ORACLE

OCI Security Overview

Alexandre Fagundes

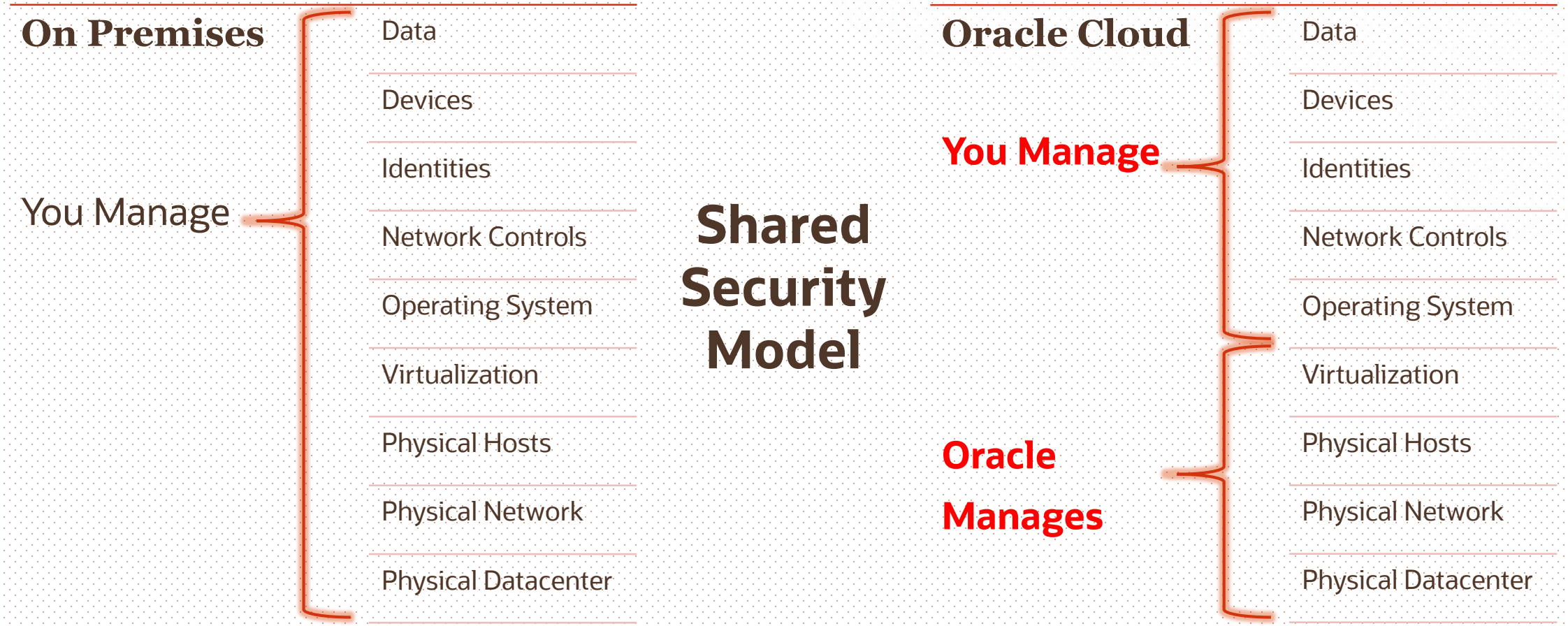
Cloud Architect, Oracle Latin America

Oracle Cloud Security

Outline

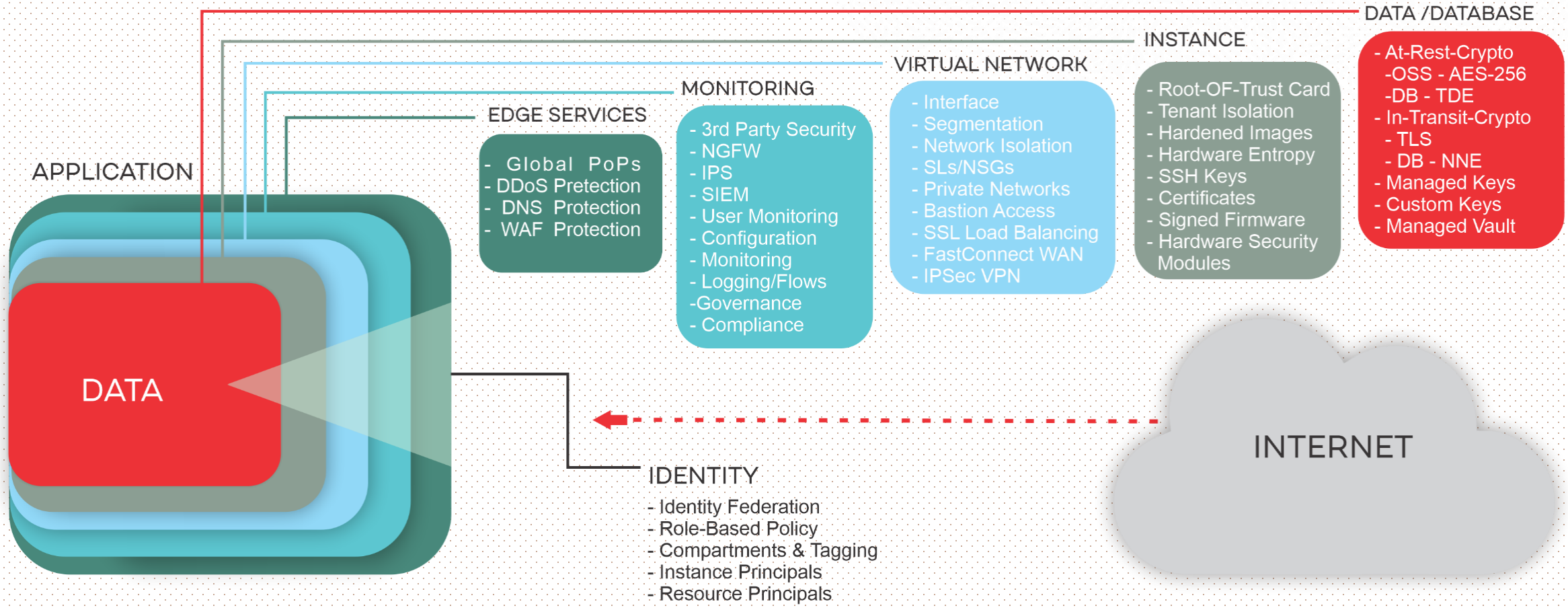
- Shared Security Model
- Certifications & Security Compliance
- Cloud Guard
- VSS – Scanning Service
- WAF
- OCI Other Tools for Security
- Secure Architecture

