Oracle Cloud Infrastructure Security Overview

L100

Umair Siddiqui
Product Manager
Oracle Cloud Infrastructure
September, 2019

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.

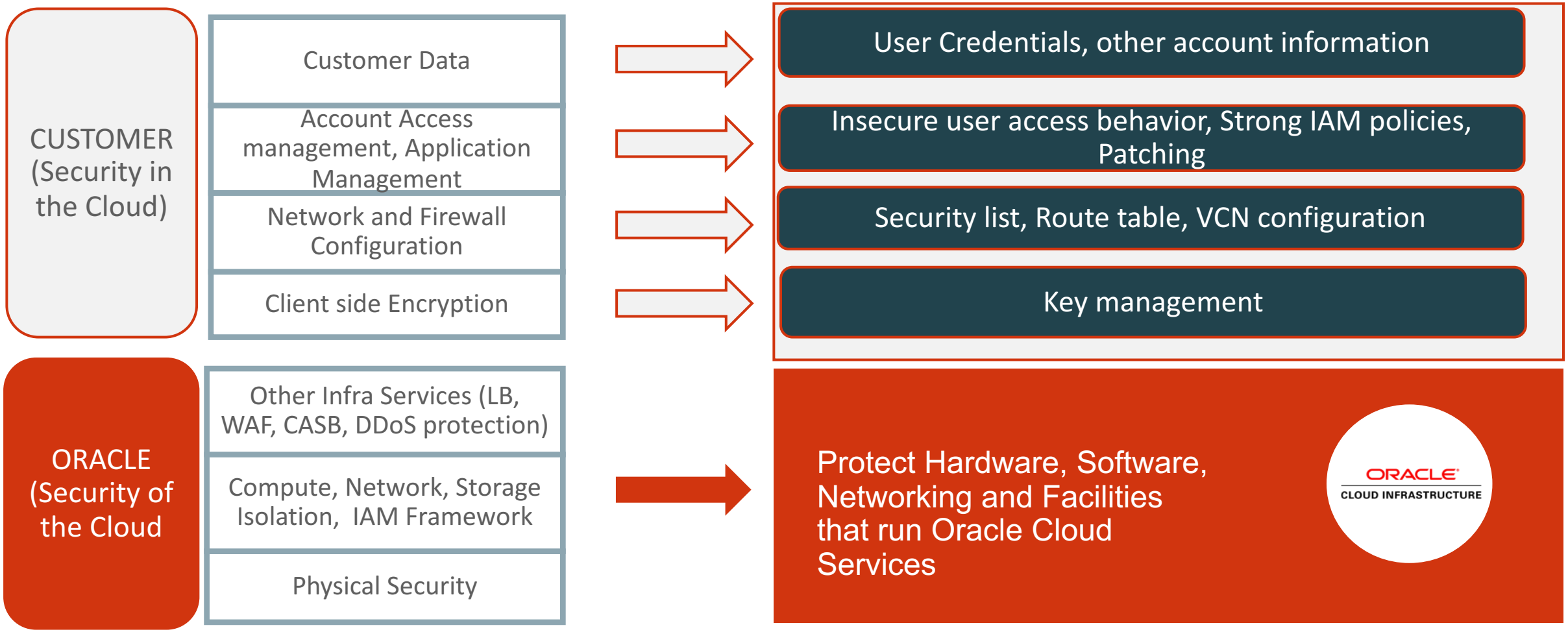
The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Agenda

- OCI Overview
- Shared Security Responsibility Model
- Security Capabilities at a glance
- OCI Security Capabilities
  - Customer Isolation
  - Data Encryption
  - Security Controls
  - Visibility
  - Secure Hybrid Cloud
  - High Availability
  - Verifiably Secure Infrastructure
- Security Considerations

Shared Security Responsibility Model

Shared Responsibility Model in Oracle Cloud Infrastructure



Overview of Security Capabilities

The 7 Pillars of a Trusted Enterprise Cloud Platform

1	**Customer Isolation**	Full isolation from other tenants and Oracle's staff, and between a tenant's workloads
2	**Data Encryption**	Meet compliance requirements regarding data encryption, cryptographic algorithms, and key management
3	**Security Controls**	Effective and easy-to-use security management to constrain access and segregate operational responsibilities | Secure application delivery
4	**Visibility**	Provide log data and security analytics for auditing and monitoring actions on customer assets
5	**Secure Hybrid Cloud**	Enable customers to use their existing security assets | Integrate with on-premise security solutions | Support for third-party security solutions
6	**High Availability**	Fault-independent data centers that enable high-availability scale-out architectures and are resilient against attacks
7	**Verifiably Secure Infrastructure**	Transparency about processes and internal security controls | Third-party audits and certifications | Customer pen-testing and vulnerability scanning | Jointly demonstrated compliance

Oracle Cloud Infrastructure Security Capabilities At a Glance

1	**Customer Isolation**	Bare Metal Instance, VM Instance, VCN IAM, Compartments
2	**Data Encryption**	Default Encryption for Storage, Key Management, DB Encryption
3	**Security Controls**	User Authentication and Authorization, Instance Principals, Network Security Control, Web Access Firewall
4	**Visibility**	Audit Logs, CASB Based monitoring and enforcement
5	**Secure Hybrid Cloud**	Identity Federation Third Party Security Solution, IPSEC VPN, Fast Connect
6	**High Availability**	Fault-independent data center, Fault Domain, SLA
7	**Verifiably Secure Infrastructure**	Security Operations, Compliance Certification and Attestation, Customer penetration and Vulnerability testing

Customer isolation

Tenant and Resource level isolation

I want to isolate my cloud resources from other tenants, Oracle staff, and external threat actors, so we can meet our security and compliance requirements.

