ORACLE

Oracle Cloud Infrastructure

Security in the cloud

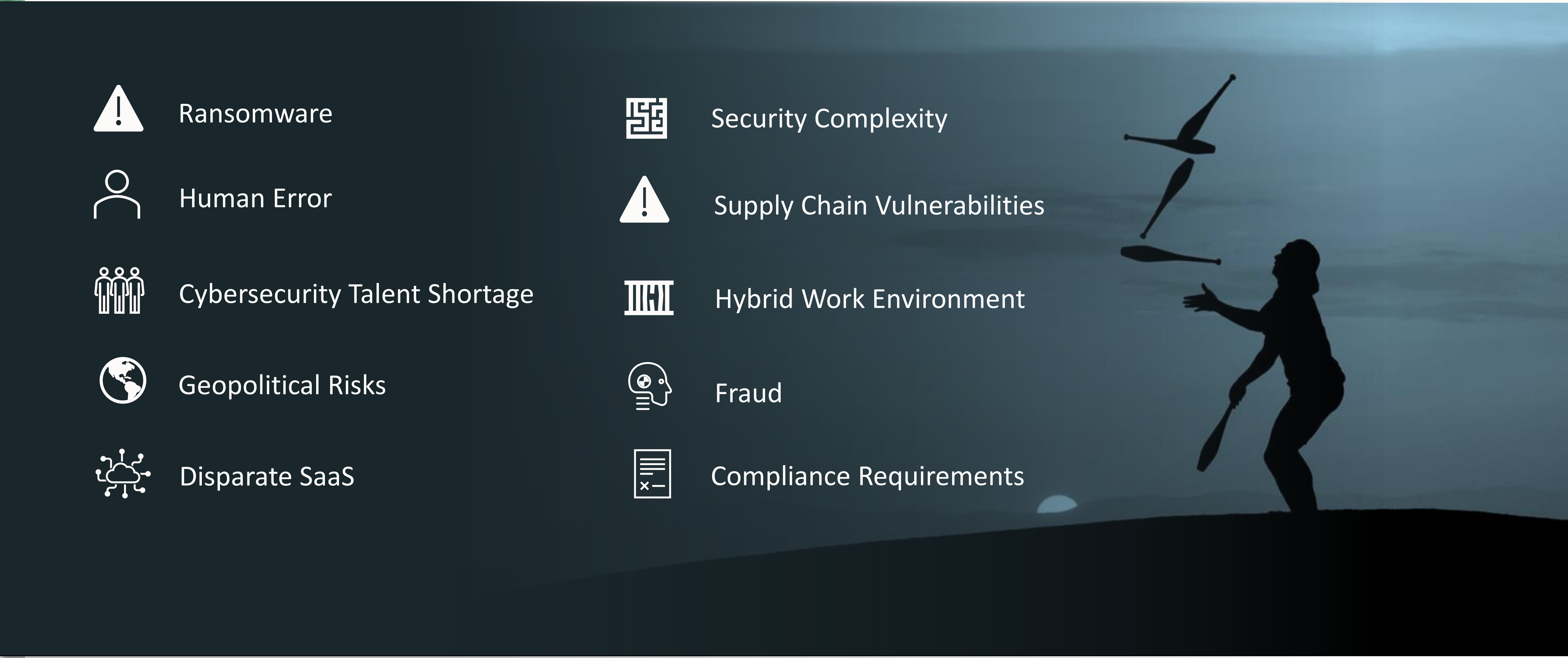
Chad Russell

Field CISO

North America Cloud Infrastructure Engineering (NACI-E)

Statements in this presentation relating to Oracle’s future plans, expectations, beliefs, intentions, and prospects are “forward-looking statements” and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle’s Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading “Risk Factors.” These filings are available on the SEC’s website or on Oracle’s website at http://www.oracle.com/investor. All information in this presentation is current as of October 24, 2023 and Oracle undertakes no duty to update any statement in light of new information or future events.

