ORACLE

OCI Security Overview

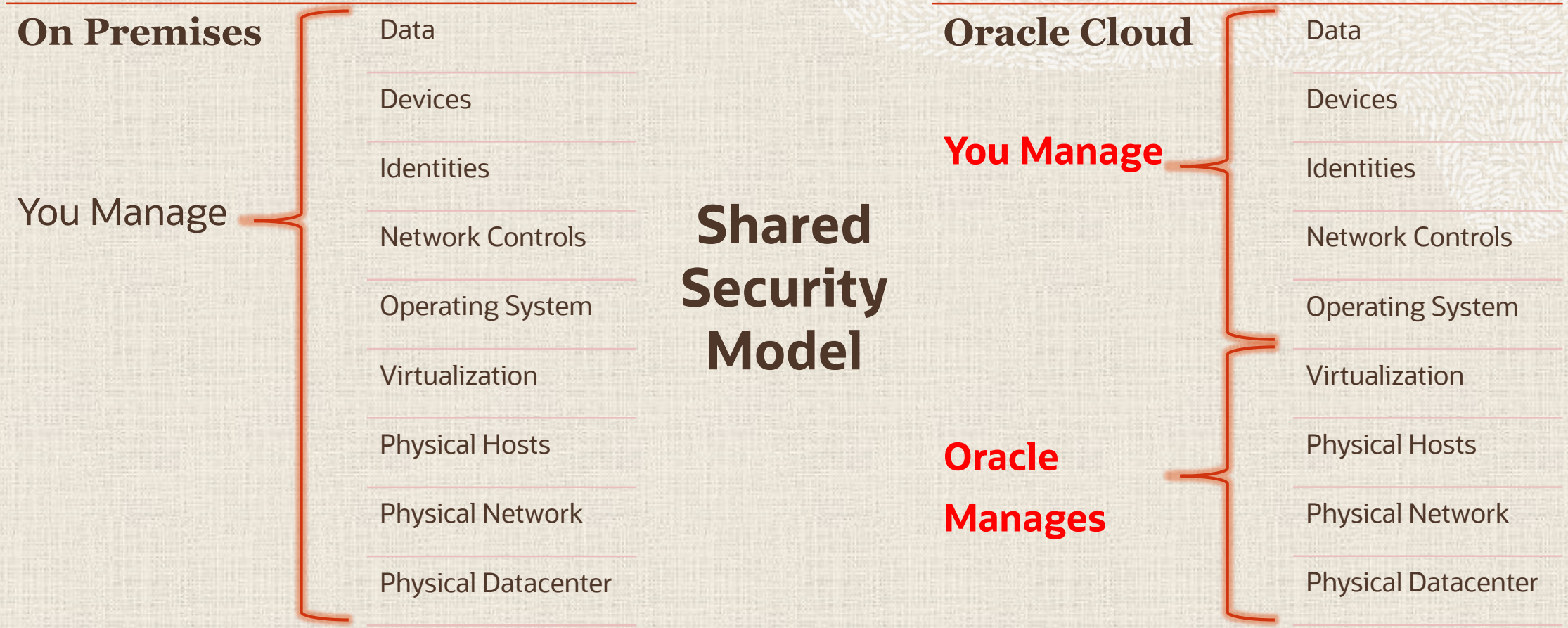
Alexandre Fagundes
LAD Partner Enablement

Oracle Cloud Security

Agenda

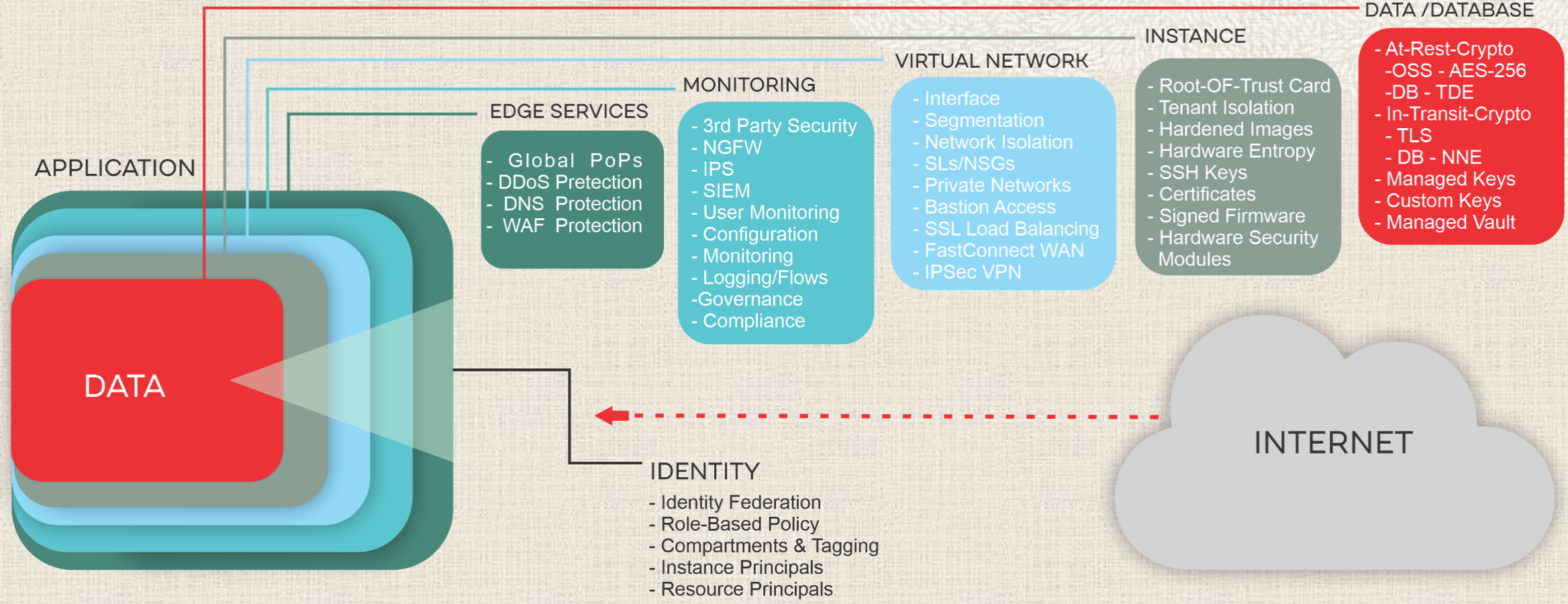
- Shared Security Model
- Certifications & Security Compliance
- Cloud Guard
- VSS – Scanning Service
- WAF
- Vault
- OCI Other Tools for Security
- Secure Architecture

Shared Security Model



Certifications & Security Compliance

Stronger isolation and control from Data to Identity



Security services and features

Functionality	Use case	OCI Service/Feature
Identity and Access Management	Manage user access and policies	OCI IAM
	Manage multi-factor authentication	MFA
	Single sign-on to identity providers	Federation
Data Protection	Encryption for data at rest, in-transit	Storage and DB services
	Discover, classify and protect your data	Data Safe
	Hardware based key storage	Vault
	Centralized key management	
OS and workload management	Patch Management	OS Management service
	Workload isolation	Bare Metal, Dedicated VM Hosts
	Log API calls	Audit
Infrastructure Protection	Network security controls	VCN NSG, SL
	Filter Malicious web traffic	Web Application Firewall
	DDoS Protection	In-built