I want to isolate different departments from each other, so visibility and access to resources can be compartmentalized.

Compute
- **Bare Metal Instances | VM Instances**

Network
- **VCN and Subnets**

Data
- **Data-at-rest encryption using customer-controlled keys**

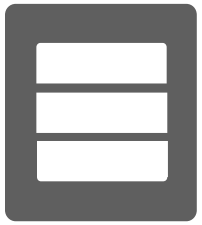
Back-end Infrastructure
- **Secure isolation between customer instances and back-end hosts (Off box Network Virtualization)**

Identity and Access Management
- **Compartments and IAM policies**

Compute

Bare Metal (BM)

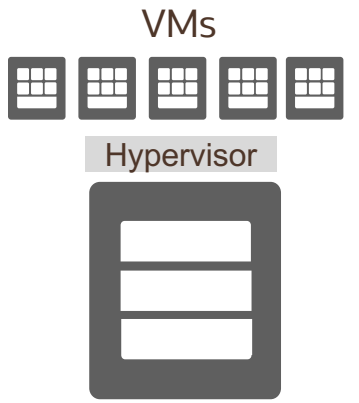
Direct Hardware Access – customers get the full Bare Metal server
(single-tenant model)



Bare Metal Server

Virtual Machine (VM)

A hypervisor to virtualize the underlying Bare Metal server into smaller VMs
(multi-tenant model)

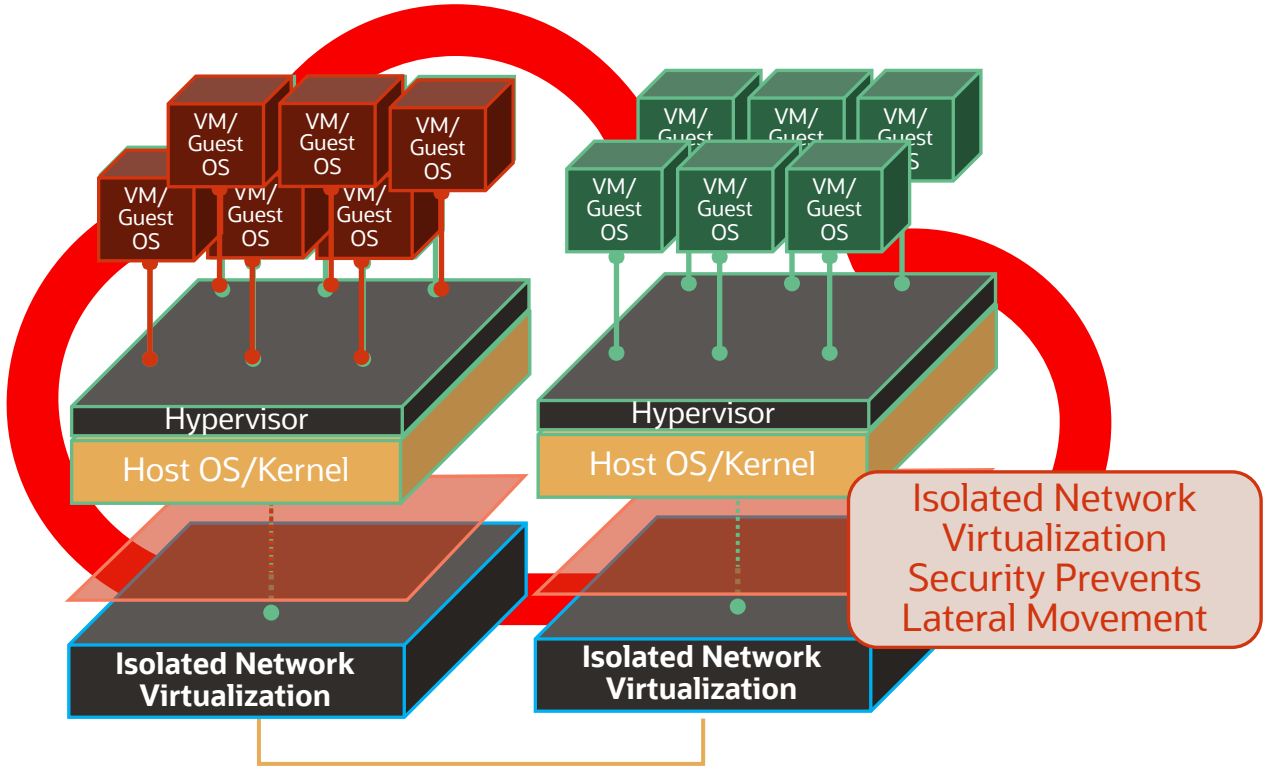


Bare Metal Server

VM compute instances runs on the same hardware as a Bare Metal instances, leveraging the same cloud-optimized hardware, firmware, software stack, and networking infrastructure