Shared Security Model

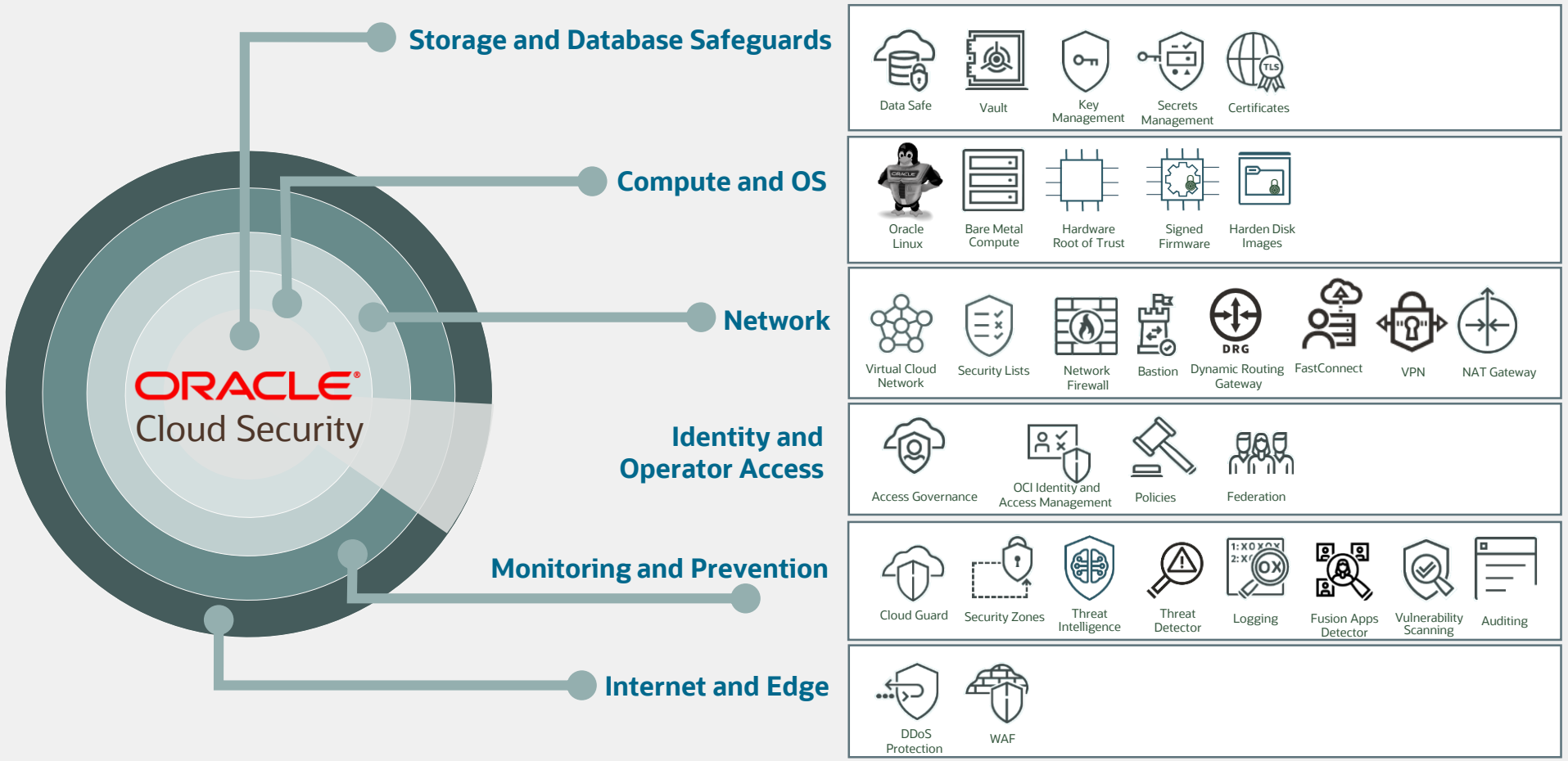


Certifications & Security Compliance

Stronger isolation and control from Data to Identity



Oracle offers a full stack of cybersecurity capabilities



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

Certifications & Security Compliance

