ORACLE

Oracle Cloud Security Design for Enterprise

Zero Trust-Security of the cloud, on the cloud, and across clouds

Rick Chuang

首席雲端顧問

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Oracle Cloud Infrastructure –
The place for your most critical workloads

Architected with security first

- Secure by design
- Automated, always-on security controls
- Deep expertise in global data protection

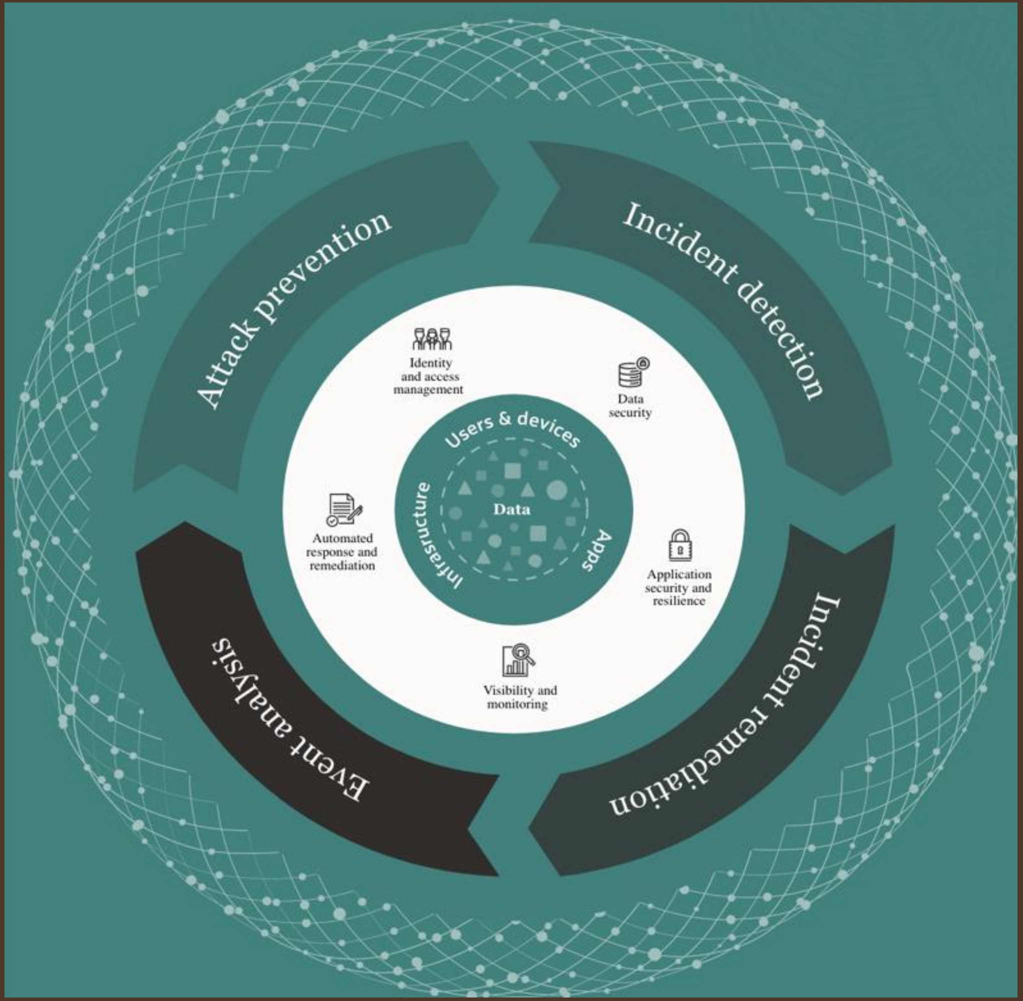
“Oracle Cloud Infrastructure 的設計目標是實現一個安全的平臺，用於執行所有操作。表單。

安全雲很容易說，但很難構建。”

"

Larry Ellison

OCI provides full stack protection for Zero Trust Security


Attack prevention
Incident detection
Incident remediation
Event analysis
Identity and access management
Data security
Application security and resilience
Visibility and monitoring
Automated response and remediation
Users & devices
Infrastructure
Apps
Data

