ORACLE

Oracle Security

Safeguarding Data and Applications

Alexandre Fagundes

Cloud Architect, Oracle Latin America

Organizations are facing more advanced threats

33% of organizations worldwide have experienced a ransomware attack or breach

80% of those who paid were victims of a second attack

92% of organizations feel they have a cloud readiness gap that places them at risk

Sources: IDC 2021 Ransomware Study: Where You Are Matters
Cybereason *Ransomware: The True Cost to Business*
Oracle Mission of the Cloud-centric CISO

There is a huge shortage of cybersecurity talent

4 Million

positions that cannot be filled

57%

of surveyed organizations have been impacted by the skills shortage

Sources: (ISC)² Cybersecurity Workforce Study 2021
ESG/ISSA: The Life and Times of Cybersecurity Professionals 2021

Human error puts organizations at greater risk

82%

of data breaches involved the "human element"

94%

of organizations had an insider data beach in the last 12 months. Human error was the most common cause.

43%

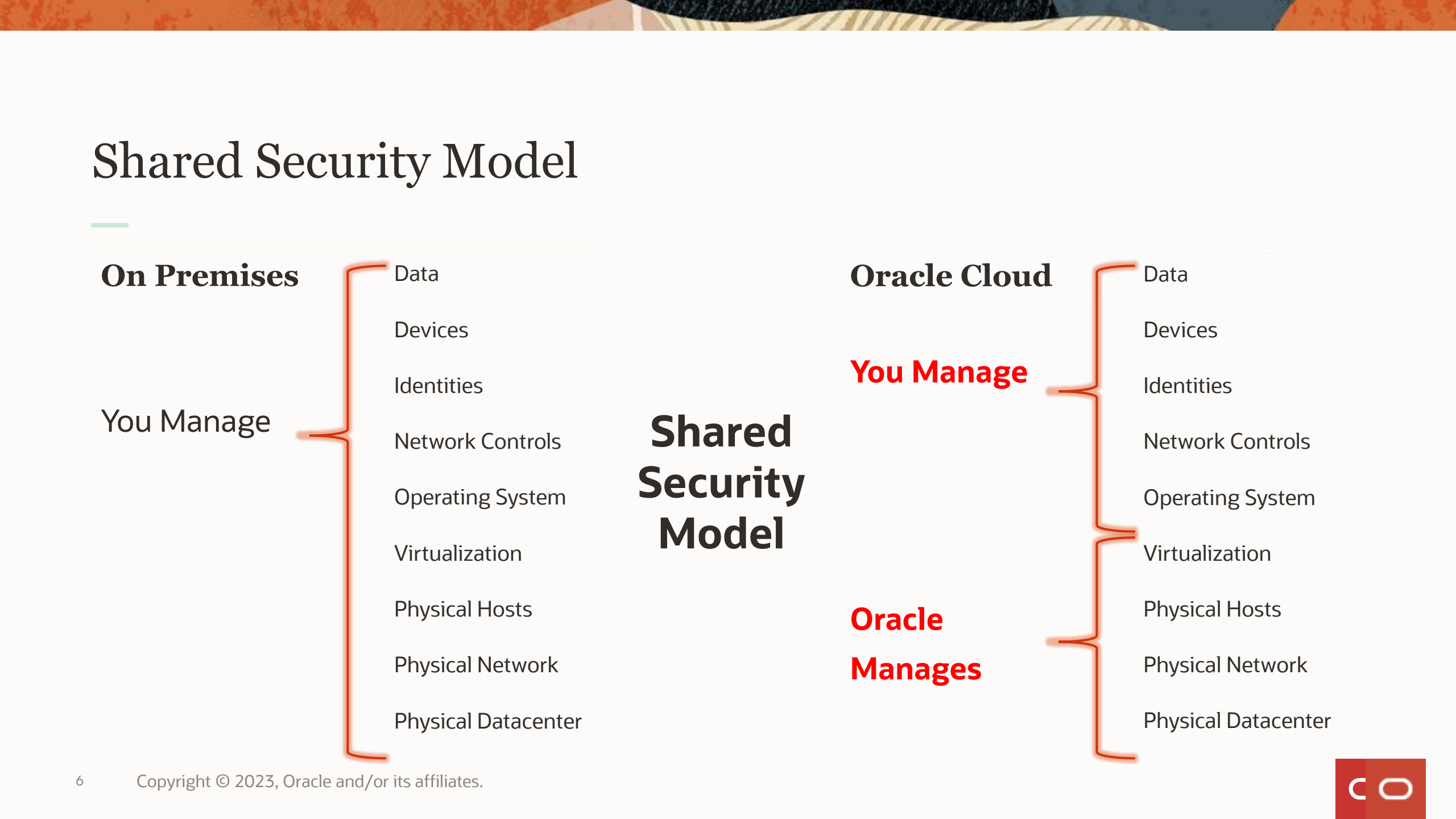
of people have made mistakes at work that compromised cybersecurity

Sources: Verizon Data Breach Investigations Report 2022
Egress, Insider Data Breach Survey 2021
Tessian, Psychology of Human Error 2022

Outline

- Shared Security Model
- Security Tools
- Certifications & Security Compliance
- Cloud Guard
- VSS – Scanning Service
- WAF
- OCI Other Tools for Security
- Secure Architecture

Shared Security Model



Security models continue to evolve

Prevent

Proactively protect data

Access controls
User risk and visibility
Discovery and classification
Zero-trust architecture

Detect

Outpace attackers

Unified platforms
Advanced threat research
Aggregated threat intelligence

Respond

Leverage automation

Scalable response
Eliminate errors
Risk remediation
Rapid resolution
Root cause visibility

Oracle's Security Approach

Reduce risk with simple and prescriptive security solutions

Automated security to reduce complexity and prevent human error

Always-On security for continuous protection

Products **Architected** with security as a primary goal, to reduce risk

Security solutions that support your cloud journey

Flexibility to meet you where you are today

Security for on-premises (e.g. IAM, database security)

Security across cloud and on-premises (e.g. Data Safe, OCI IAM, Access Governance)