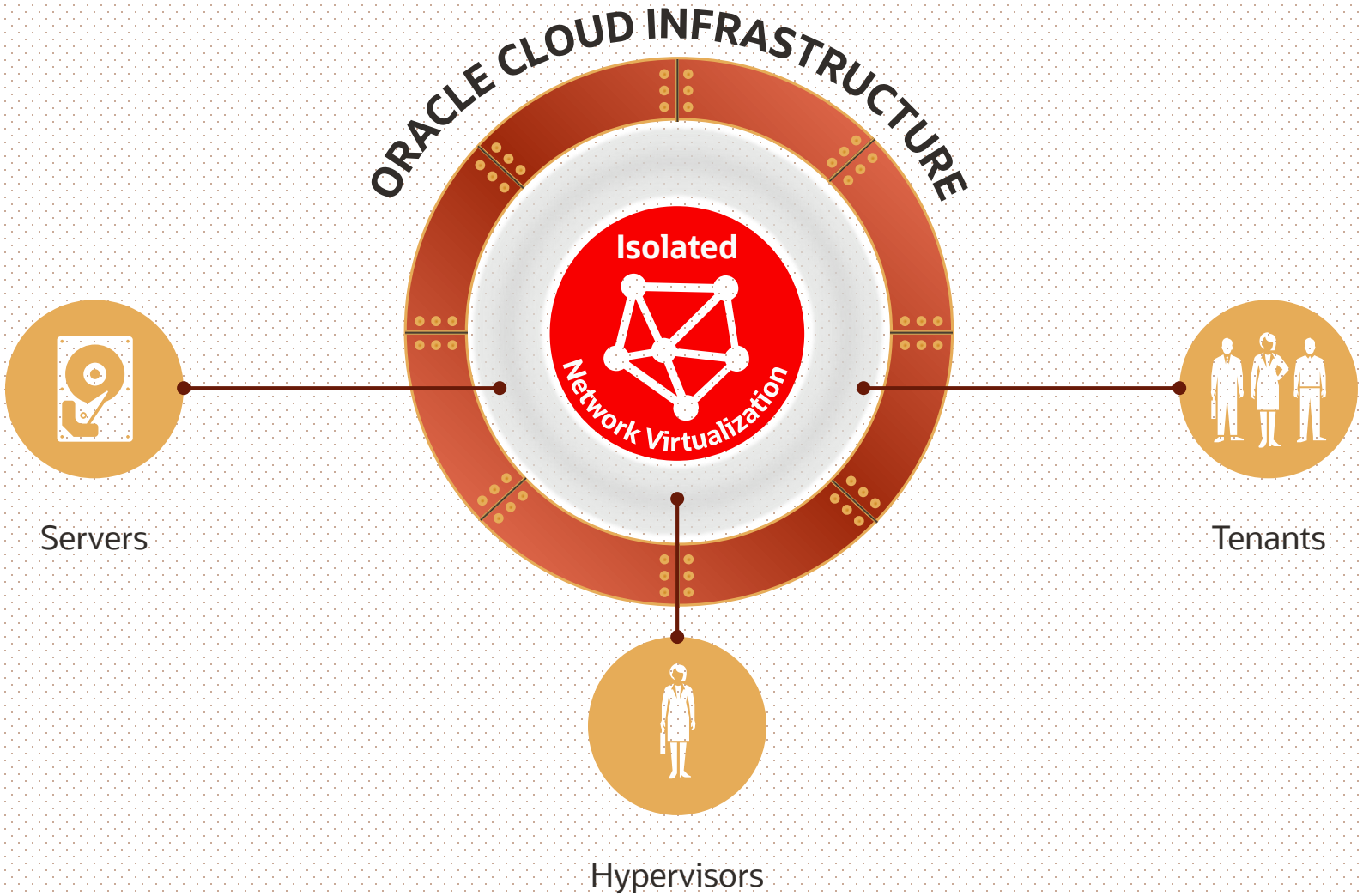
Zero Trust Architecture Model - https://www.oracle.com/security/what-is-zero-trust

- 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

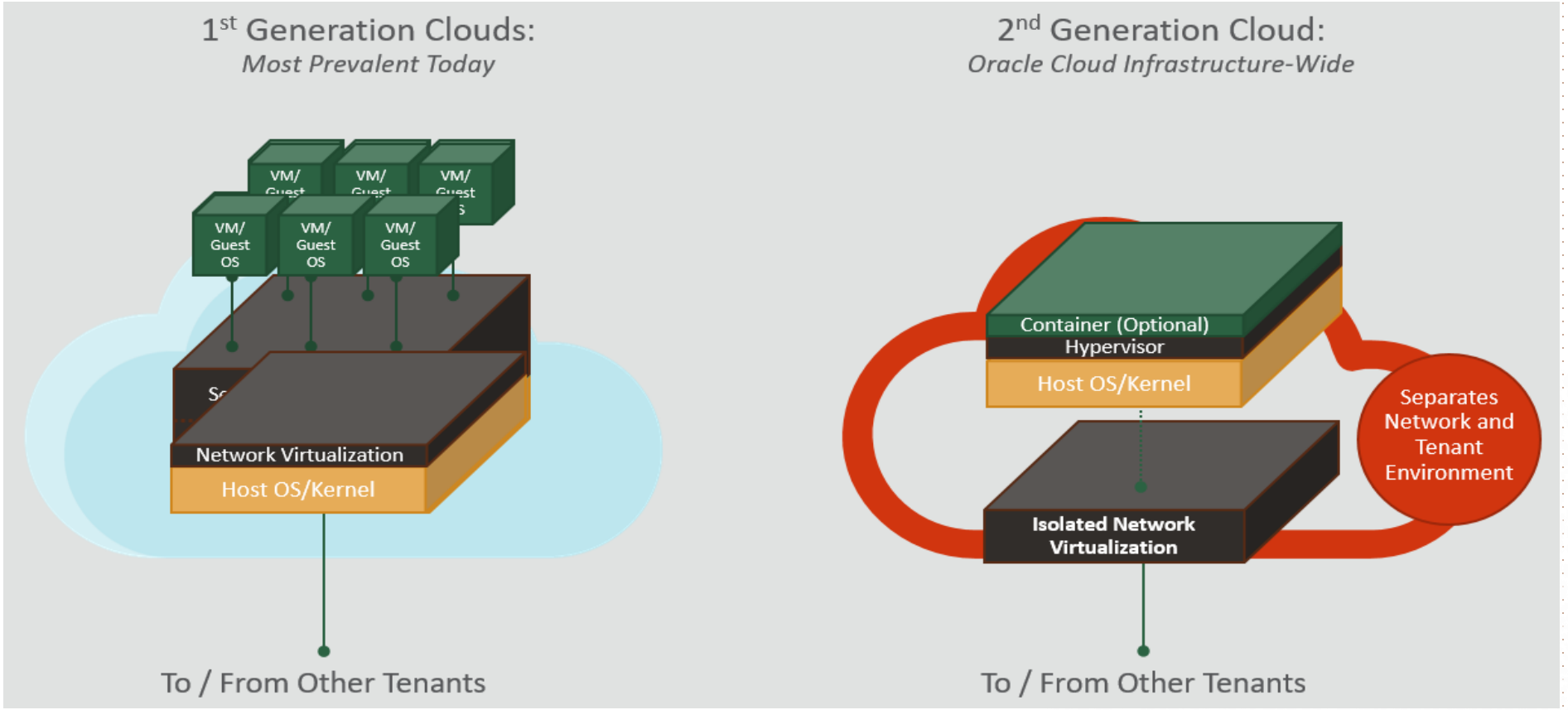
- Reduce risk
- Fine-Grained Control Access
- Enhance Organization's Security posture