Certifications & Security Compliance

Global

- SOC 1 : SOC 2 : SOC 3
- 27001 : 27017 : 27018
- Level 1
- US Privacy Shield

Government

- DoD DISA SRG IL2
- DoD DISA SRG IL5
- Moderate – Agency ATO
- VPAT – Section 508
- G-Cloud 11 - UK
- Model Clauses - EU

Industry

- HIPAA
- PCI DSS
- FISC - Japan
- IG Toolkit - UK
- FINMA - Switzerland

Regional

- GDPR - EU
- BSI C5 - Germany
- TISAX - Germany
- PIPEDA - Canada
- Cyber Essentials Plus - UK
- My Number - Japan
- Cloud Security Principles - UK

ORACLE

Certifications & Security Compliance

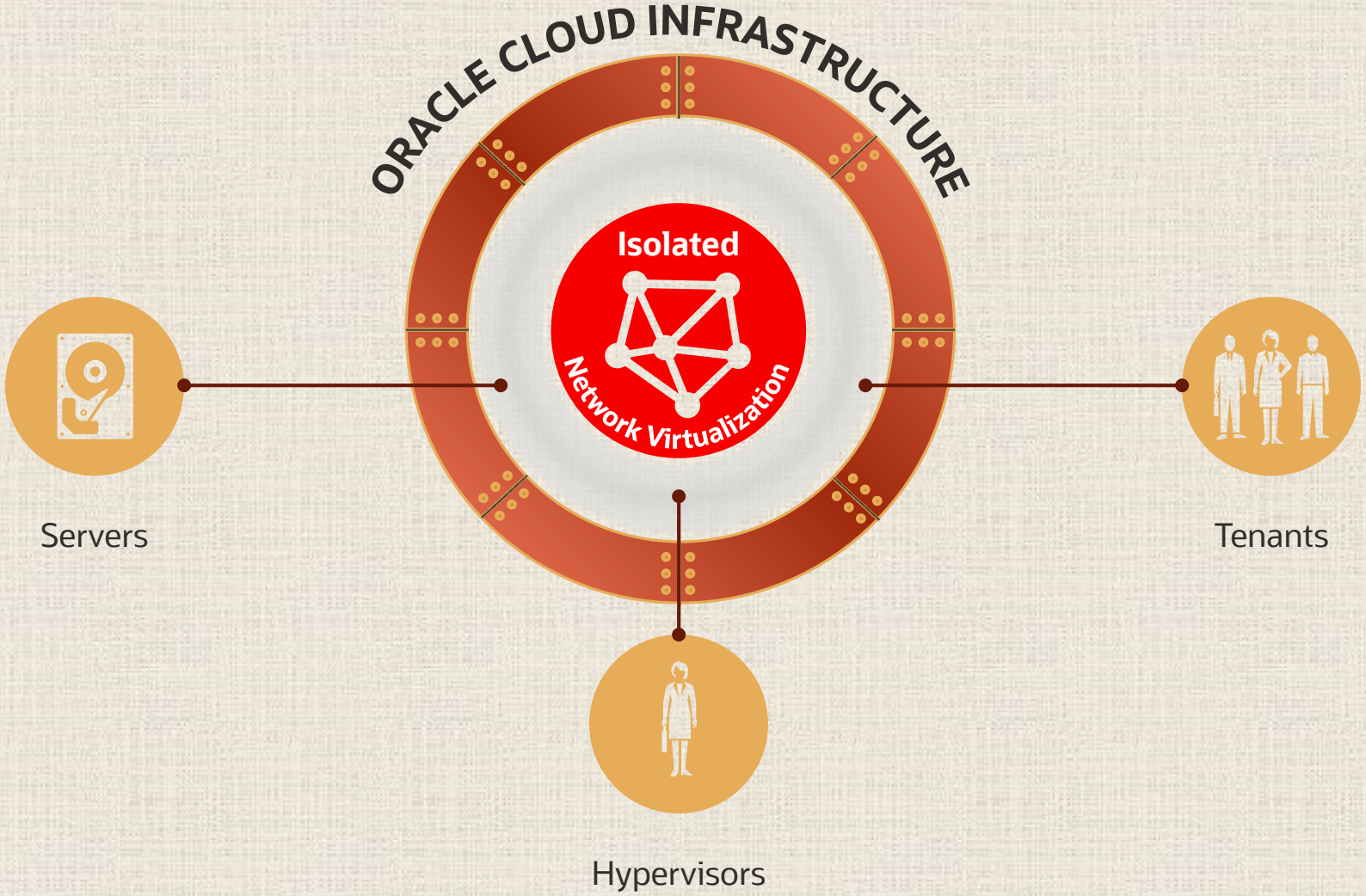
Zero Trust Architecture Model - https://www.oracle.com/security/what-is-zero-trust

- 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

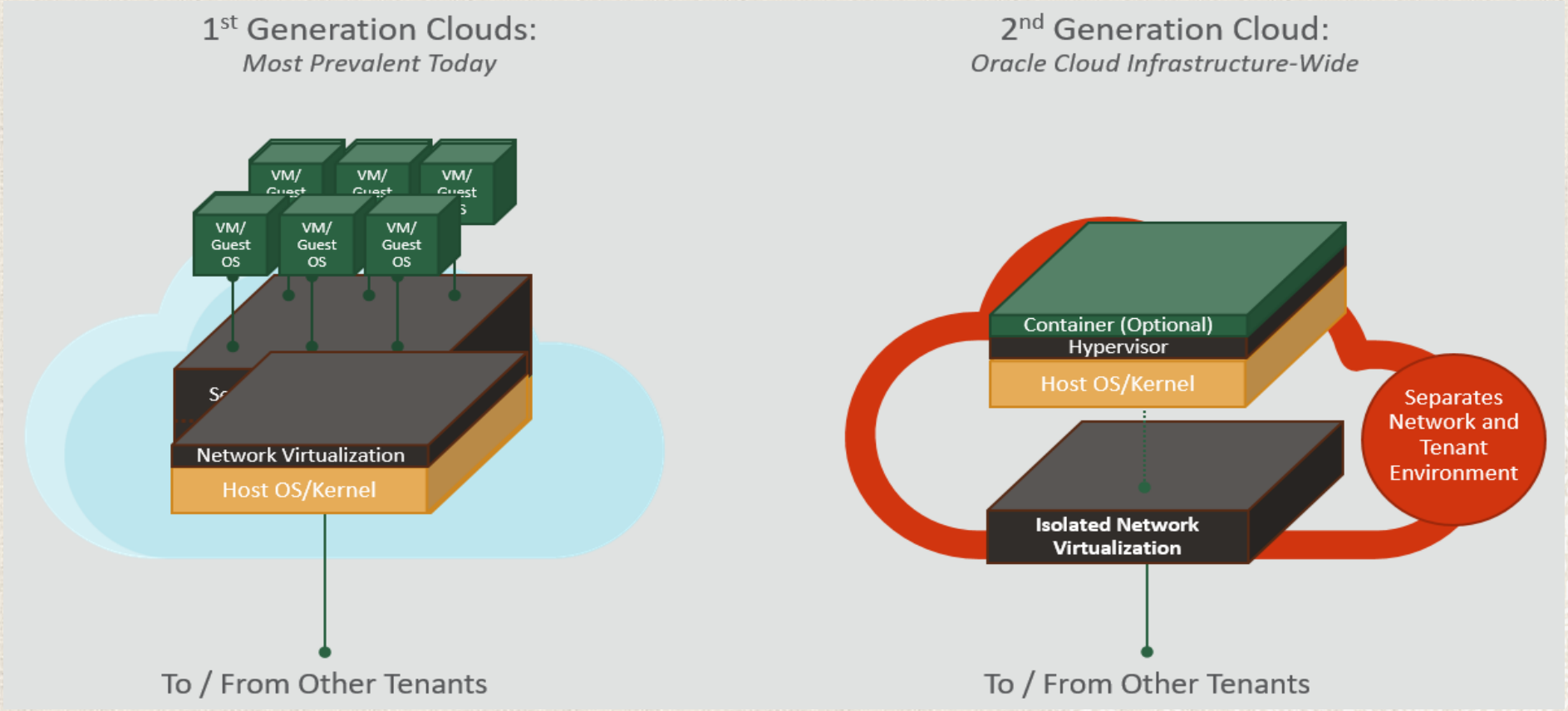
- Reduce risk
- Fine-Grained Control Access
- Enhance Organization's Security posture

