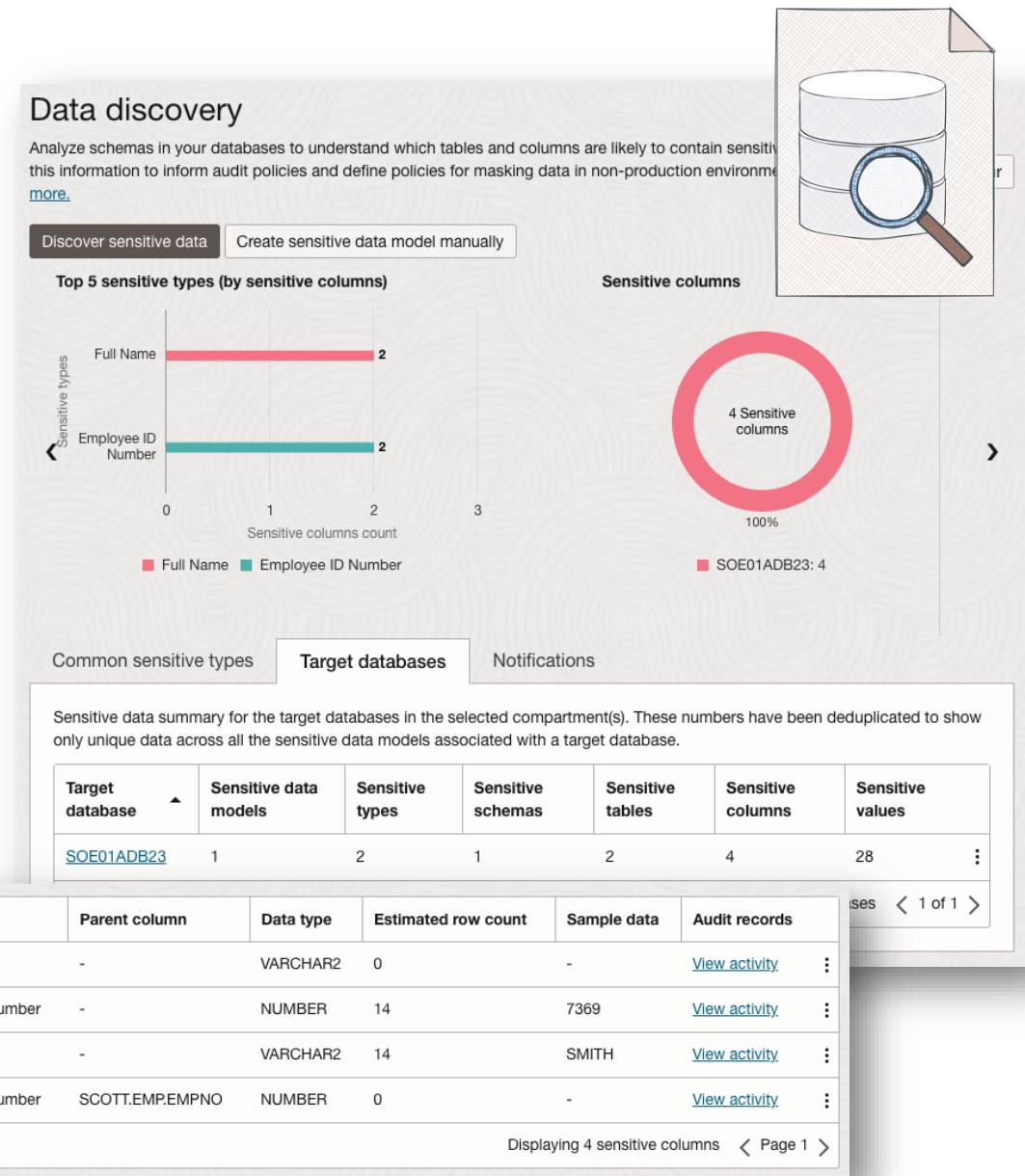
- Allows user-defined sensitive data types for tailored discovery.

Incremental Discovery

- Supports ongoing scans to identify newly added sensitive data.

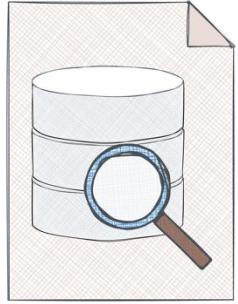
Detailed Reporting

- Provides reports on the amount and types of sensitive data.