Least Trust Design – Assumption of Compromise

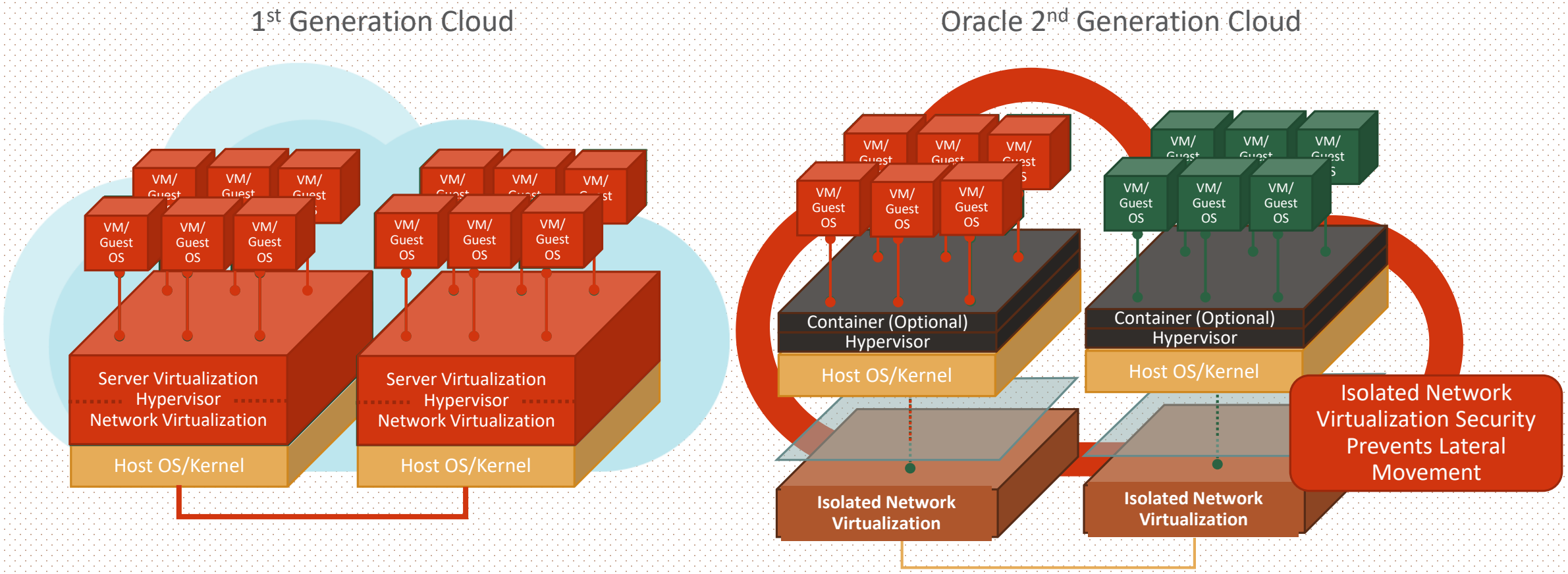


Certifications & Security Compliance

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



Threat Containment & Reduced Risk



ORACLE

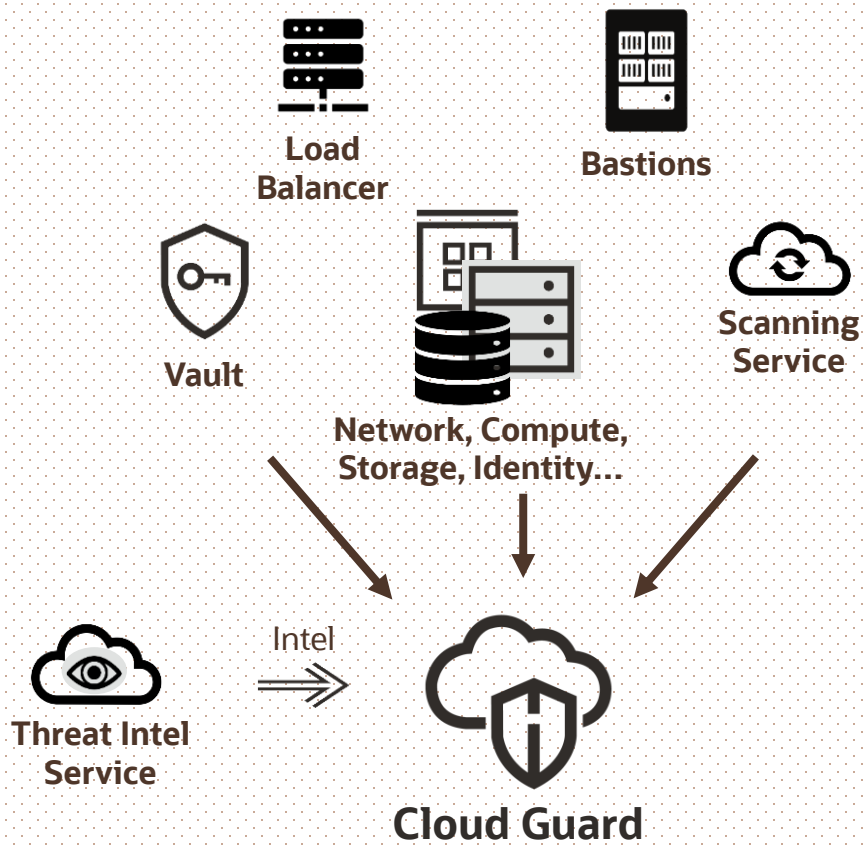
Cloud Guard

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

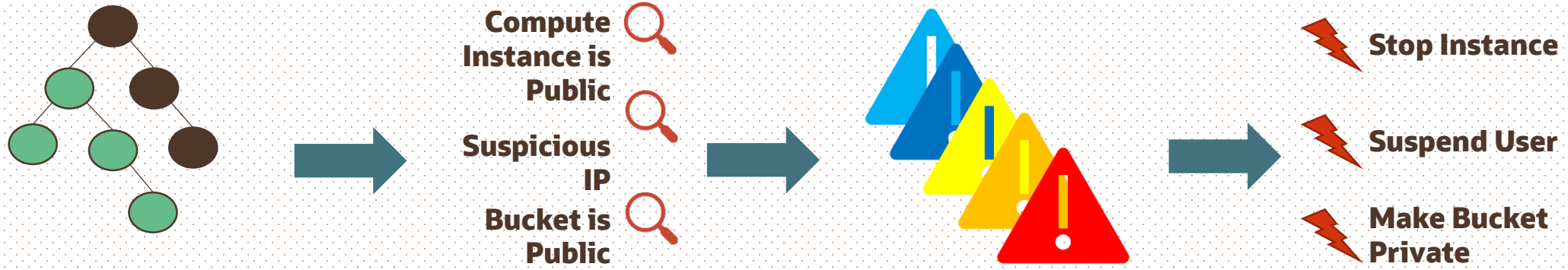
Free Service

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

Easily integrate with external tools using OCI Events



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.