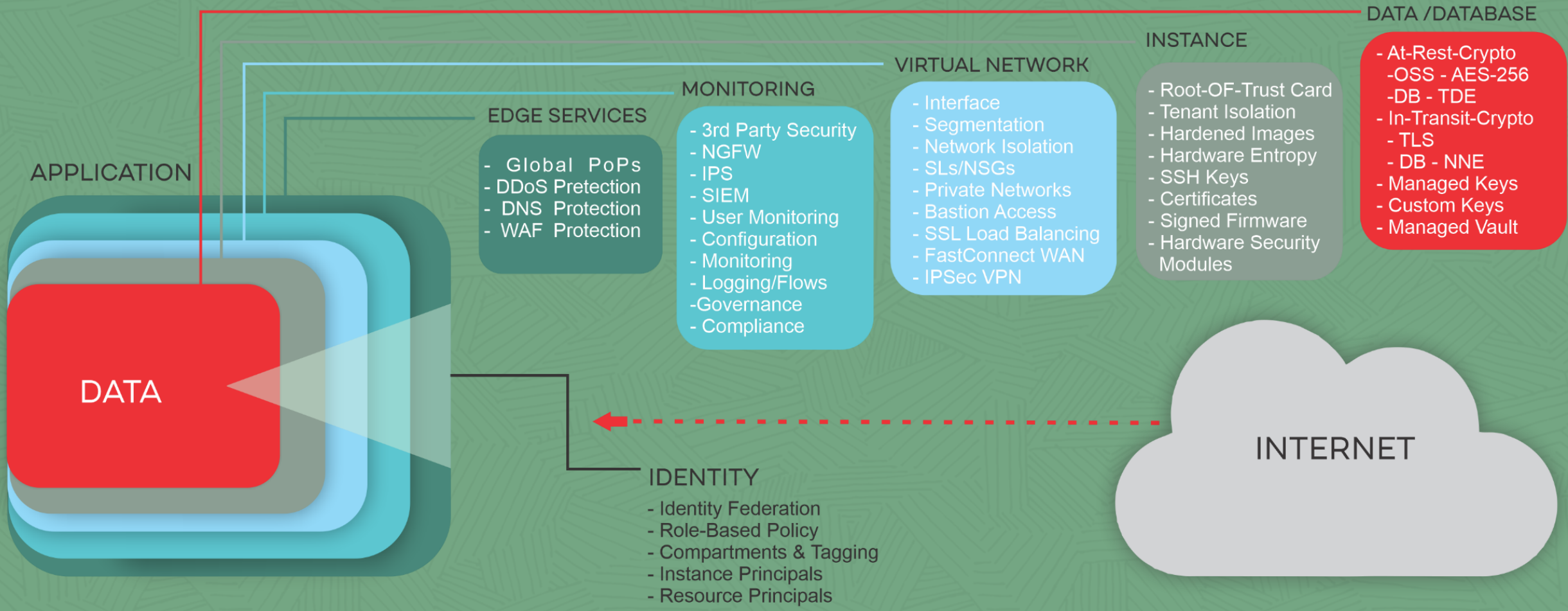
OCI security (e.g. Cloud Guard, Security Zones, Network Firewall)

Multicloud security (e.g. OCI IAM, Cloud Guard, WAF)

On-premises ⟷ Cloud

Certifications & Security Compliance

Stronger isolation and control from Data to Identity



Comprehensive security portfolio and ecosystem

SaaS
Isolated VM environments, policy, monitoring

Governance
Automation, policy, monitoring, scanning, patching, remediation, data masking

Multicloud, Hybrid Cloud
Identity, Monitoring, Data & Application Protection

Customer Services
Oracle managed cloud services, expert security talent

Compliance
Managing 70+ global, industry, and regional standards

Identity and Access Management
Strong authentication, authorization, resource principals

Applications
Java security library, security capabilities for industry applications

Database and Storage
Strong Oracle DB security, pervasive storage encryption

Operating System
Autonomous Linux, Hardened OS images, OS management

Virtual Network
Micro-segmentation, network and web application firewalls

Secure Infrastructure
Isolated network virtualization, Root of Trust

Partners
Integrate or offer best of breed technologies

Oracle Cloud Infrastructure Security

Build Confidence with Simple, Prescriptive, and Integrated Security

Easy to Use, Deploy, and Operate Cloud Security

Increase the confidence in your ability to detect and respond to emerging risks from possible security errors with simple, built-in security that is turned on by default.

- Isolated Network Virtualization
- Least privilege access
- Oracle Threat Intelligence
- OCI Network Firewall
- OCI WAF for Fusion Applications

Breadth of Security Integrated for a Zero Trust Architecture

Security services are integrated across the cloud infrastructure and applications to avoid misconfigurations and streamline security.

- OCI Bastion
- Oracle Cloud Guard Fusion Applications Detector
- OCI Identity and Access Management
- OCI Vault
- OCI WAF

Prescriptive Guidance Which Requires Less Expertise

Adopt guardrails to help consistently apply Oracle security best practices with reduced dependency on costly security experts.

- Oracle Security Zones
- Oracle Cloud Guard
- Oracle Cloud Guard Threat Detector
- OCI Vulnerability Scanning Service

Oracle Database Security

Reduce the risk of a data breach and simplify compliance

Identify Security Posture

Discover sensitive and personal data, assess how securely database is configured, and get recommendations on improving security posture

- Oracle Data Safe
- Oracle Database Security Assessment Tool (DBSAT)

Prevent Unauthorized Access to Data

Enforce least privilege and mitigate exposure to stolen credentials and compromised accounts with solutions that offer separation of duties and multifactor authentication

- Oracle Data Safe
- Oracle Database Vault
- Oracle Label Security

Secure Private Information

Meet global compliance requirements, data governance, regulatory mandates, and industry requirements while addressing local needs for data sovereignty, privacy, and transparency

- Oracle Advanced Security
- Oracle Data Masking and Subsetting
- Oracle Data Safe
- Oracle Key Vault

Monitor for Threats

Identify risky user behavior, detect and block threats, and simplify and accelerate compliance reporting

- Oracle Audit Vault & Database Firewall
- Oracle Data Safe

Oracle Identity and Access Management

Securely manage access to data and applications for cloud and on-premises

Manage Access with a Zero-Trust Approach

Effectively manage access across complex environments with advanced adaptive authentication, easy to manage policies and risk scoring. Supports a zero-trust model for user identity across a wide range of applications and services.

- OCI Identity and Access Management
- Oracle Access Management 12c with microservices

Streamline Governance with Scalable Lifecycle Management

Enable complete lifecycle management of your entitlements using flexible Identity, Governance, and Administration (IGA) controls that address complex governance and compliance needs. Using advanced analytics, organizations can reduce manual certification efforts and automate access control and provisioning.