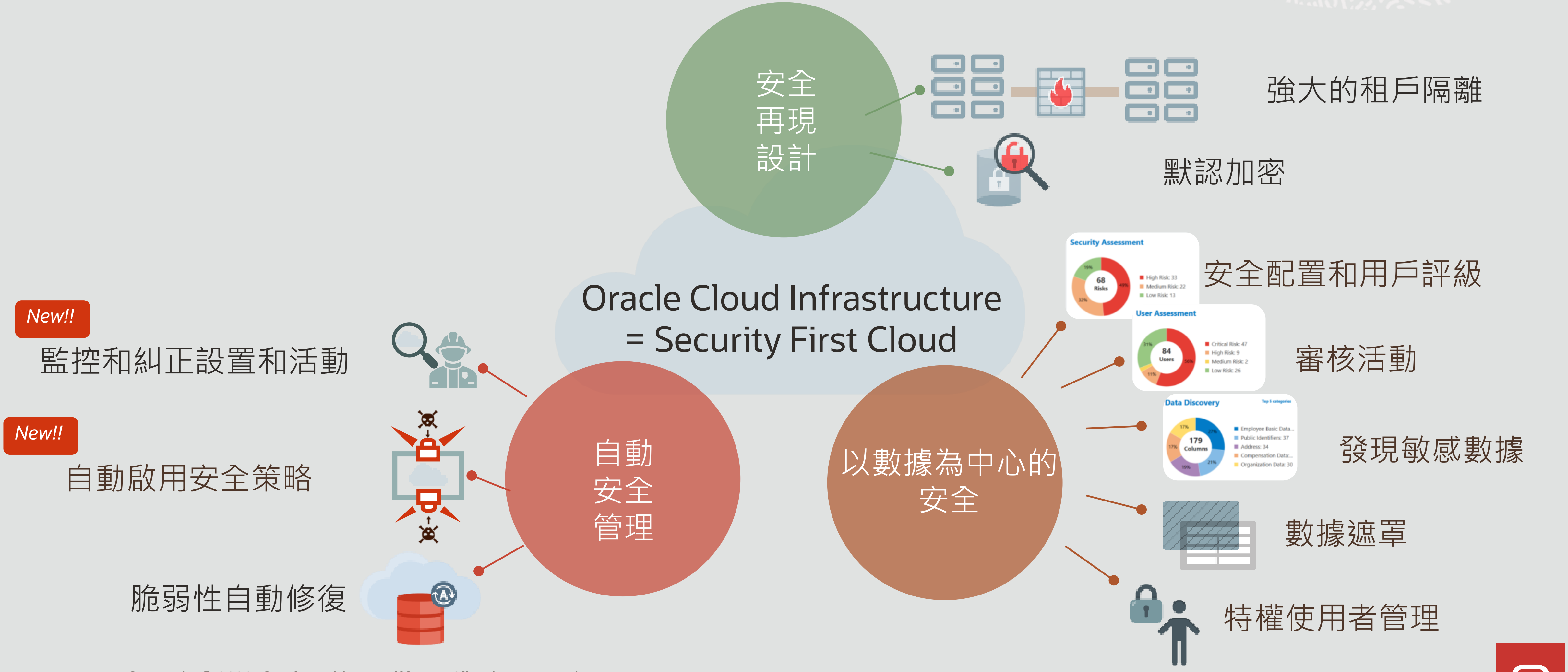
Automated

Always-on

Architected-in

https://www.oracle.com/webfolder/s/assets/ebook/security-first/index.html

安全優先所設計的雲服務
Oracle Cloud Infrastructure



Oracle Cloud Infrastructure
= Security First Cloud

安全
再現
設計

強大的租戶隔離

默認加密

自動
安全
管理

New!!
監控和糾正設置和活動

New!!
自動啟用安全策略

脆弱性自動修復

以數據為中心的
安全

安全配置和用戶評級

審核活動

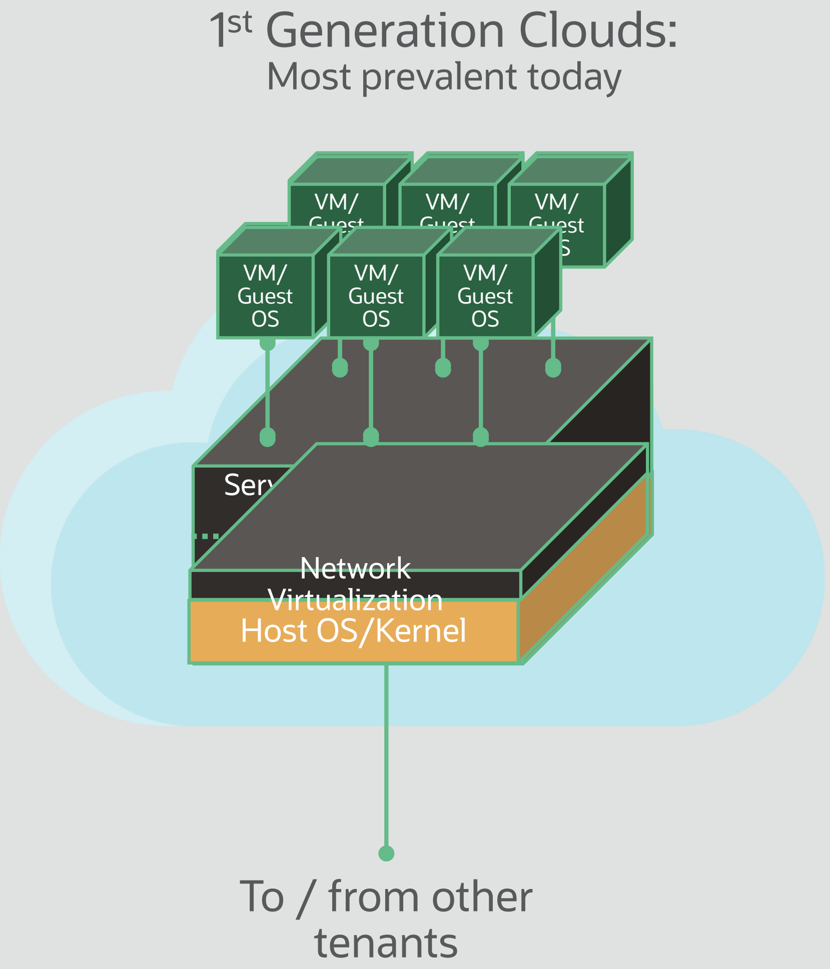
發現敏感數據

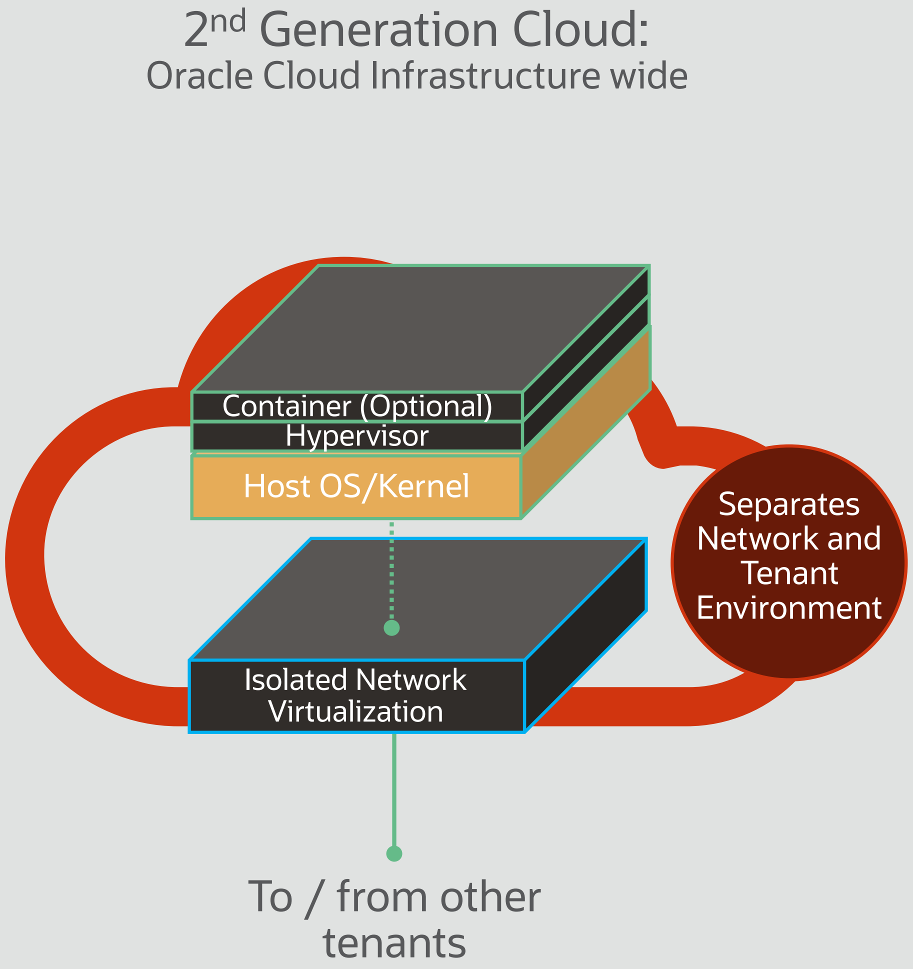
數據遮罩

特權使用者管理

A tale of two clouds

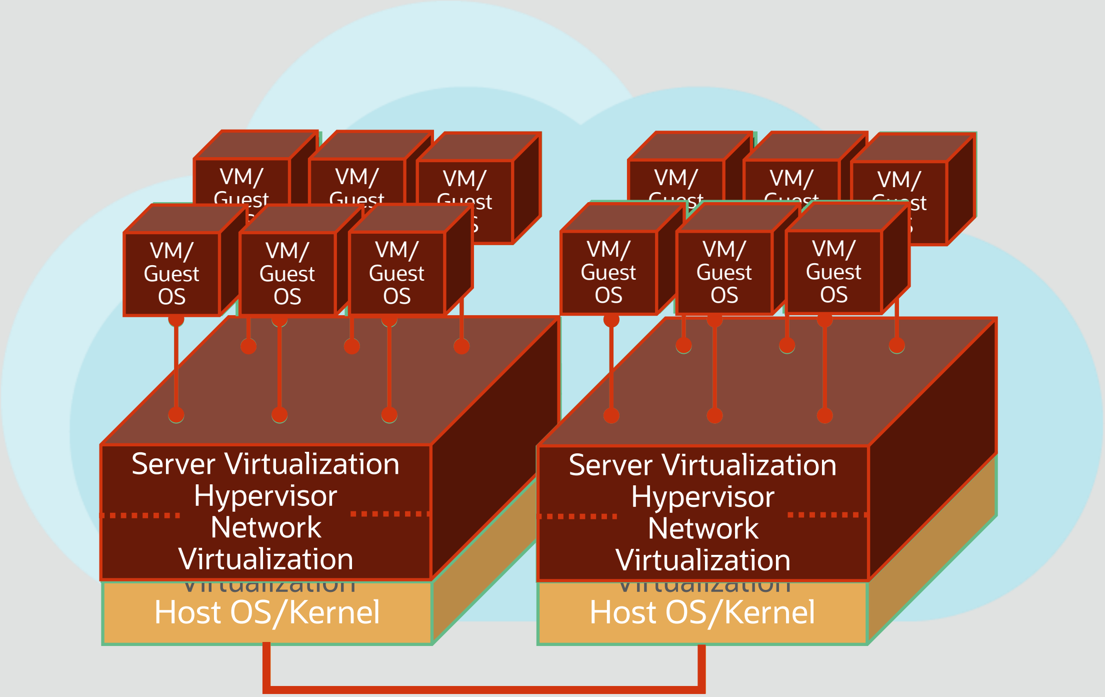
Better protection through isolated network virtualization