Sensitive Data Discovery

150+ Pre-Defined Sensitive Data Types



Identification	Biographic	IT	Financial	Healthcare	Employment	Academic
SSN Name Email Phone Passport DL Tax ID ...	Age Gender Race Citizenship Address Family Data Date of Birth Place of Birth ...	IP Address User ID Password Hostname GPS location ...	Credit Card CC Security PIN Bank Name Bank Account IBAN Swift Code ...	Provider Insurance Height Blood Type Disability Pregnancy Test Results ICD Code ...	Employee ID Job Title Department Hire Date Salary Stock ...	College Name Grade Student ID Financial Aid Admission Date Graduation Date Attendance ...

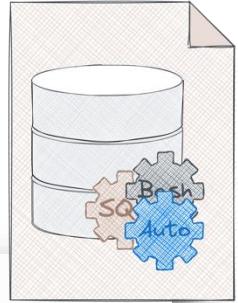
A row of seven icons, each enclosed in a rounded square frame with a grid pattern. From left to right: 1. Five stylized human figures (three adults, two children) sitting at desks with laptops, with a sun icon above them. 2. Four stylized human figures (two adults, two children) standing together. 3. A stack of four server racks next to a large cylindrical database icon with a red 'X' mark. 4. A stylized human figure sitting at a desk with a laptop that has a large dollar sign (\$) on its screen. 5. An open yellow folder labeled 'Important' containing a red heart with a ECG line. 6. An open yellow folder labeled 'Important' containing a white house icon. 7. An open yellow folder labeled 'Important' containing a black graduation cap icon.

7

Data Masking

Mask test and dev data
using sensitive Data
Masking

Sensitive Data Masking



Minimize Sensitive Data Exposure in Development and Testing

Sensitive Data Masking

- Mask data identified as sensitive to protect privacy.

Predefined Masking Formats

- Over 50 predefined formats for common data types.

Automated Format Selection

- Automatically selects appropriate formats based on data type.

Custom Masking Options

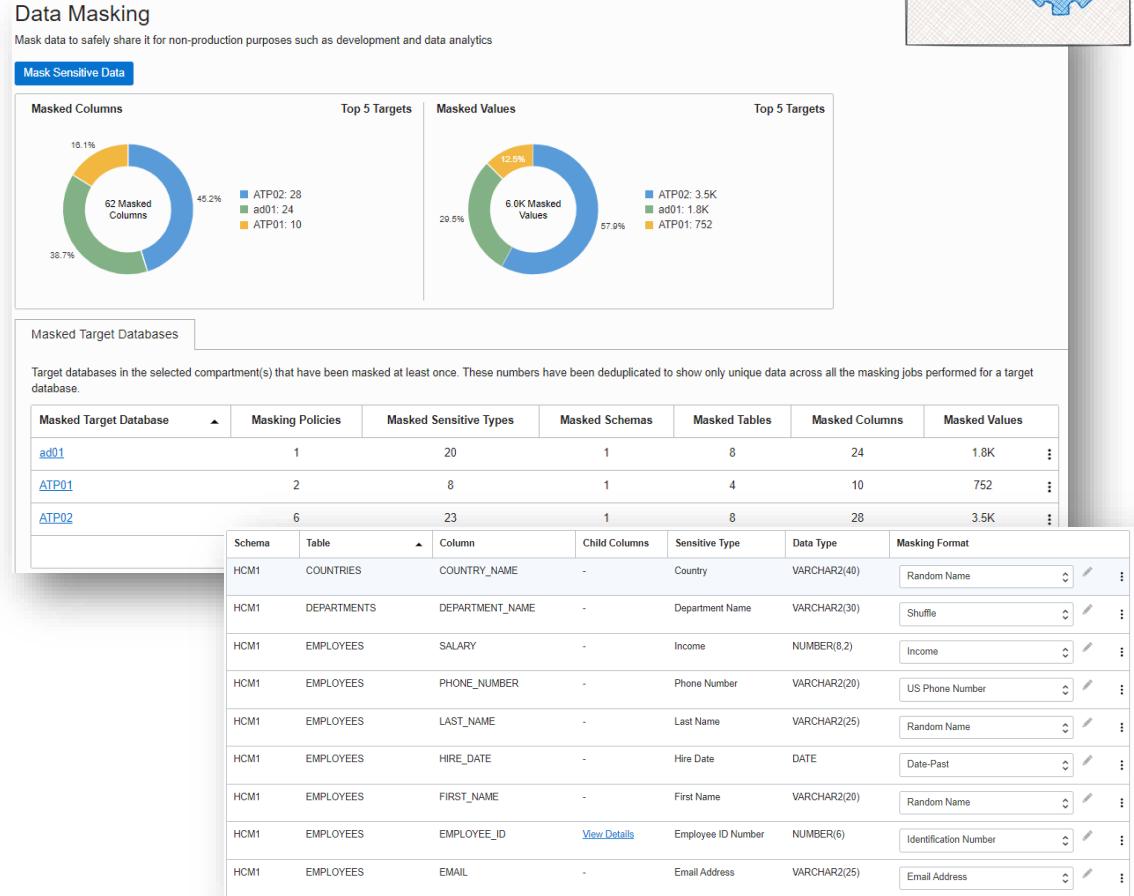
- Supports user-defined formats for specialized requirements.