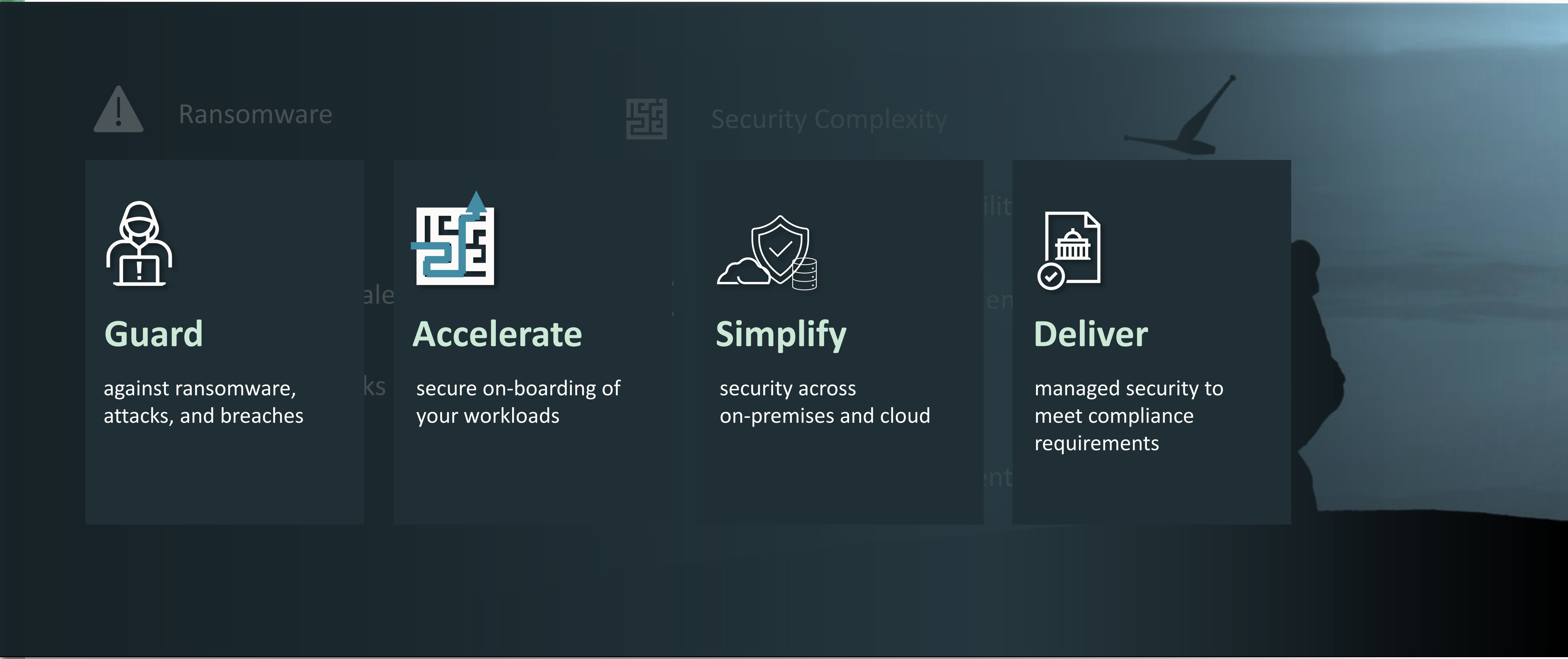
Top enterprise security concerns



- Ransomware
- Human Error
- Cybersecurity Talent Shortage
- Geopolitical Risks
- Disparate SaaS

- Security Complexity
- Supply Chain Vulnerabilities
- Hybrid Work Environment
- Fraud
- Compliance Requirements