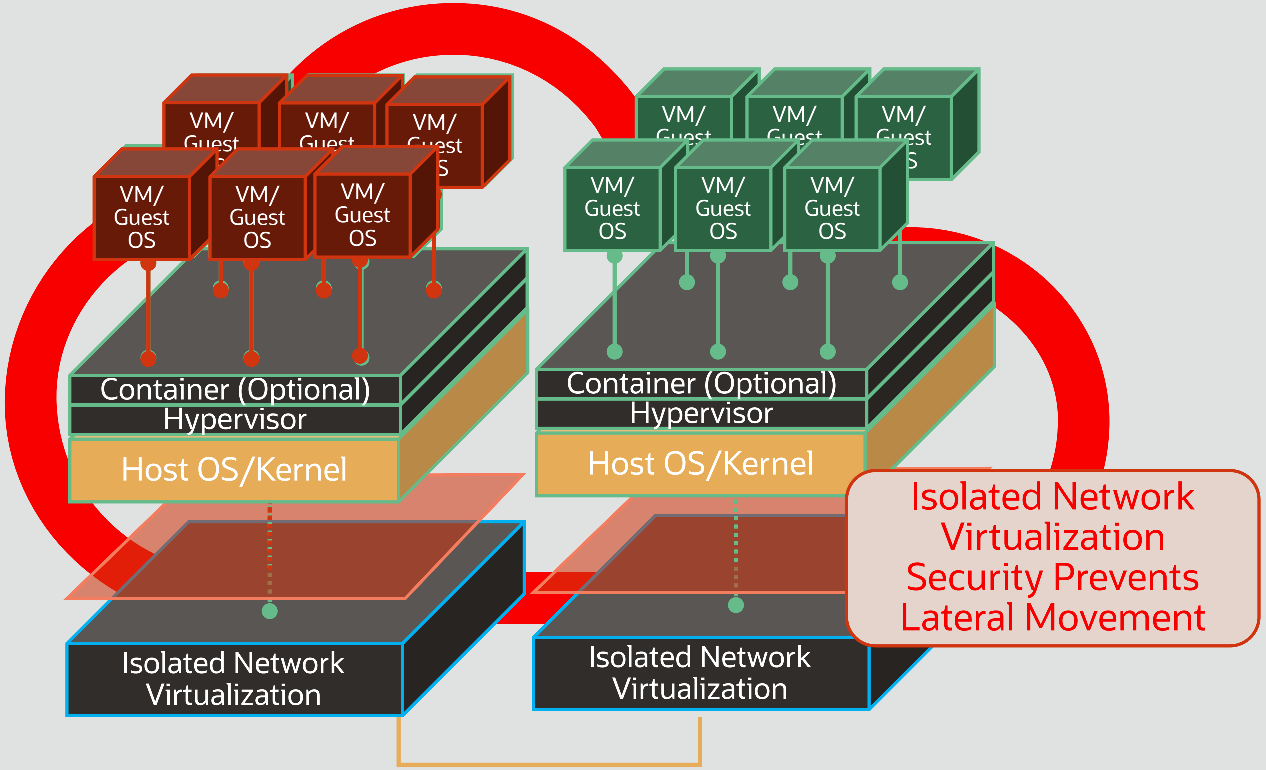

2nd Generation Cloud:
Oracle Cloud Infrastructure wide
Container (Optional)
Hypervisor
Host OS/Kernel
Isolated Network Virtualization
Separates Network and Tenant Environment
To / from other tenants

Isolation: threat containment and reduced risk

1st Generation Cloud

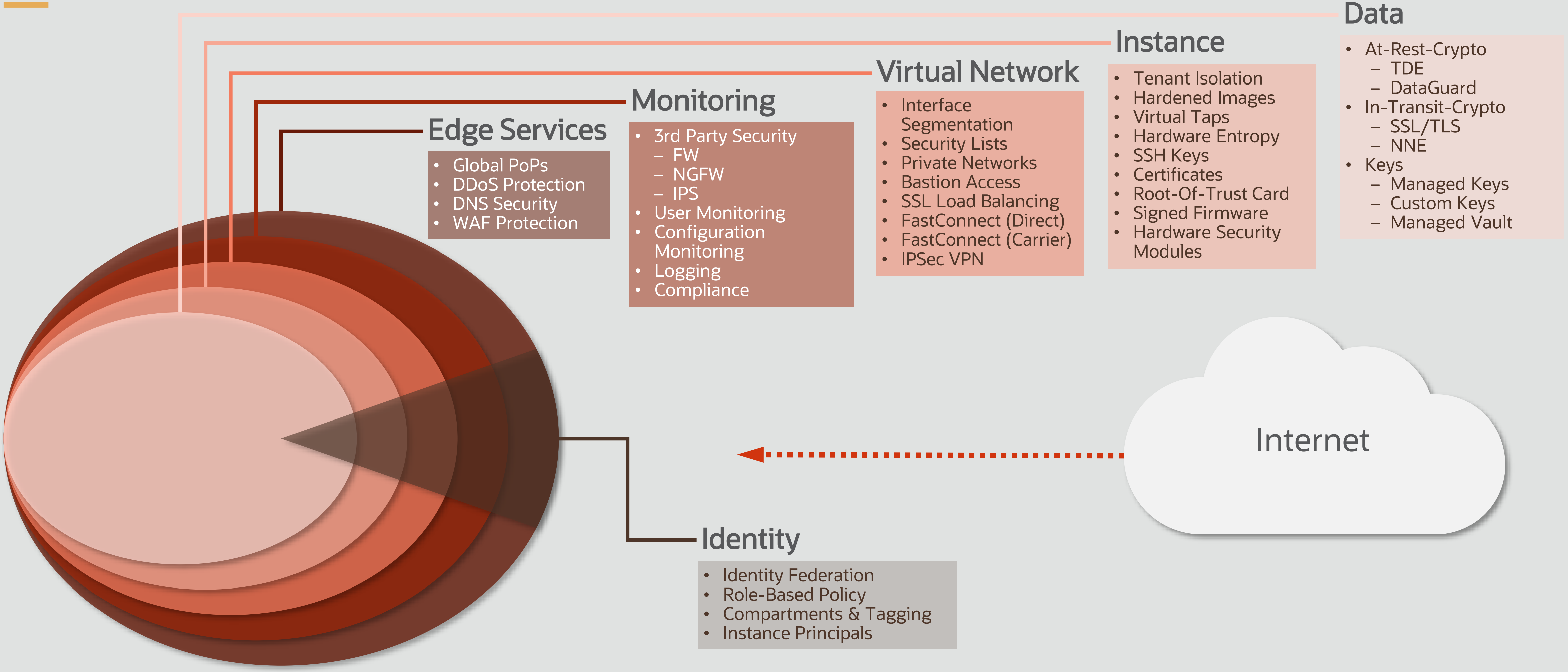


Oracle 2nd Generation Cloud



Isolated Network Virtualization Security Prevents Lateral Movement

Multiple layers of defense in depth



Edge Services

- Global PoPs
- DDoS Protection
- DNS Security
- WAF Protection

Monitoring

- 3rd Party Security
  - FW
  - NGFW
  - IPS
- User Monitoring
- Configuration Monitoring
- Logging
- Compliance