Least Trust Design – Assumption of Compromise



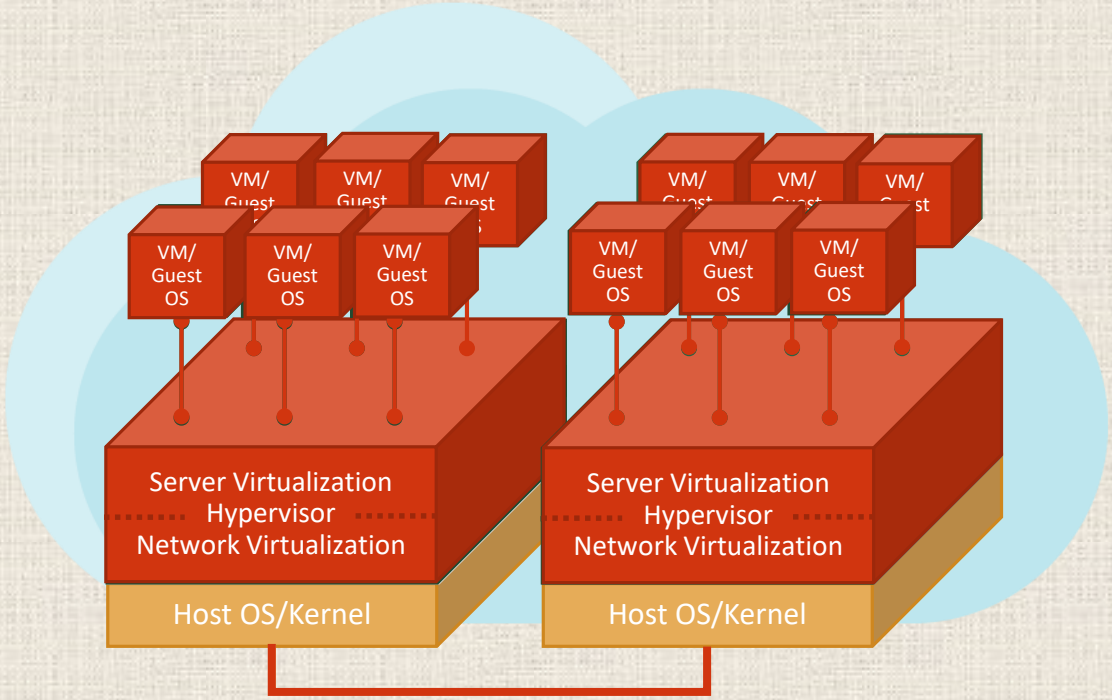
Certifications & Security Compliance

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

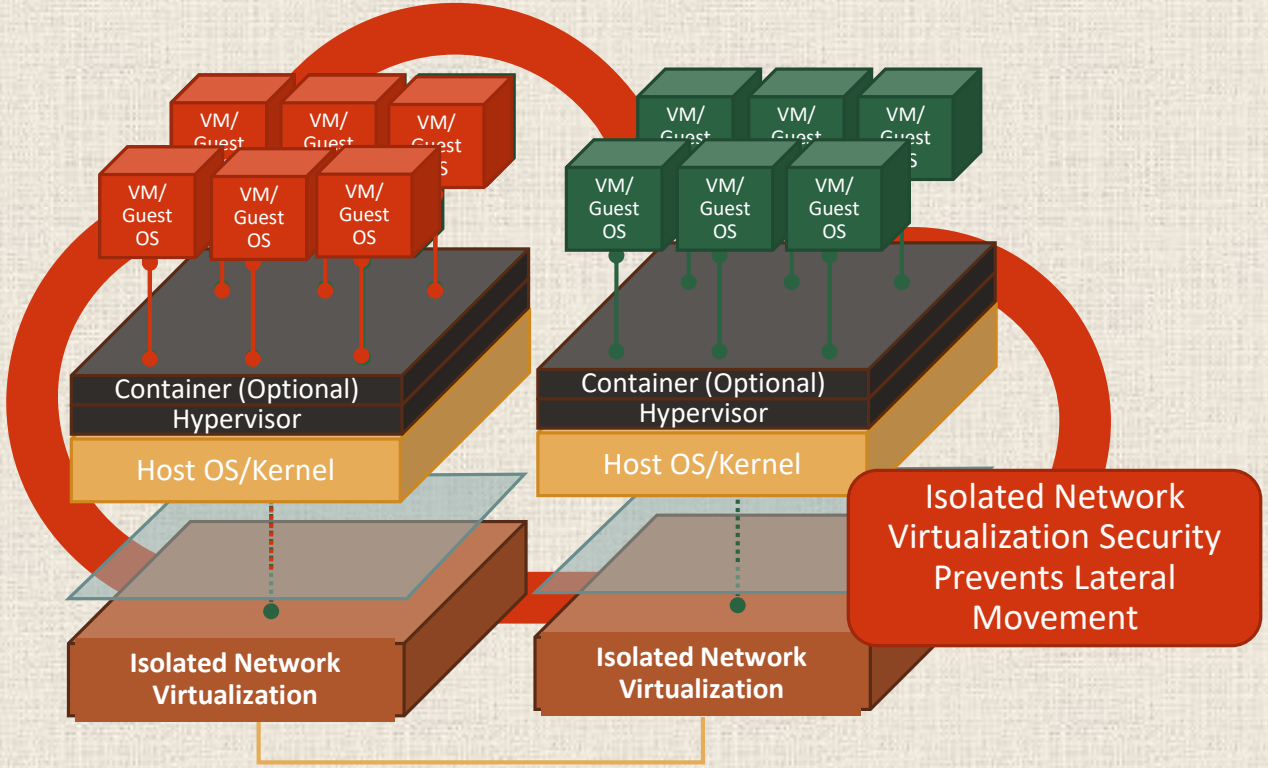


Threat Containment & Reduced Risk

1st Generation Cloud



Oracle 2nd Generation Cloud



ORACLE

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

Detect Problems

- Check Configuration
- Monitor Activities

Apply Response

- Correlate Problems
- Apply Fix

Examine Targets

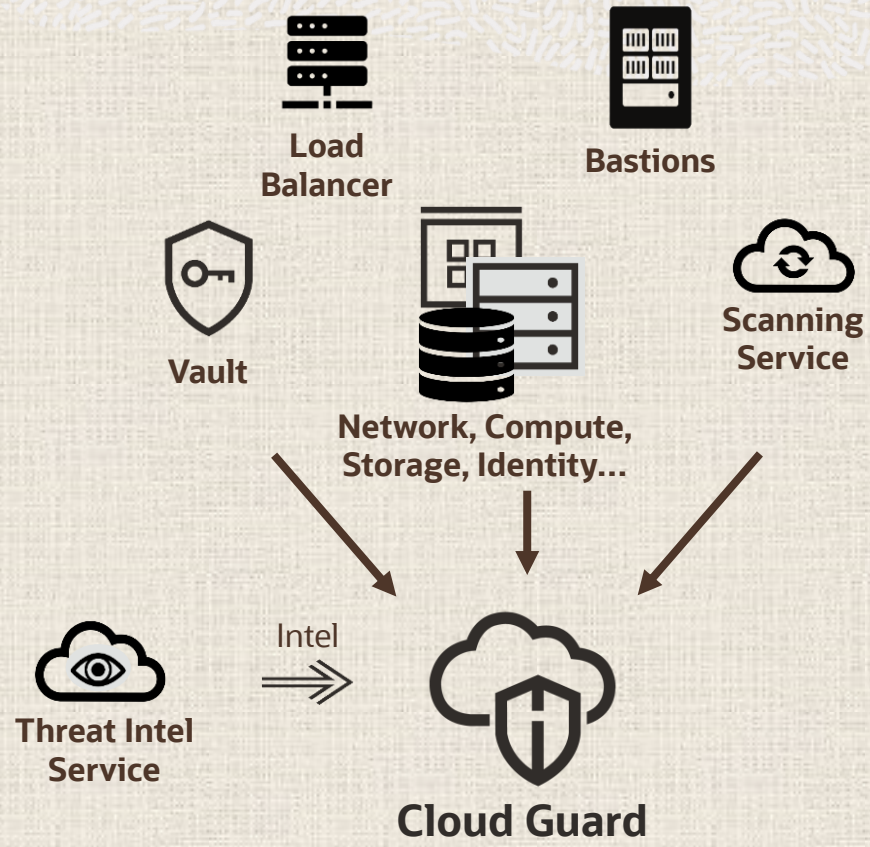
- Quantify Security Stance
- Assess Risk Posture

Cloud Guard

Cloud Security Posture Management – (CSPM)

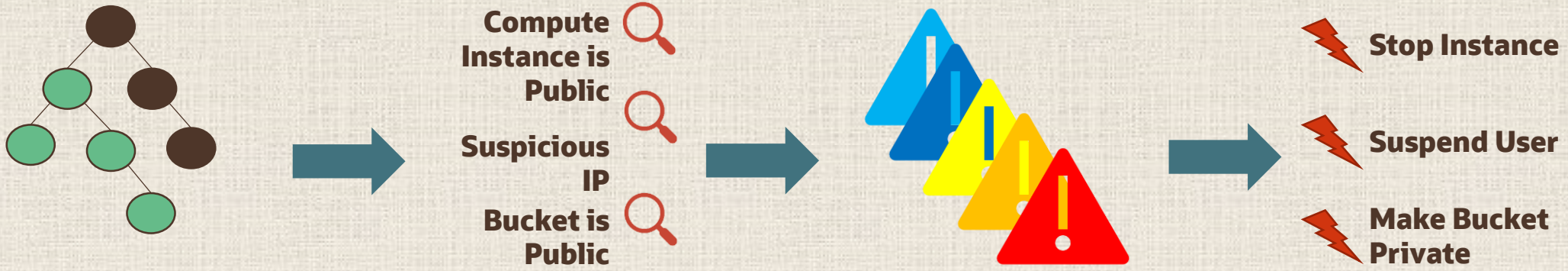
Provides a global view of security problems in a single console

Includes OCI Configuration, OCI Activity, and Threat Detector with more coming



Cloud Guard

Few Concepts



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.