Oracle Security helps address top security concerns



Ransomware

Security Complexity

Guard

against ransomware, attacks, and breaches

Accelerate

secure on-boarding of your workloads

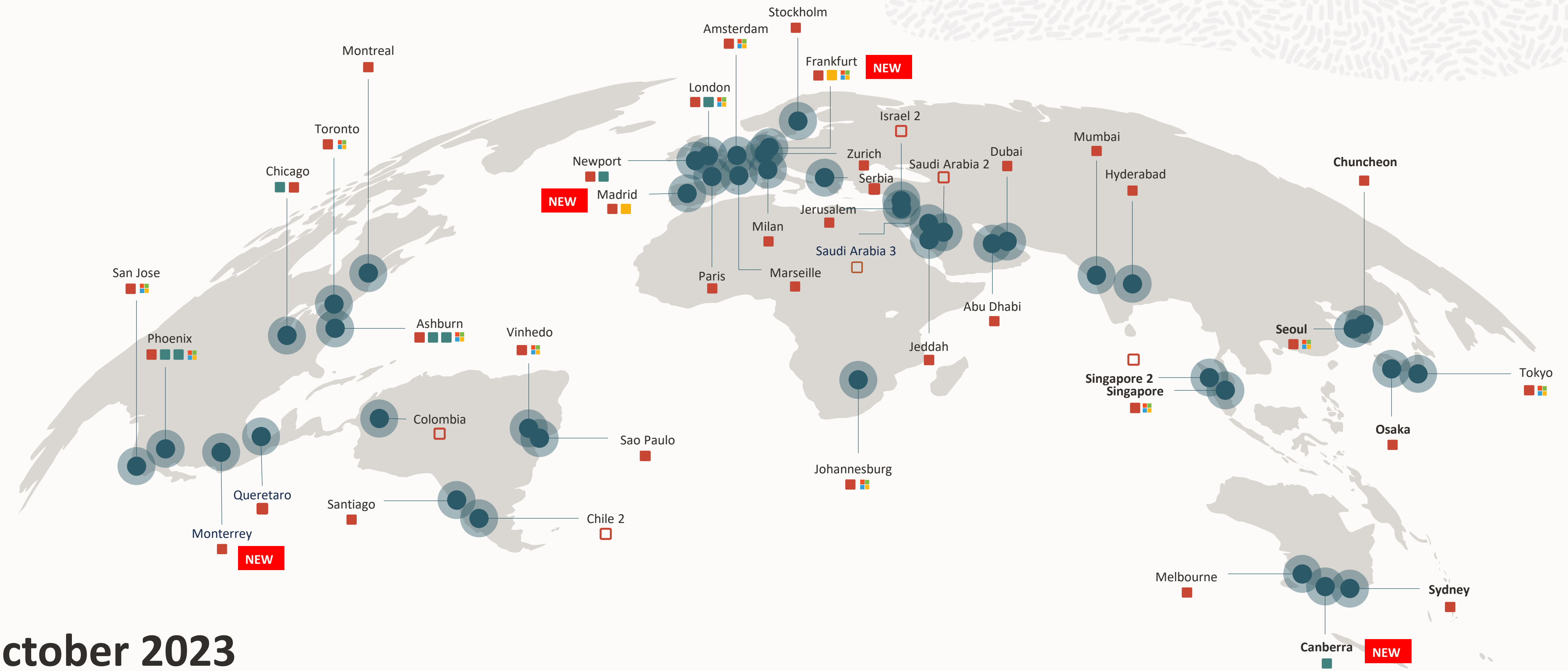
Simplify

security across on-premises and cloud

Deliver

managed security to meet compliance requirements

Oracle Cloud Infrastructure Global Footprint



🟥 Commercial

□ Commercial Planned

🟨 Sovereign

🟩 Government

⊞ Microsoft Interconnect Azure

October 2023

46 regions; 6 more planned

12 Azure Interconnect Regions

Cloud Shared Responsibility Model

🔴 Customer Responsibility

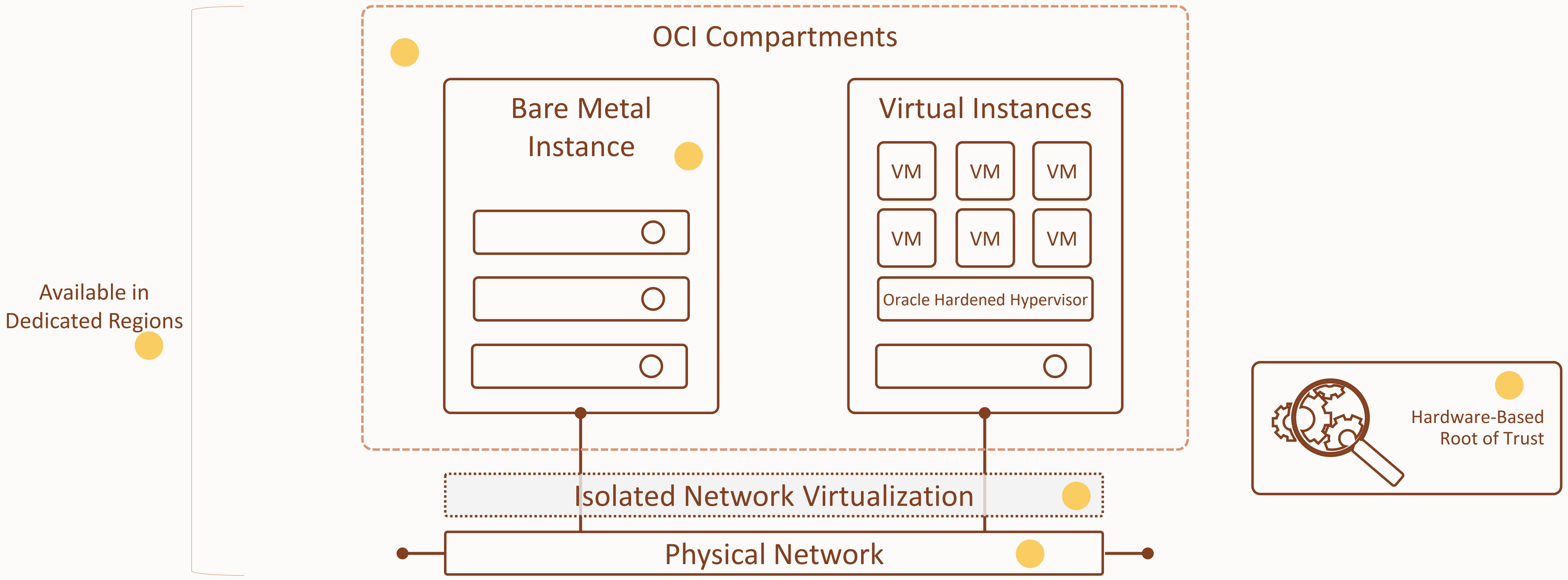
🔵 Cloud Service Provider Responsibility

On-premises	IaaS (Infrastructure-as-a-Service)	PaaS (Platform-as-a-Service)	SaaS (Software-as-a-Service)
🔴 User Access/Identity	🔴 User Access/Identity	🔴 User Access/Identity	🔴 User Access/Identity
🔴 Data	🔴 Data	🔴 Data	🔴 Data
🔴 Application	🔴 Application	🔴 Application	🔵 Application
🔴 Guest OS	🔴 Guest OS	🔵 Guest OS	🔵 Guest OS
🔴 Virtualization	🔵 Virtualization	🔵 Virtualization	🔵 Virtualization
🔴 Network	🔵 Network	🔵 Network	🔵 Network
🔴 Infrastructure	🔵 Infrastructure	🔵 Infrastructure	🔵 Infrastructure
🔴 Physical	🔵 Physical	🔵 Physical	🔵 Physical