Off-box Network Virtualization

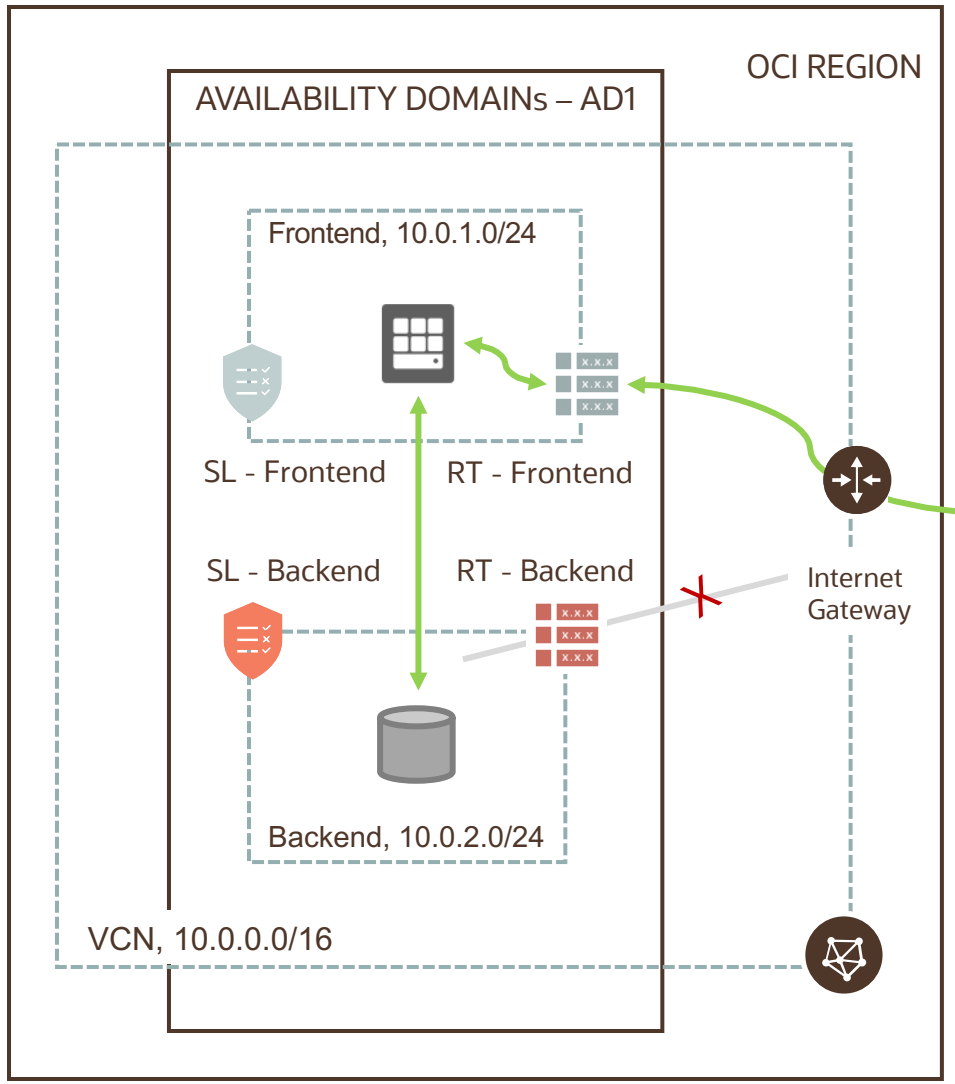
- Moves management and IO out of the hypervisor
- Highly configurable private overlay networks



VCN and subnets

- Each customer's traffic is completely isolated in a private L3 overlay network
- Network segmentation is done via subnets
  - Private subnets: No internet access
  - Public subnets: Instances have public IP addresses
- Customers can control VCN traffic
  - VCN stateful and stateless security lists
  - Route table rules
- Customers can use a Service Gateway that provides a path for private network traffic between a VCN and a public Oracle Cloud Infrastructure service such as Object Storage
- Customers can use VCN peering for securely connecting multiple VCNs without routing the traffic over the internet or through your on-premises network

VCN and Subnet



Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway

	Type	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521

Destination CIDR	Route Target
0.0.0.0/0	NAT/ Service gateway /DRG

	Type	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	10.0.1.0/24	TCP	All	1521
~~Stateful~~	~~Egress~~		~~All~~	~~All~~	