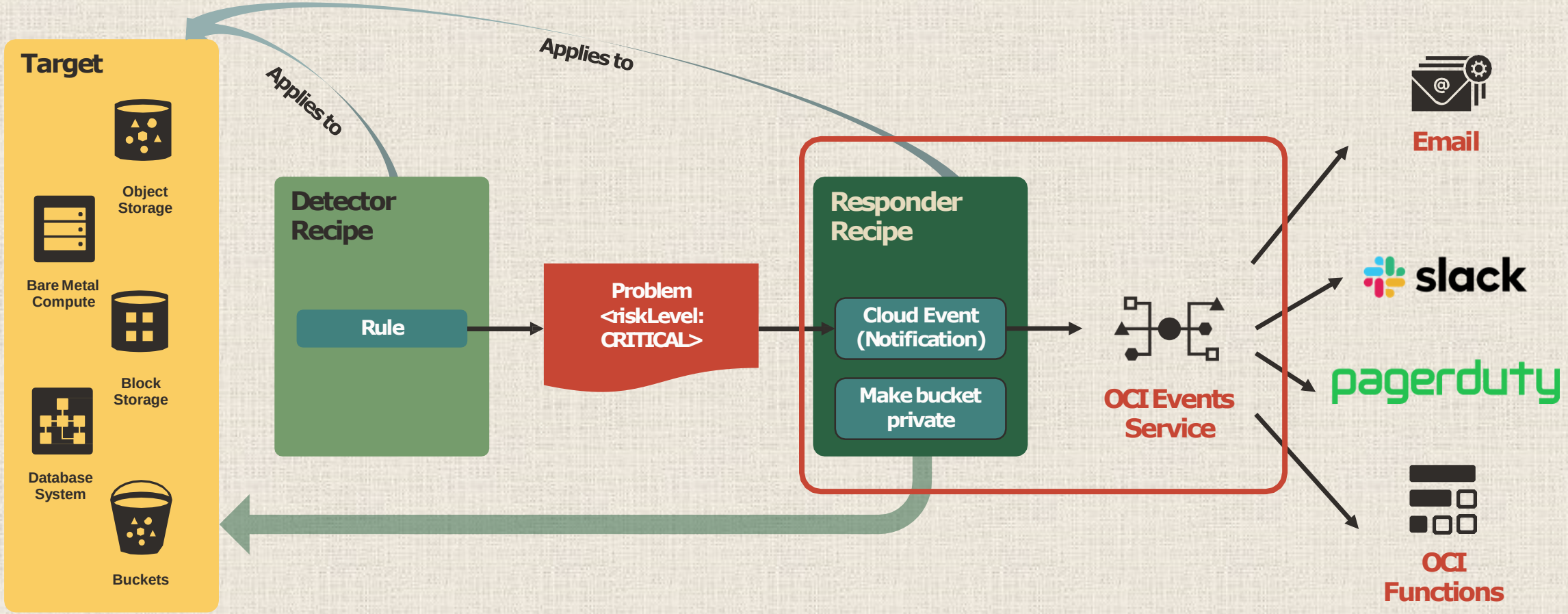
Problems

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

Responders

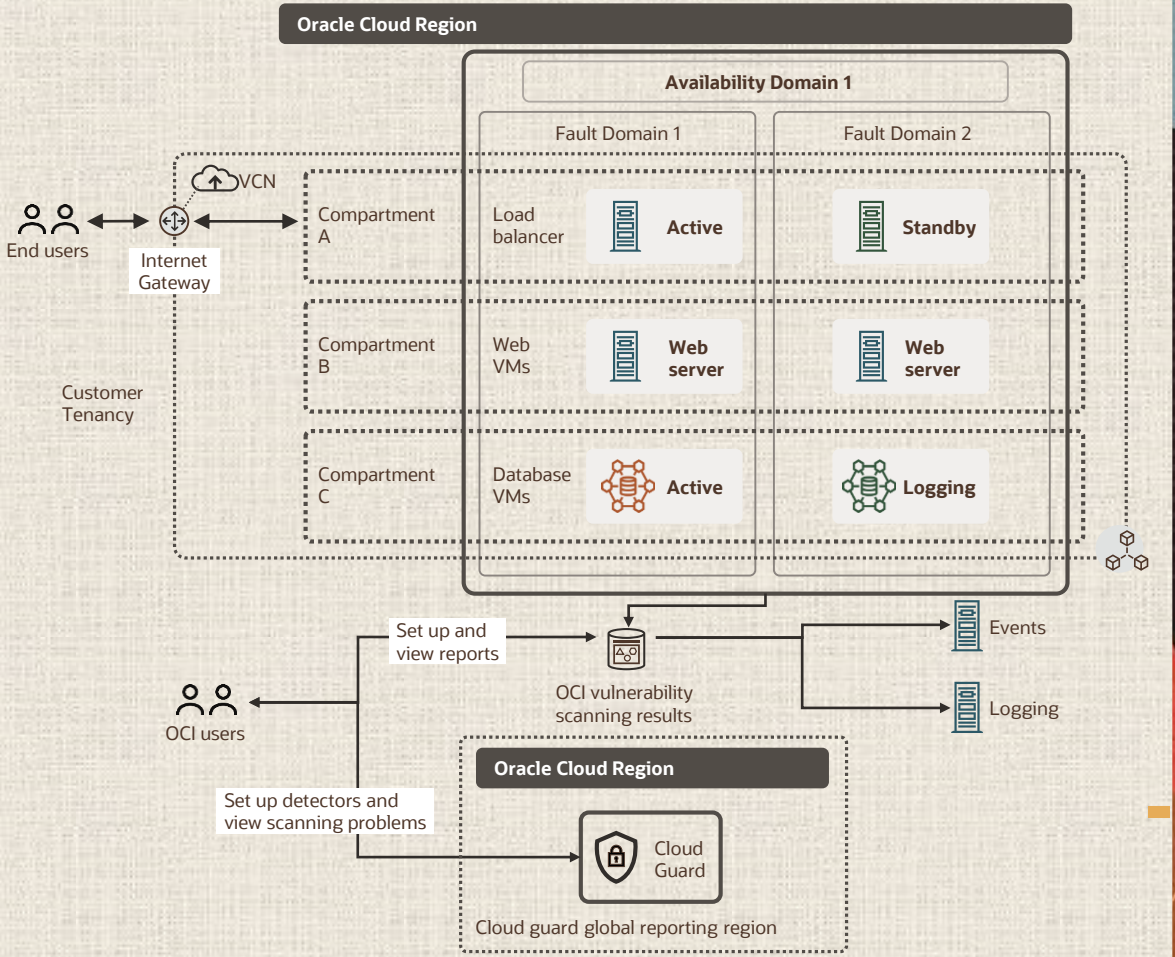
Responders notifies and take corrective actions for security problems.