- Oracle Access Governance
- Oracle Identity Governance 12c with microservices

Scale Operational Capabilities with Advanced Directory

Meet your growing needs with scalability and reliability for multi-platform needs. Support billions of users and devices with easy implementation and configuration.

- Oracle Unified Directory
- Oracle Internet Directory

Certifications & Security Compliance

Zero Trust Architecture Model - https://www.oracle.com/security/what-is-zero-trust

- Established by the National Institute of Standards & Technology (NIST)
- Approach that enforces less privilege per-request model
- Granular duties separation
- Automated threat mitigation and remediation
- Continous monitoring

Advantages

- Reduce risk
- Fine-Grained Control Access
- Enhance Organization's Security posture

OCI Compliance

Expansive list of independent assessments across industries and regions

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

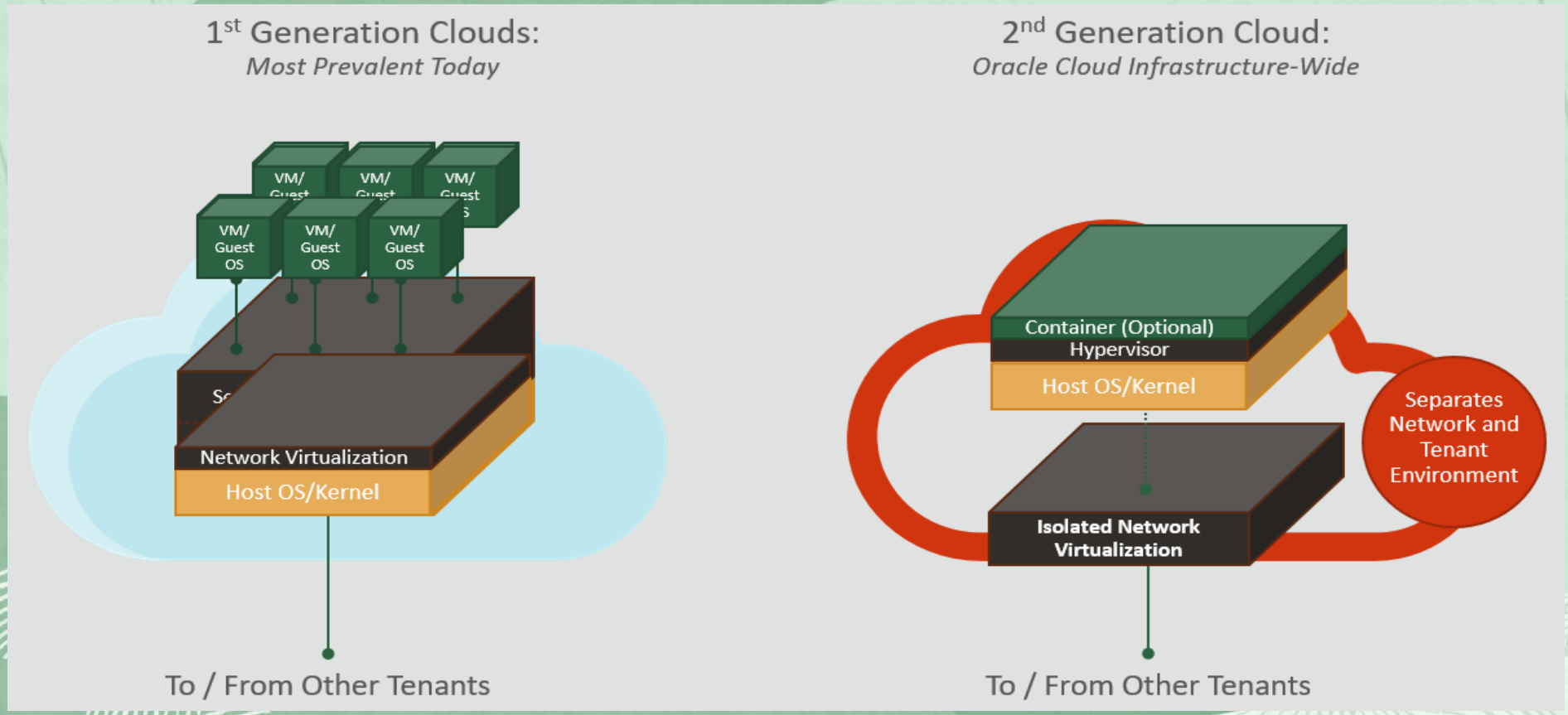
- HIPAA
- PCI DSS – Level 1
- HITRUST CSF
- TISAX
- FINMA
- BACEN
- EBA
- GxP
- FISC

GLOBAL

- SOC 1 : SOC 2 : SOC 3
- 9001 : 27001 : 27017 : 27018 : 27701: 20000-1
- Level 2

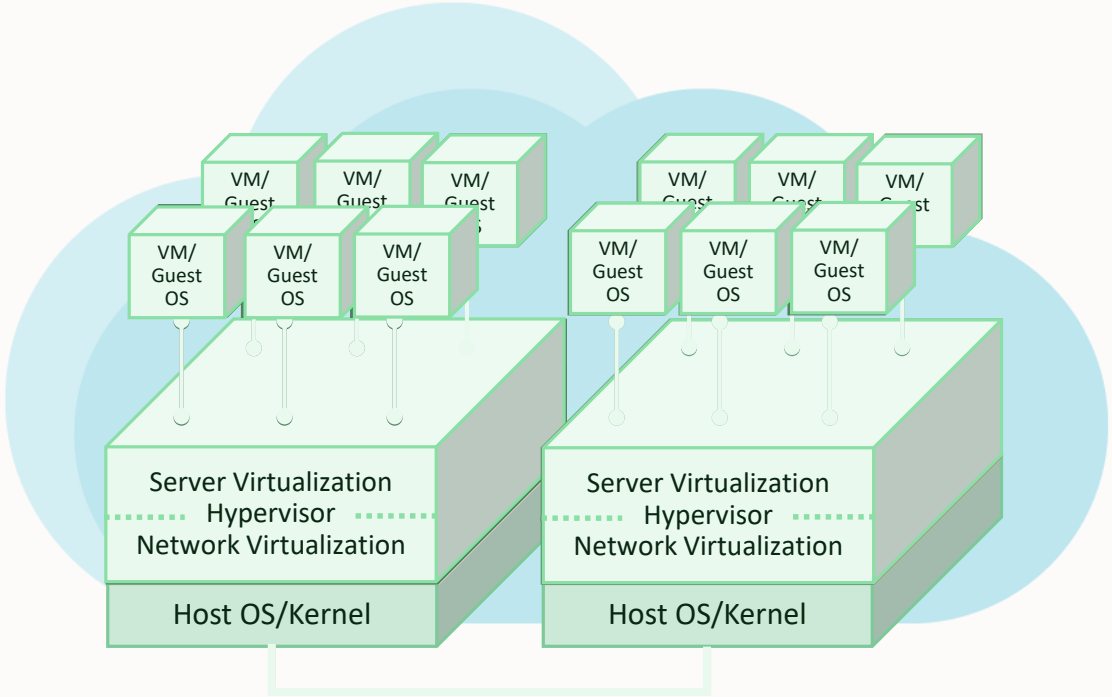
Certifications & Security Compliance

Cloud Secure Design: Prevents Lateral Movement, Tenant Isolation with Isolated Network Layer