Advanced Transformations

- Offers rich masking options for complex data scenarios.

Comprehensive Masking Report

- Detailed reports on masked data for compliance and review.



Sensitive Data Masking



Pre-Defined Masking Formats for Comprehensive Data Protection

50+ Pre-Defined Formats

- Data Safe offers a wide range of masking options, including
 - **Specific Formats** – Social security number, credit card number, email address, and more.
 - **Generic Formats** – Random date, random number, random name, fixed number, fixed string.
 - **Advanced Techniques** – Format-preserving randomization, regular expression, data truncation, group masking.

Masking Formats

Masking formats define the logic for masking data. This page lists the user-defined masking formats in the selected compartment, along with all the predefined masking formats. [Learn more.](#)

Create Masking Format		
Name	Description	Oracle Predefined
Age	Replaces values with random numbers between 0 and 110	Yes
Bank Account Number	Replaces values with random 9 to 16 digit numbers	Yes
Bank Routing Number	Replaces values with random 9-digit numbers	Yes
Betting	-	No
Blood Type	Replaces with values picked randomly from a list. Possible values are A+, A-, B+, B-, AB+, AB-, O+, and O-	Yes
Canada Postal Code (Space-Separated)	Replaces values with random Canada postal codes. Postal codes are in A9A A9A format, where A signifies a letter and 9 a digit	Yes
Canada Social Insurance Number	Replaces values with random Canada Social Insurance Numbers	Yes
Canada Social Insurance Number (Hyphenated)	Replaces values with random Canada Social Insurance Numbers. Social Insurance Numbers are in 999-999-999 format, where 9 signifies a digit	Yes
Credit Card Number	Replaces values with random credit card numbers. Card types covered are American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa	Yes
Credit Card Number (Hyphenated)	Replaces values with random hyphenated credit card numbers. Card types covered are American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa	Yes
Credit Card Number (Type and Format Preserving)	Replaces values with random credit card numbers while preserving their type and format. Card types covered are American Express, Diners Club, Discover, enRoute, JCB, Mastercard, and Visa. For other card types, preserves the number of digits and Luhn's check but may not preserve the card type	Yes
Credit Card Number-American Express	Replaces values with random 15-digit American Express credit card numbers	Yes

8

Hands-On Labs

What about the
Database Security?

Hands-On Labs

List of Hands-On Labs

- **Data Safe Configuration and Register ADB** – Initial setup of Oracle Data Safe, including registration of an Autonomous Database.
- **Assess Database Configurations** – Use Oracle Data Safe to assess database configurations for compliance.
- **Assess Database Users** – Review and analyze database user accounts with Oracle Data Safe.
- **Audit Database Activity** – Monitor and audit database activity for enhanced security visibility.
- **Generate Alerts** – Configure and generate alerts based on Oracle Data Safe findings.
- **Discover Sensitive Data** – Identify and classify sensitive data within the database using Oracle Data Safe.
- **SQL Firewall** – Implement SQL Firewall to manage and restrict SQL execution within the database.

Oracle Cloud Infrastructure Security

Security Zones

Martin Berger
Stefan Oehrli

Security Zones

Security for free.