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

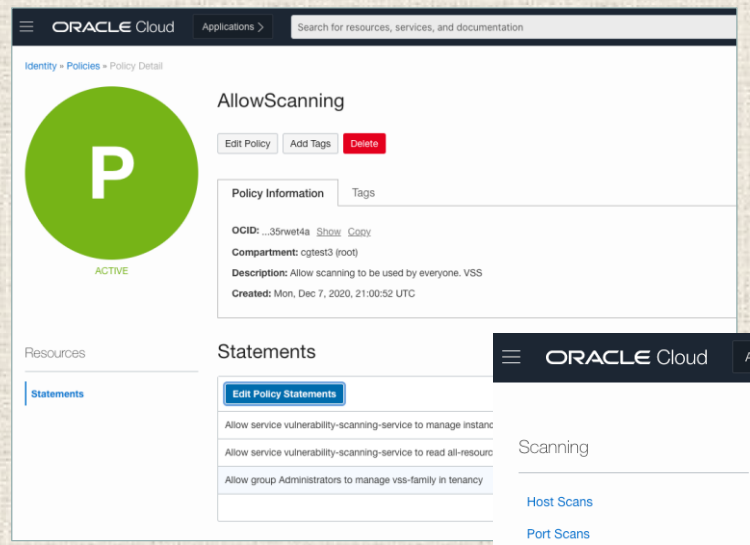


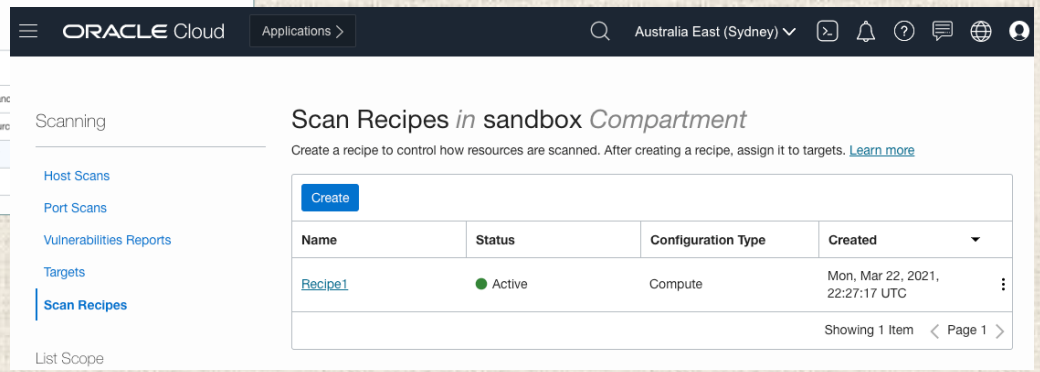
VSS Configuration

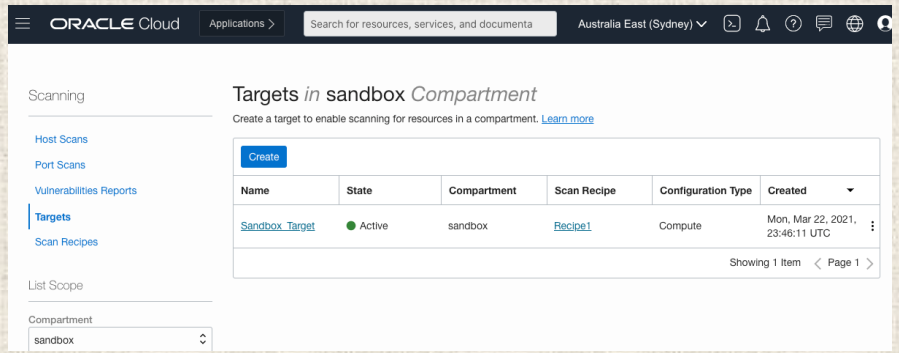
Customers do not need to install anything or worry about updating agents