Virtual Network

- Interface Segmentation
- Security Lists
- Private Networks
- Bastion Access
- SSL Load Balancing
- FastConnect (Direct)
- FastConnect (Carrier)
- IPSec VPN

Instance

- Tenant Isolation
- Hardened Images
- Virtual Taps
- Hardware Entropy
- SSH Keys
- Certificates
- Root-Of-Trust Card
- Signed Firmware
- Hardware Security Modules

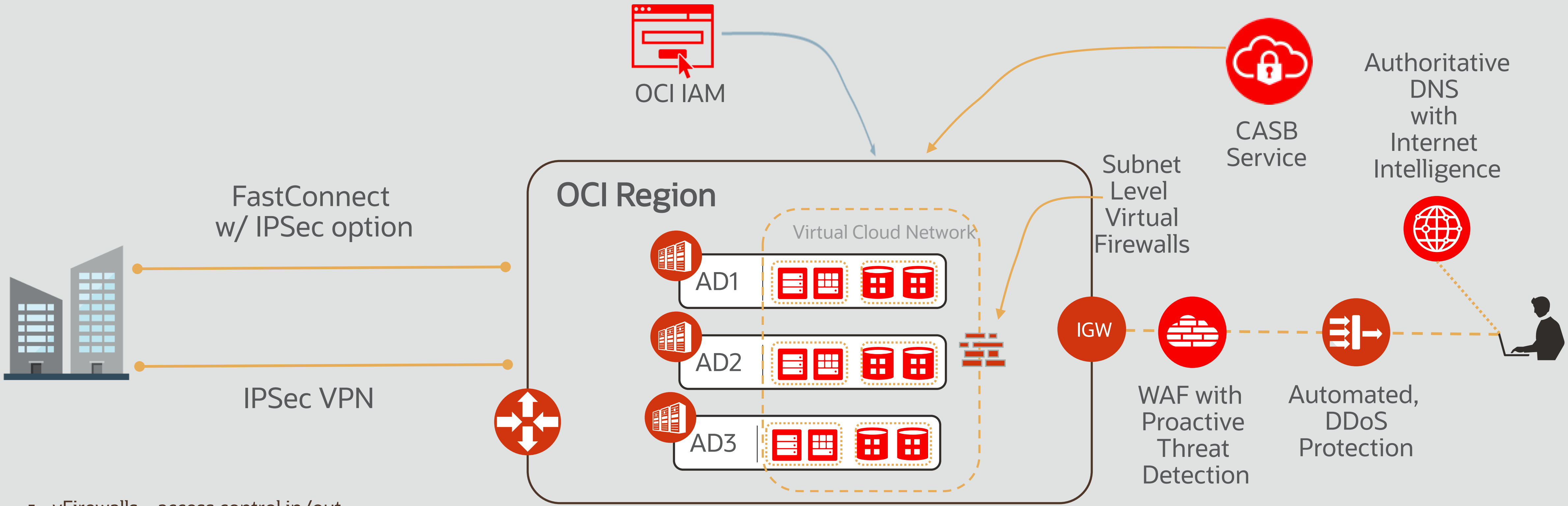
Data

- At-Rest-Crypto
  - TDE
  - DataGuard
- In-Transit-Crypto
  - SSL/TLS
  - NNE
- Keys
  - Managed Keys
  - Custom Keys
  - Managed Vault

Identity

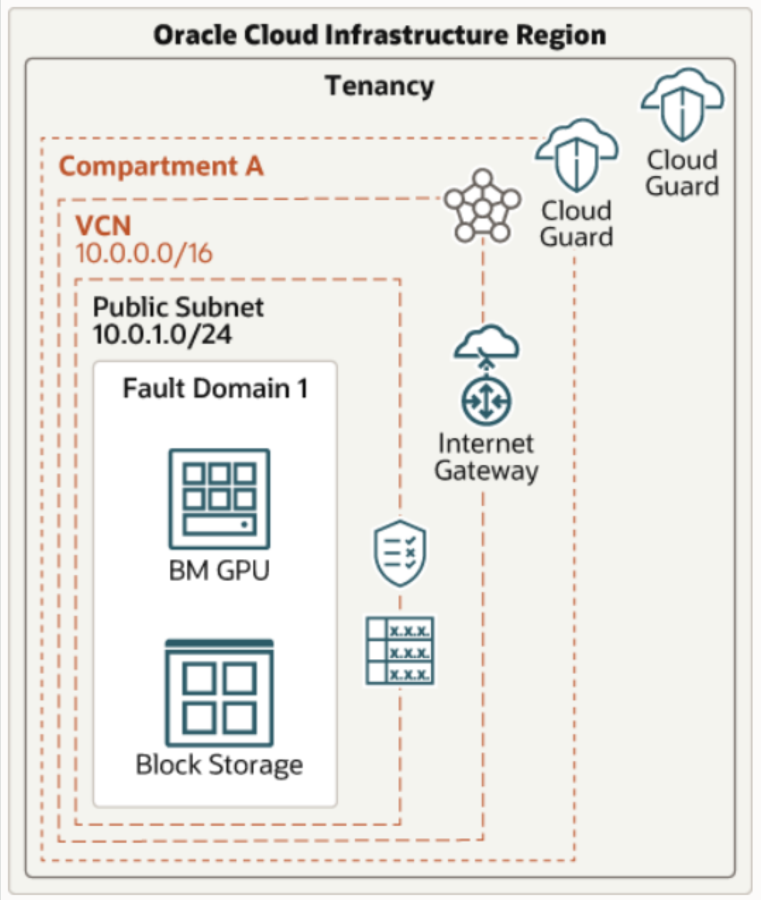
- Identity Federation
- Role-Based Policy
- Compartments & Tagging
- Instance Principals

Advanced control: Defense in-depth and breadth


OCI IAM
CASB Service
Authoritative DNS with Internet Intelligence
FastConnect w/ IPSec option
OCI Region
Virtual Cloud Network
Subnet Level Virtual Firewalls
AD1
AD2
AD3
IPSec VPN
IGW
WAF with Proactive Threat Detection
Automated, DDoS Protection

- vFirewalls – access control in/out
- Distributed Denial of Service (DDoS) – network layer attack protection
- Web Application firewall (WAF) – application layer attack protection
- Cloud Access Security Broker (CASB) – visibility, compliance, control drift alerting
- Virtual Private Network (VPN) – protection/encryption in transit over Internet & private links
- Domain Name Service (DNS) – managed DNS from Oracle for OCI customers
- Identity & Access Management (IAM) – control who can access and manage OCI resources

Key service to protect your environment



區域Oracle Cloud Infrastructure 區域是包含一或多個資料中心 (稱為可用性網域) 的本地化地理區域。

可用性網域可用性網域是區域內獨立的獨立資料中心。每個可用性網域中的實體資源都會與其他可用性網域中的資源隔離，以提供容錯。可用性網域不會共用基礎架構，例如電源、冷卻或內部可用性網域網路。

容錯域容錯域是一組可用網域內的硬體和基礎架構。每個可用網域都有三個具有獨立電源與硬體的容錯域。

虛擬雲端網路 (VCN) 和子網路VCN 是您在 Oracle Cloud Infrastructure 區域中設定的可自訂軟體定義網路。VCN 就像傳統資料中心網路一樣，可讓您完全控制網路環境。VCN 可以有多個非重疊的 CIDR 區塊，供您在建立 VCN 之後變更。您可以將 VCN 區隔為子網路，子網路範圍可設為某個區域或可用網域。