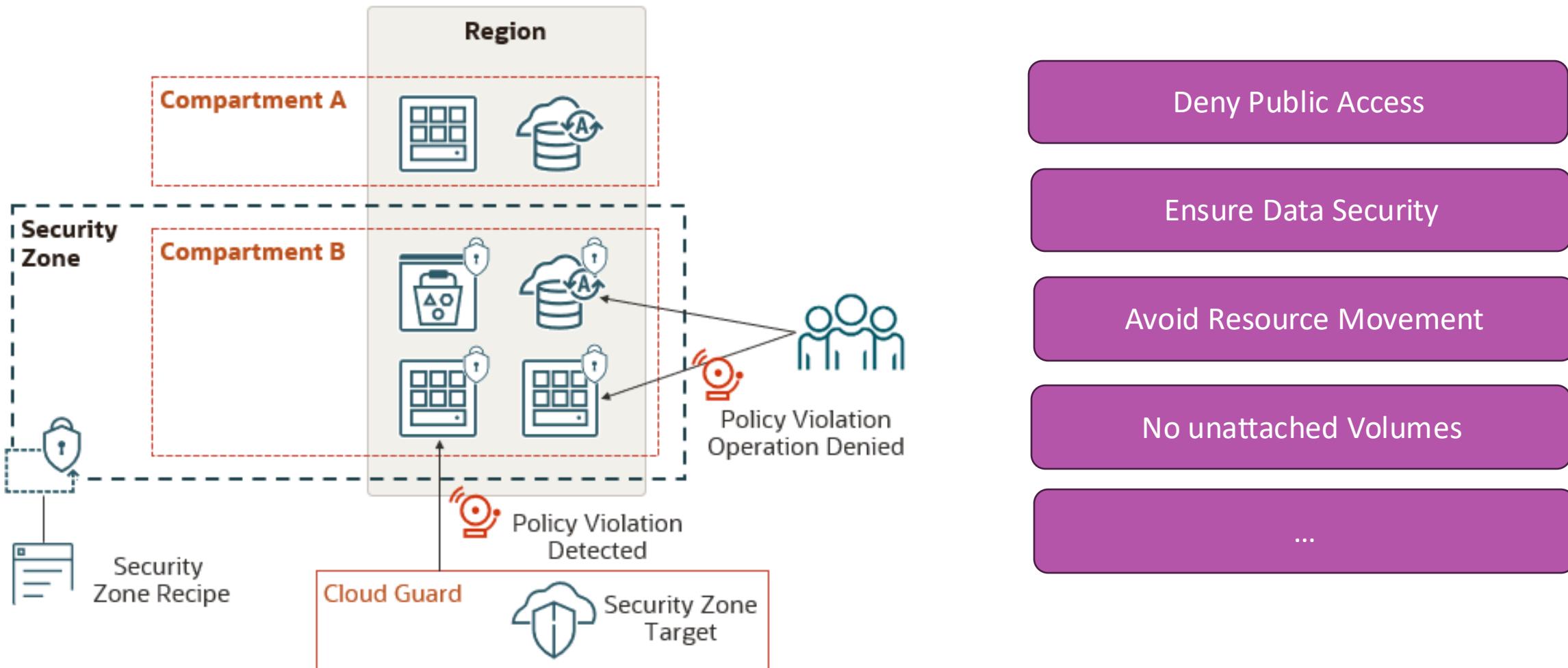
- 1 Security Zones
- 2 Web Application Firewall
- 3 Hands-On Labs

1

Security Zones

Security for free.

Concept



Source: oracle.com

Maximum Security Recipe - 20200914

Policies

Each policy in a Security Zone Recipe prohibits some action that violates a security best practice. Policies are categorized by security principle. [Learn more](#)

Policy statement	Type	Resource types	⋮
deny instance_without_sanctioned_image	Use Only Configurations Approved by Oracle	COMPUTE, COMPUTEMANAGEMENT	⋮
deny instance_in_security_zone_in_subnet_not_in_security_zone	Restrict Resource Association	COMPUTE, COMPUTEMANAGEMENT	⋮
deny block_volume_in_security_zone_attach_to_instance_not_in_security_zone	Restrict Resource Association	COMPUTE	⋮
deny block_volume_not_in_security_zone_attach_to_instance_in_security_zone	Restrict Resource Association	COMPUTE	⋮
deny boot_volume_in_security_zone_attach_to_instance_not_in_security_zone	Restrict Resource Association	COMPUTE	⋮
deny boot_volume_not_in_security_zone_attach_to_instance_in_security_zone	Restrict Resource Association	COMPUTE	⋮
deny instance_in_security_zone_launch_from_boot_volume_not_in_security_zone	Restrict Resource Association	COMPUTE, COMPUTEMANAGEMENT	⋮
deny instance_not_in_security_zone_launch_from_boot_volume_in_security_zone	Restrict Resource Association	COMPUTE, COMPUTEMANAGEMENT	⋮
deny instance_in_security_zone_move_to_compartment_not_in_security_zone	Restrict Resource Movement	COMPUTE	⋮

Components

- **Proactive** enforcement of security policies in a compartment.
- **Policy Compliance:**
 - Security Zones ensure that resources like Compute, Networking, Object Storage, Block Volume, and Database comply with security policies.
- **Validation and Enforcement:**
 - OCI validates and enforces security policies when creating or updating resources in a Security Zone, denying operations that violate policies.
- **Predefined and Custom Recipes:**
 - Use the **Maximum Security Recipe** provided by Oracle, or create custom recipes to meet specific security needs.
- **Oracle Cloud Guard Integration:**
 - Enable Cloud Guard to detect policy violations in existing resources before creating Security Zones.