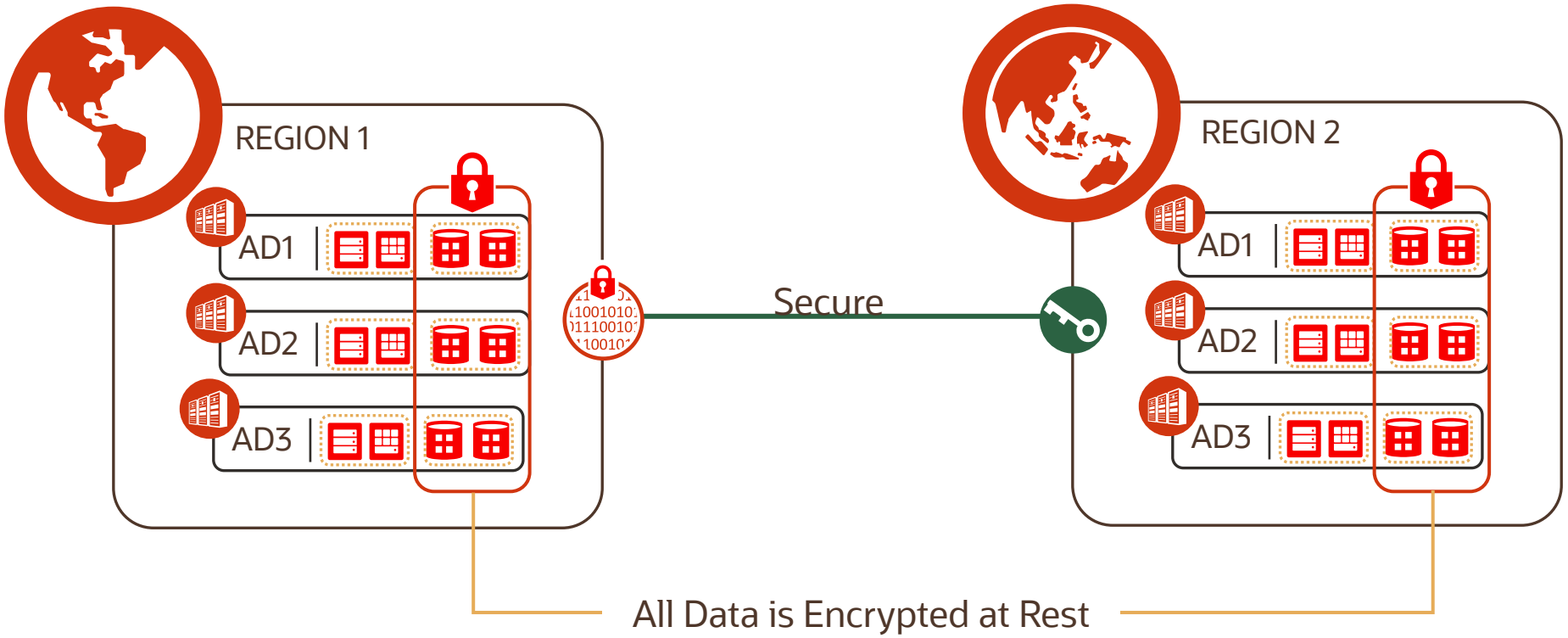
Data Encryption

Storage Encryption

- Block Storage and Remote Boot Volumes
  - Volumes and backups encrypted at rest using AES 256-bit key (keys managed by Oracle)
  - Data moving between instance and block volume is transferred over internal and highly secure network.
  - in-transit encryption can be enabled (paravirtualized volume attachments.)
- Object Storage
  - Client-side encryption using customer keys
  - Data encrypted with per-object keys managed by Oracle
  - All traffic to and from Object Storage service encrypted using TLS
  - Object integrity verification
- File System Storage
  - Encrypted at rest and between backends (NFS servers and storage servers)
- Data Transfer Service
  - Uses standard Linux dm-crypt and LUKS utilities to encrypt block devices

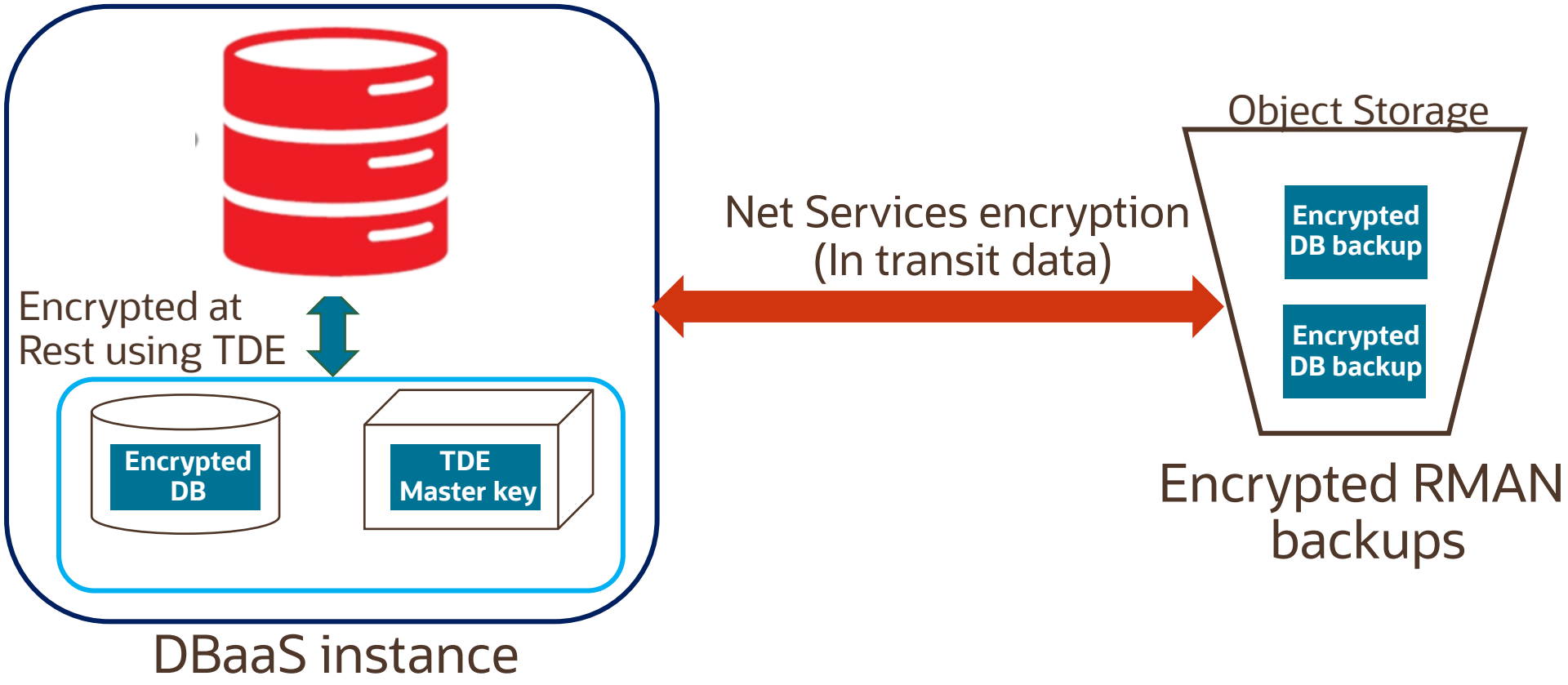
Data Encryption At Rest and In Transit

- Oracle manager OR Customer managed keys (KMS)