Highly Secure Cloud Architecture

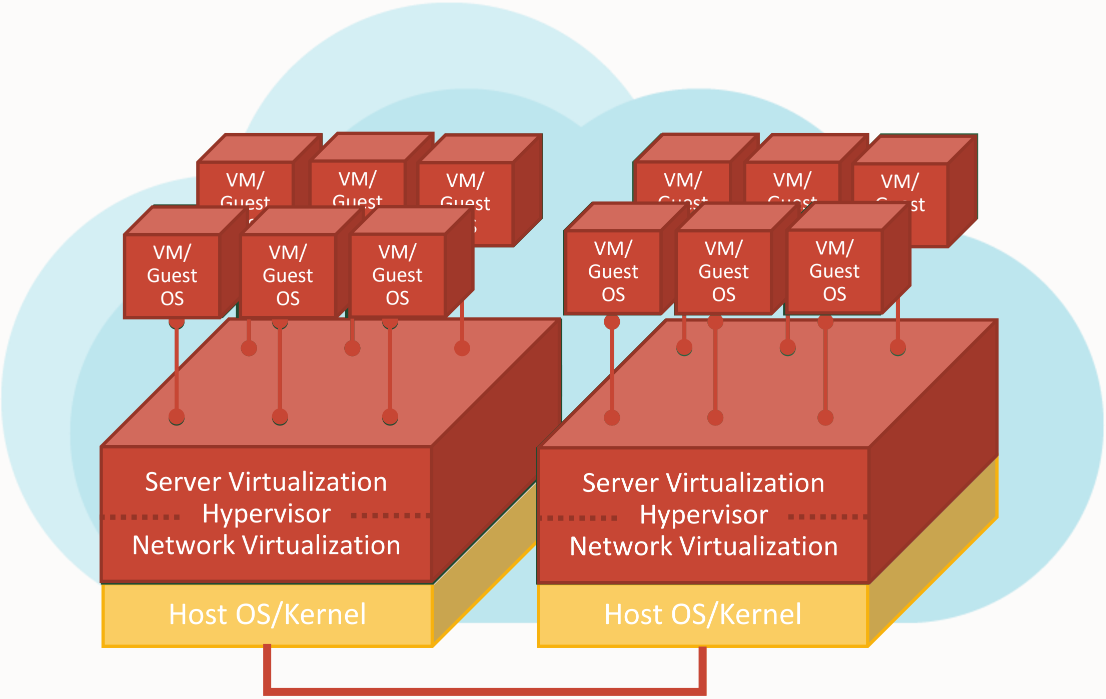
OCI Shielded Instances

OCI Confidential Compute

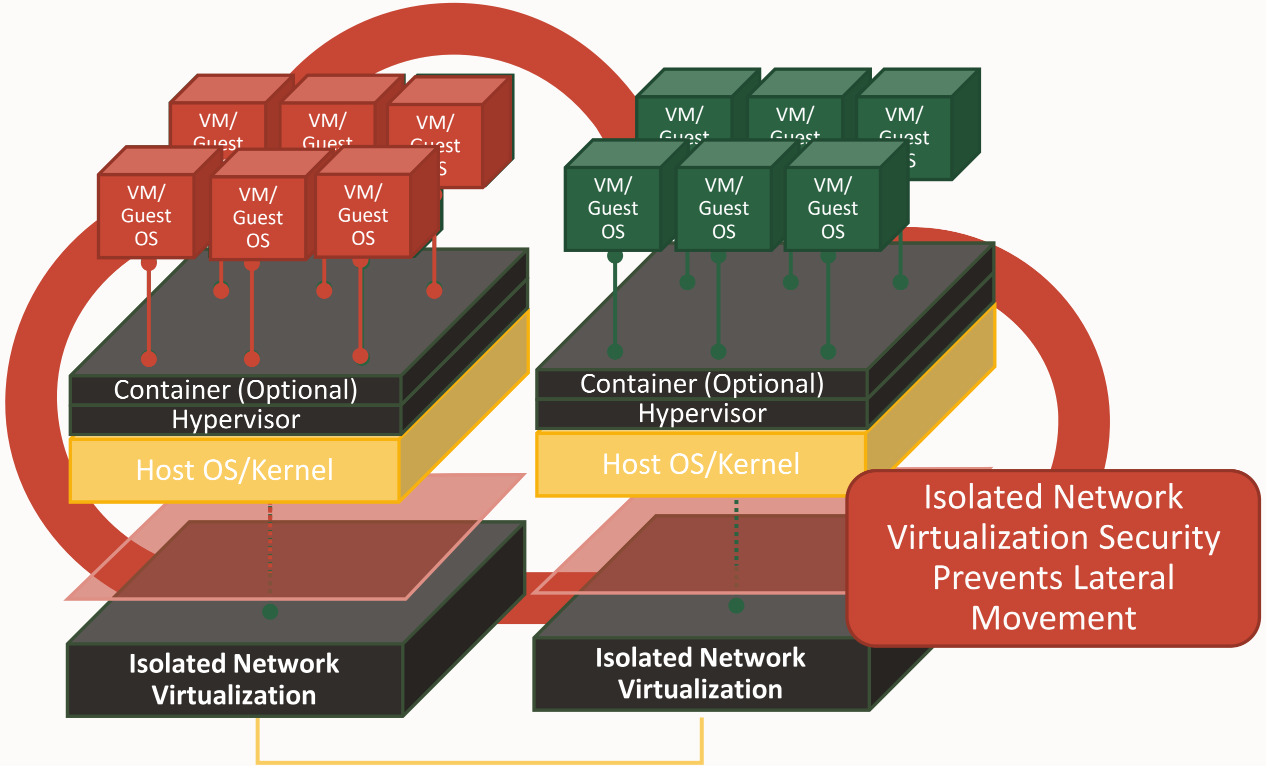

OCI Compartments
Bare Metal Instance
Virtual Instances
VM
VM
VM
VM
VM
VM
Oracle Hardened Hypervisor
Available in Dedicated Regions
Isolated Network Virtualization
Physical Network
Hardware-Based Root of Trust

Threat Containment & Reduced Risk

1st Generation Cloud

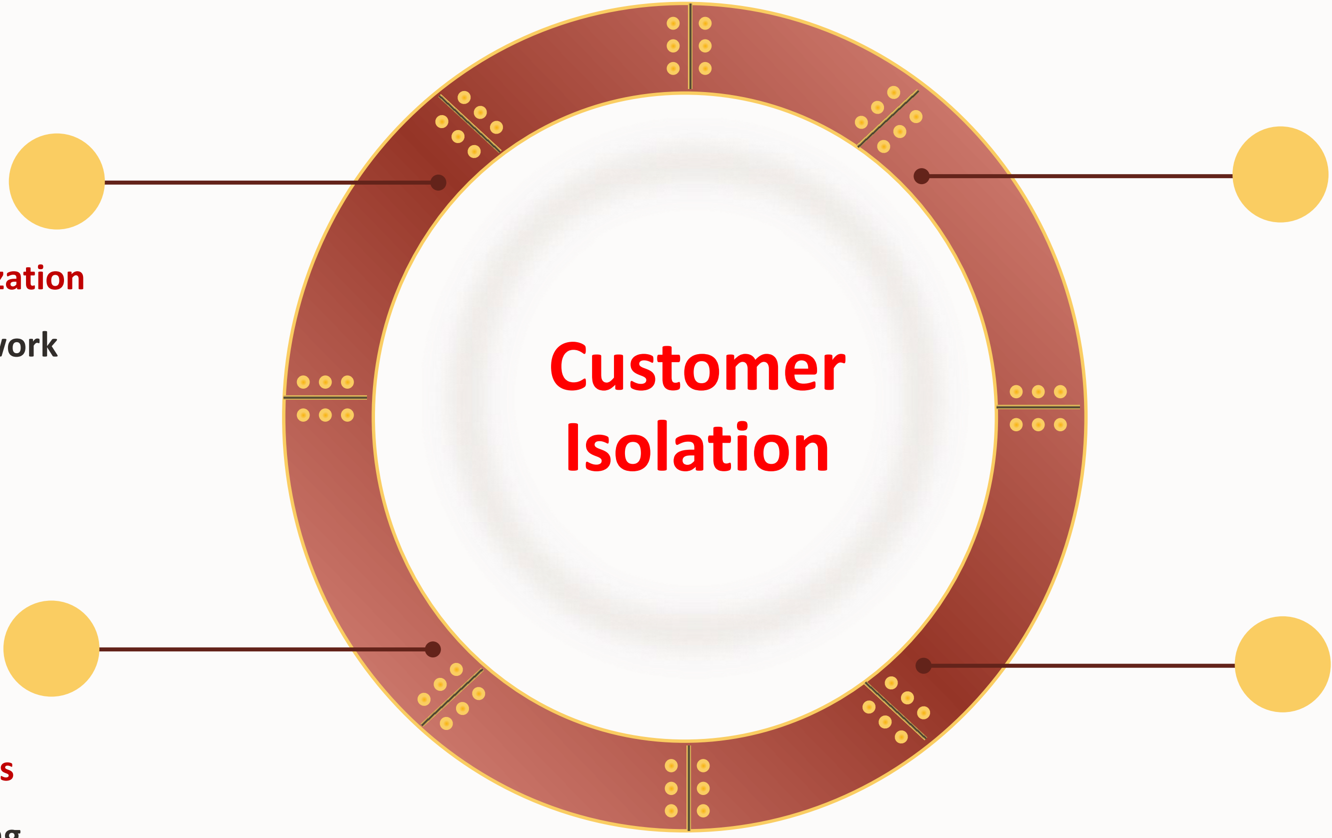


Oracle 2nd Generation Cloud



Isolated Network Virtualization Security Prevents Lateral Movement

Isolation is important to our Customers



Customer Isolation

Other Tenants

- **Isolated Network Virtualization**
- **Secure Virtual Cloud Network**

Cloud Provider Staff

- **Physical network segments**
- **Always-on encryption using customer-controlled keys**