Principles

- Resources in a security zone **can't be moved to a compartment outside** of the security zone because it might be less secure.
- All the required components for a resource in a security zone **must also be located in the same security zone**.
 - Example, an instance (Compute) in a security zone **can't use a boot volume that is not in the same security zone**.
- Resources in a security zone must **not be accessible from the public internet**.
- Resources in a security zone must be **encrypted using customer-managed keys**.
- Resources in a security zone must be **regularly and automatically backed up**.
- Data in a security zone is considered privileged and **can't be copied outside of the security zone** because it might be less secure.
- Resources in a security zone must use only **configurations and templates approved by Oracle**.

Create a new Security Zone

- You can create your own recipes for a zone based on a template,
- Any pre-defined Cloud Guard target settings are replaced by Oracle recipes if there is an existing detector configuration.

The screenshot shows the Oracle Cloud Infrastructure Security Zones interface. On the left, a sidebar has 'Overview' selected under 'Security Zones'. Below it are 'Recipes', 'List scope', and 'Compartment' dropdowns set to 'sec-zone-comp-oci-bootcamp-33'. A message bar at the top right says 'The latest Security Zones release includes many significant enhancements and user interface changes. See the [release notes](#) for details.' The main area is titled 'Security Zones' and contains a table with one row. The table has columns for 'Name', 'Status', and 'Recipe'. The row shows 'sec-zone-comp-oci-bootcamp-33' in the Name column, 'Active' in the Status column, and a link 'Maximum Security Recipe - 20200914' in the Recipe column.

Name	Status	Recipe
sec-zone-comp-oci-bootcamp-33	Active	Maximum Security Recipe - 20200914

- Rules are immediately active.

A red message bar at the bottom of the screen displays the text: 'Security zone violation: Encrypt the bucket with a customer-managed encryption key or use the following workflow to create a new key and bucket: [Create Secure Bucket](#)'.

Security Zones and Cloud Guard

- **Compartment and Security Zone Integration:**
 - Security Zones enforce policies on resource operations within compartments, including existing resources created before the zone.
- **Cloud Guard Integration:**
 - Security Zones work with Cloud Guard to identify and address policy violations in existing resources.
- **Centralized Monitoring:**
 - Cloud Guard provides a dashboard to monitor and manage security weaknesses across cloud resources, offering suggestions and corrective actions.



Targets				
Targets identify a compartment to be monitored by Cloud Guard. Learn more				
Create new target		Delete		
<input type="checkbox"/>	Target name	Compartment	Type	Monitoring coverage
<input type="checkbox"/>	sec-zone-comp-oci-bootcamp-33	sec-zone-comp-oci-bootcamp-33	Security Zone	3/4 View
0 selected				