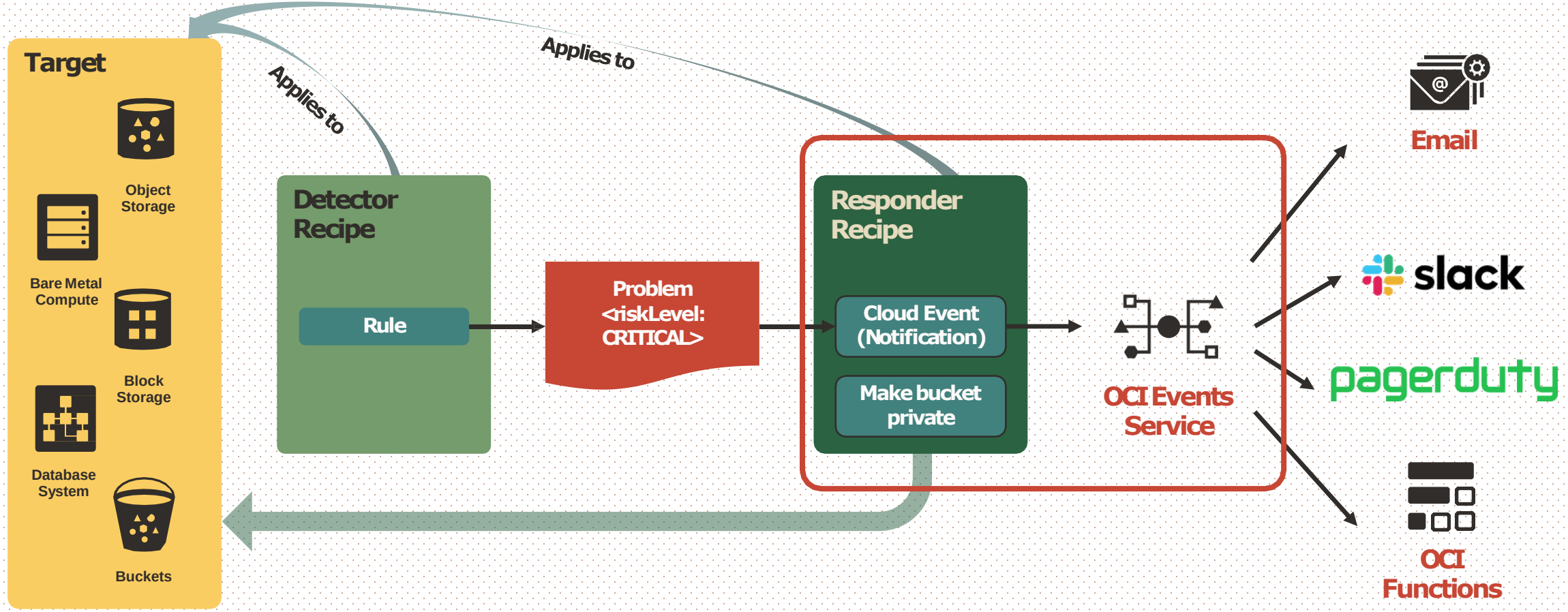
Problems

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

Responders

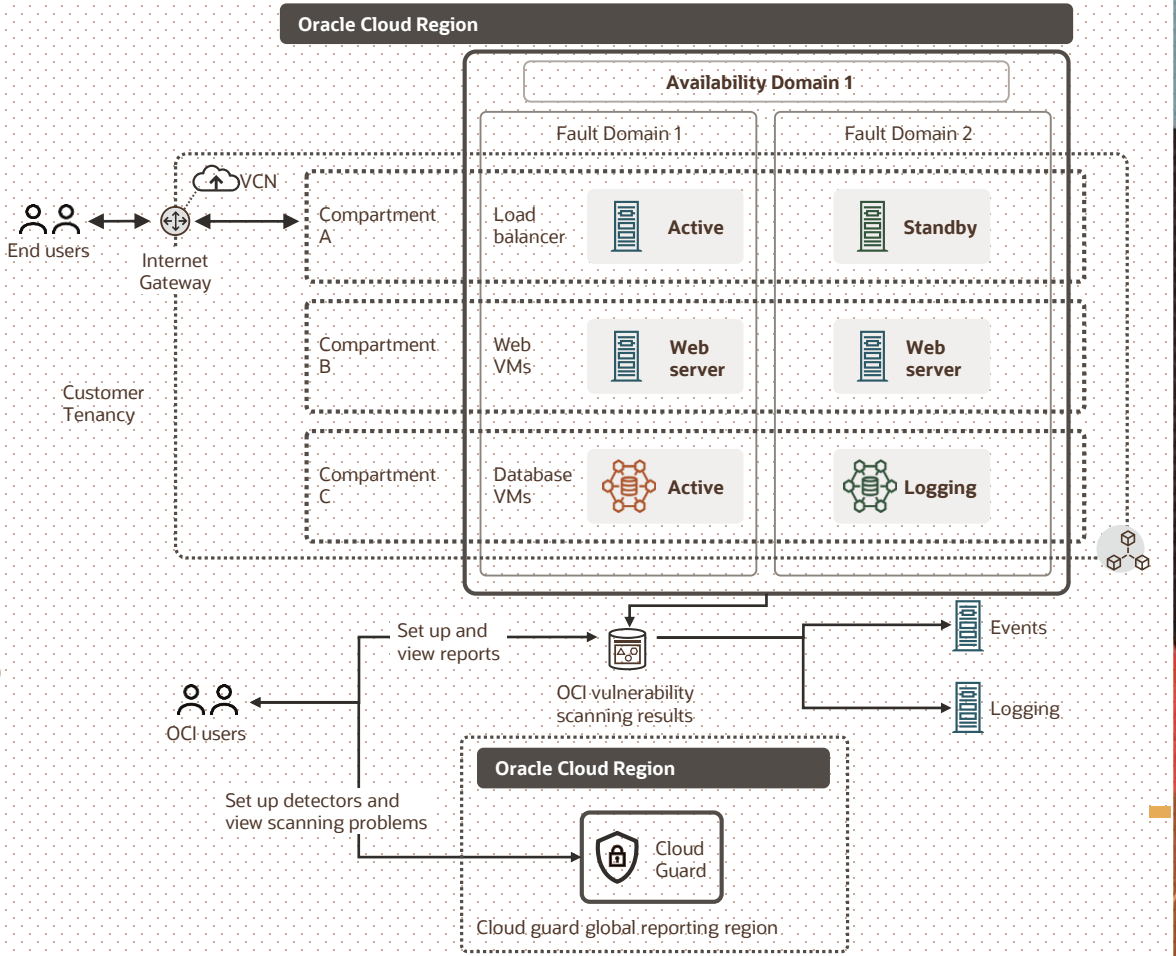
Responders notifies and take corrective actions for security problems.