Database Encryption: At rest and in Transit

- Oracle TDE encryption for DB files and Backups at Rest. Key Store/Wallet for managing master key
- For improved security, you can configure backup encryption for RMAN backup sets
- Native Oracle Net Services encryption and integrity capabilities for encrypting data in transit
  - Advanced Encryption Standard (AES), DES, 3DES, and RC4 symmetric cryptosystems for protecting the confidentiality of Oracle Net Services traffic



Key Management

- Oracle Key Management provides you with
  - Highly available, durable, and secure key storage. Encrypt your data using keys that you control
  - Centralized key management capabilities (Create/Delete, Disable/Enable, rotate)
  - IAM Policies for Users/Groups and OCI resources
  - Key Life Cycle management
  - FIPS 140-2 Security Level 3 security certification.

Your Keys - Protected

Oracle protects the security of your keys by storing them in a FIPS 140-2 Level 3 certified hardware security module (HSM).

Managed Service

Oracle Key Management is a managed service, so you can focus on your encryption needs rather than on procuring, provisioning, configuring, updating and maintaining HSMs and key management software.

Enhance Compliance

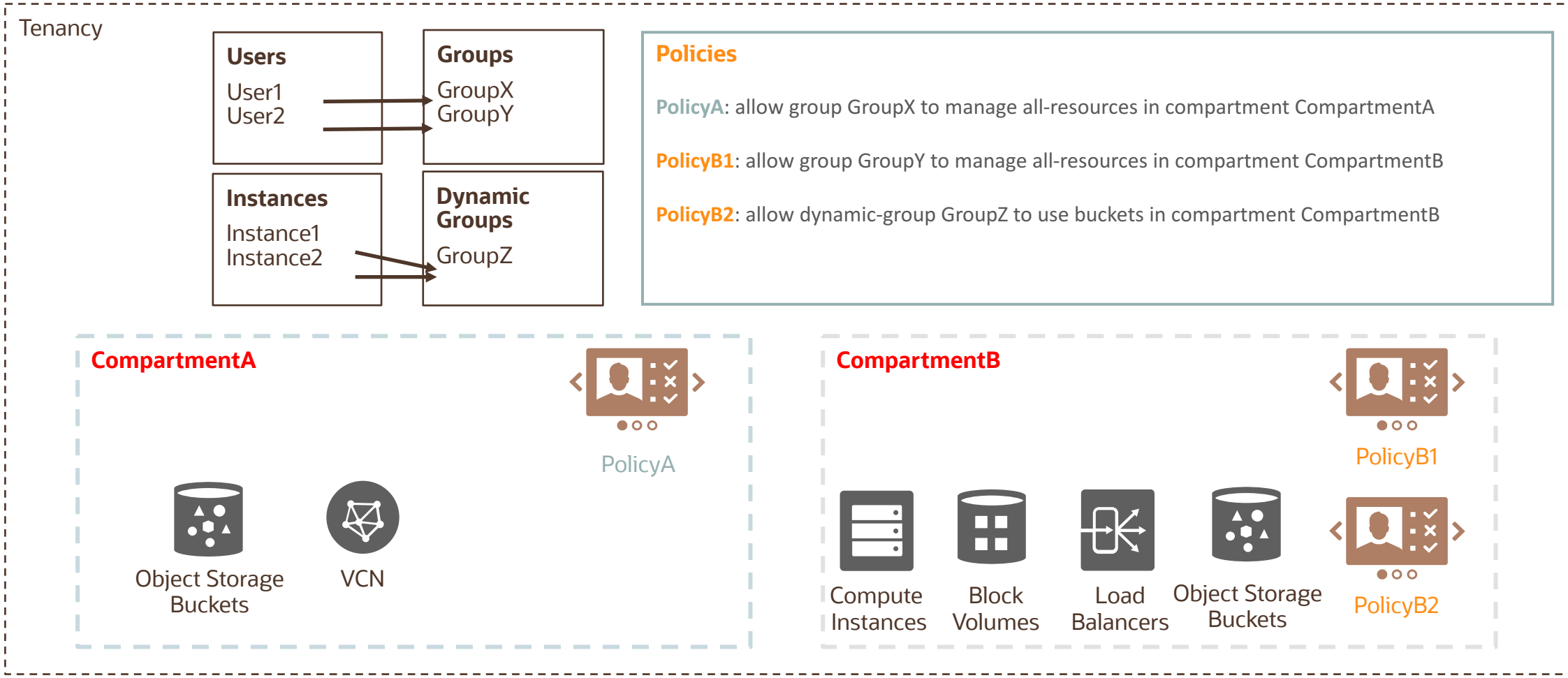
Integrates with Oracle Identity and Access Management (IAM) so you can control permissions on individual keys and key vaults, and monitor their lifecycle via integration with Oracle Audit.