Customers only need to:

- Create a policy to give permissions to VSS and their administrators
- Create a scan recipe to set up the scanning configuration settings
- Create a scan target to select which compute instances get scanned



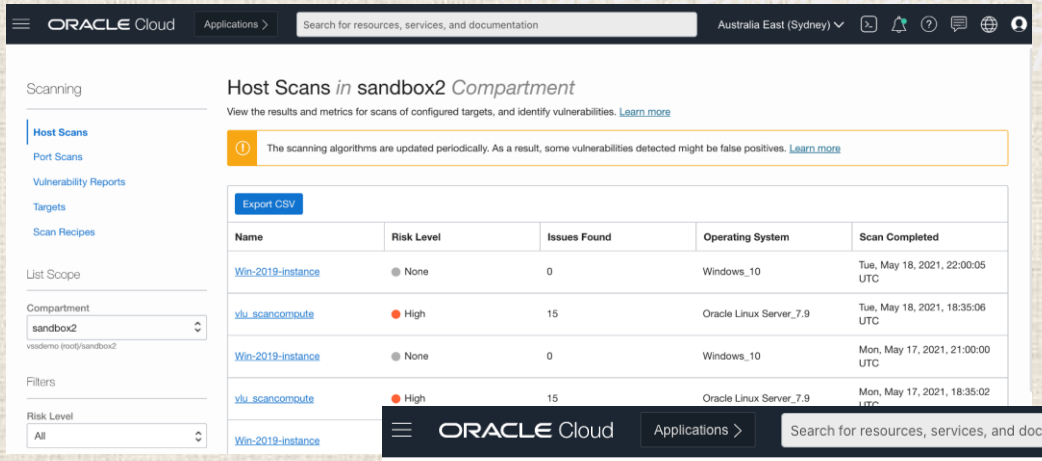


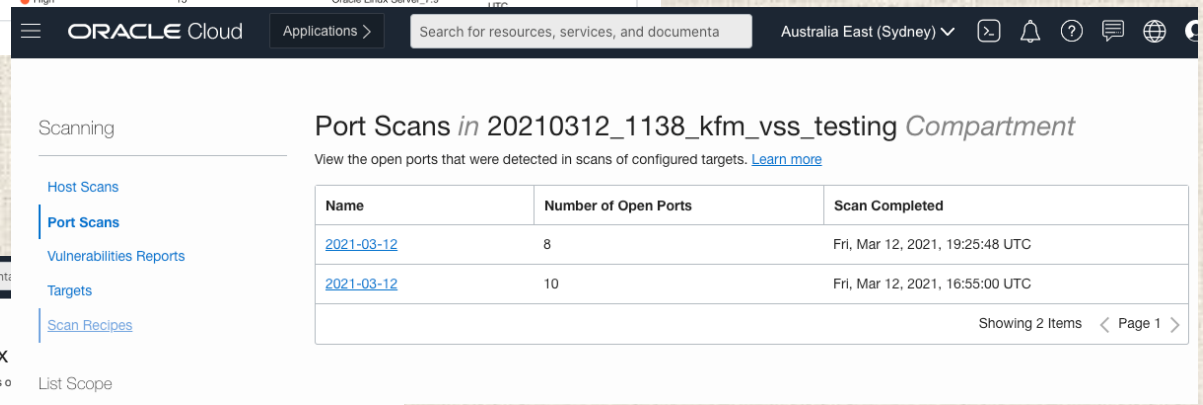


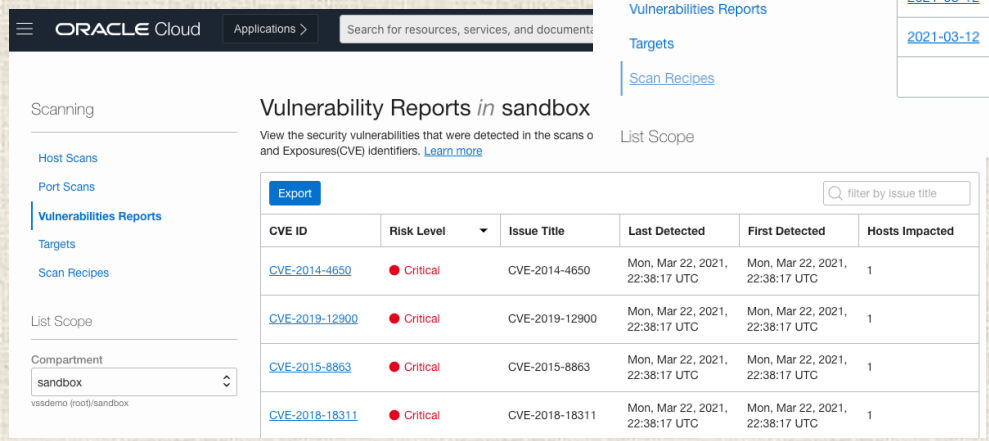
VSS Reports

Once configured the customer will see results within an hour and then daily.

The Scanning Reports cover hosts, ports, benchmarks and overall vulnerabilities across all resources