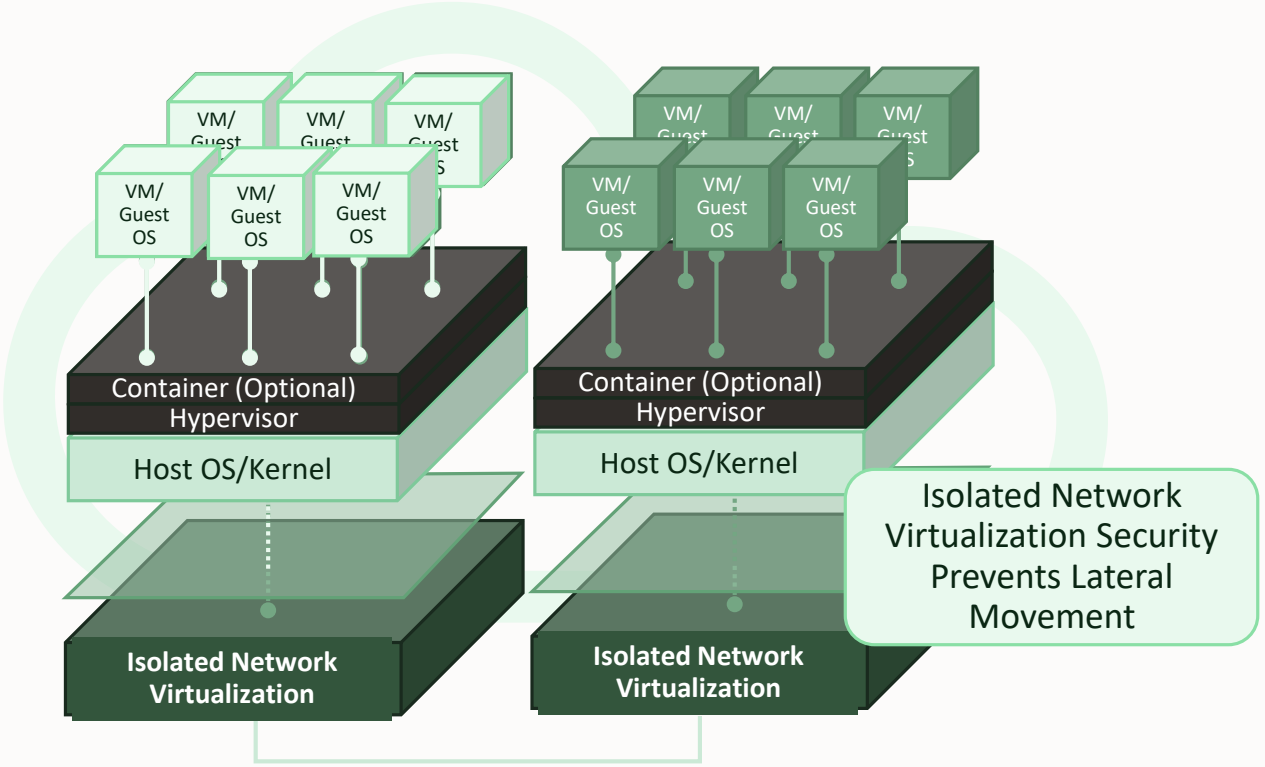


Threat Containment & Reduced Risk

1st Generation Cloud



Oracle 2nd Generation Cloud



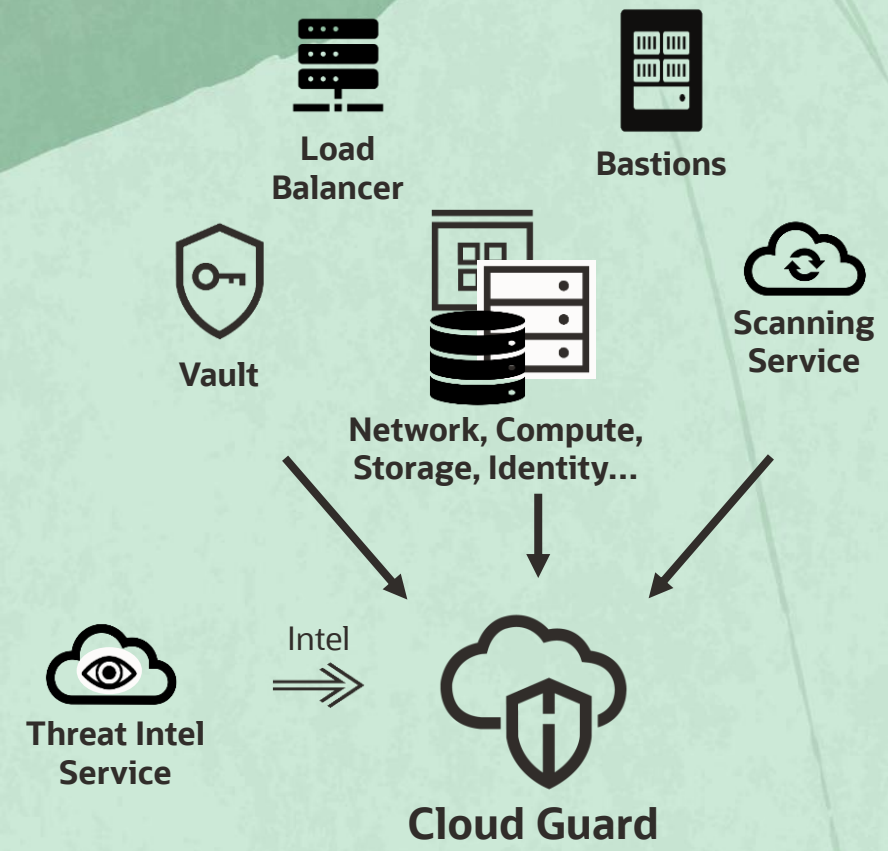
Cloud Guard

Cloud Guard is a service that helps customers achieve and sustain a strong security posture on Oracle Cloud Infrastructure