雲端保全您可以使用 Oracle Cloud Guard 來監督及維護您在 Oracle Cloud Infrastructure 中的資源安全。「雲端保全」使用*可定義的偵測器方法*來檢查安全弱點的資源，以及監督操作員和使用者是否有風險活動。

BM GPU/CPU使用裸機 GPU/HPC 資源配置進行硬體輔助分析與其他運算。

區塊儲存將您的應用程式儲存在區塊儲存中。

網路閘道網際網路閘道可讓 VCN 中的公用子網路與公用網際網路之間的流量。

安全清單您可以為每個子網路建立安全規則，以指定子網路中必須允許的來源、目的地以及流量類型。

路由表虛擬路由表包含將流量從子網路路由至 VCN 外部之目的地的規則，通常會透過閘道。

Oracle Cloud Infrastructure和零信任

- OCI 是預設拒絕（連接、身份驗證和使用以拒絕為前提）
- 未經許可，您就無法執行任何操作：安全清單、隔間、策略設置等。

非常安全的地方

Maximum Security Zone

- 始終打開安全設置
  -你不能從"拒絕"中更改它

持續監控安全位置

Cloud Guard

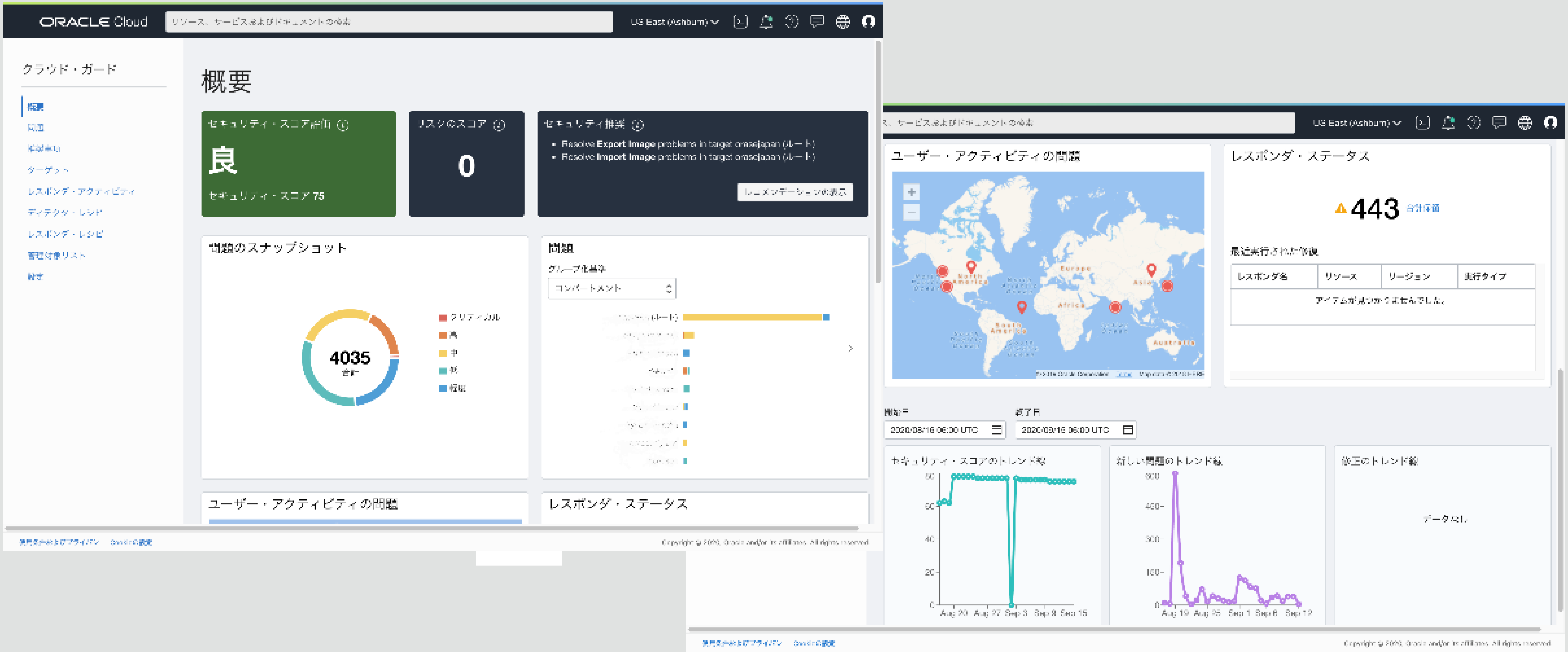
- 自動識別從「拒絕」更改時的問題，根據需要自動糾正

Cloud Guard

Pervasive watch and kill

- Cloud Guard constantly watches and collects data from Audit, Data Safe, OS Management, Logging, and Network Flow Logs services.
  - Gen 1 clouds don’t offer a unified system to collect data from all services.
- Cloud Guard analyzes data, and detects threats and misconfigurations. It can alert you, and better yet, it can kill threats with no human intervention.
  - Gen 1 clouds are only reactive and alert you. You’re left with the hard, slow, and manual task of killing the threat yourself.

Oracle Cloud Guard：儀表板



概要

セキュリティ・スコア評価
良
セキュリティ・スコア 75

リスクのスコア
0

セキュリティ推奨
- Resolve Export Image problems in target omasjapan (ルート)
- Resolve Import Image problems in target omasjapan (ルート)