Security Control (Authentication)

Identity and Access Management

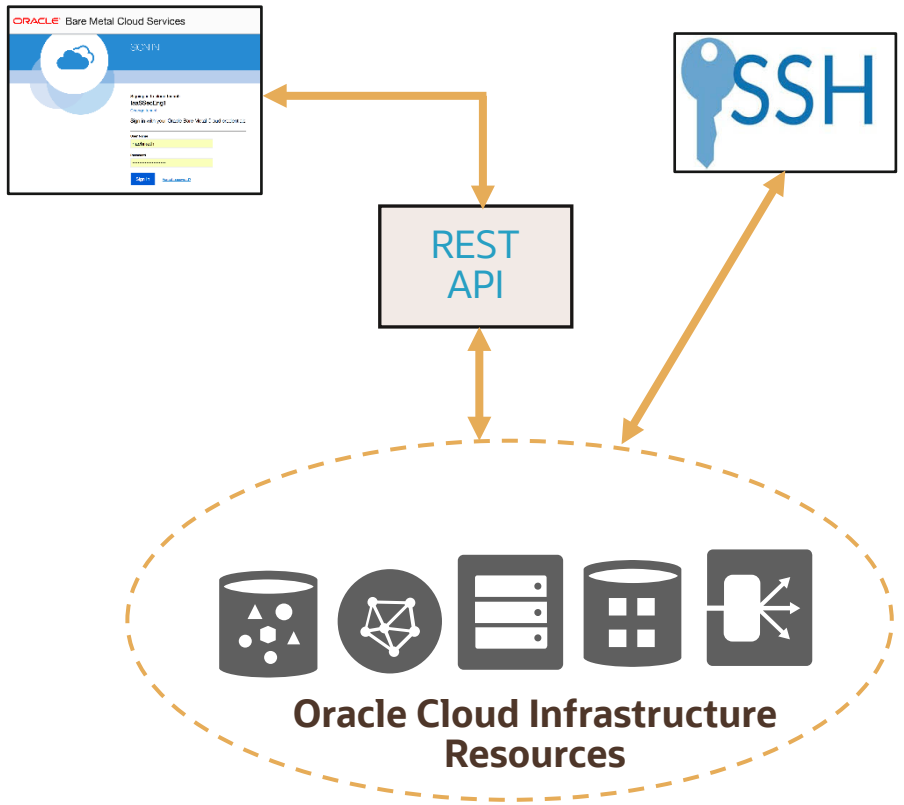
- Identity and Access Management (IAM) service enables you to control what type of access a group of users have and to which specific resources
- Each OCI resource has a unique, Oracle-assigned identifier called an Oracle Cloud ID (OCID)
- IAM uses traditional identity concepts such as Principals, Users, Groups, Policies and introduces a new feature called Compartments

Identity and Access Management (IAM)



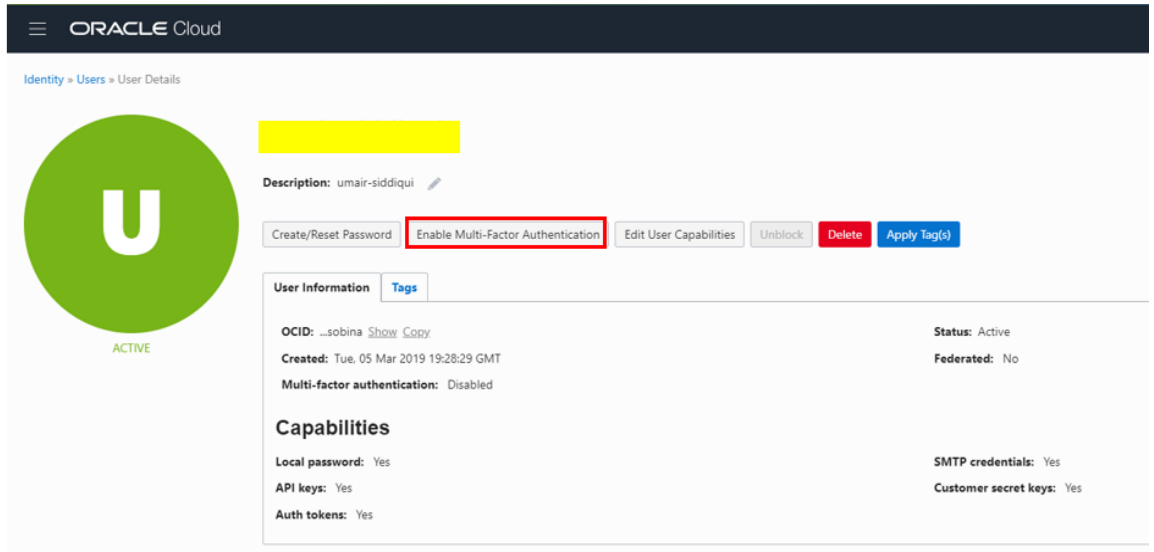
User Authentication (Password, API key, Auth token)

- Console password to access OCI resources
- API signing key to access REST APIs
  - ➢API calls protected by asymmetrically signed requests over TLS 1.2
  - ➢Only customers have the private key that corresponds to the signing public API key
  - ➢2048-bit RSA key pair
- SSH key pair to authenticate compute login
  - ➢2048-bit RSA or DSA, 128-bit ECC
- Auth tokens
  - ➢Can be use to authenticate with third-party APIs that do no support Oracle Cloud Infrastructure's signature-based authentication



User Authentication (MFA)