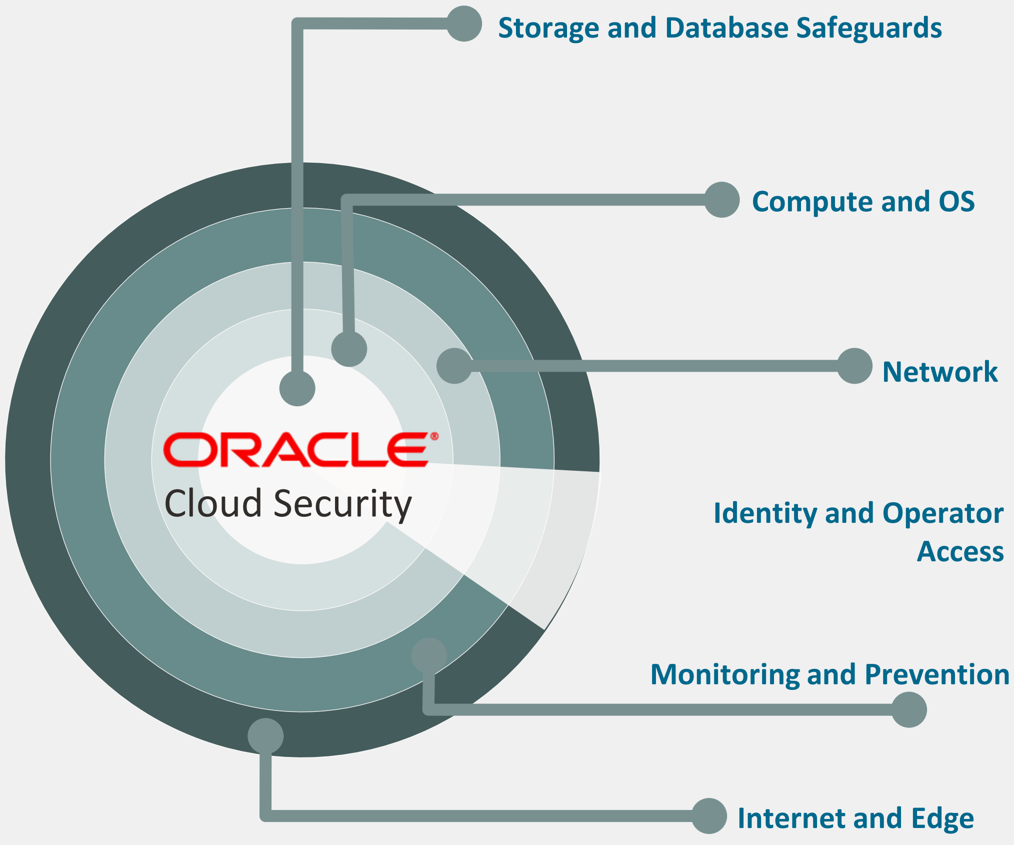
External Threat Actors

- **DDOS Protection**
- **Hardware-Based Root of Trust**
- **Top-of-rack ACLs**
- **Security Automation**
  - **Maximum Security Zones**
  - **Cloud Guard**
  - **Autonomous Database**
  - **Autonomous Linux**

Customer LoB Apps

- **IAM Compartments**

Oracle offers a full stack of cybersecurity capabilities



Storage and Database Safeguards

- Data Safe
- Vault
- Key Management
- Secrets Management
- Certificates

Compute and OS

- Oracle Linux
- Bare Metal Compute
- Hardware Root of Trust
- Signed Firmware
- Harden Disk Images

Network

- Virtual Cloud Network
- Security Lists
- Network Firewall
- Bastion
- Dynamic Routing Gateway
- FastConnect
- VPN
- NAT Gateway