最近実行された修復

レスポンダ名	リソース	リージョン	実行タイプ
アイテムが見つかりませんでした。			

開始日
2020/08/16 06:00 UTC

終了日
2020/09/16 06:00 UTC

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

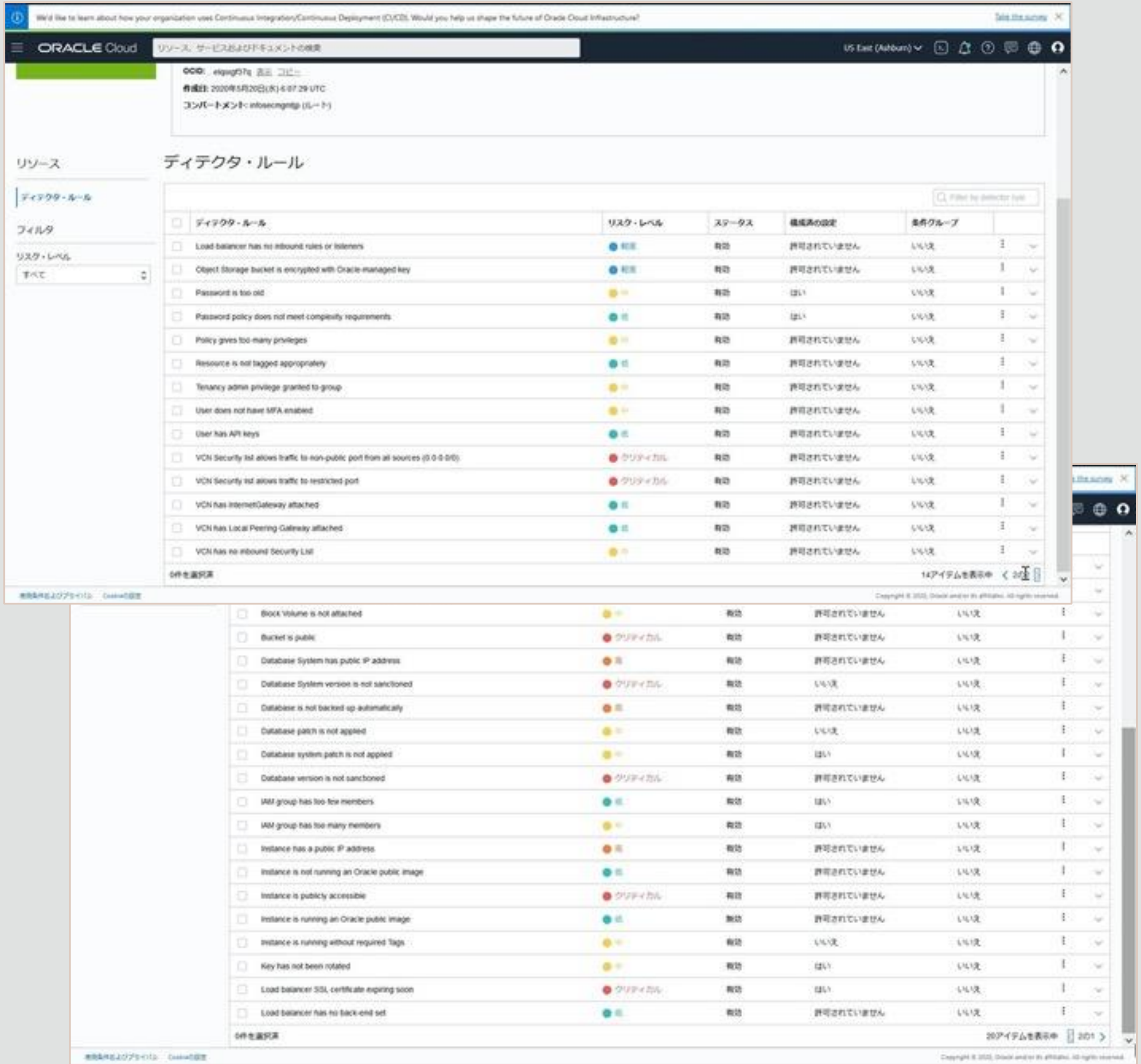
Oracle Cloud Guard檢測內容示例

資料庫：

- ✓ 資料庫備份未自動檢索
- ✓ 資料庫是公共IP
- ✓ 資料庫版本已過期
- ✓

OCI：

- ✓ 存儲更改為公共
- ✓ VCN 已更改
- ✓ 存取遠端存取埠（SSH 等）沒有IP限制
- ✓ 未設定 MFA（多重身份驗證）
- ✓ SSL 在負載均衡器中的驗證即將到期
- ✓



OCID: ...elqsgf37q 表示 コピー
作成日: 2020年5月20日(水) 6:07:29 UTC
コンパートメント: infosecmgmtp (ルート)

ディテクタ・ルール

ディテクタ・ルール	リスク・レベル	ステータス	構成済の設定	条件グループ
Load balancer has no inbound rules or listeners	● 軽度	有効	許可されていません	いいえ
Object Storage bucket is encrypted with Oracle-managed key	● 軽度	有効	許可されていません	いいえ
Password is too old	● 中	有効	はい	いいえ
Password policy does not meet complexity requirements	● 低	有効	はい	いいえ
Policy gives too many privileges	● 中	有効	許可されていません	いいえ
Resource is not tagged appropriately	● 低	有効	許可されていません	いいえ
Tenancy admin privilege granted to group	● 中	有効	許可されていません	いいえ
User does not have MFA enabled	● 中	有効	許可されていません	いいえ
User has API keys	● 低	有効	許可されていません	いいえ
VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0)	● クリティカル	有効	許可されていません	いいえ
VCN Security list allows traffic to restricted port	● クリティカル	有効	許可されていません	いいえ
VCN has InternetGateway attached	● 低	有効	許可されていません	いいえ
VCN has Local Peering Gateway attached	● 低	有効	許可されていません	いいえ
VCN has no inbound Security List	● 中	有効	許可されていません	いいえ

0件を選択済　　14アイテムを表示中

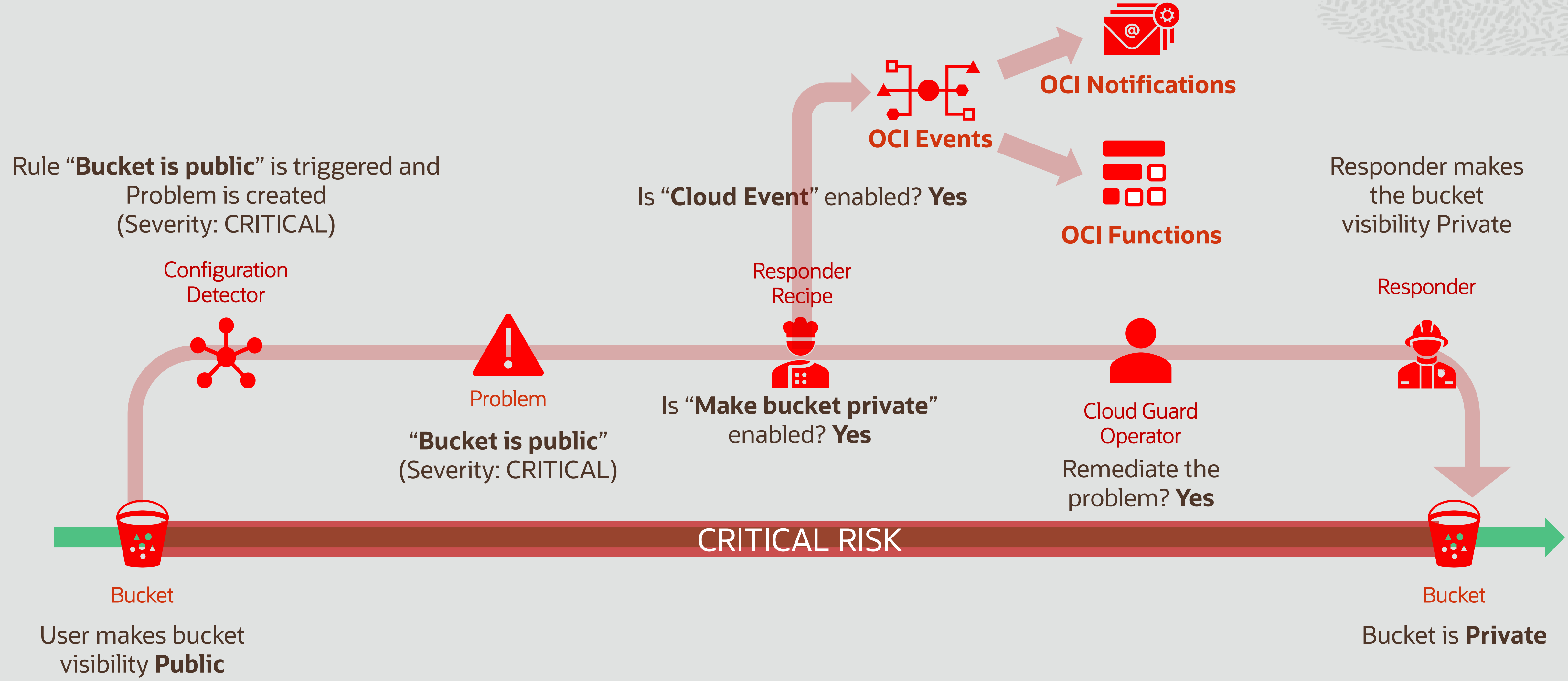
ディテクタ・ルール	リスク・レベル	ステータス	構成済の設定	条件グループ
Block Volume is not attached	● 中	有効	許可されていません	いいえ
Bucket is public	● クリティカル	有効	許可されていません	いいえ
Database System has public IP address	● 高	有効	許可されていません	いいえ
Database System version is not sanctioned	● クリティカル	有効	いいえ	いいえ
Database is not backed up automatically	● 高	有効	許可されていません	いいえ
Database patch is not applied	● 中	有効	いいえ	いいえ
Database system patch is not applied	● 中	有効	はい	いいえ
Database version is not sanctioned	● クリティカル	有効	許可されていません	いいえ
IAM group has too few members	● 低	有効	はい	いいえ
IAM group has too many members	● 中	有効	はい	いいえ
Instance has a public IP address	● 高	有効	許可されていません	いいえ
Instance is not running an Oracle public image	● 低	有効	許可されていません	いいえ
Instance is publicly accessible	● クリティカル	有効	許可されていません	いいえ
Instance is running an Oracle public image	● 低	無効	許可されていません	いいえ
Instance is running without required Tags	● 中	有効	いいえ	いいえ
Key has not been rotated	● 中	有効	はい	いいえ
Load balancer SSL certificate expiring soon	● クリティカル	有効	はい	いいえ
Load balancer has no back-end set	● 低	有効	許可されていません	いいえ

0件を選択済　　20アイテムを表示中　2の1

Where does Cloud Guard help?