2

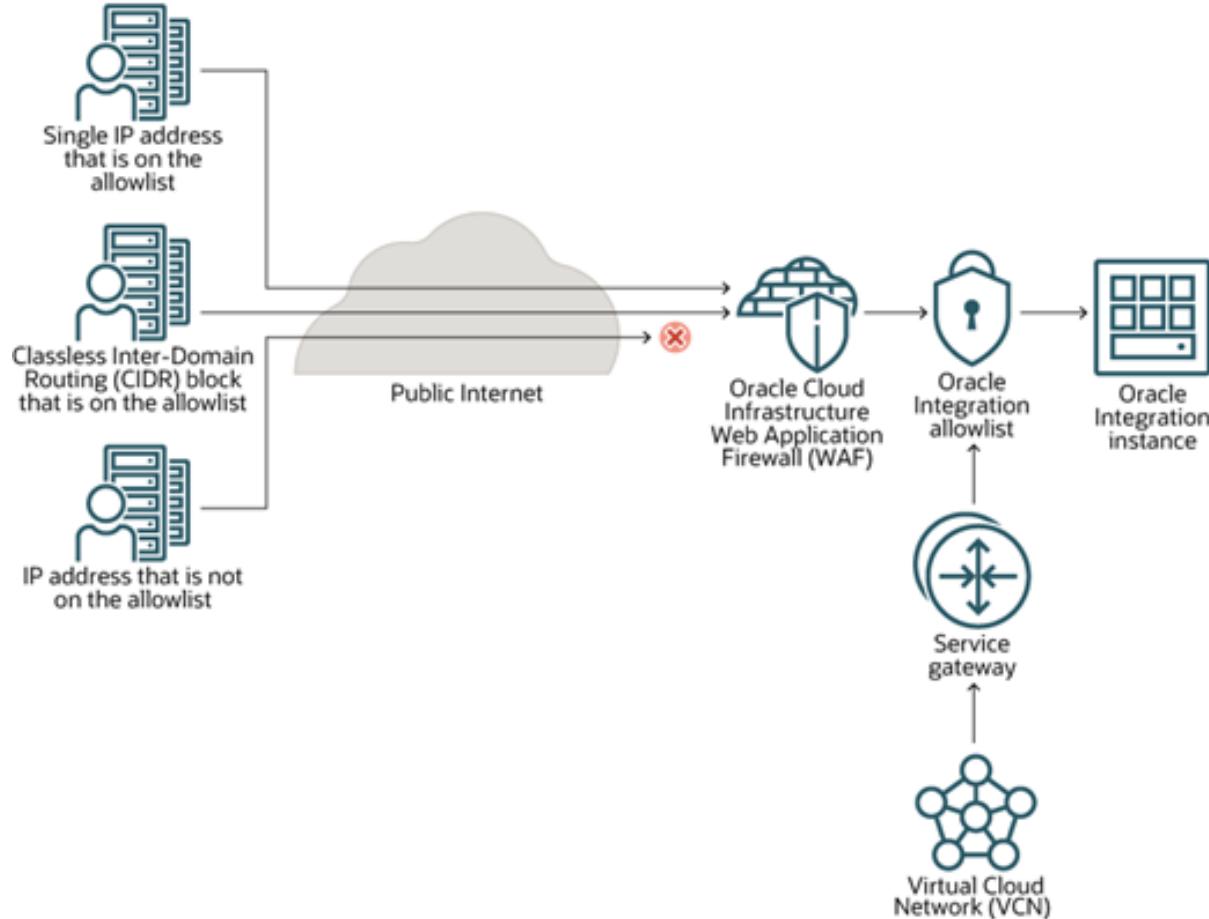
Web Application Firewall

Security for free.

Web Application Firewall WAF

- **Comprehensive Protection:**
 - WAF shields applications from malicious internet traffic and enforces consistent security rules across all applications.
- **Advanced Threat Management:**
 - Create and manage rules to defend against threats like XSS, SQL Injection, and other OWASP-defined vulnerabilities; access rules can limit traffic by geography or request signature.
- **Regional and Edge Solutions:**
 - WAF policies are regional and act as load balancer plug-ins, while edge policies provide global protection; allowlist Oracle nodes for edge enforcement.

Web Application Firewall WAF Architecture



Load Balancer and WAF

- A WAF – Layer 7 - can be configured in front of a load balancer to enforce security
- You can define policies like regions, verify for XSS injections, rate limitations etc.
- Response can be another check or a 401 error

Protection capabilities

Choose protection capabilities Actions ▾

<input type="checkbox"/>	Key	Name	Collaborative	Tags	Action name
<input type="checkbox"/>	942270	SQL Injection (SQLi) Common SQLi attacks for various dbs	No	vendor-oracle, db-oracle, db-mysql, vendor-microsoft, db-mssql, db-postgresql, rdbms, PCI, Request-Body-Inspection, Recommended, OWASP-A1-2017, OWASP-A3-2021, CAPEC-1000, CAPEC-152, CAPEC-248, CAPEC-66, Command Injection, SQL Injection (SQLi), CVE-2023-0875	:
<input type="checkbox"/>	9420000	SQL Injection (SQLi) Collaborative Group - SQLi Filters Categories	Yes	db-mysql, db-mssql, db-mongodb, db-postgresql, db-oracle, db-sqlite, rdbms, nosql, Request-Body-Inspection, PCI, Collaborative, Recommended, OWASP-A1-2017, OWASP-A3-2021, Command Injection, SQL Injection (SQLi), CVE-2023-0630, CVE-2023-0875, CVE-2023-28661, CVE-2023-23488, CVE-2023-23489, CVE-2023-23490, CVE-2023-26325, CVE-2023-28659, CVE-2023-28660, CVE-2023-28662, CVE-2023-28663	:

3

Hands-On Labs

What about the
Database Security?

Hands-On Labs

List of Hands-On Labs

- **Security Zones** – Configure Security Zones to enforce compliance and security policies.
- **Web Application Firewall (WAF)** – Set up and test the Web Application Firewall to protect applications from threats.

5

Wrap-Up

Key Takeaways,
Resources, and Next
Steps

Basics of OCI Security

Foundational Security Features

Key Management

- Centralized control over encryption keys to protect data at rest and in transit.

OS Management

- Simplifies OS updates and patching for enhanced security.

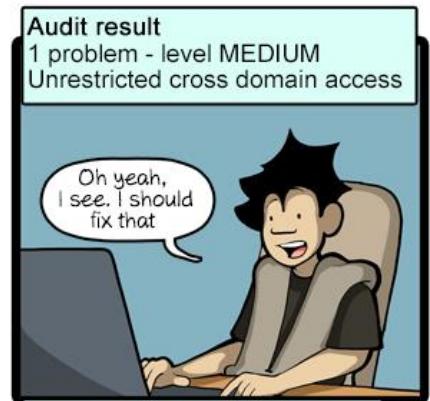
Vulnerability Scanning

- Automated detection of system vulnerabilities to proactively manage risks.