Identity and Operator Access

- Access Governance
- OCI Identity and Access Management
- Policies
- Federation

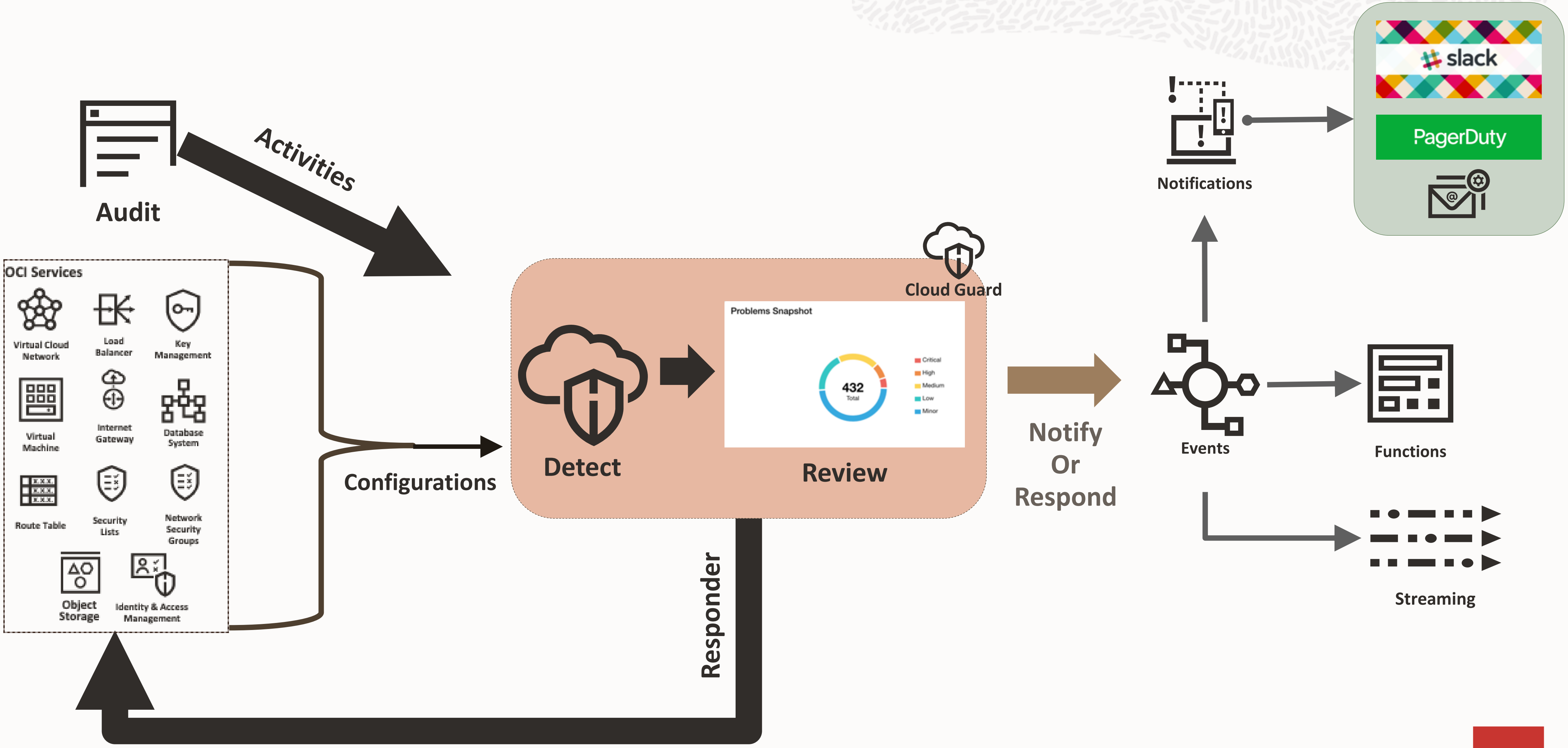
Monitoring and Prevention

- Cloud Guard
- Security Zones
- Threat Intelligence
- Threat Detector
- Logging
- Fusion Apps Detector
- Vulnerability Scanning
- Auditing

Internet and Edge

- DDoS Protection
- WAF

Cloud Security Posture Management – Cloud Guard



Audit

Activities

OCI Services

Virtual Cloud Network

Load Balancer

Key Management

Virtual Machine

Internet Gateway

Database System

Route Table

Security Lists

Network Security Groups

Object Storage

Identity & Access Management

Configurations

Cloud Guard

Detect

Problems Snapshot

432 Total

Critical

High

Medium

Low

Minor

Review

Responder

Notify Or Respond

Notifications

slack

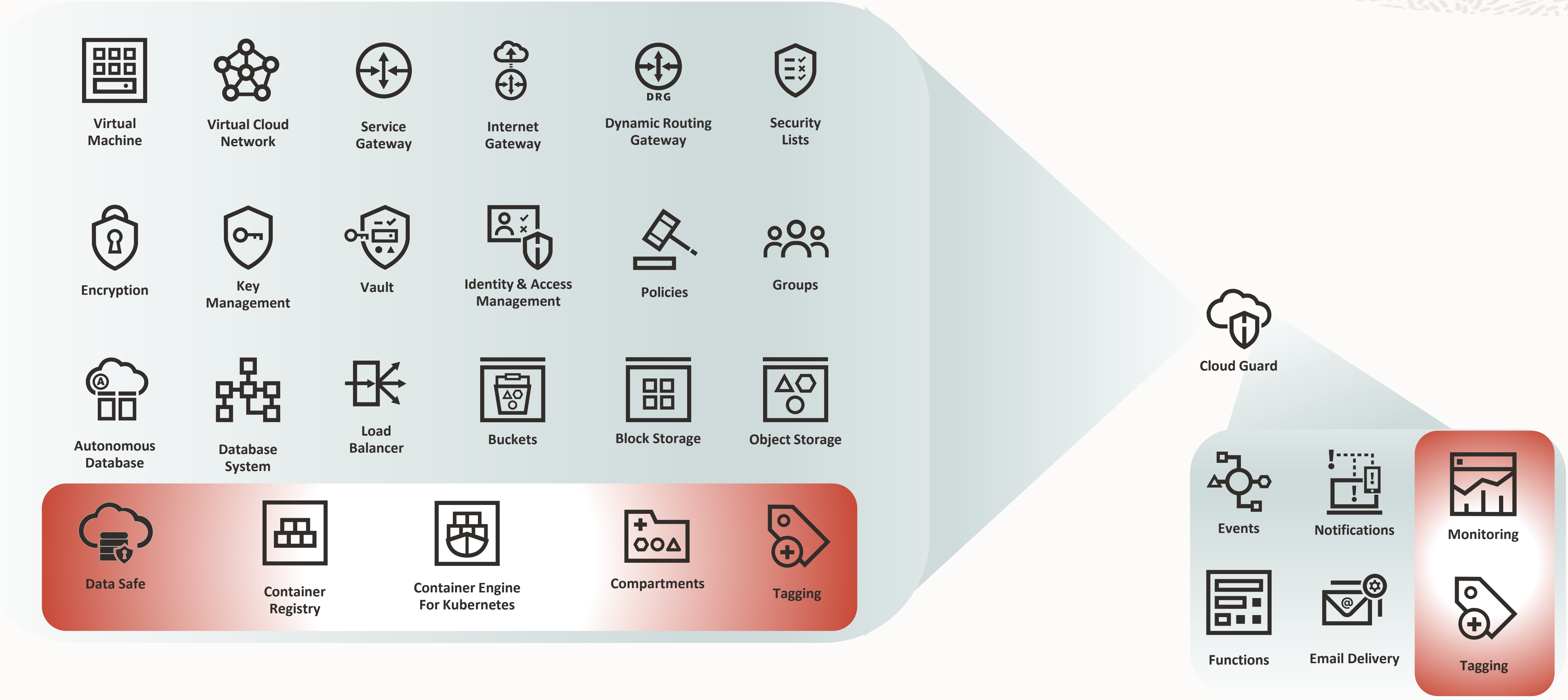
PagerDuty

Events

Functions

Streaming

Cloud Guard – OCI Config & OCI Activity



Oracle Cloud Guard Threat Detector

Threat Detector uses an ML-based data platform to run threat models aligned with MITRE ATT&CK® techniques to identify attackers quickly.