Can I get a view of my security posture globally?	✓ Yes, you can monitor and detect issues across global OCI tenancy of compartments and resources.
How do I identify problems for my newly created resources?	✓ Cloud Guard can be applied to your root compartment and inherit every child compartment and resource.
Do I need to create or manage my own security policies?	✓ Cloud Guard has OOTB and customizable configurations to address many common security concerns.
How do I integrate with external SIEM based tools?	✓ Cloud Guard is part of OCI and allows integrates with Events, Notifications, and Functions to provide robust extensibility.

Scenario: Public Bucket



Rule “**Bucket is public**” is triggered and Problem is created (Severity: CRITICAL)

Configuration Detector

Problem

“**Bucket is public**” (Severity: CRITICAL)

Is “**Cloud Event**” enabled? **Yes**

Responder Recipe

Is “**Make bucket private**” enabled? **Yes**

OCI Events

OCI Notifications

OCI Functions

Cloud Guard Operator

Remediate the problem? **Yes**

Responder makes the bucket visibility Private

Responder

CRITICAL RISK

Bucket

User makes bucket visibility **Public**

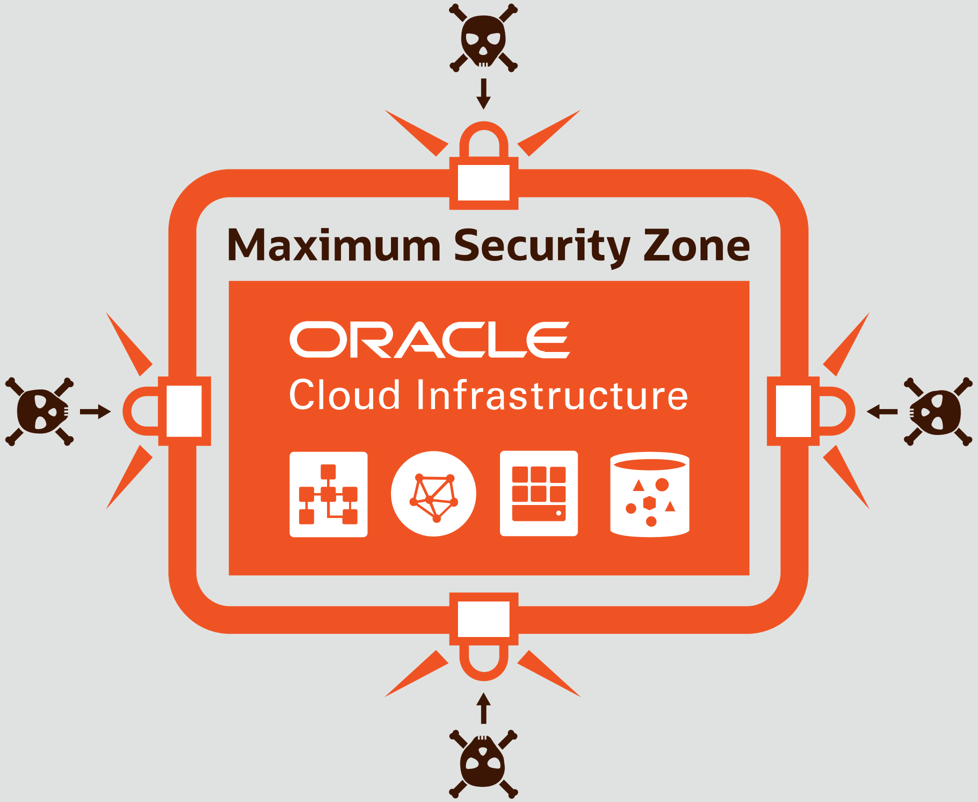
Bucket

Bucket is **Private**

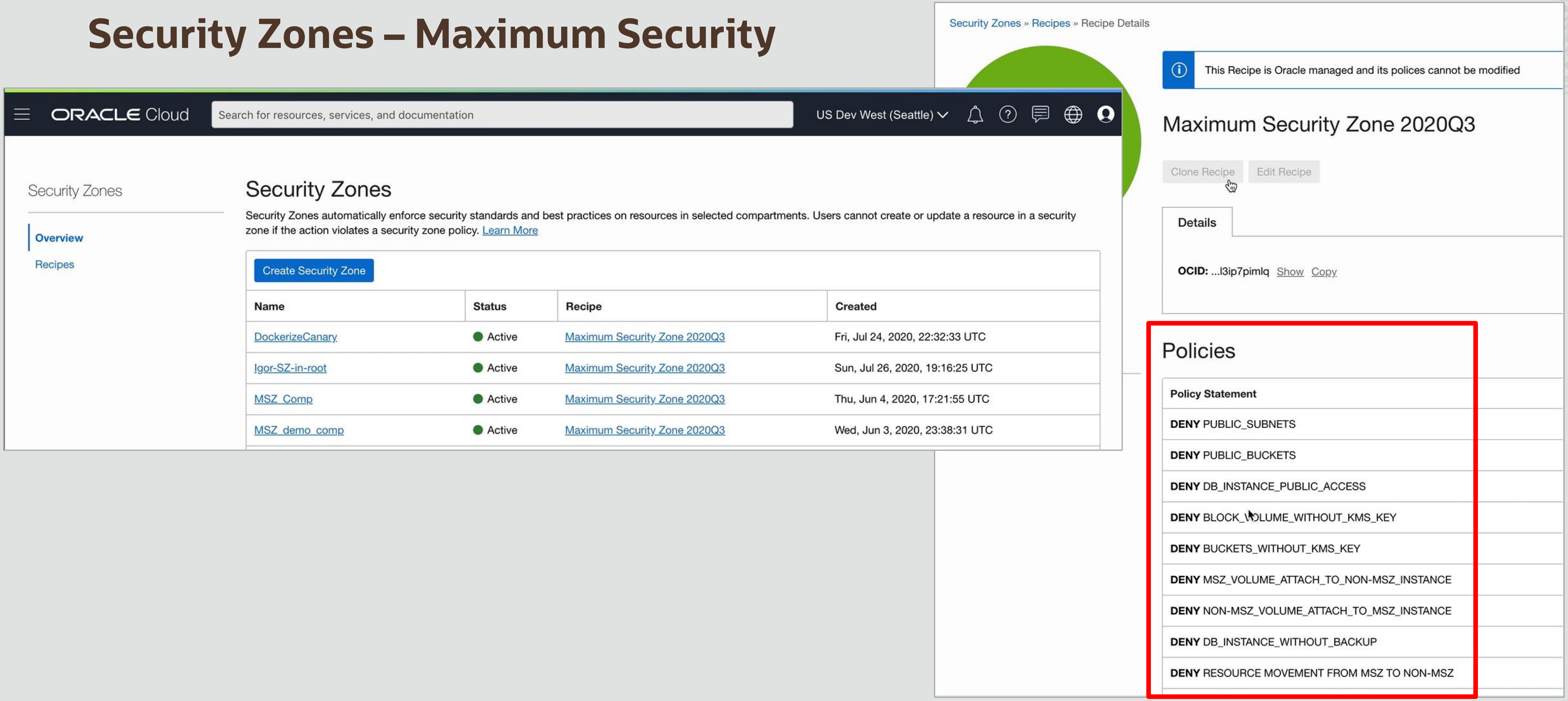
Maximum security zones

Maximum security can be easy and always on

- Oracle Maximum Security Zone is a zone within your environment where security is not a choice. It's always on.
- Resources launched in this zone will be on dedicated infrastructure with the highest levels of data encryption and network security.
- Gen 1 clouds offer a long list of security tools that are extremely complex to set up, and very easy to screw up.