Shielded Instances

- Ensures uncompromised boot security with Secure Boot, Measured Boot, and Trusted Platform Module (TPM).

When I get the results from the security audit



CommitStrip.com

Cloud Guard Overview

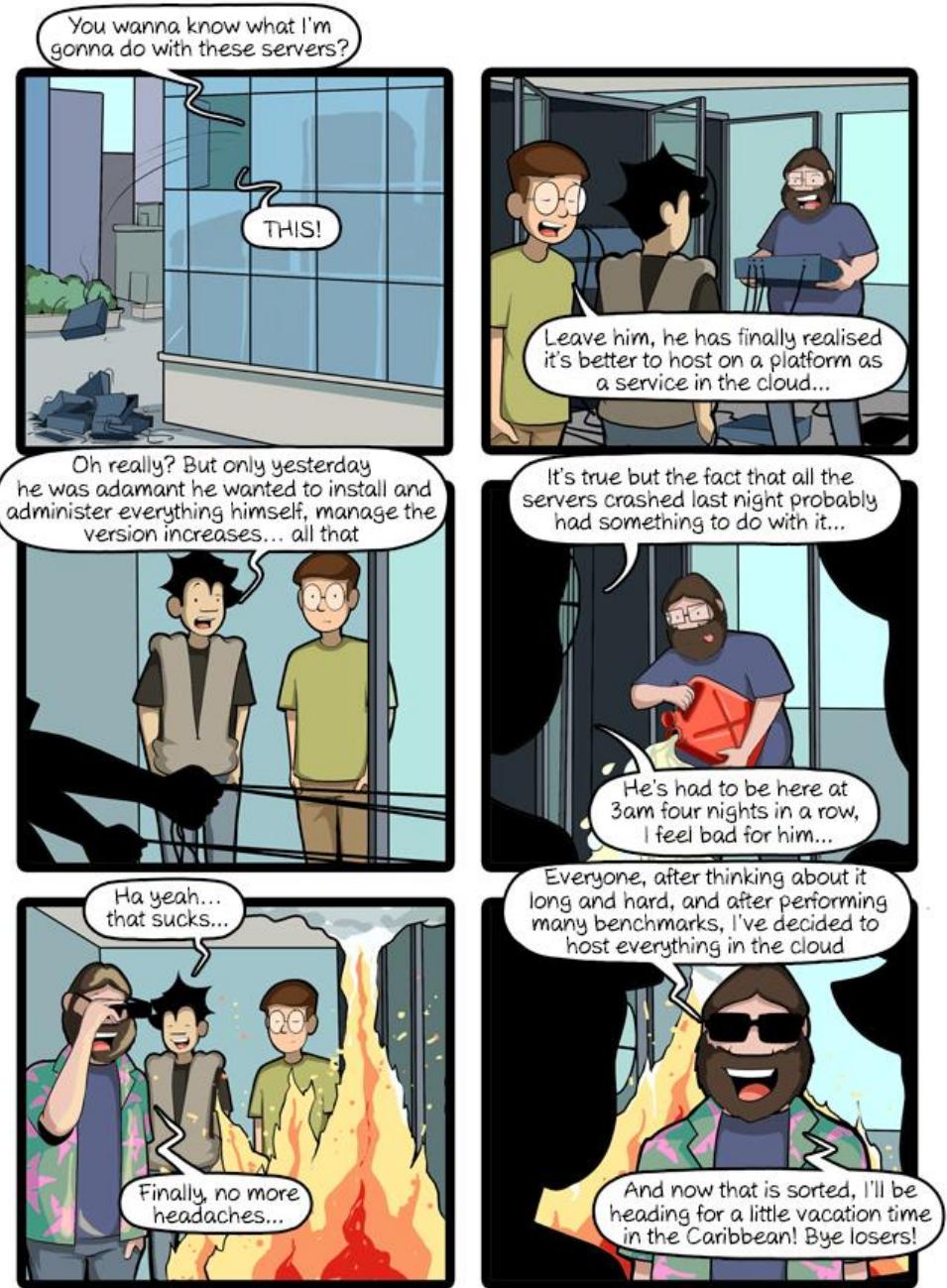
Proactive Threat Monitoring

Key Features

- Detect misconfigurations, vulnerabilities, and anomalous activities.
- Responder recipes for automated remediation of identified risks.
- Centralized monitoring and scoring for better risk management.

Use Case

- Monitor resources like Object Storage, Compute Instances, and Networking.