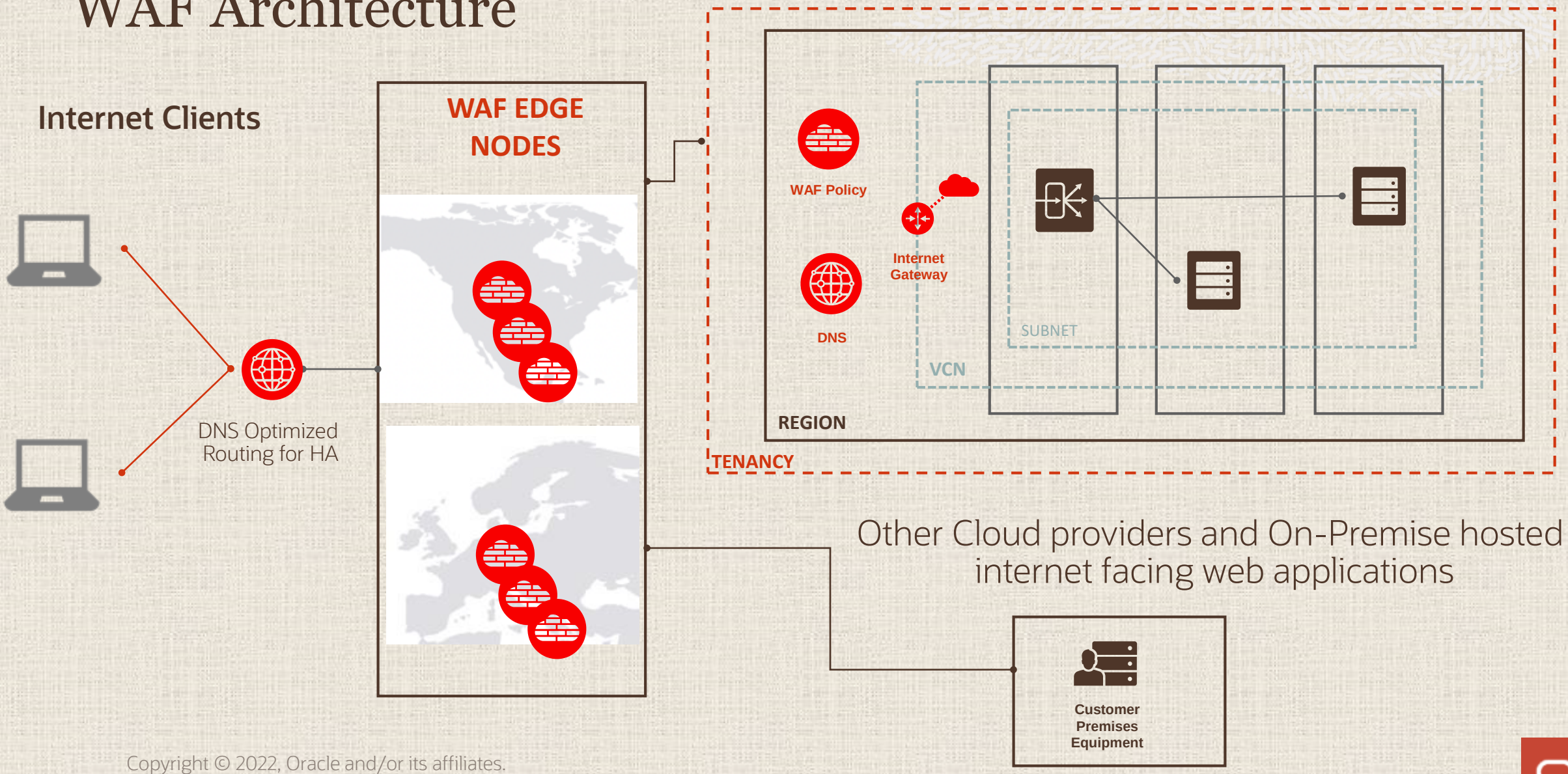
WAF Overview

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

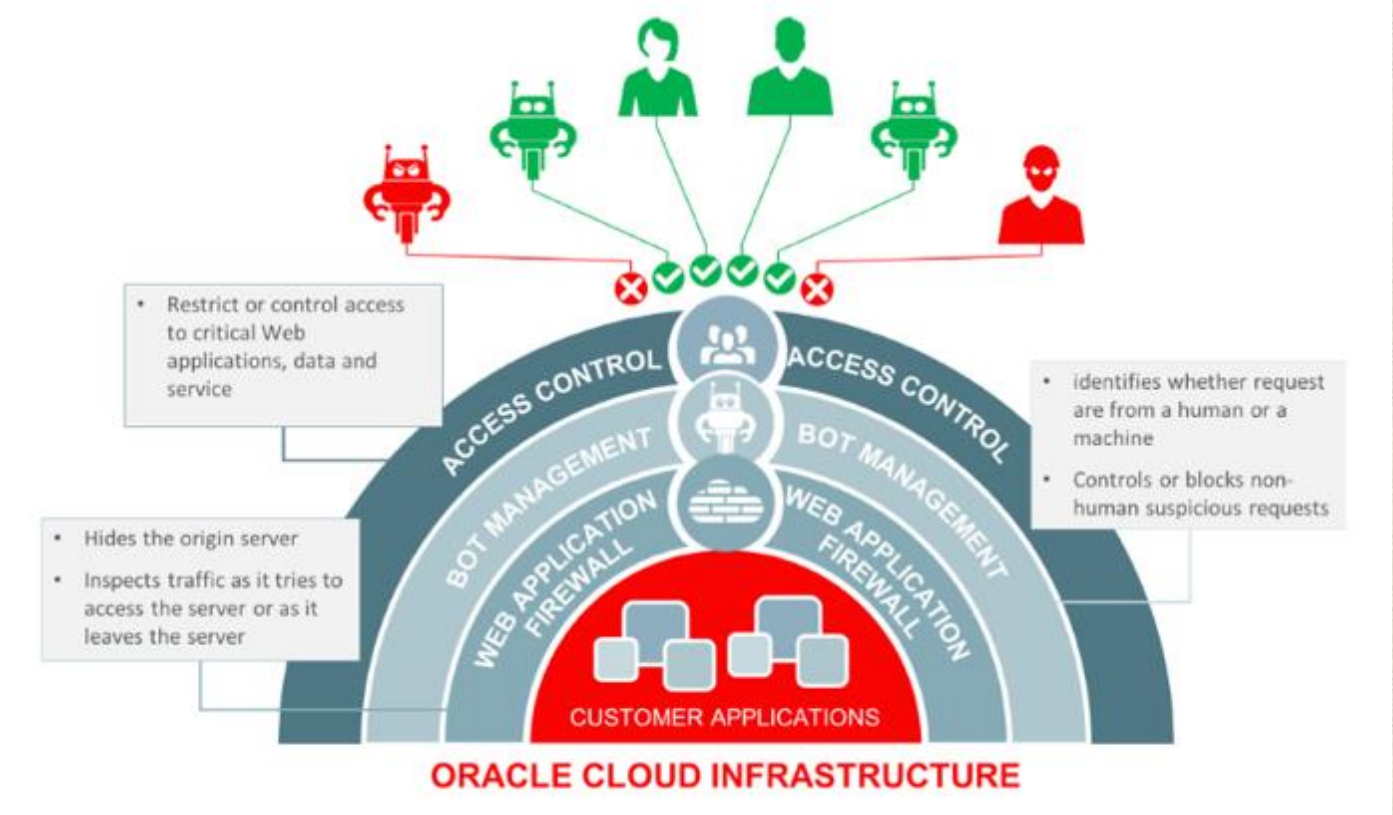
- Whitelisting: Allows you to manage which IP addresses appear on the IP whitelist

  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



ORACLE

OCI Vault

Oracle Cloud Infrastructure Vault is **a managed service that lets you centrally manage the encryption keys** that protect your data and the secret credentials that you use to securely access resources.

Keys and secrets not exposed in code or config files

Secrets are credentials such as passwords, certificates, SSH keys, or authentication tokens

Keys are logical entities that represent one or more key versions, each of which contains cryptographic material. A key's cryptographic material is generated for a specific algorithm that lets you use the key for encryption or in digital signing