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

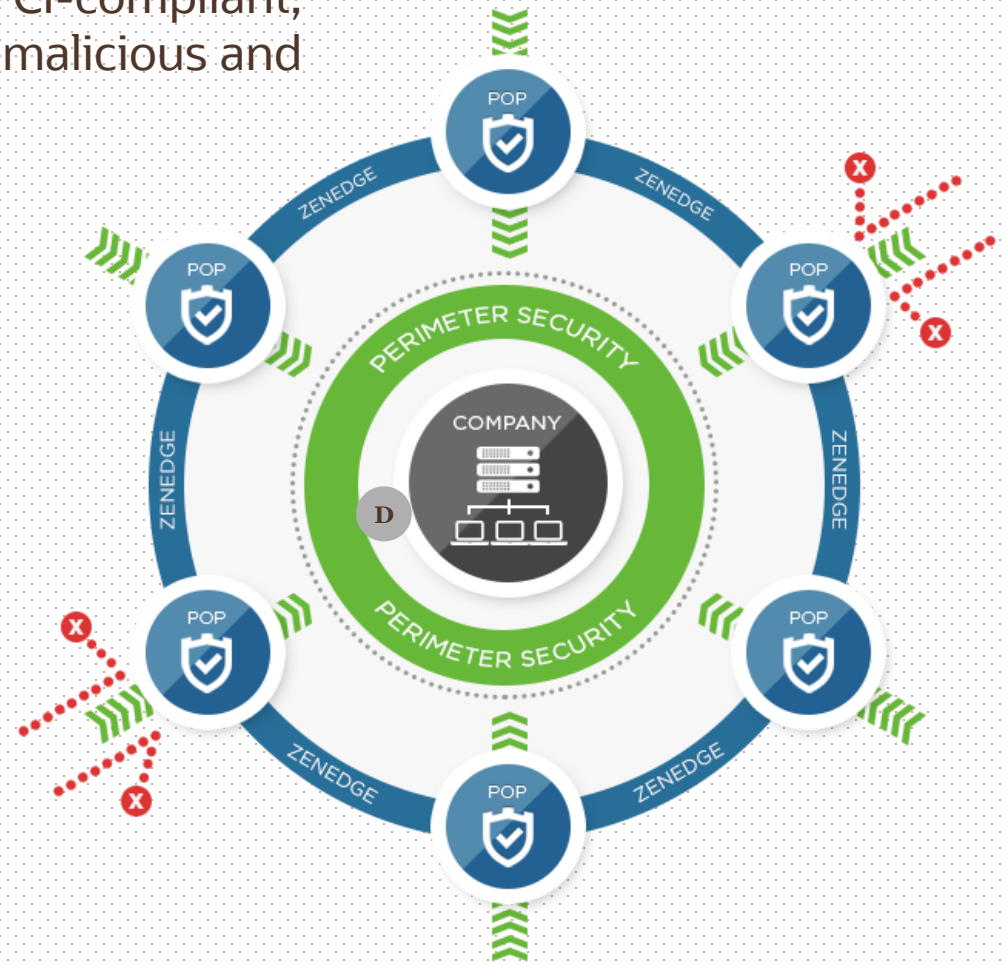


WAF Overview

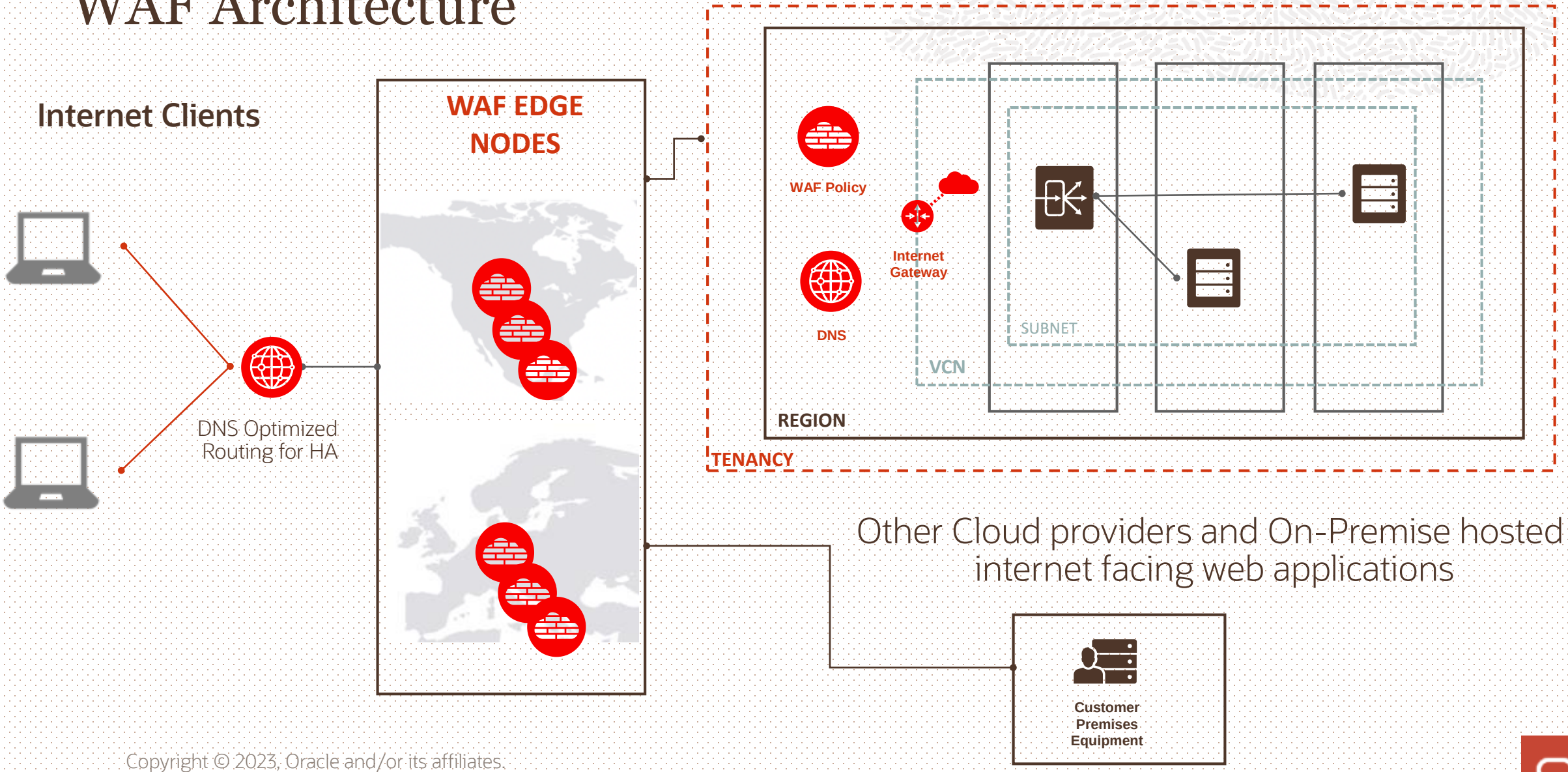
OCI Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic

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

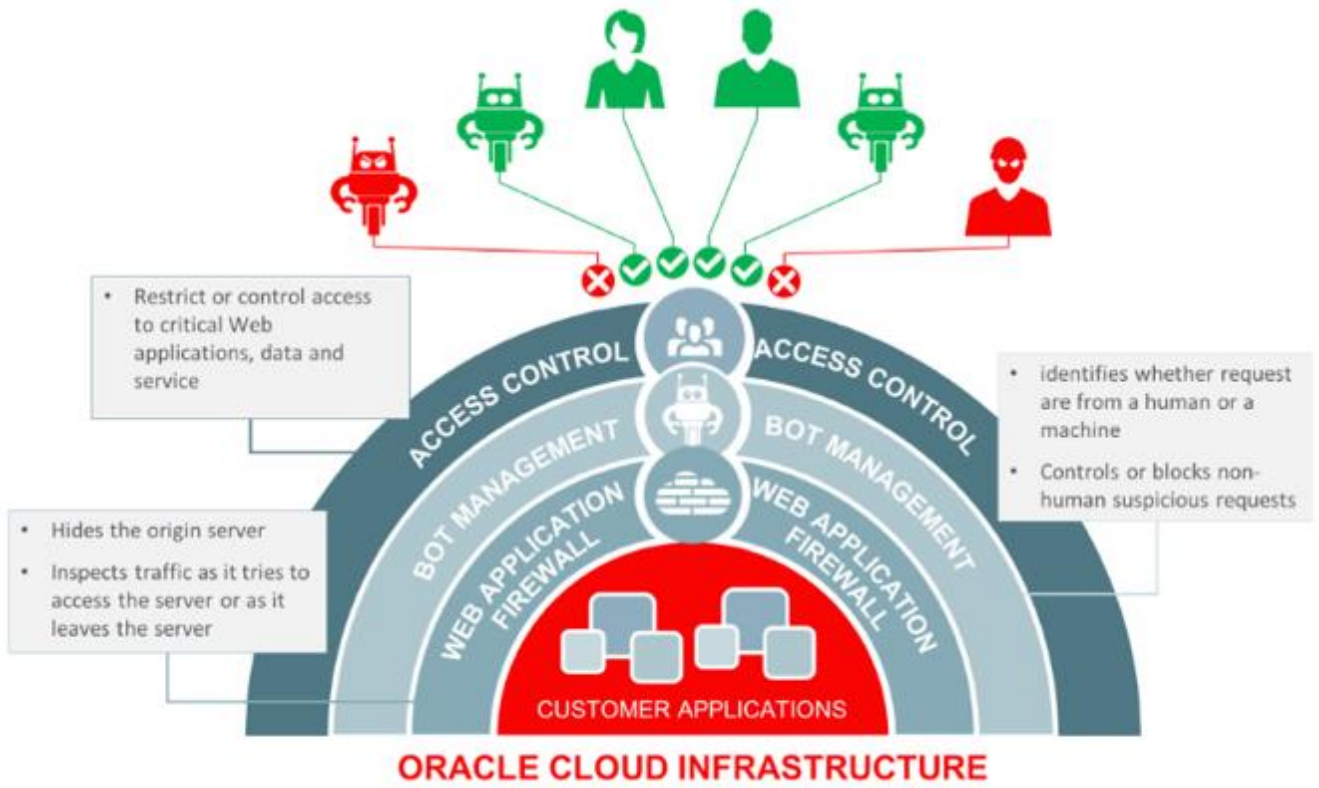
- Whitelisting: Allows you to manage which IP addresses appear on the IP whitelist

  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



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