Security Zones – Maximum Security



Security Zones

Security Zones automatically enforce security standards and best practices on resources in selected compartments. Users cannot create or update a resource in a security zone if the action violates a security zone policy. Learn More

Name	Status	Recipe	Created
DockerizeCanary	● Active	Maximum Security Zone 2020Q3	Fri, Jul 24, 2020, 22:32:33 UTC
Igor-SZ-in-root	● Active	Maximum Security Zone 2020Q3	Sun, Jul 26, 2020, 19:16:25 UTC
MSZ_Comp	● Active	Maximum Security Zone 2020Q3	Thu, Jun 4, 2020, 17:21:55 UTC
MSZ_demo_comp	● Active	Maximum Security Zone 2020Q3	Wed, Jun 3, 2020, 23:38:31 UTC

This Recipe is Oracle managed and its polices cannot be modified

Maximum Security Zone 2020Q3

OCID: ...l3ip7pimlq Show Copy

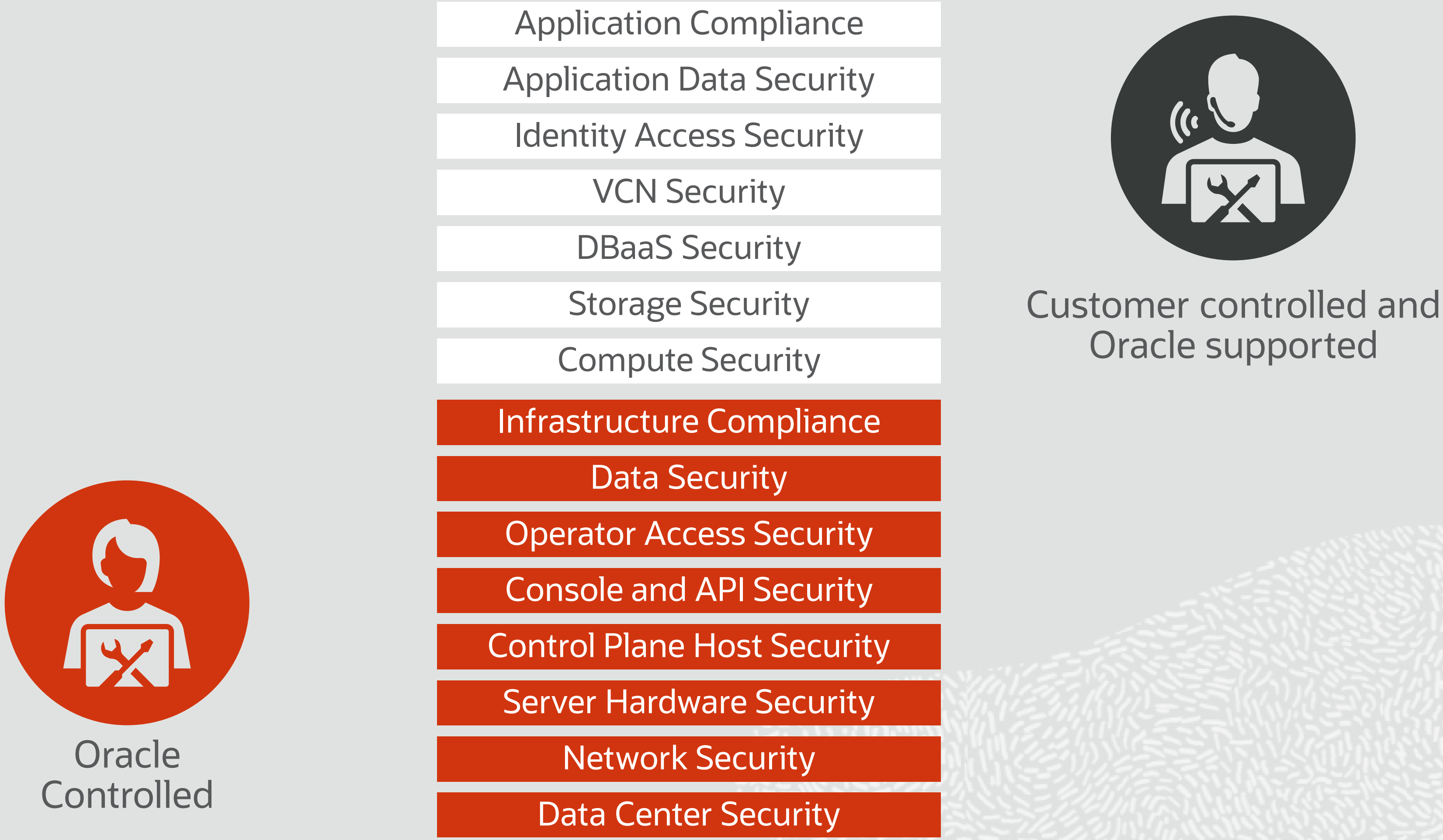
Policies

Policy Statement
DENY PUBLIC_SUBNETS
DENY PUBLIC_BUCKETS
DENY DB_INSTANCE_PUBLIC_ACCESS
DENY BLOCK_VOLUME_WITHOUT_KMS_KEY
DENY BUCKETS_WITHOUT_KMS_KEY
DENY MSZ_VOLUME_ATTACH_TO_NON-MSZ_INSTANCE
DENY NON-MSZ_VOLUME_ATTACH_TO_MSZ_INSTANCE
DENY DB_INSTANCE_WITHOUT_BACKUP
DENY RESOURCE MOVEMENT FROM MSZ TO NON-MSZ

OCI compliance: Current audit programs

Global	SOC 1 : SOC 2 : SOC 3	27001 : 27017 : 27018	Self-Assessment	US Privacy Shield		
Government	DoD DISA SRG IL2	Moderate – Agency ATO	VPAT – Section 508	G-Cloud 11 - UK	Model Clauses - EU	
Industry	HIPAA	PCI DSS	FISC - Japan	IG Toolkit - UK		
Regional	GDPR - EU	BSI C5 - Germany	TISAX - Germany	PIPEDA - Canada	Cyber Essentials Plus - UK	My Number - Japan	Cloud Security Principles - UK

Shared responsibility and how we differ



Application Compliance

Application Data Security

Identity Access Security

VCN Security

DBaaS Security

Storage Security

Compute Security

Customer controlled and Oracle supported

Infrastructure Compliance

Data Security

Operator Access Security

Console and API Security

Control Plane Host Security

Server Hardware Security

Network Security

Data Center Security

Oracle Controlled

ZTS is NOT a product or a checkbox!

It is a multi-phased approach that takes time, effort, and investment to adopt.

OCI can accelerate your ZTS journey!

Summary

- OCI has security architected-in from the ground up using security-first design principles
- OCI provides always-on security to help secure our customer’s data
- Oracle is taking more responsibility for security through automated services and embedded expertise

Network-centric

Services-centric

Identity-centric

https://www.oracle.com/security/what-is-zero-trust/

ORACLE