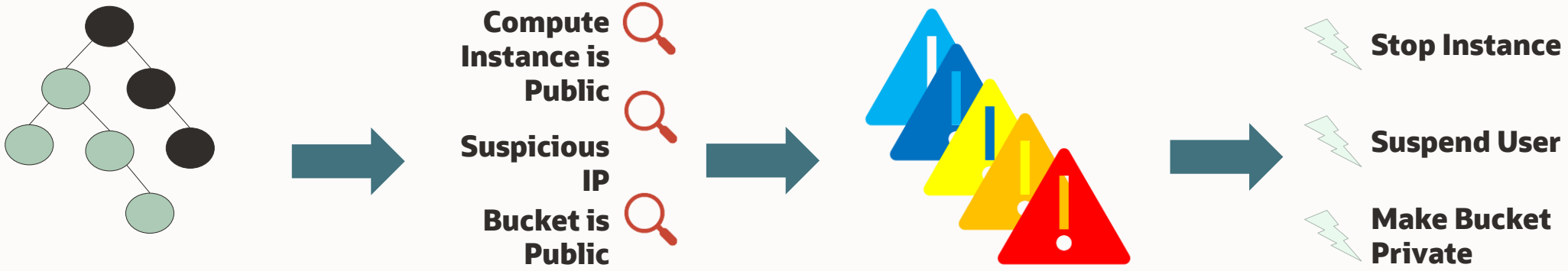
Free Service

Monitors OCI resources/targets, identifies problems and helps fixing those problems

Easily integrate with external tools using OCI Events



Cloud Guard



Targets

Targets are the scope of resources to be examined. For OCI, Compartments and all resources within

Detectors

Detectors are Cloud Guard components that identify and notify issues with resources or user actions.

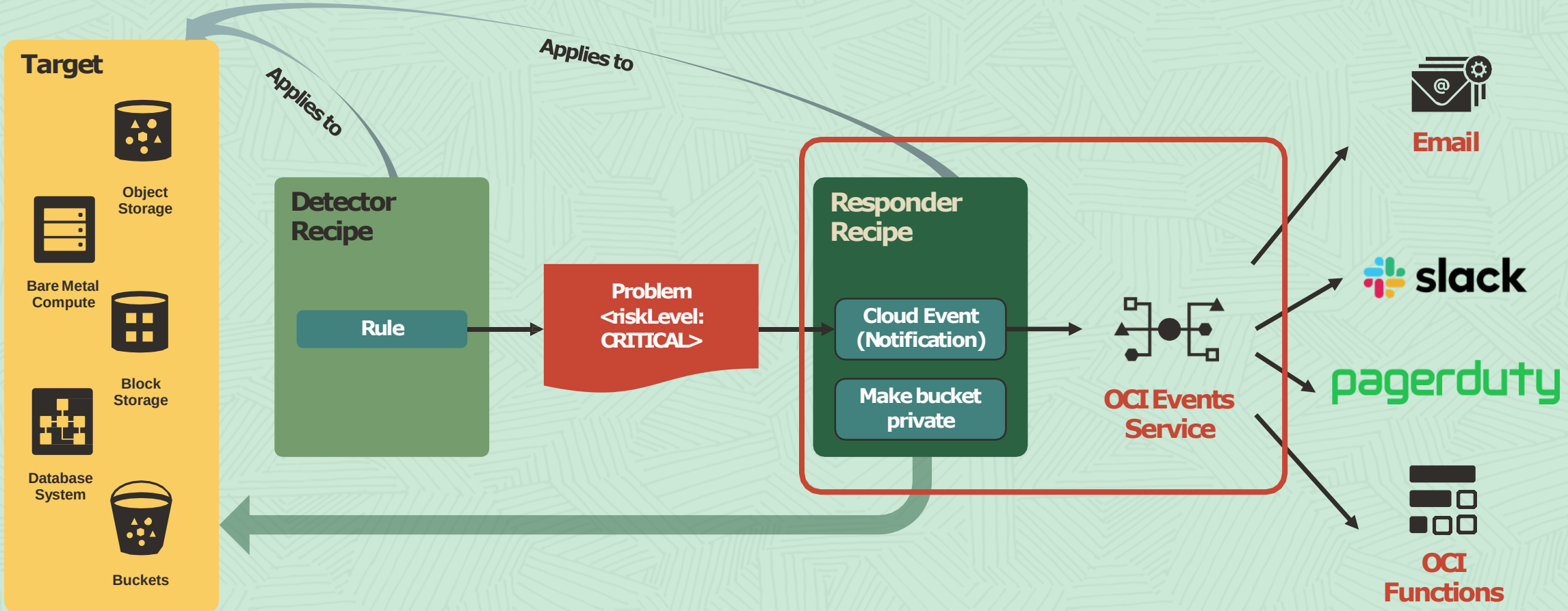
Problems

Problem is a potential security issue, notified as misconfiguration or suspect activity.