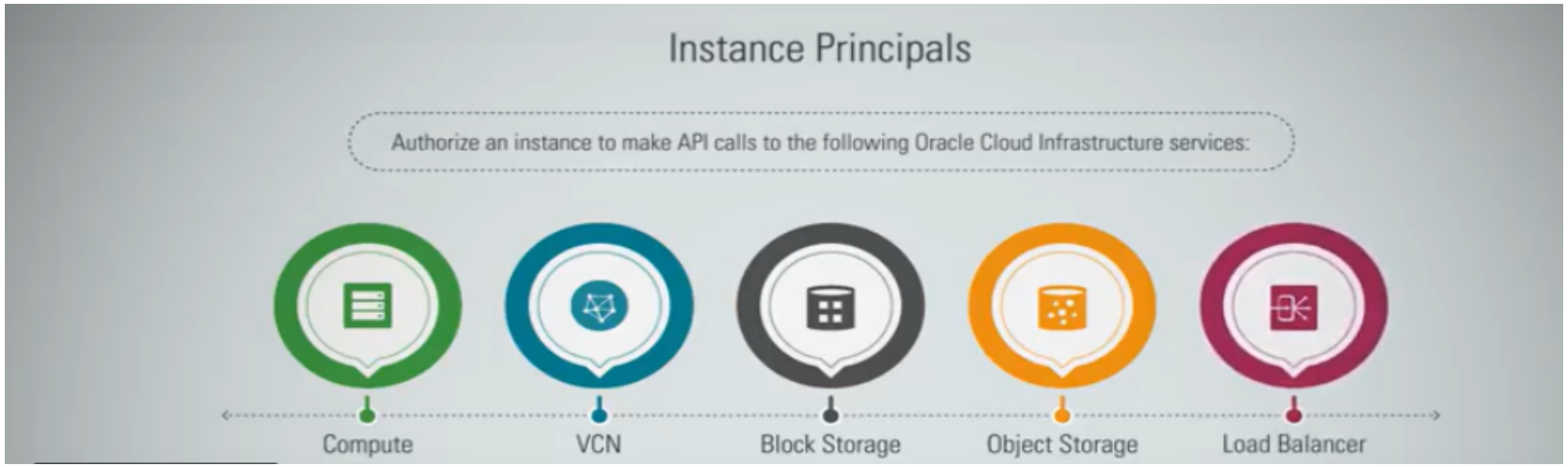
- Multi-factor authentication is a method of authentication that requires the use of more than one factor to verify a user's identity.
  - ➢First Authentication using Password
  - ➢Second Authentication using Authentication app such as Oracle Mobile Authenticator or Google Authenticator
- Authentication app must be installed on your mobile device
- Can be enabled from OCI Console



Instance authentication (Instance Principal)

- Instances have their own credentials that are provisioned and rotated automatically
- Dynamic Groups allow customers to group instances as principal actors, similar to user groups
- Membership in a dynamic group is determined by a set of matching rules (example rule: all instances in the HR compartment)
- Customers can create policies to permit instances in these groups to make API calls against Oracle Cloud Infrastructure services

```
Allow dynamic-group <dynamic_group_name> to <verb> <resource-type> in tenancy
```



Security Control (Authorization)