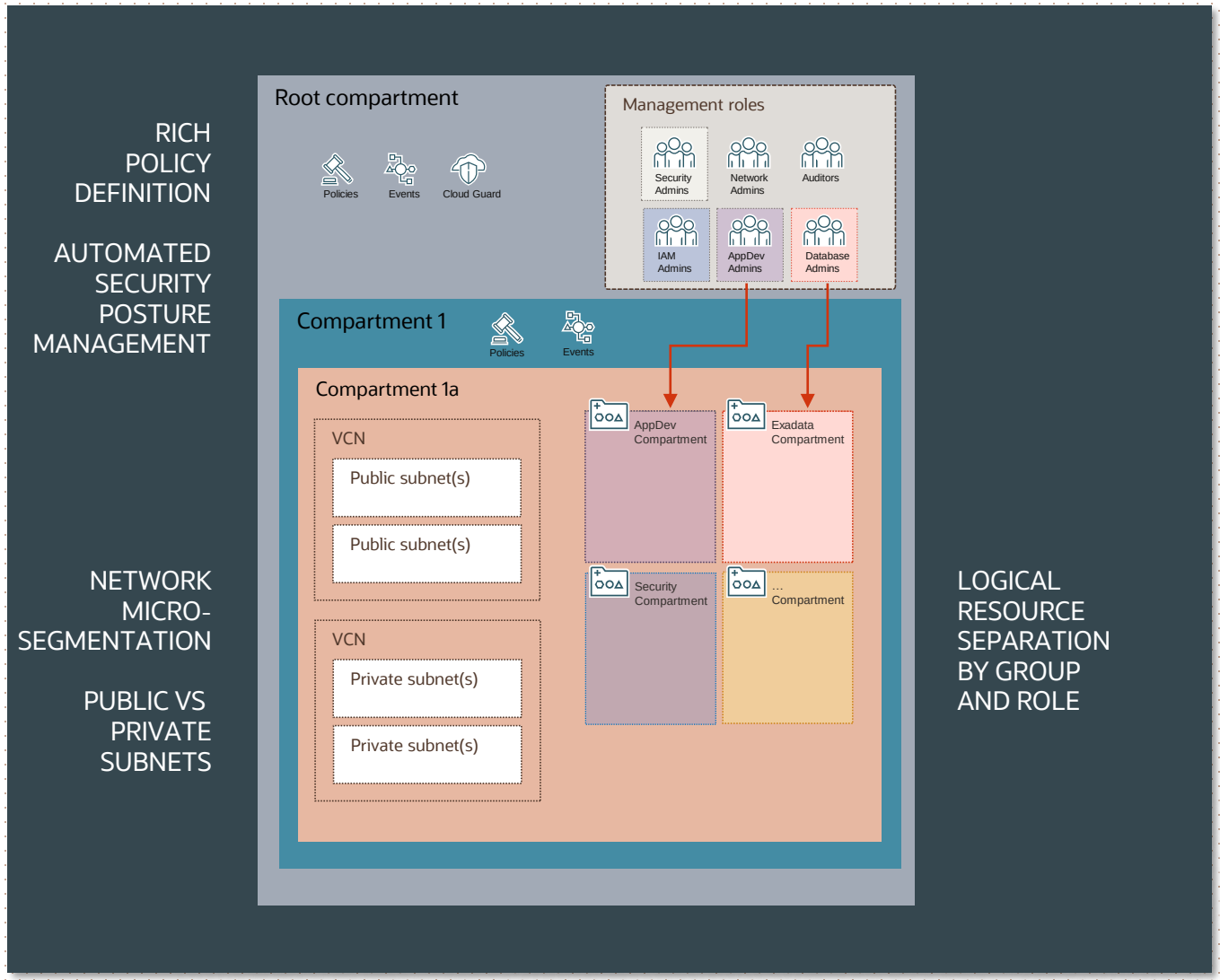
CIS Compliance checking script → Applicable to any existing tenancy

[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

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:

Thank you

Alexandre Fagundes
Cloud Architect, Oracle Latin America

Oracle Cloud Security