Responders

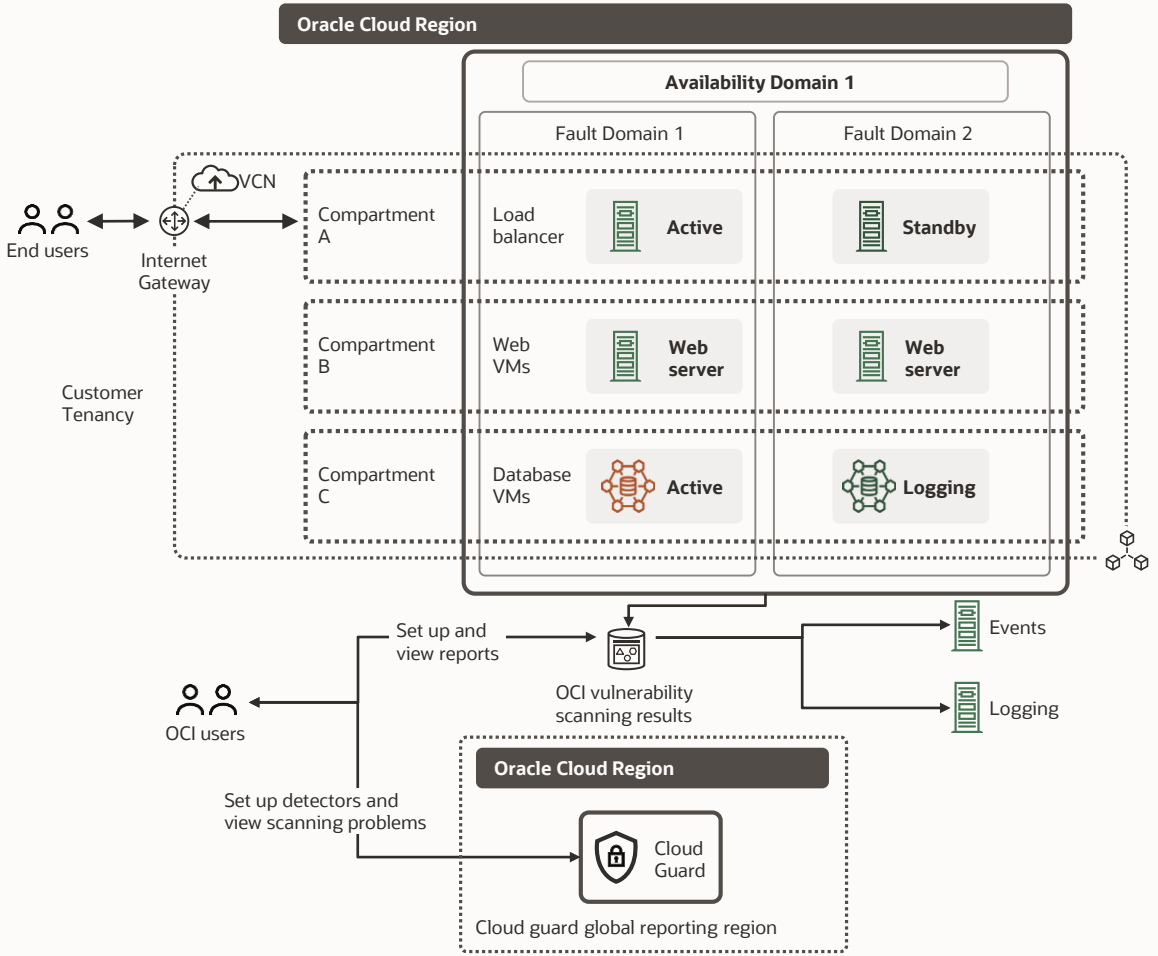
Responders notifies and take corrective actions for security problems.

Cloud Guard - Concepts



Vulnerability Scanning Service

- Simple, on by default, prescriptive, and free scanning suite that is tightly integrated with the OCI platform
- Default plugins and engines based on OCI created and open-source scanning engines for **host** and **container image** scanning
- OCI manages the deployment, configuration and upgrade of these engines and agents across the customer fleet
- Problems detected by the scanning suite will be surfaced through Cloud Guard, with rules and ML to prioritize critical vulnerabilities
- OCI will take action (alert, auto-remediate, or quarantine) through responders to shorten the time from detection to remediation

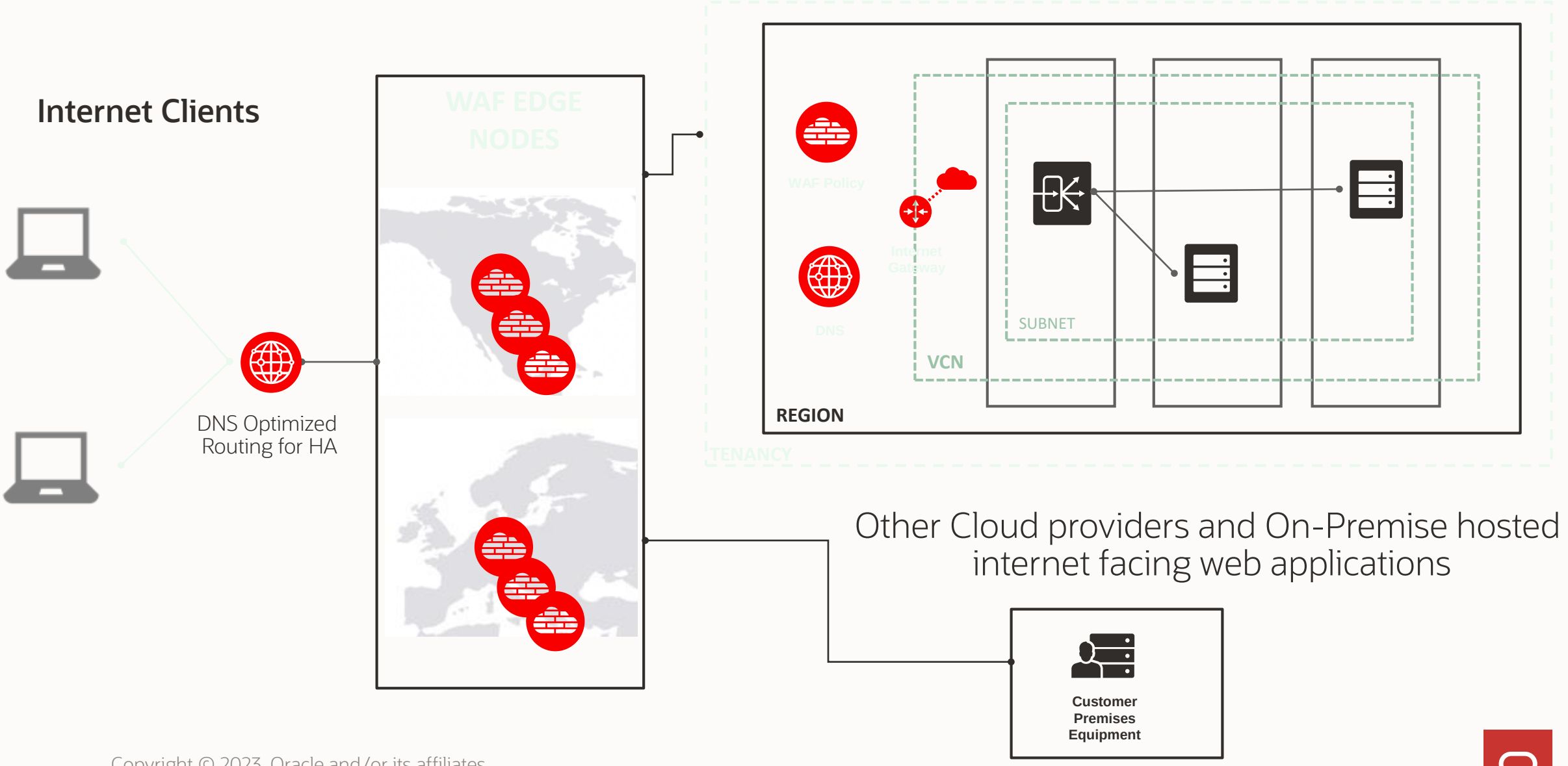


WAF Overview

OCI Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic

- Use cases:
  - Protect any internet-facing endpoint from cyberattacks and malicious actors
  - Protect against cross-site scripting (XSS) and SQL injection, activities that allow attackers to gain unauthorized access to privileged information
  - Bot management – dynamically blocking bad bots
  - Protection against layer 7 distributed denial-of-service (DDoS) attacks