- **Simple, Prescriptive, Integrated**

  Simple: resource profiles are created and scored automatically

  Prescriptive: helps customers align with ATT&CK

  Integrated: just attach the new recipe to existing target(s

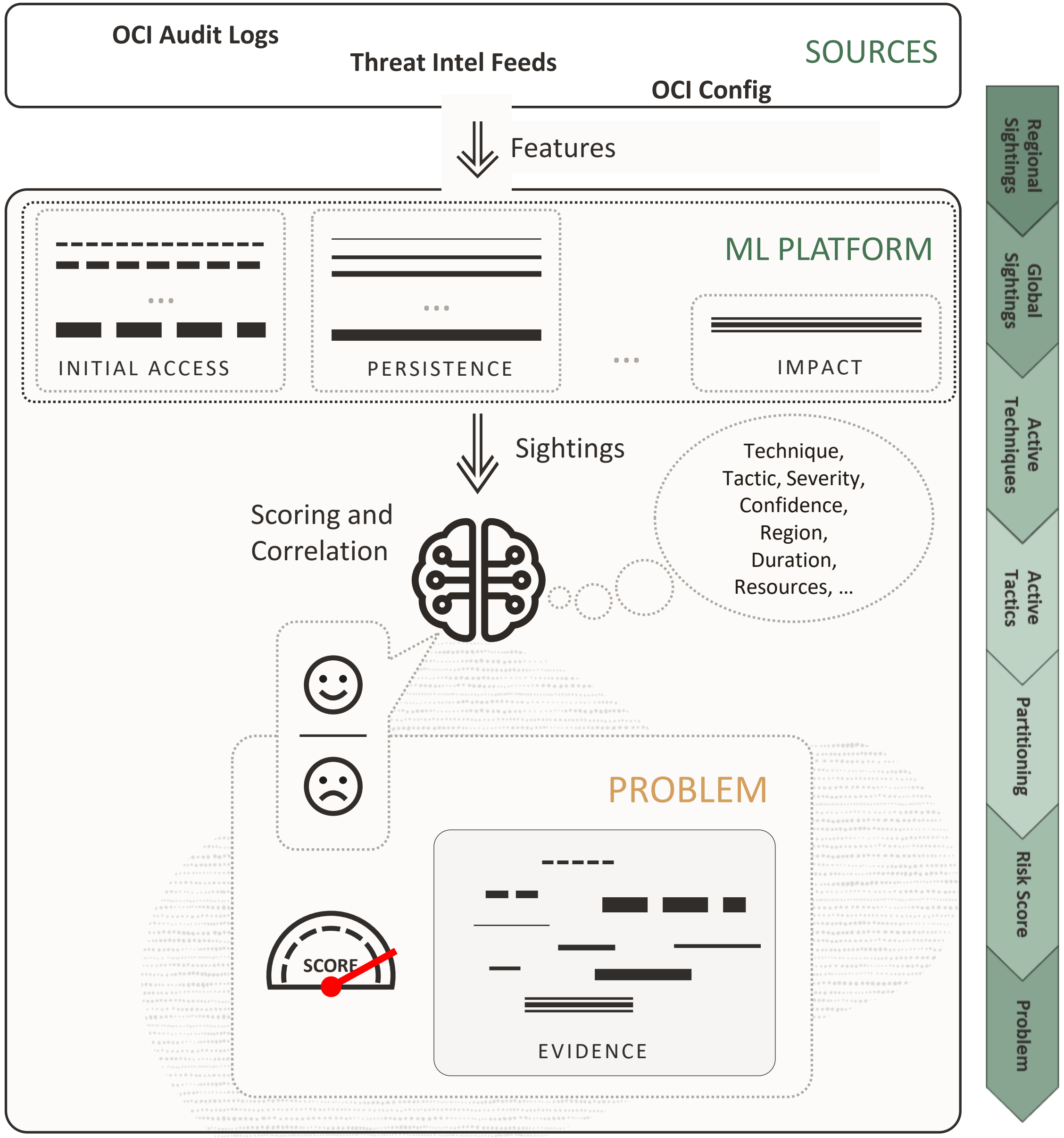
- **Low noise & Prioritized**

  Low noise: considers both severity and confidence

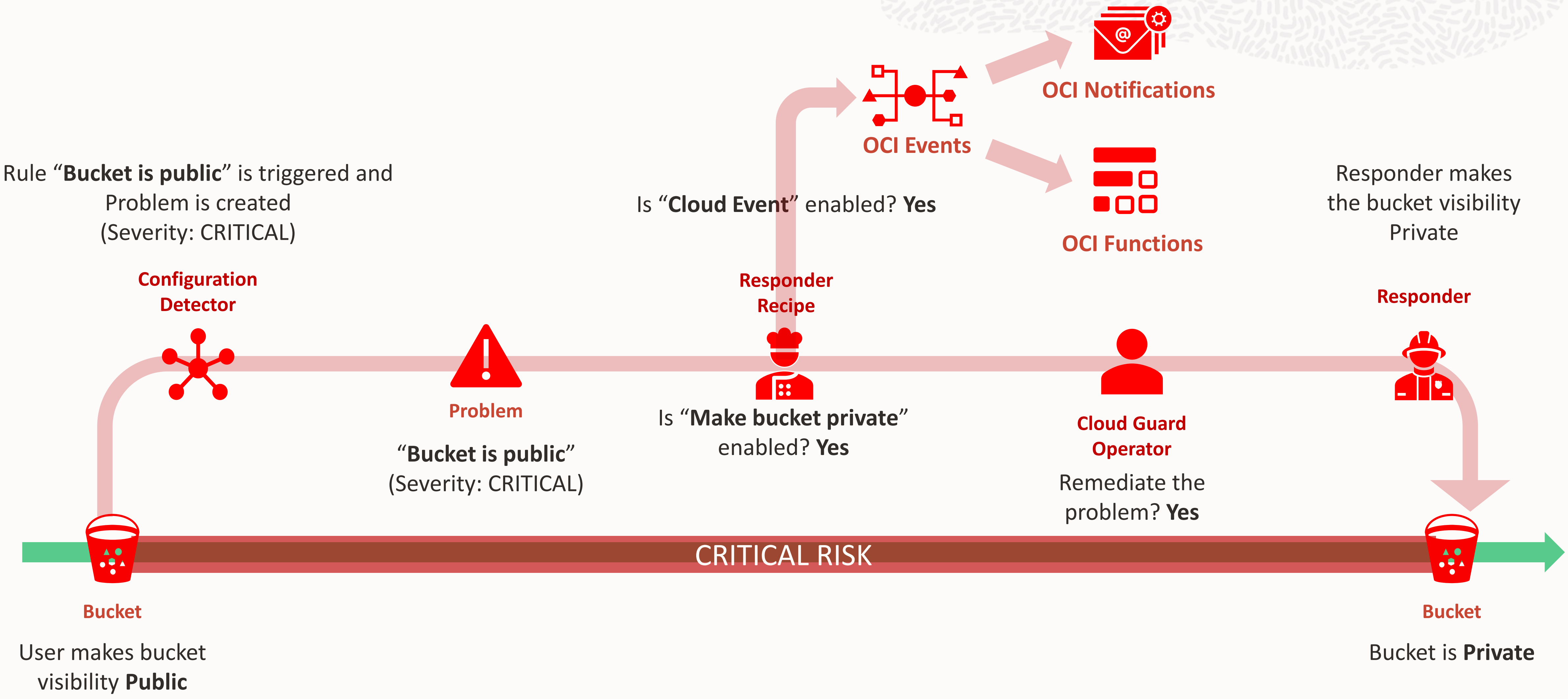
  Prioritized: risk scores biased towards attack progression