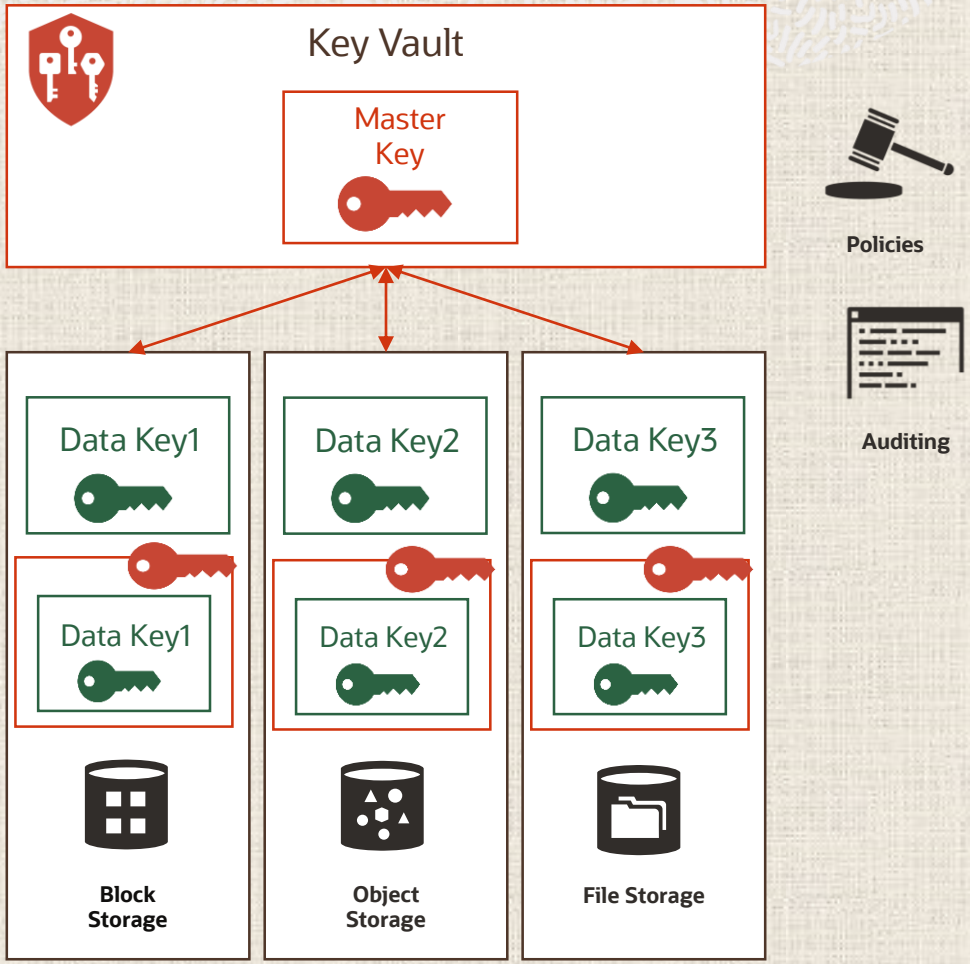
Keys basic concept

Two-tiered hierarchy for keys

- Data encryption keys (DEK) used to encrypt customer data
- Master encryption keys (MEK) to encrypt data keys
- IAM policies to authorize access to master keys
- Audit logs to monitor all key related activity

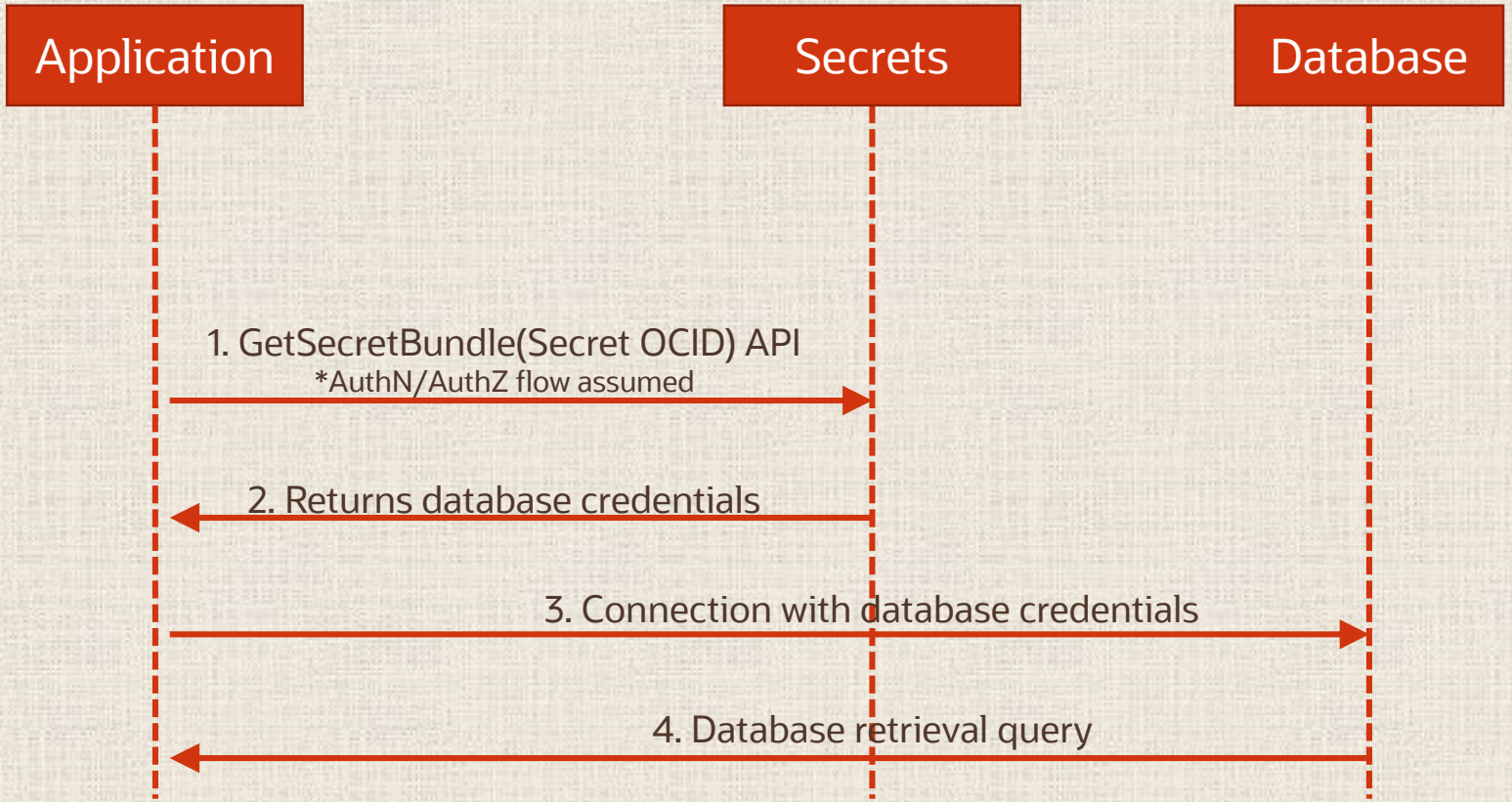
Benefits of envelope encryption

- Easier to manage a small number of master keys than numerous data keys
- Limits blast radius of compromised resources and their keys
- Key rotation doesn't generate a complete data re-encryption



Example Use Case: Application Runtime

- Secrets are stored under paths
- Rotation can be programmatically implemented
- Integrates with any compute shapes, Oracle DBs, Function and Terraform
- Integrated with Audits logs and possible SIEM integration



OCI Other Tools for Security

Bastion-as-a-Service

- Jump-Server/Jumpbox role
- CIDR Allow List
- Port Forwarding
- Managed SSH sessions

OS Management

- Automates OS related maintenance tasks
- Package Management
- Patch Install Automation
- Available for Linux & Windows

Both for free

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

Comments, Questions, Answers

WAF does not work as regular Firewall

Gen2 Cloud has better tenant virtual network isolation than other CSPs

Thank you

Alexandre Fagundes
LAD Partner Enablement

Oracle Cloud Security Overview