WAF Architecture



WAF Rulesets

OCI WAF uses OWASP ModSecurity Core Rule Set to protect against the most common web vulnerabilities. These rules are managed and maintained by the open source community.

OCI WAF comes pre-configured with protection against the most important threats on the Internet as defined by OWASP Top 10. These include

- A1 – Injections (SQL, LDAP, OS, etc.)
- A2 – Broken Authentication and Session Management
- A3 – Cross-site Scripting (XSS)
- A4 – Insecure Direct Object References
- A6 – Sensitive Data Exposure
- A7 – Missing Function-Level Access Control

Each type of vulnerability ruleset is shown within the OCI console, with granular controls for each specific rule.

WAF Challenges & Whitelisting Capabilities

- JavaScript Challenge: fast and efficient way to block a large percentage of bot attacks
  - After receiving an HTTP request, a piece of JavaScript is sent back to the browser of every client, attacker, and real user. It instructs the browser to perform an action. Legitimate browsers will pass the challenge without the user's knowledge, while bots—which are typically not equipped with JavaScript—will fail and be blocked

- CAPTCHA Challenge
  - If a specific URL should be accessed only by a human, you can control it with CAPTCHA protection.
  - You can customize the comments for the CAPTCHA Challenge for each URL

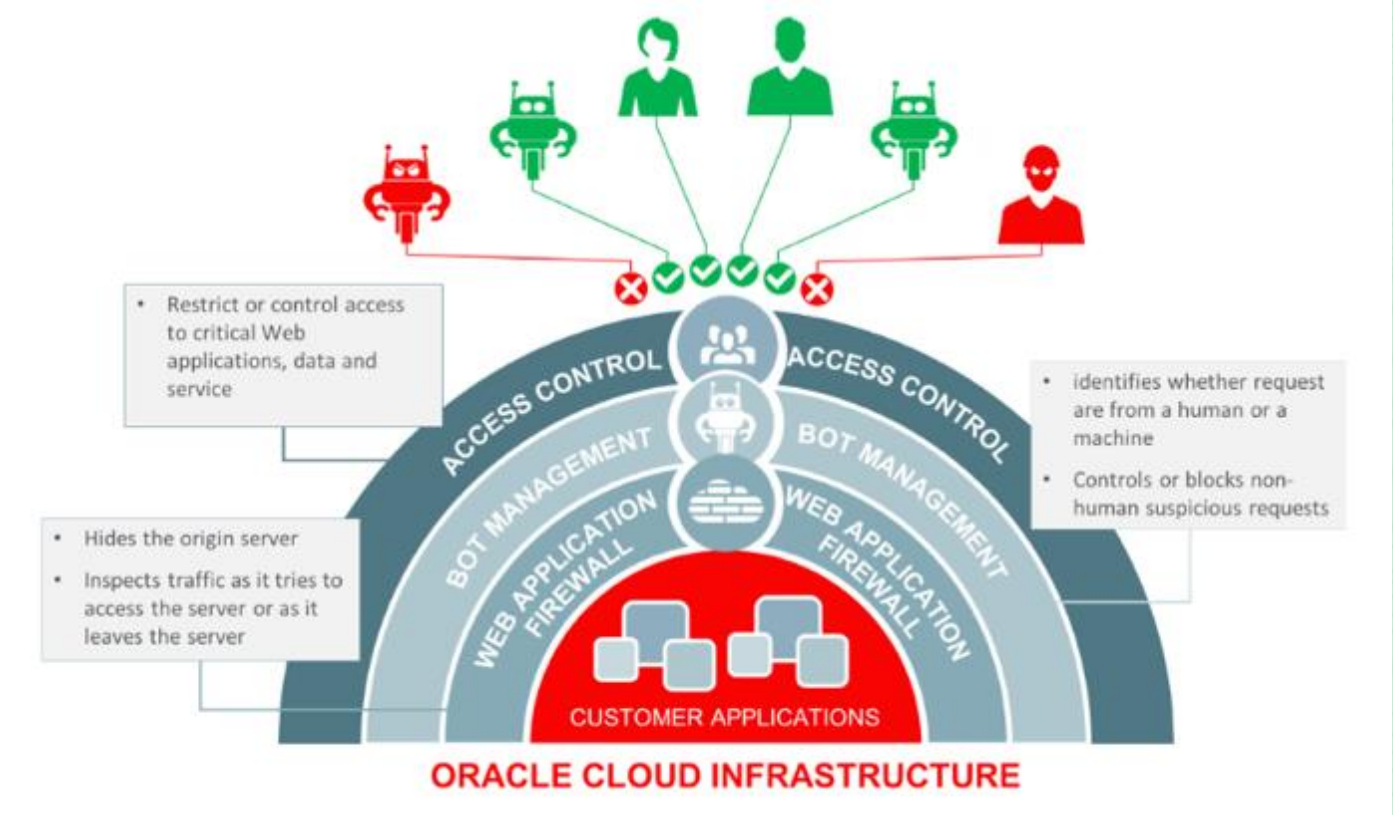
- Whitelisting: Allows you to manage which IP addresses appear on the IP whitelist
  - Requests from the whitelisted IP addresses bypass all challenges, such as DDoS policies and WAF rulesets.

WAF Access Controls

Use the access controls to restrict or control access to your critical web applications, data and services. E.g., in some cases, an offering may need to stay within a specific country. Regional access control can be used to restrict users from certain geographies.