- **Actionable**

  Focuses on malicious behavior not anomalies to find internal threats and account takeovers



Scenario: Public Bucket



Bucket

User makes bucket visibility **Public**

Configuration Detector

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

Problem

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

Responder Recipe

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

Is “**Cloud Event**” enabled? **Yes**

OCI Events

OCI Notifications

OCI Functions

Cloud Guard Operator

Remediate the problem? **Yes**

Responder

Responder makes the bucket visibility Private

Bucket

Bucket is **Private**

CRITICAL RISK

OCI manages 70+ compliance programs across regions and industries

REGIONAL

- GDPR [EU]
- PIPEDA [Canada]
- ENS [Spain]
- BSI C5 [Germany]
- ISMS [Korea]
- NISC [Japan]
- CITC [Saudi Arabia]
- Cyber Essentials Plus [UK]
- IRAP [Australia]

GOVERNMENT

- DoD DISA SRG IL5
- JAB P-ATO
- CJIS
- EU Model Clauses
- LGPD
- VPAT-Section 508
- Canada Protected B
- G-Cloud 12
- NIST

INDUSTRY

- HIPAA
- PCI DSS – Level 1
- HITRUST CSF
- TISAX
- FINMA
- BACEN
- EBA
- GxP
- FISC

GLOBAL

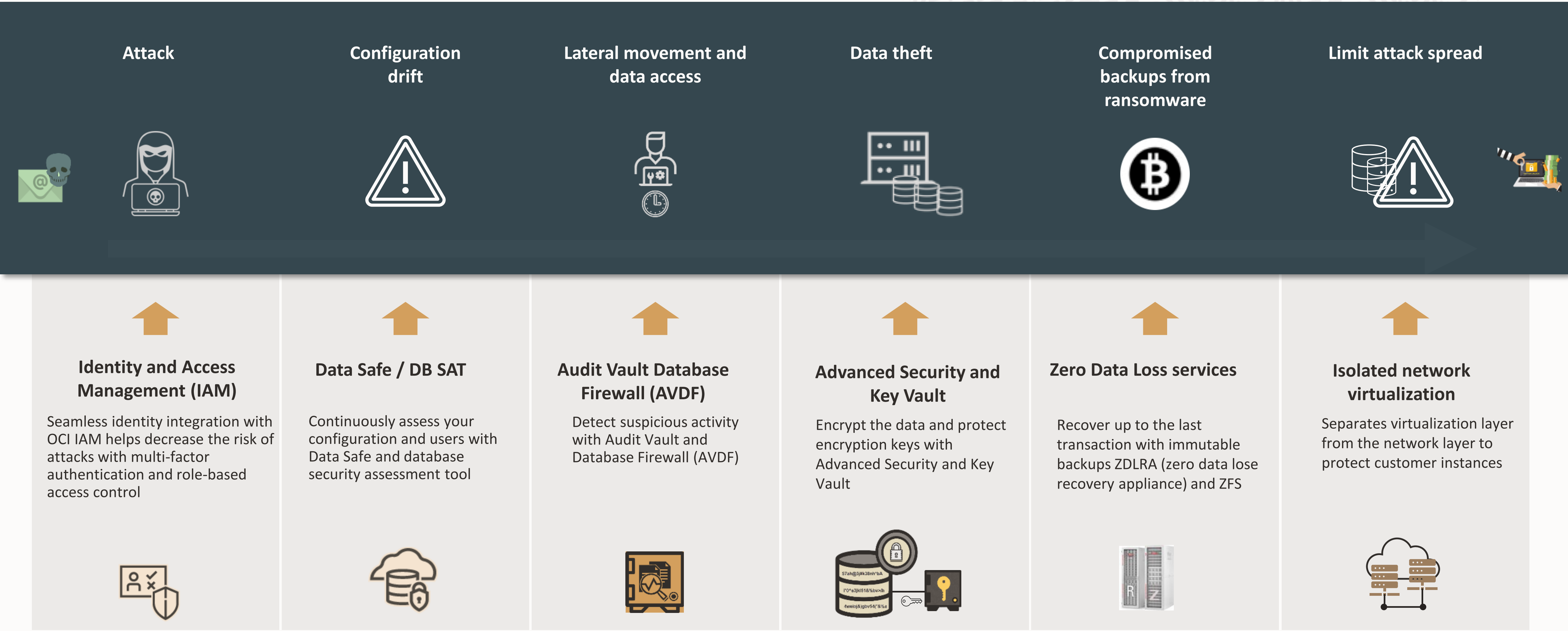
SOC 1 : SOC 2 : SOC 3

9001 : 27001 : 27017 : 27018 : 27701: 20000-1

Level 2

Oracle database security helps protect against attacks

Built-in capabilities and cloud-native services



Attack

Configuration drift

Lateral movement and data access

Data theft

Compromised backups from ransomware

Limit attack spread

Identity and Access Management (IAM)

Seamless identity integration with OCI IAM helps decrease the risk of attacks with multi-factor authentication and role-based access control

Data Safe / DB SAT

Continuously assess your configuration and users with Data Safe and database security assessment tool

Audit Vault Database Firewall (AVDF)

Detect suspicious activity with Audit Vault and Database Firewall (AVDF)

Advanced Security and Key Vault

Encrypt the data and protect encryption keys with Advanced Security and Key Vault

Zero Data Loss services

Recover up to the last transaction with immutable backups ZDLRA (zero data lose recovery appliance) and ZFS

Isolated network virtualization

Separates virtualization layer from the network layer to protect customer instances