CommitStrip.com

Enhancing Database Security with Data Safe

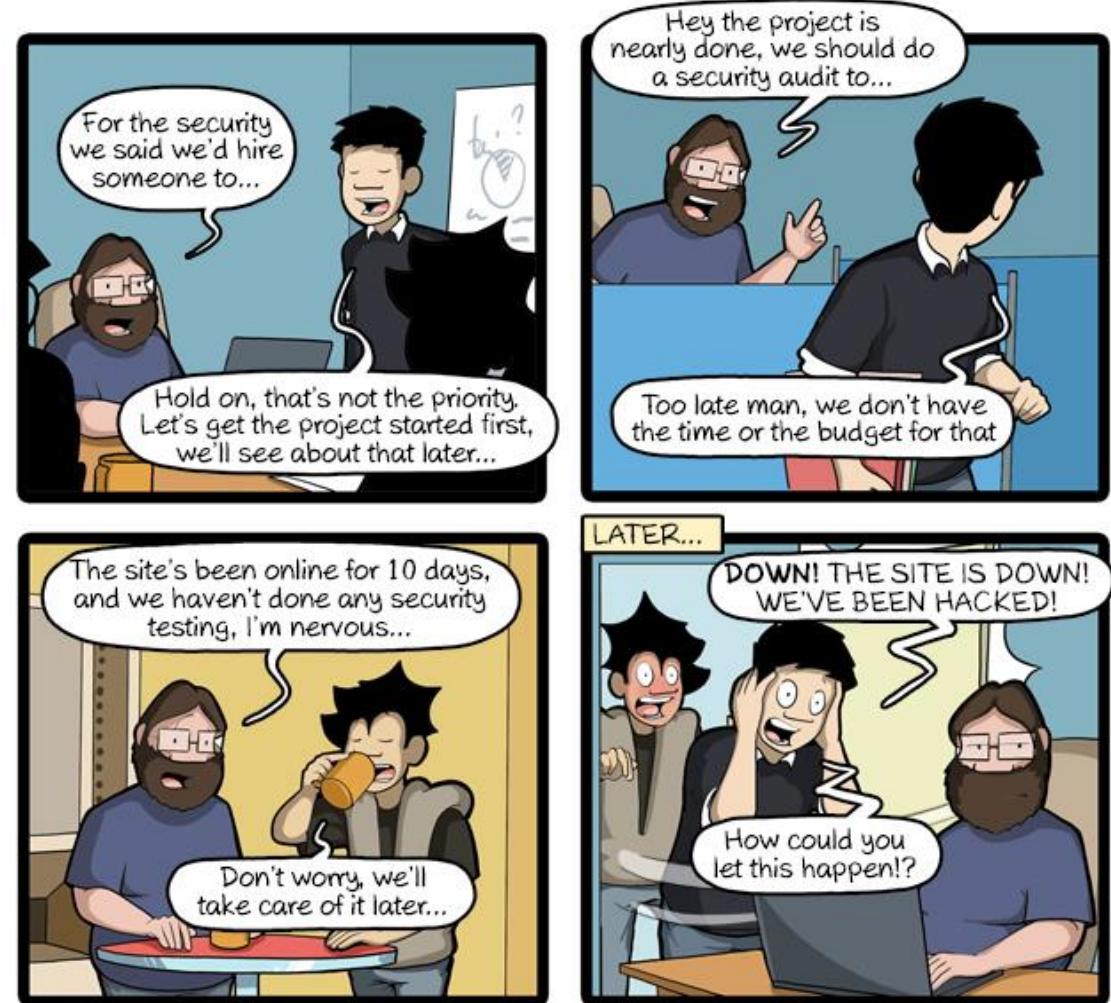
Centralized Database Security Management

Core Capabilities

- **Security Assessment:** Analyze configurations for compliance.
- **User Assessment:** Monitor high-risk users and their actions.
- **Audit Activity:** Comprehensive logs for user actions and compliance.
- **Sensitive Data Discovery:** Locate and classify sensitive data for protection.

Advanced Feature

- SQL Firewall for real-time SQL execution monitoring and restriction.



CommitStrip.com

Security Zones and Wrap-Up

Enforcing and Consolidating Security Policies

Security Zones:

- Enforce strict compliance for OCI resources.
- Block public access, mandate encryption, and ensure regular backups.
- Seamlessly integrate with Cloud Guard for enhanced monitoring.

Overall Takeaways:

- Built-in OCI features simplify complex security challenges.
- Proactive tools like Cloud Guard and Data Safe mitigate risks effectively.
- Security Zones ensure consistent policy enforcement across resources.
- **Next Steps:** Explore hands-on labs to apply these concepts.

OCI Access Information

Resources and Cloud Environment Details

The course materials and exercises are available via the GitHub repository/website:

- OCI Walkthrough: <https://code.oradba.ch/oci-sec-ws>
- PDFs and Course Materials: <https://code.oradba.ch/oci-sec-ws/others>



Thank You