- Control access, based on HTTP header information. Block requests if the HTTP header contains specific names or values or allow traffic with proper HTTP regular expression

- Control access based on URL address matching or partial matching or match proper URL regular expressions



Secure Architecture

CIS Landing Zones → Segregates access (based on job function) to resources

Multiple compartments, groups and IAM policies

Secure Network, inbound and outbound interfaces secured with NSGs

VCN flow Network logging

Alerts for IAM and Network changes

Cloud Guard

Logging Consolidation - Service connector Hub

Automatic host scanning with Vulnerability Scanning Service

Secure Architecture

CIS Landing Zones

Terraform configuration for tenancy creation → CIS Benchmark for OCI +Architecture Best Practices

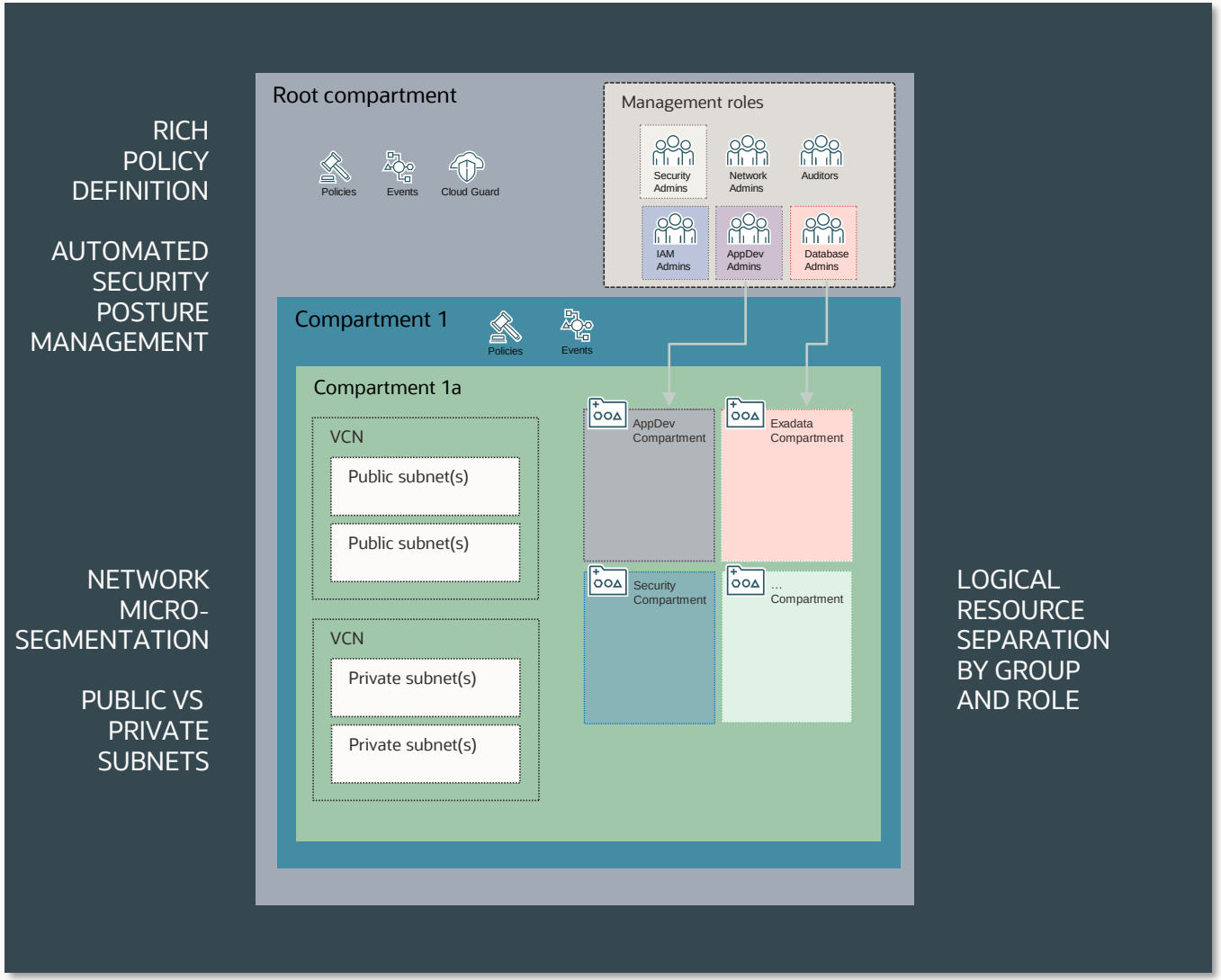
CIS Compliance checking script → Applicable to any existing tenancy

[Secure Landing Zone]

[CIS Landizone Start]

Network Design

Hub / Spoke Model with Next Generation Firewall between Public & Private VCNs



Oracle security takes away an attacker's advantage

Misconfiguration	Prevent and find misconfigurations including mistakes and weak posture **Cloud Guard, Security Zones, Data Safe, Network Firewall, Web Application Firewall, Threat Intelligence**
Vulnerabilities	Automate patching and scanning **Autonomous Database, Autonomous Linux, Vulnerability Scanning, Data Safe**
Privilege Misuse	IAM and least privilege – enable zero-trust controls across apps/infrastructure **OCI IAM, Access Governance, Data Safe, DB Vault, Bastion**
Encryption	Encrypt data pervasively and transparently **Autonomous Database, TDE, OCI Vault, Secrets, Certificates**
Humans	Enforce automation, limit lateral movement, detect malicious insiders **Automation, policy, monitoring, MFA, privilege and access, DB Vault, Label Security, Data Masking and Subsetting, Isolated Network Virtualization**

Oracle Security

Automated, Always-on, Architected-in

- Decades of experience safeguarding the world's most valuable data
- Security built-in as a foundational element
- Portfolio of integrated security services that make security easier to manage with automation and actionable insights
- Provides support for multicloud and hybrid cloud use cases

45
Oracle Cloud Regions

60+
Commercial and public sector compliance programs

500 Million
Identities managed

Stay Connected with the Latin America Partner Community!

Information, collaboration and training all in a single spot.

The **LAD Partner Community** is a space dedicated to our partners in Latin America, where you can find information and stay up to date on what OPN has to offer.

In the Community, you will find all the information that we communicate to our ecosystem by email.

- Explore **Categories**: organized by grouping publications on a same topic;
- Access the **Recent Discussions** tab to check the latest posts published;
- Take part in **Groups** and interact with Oracle Experts and other partners.

Important: An Oracle SSO account is required to access the Community and other OPN resources. If you don't have this account yet, access **this link** or the QR code below.

Access the Community:

Create your SSO account:


ORACLE