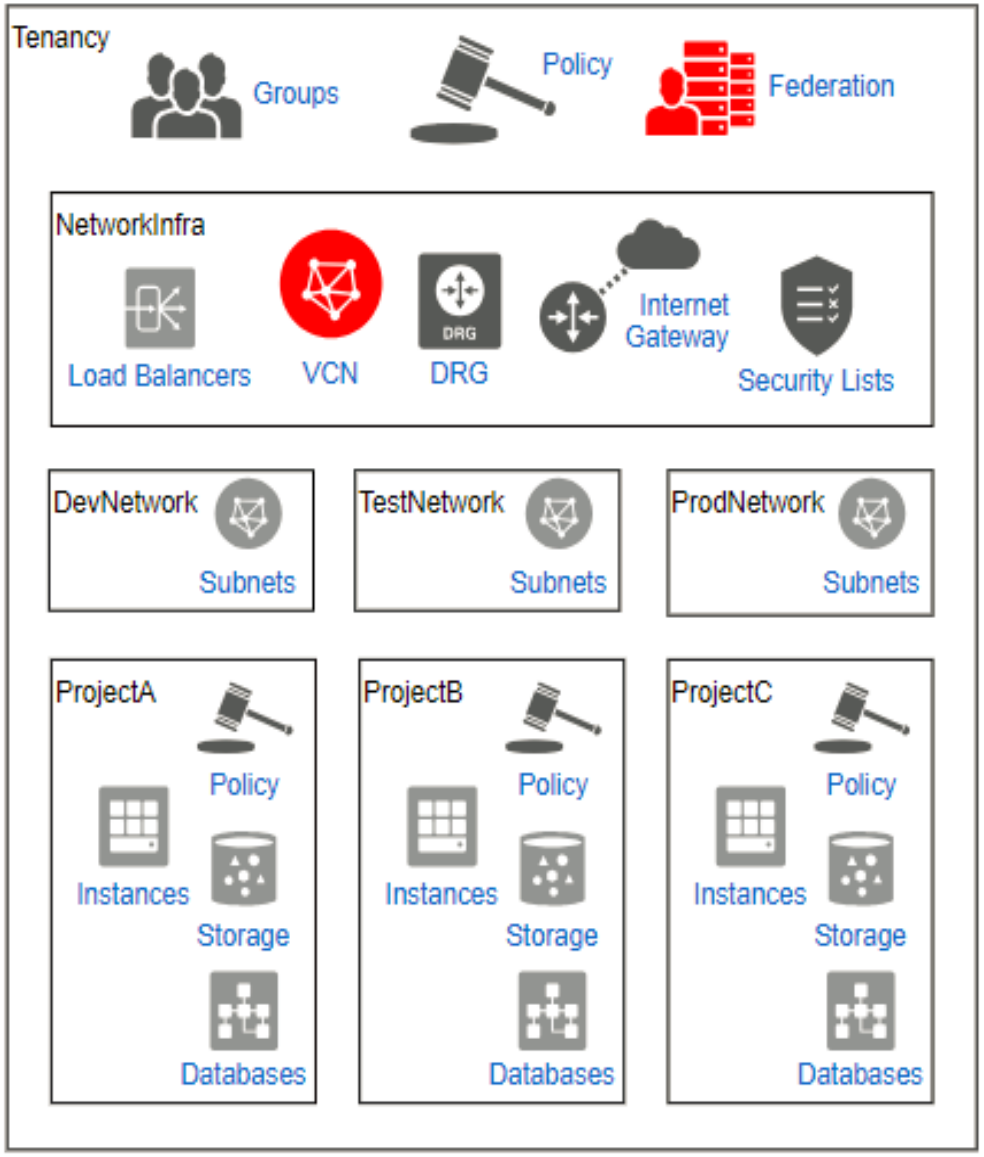
Authorization

- **Tenant** – An account provisioned with a top-level “root compartment”
- **Compartment** – A logical container to organize and isolate cloud resources
- **Group** – A collection of users
- **Dynamic Group** – A collection of instances
- **Resource** – An Oracle Cloud Infrastructure resource
- **Policy** – Specifies who can access which resources and how, via an intuitive policy language. Example policies:

  allow group SuperAdmins to manage groups in tenancy

  allow dynamic-group FrontEnd to use load-balancers in compartment ProjectA

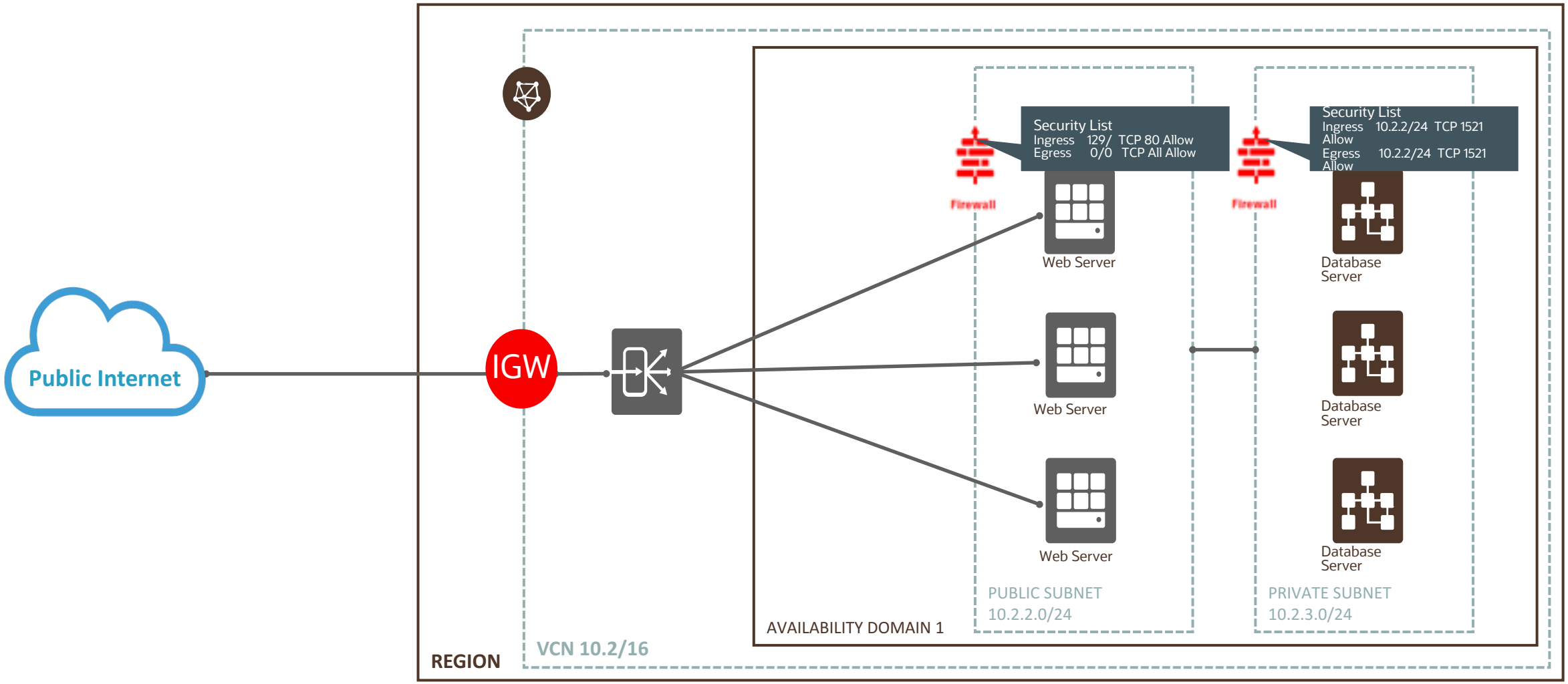
Compartments



- Compartment: NetworkInfra
  - Critical network infrastructure centrally managed by network admins
  - Resources: top level VCN, Security Lists, Internet Gateways, DRGs
- Compartment: Dev, Test, Prod Networks
  - Modeled as a separate compartment to easily write policy about who can use the network
  - Resources: Subnets, Databases, Storage(if shared)
- Compartment: Projects
  - The resources used by a particular team or project; separated for the purposes of distributed management
  - Resources: Compute Instances, Databases, Block Volumes, etc.
  - There will be multiple of these, one per team that needs it's own DevOps environment

Security Control (Resource Access)

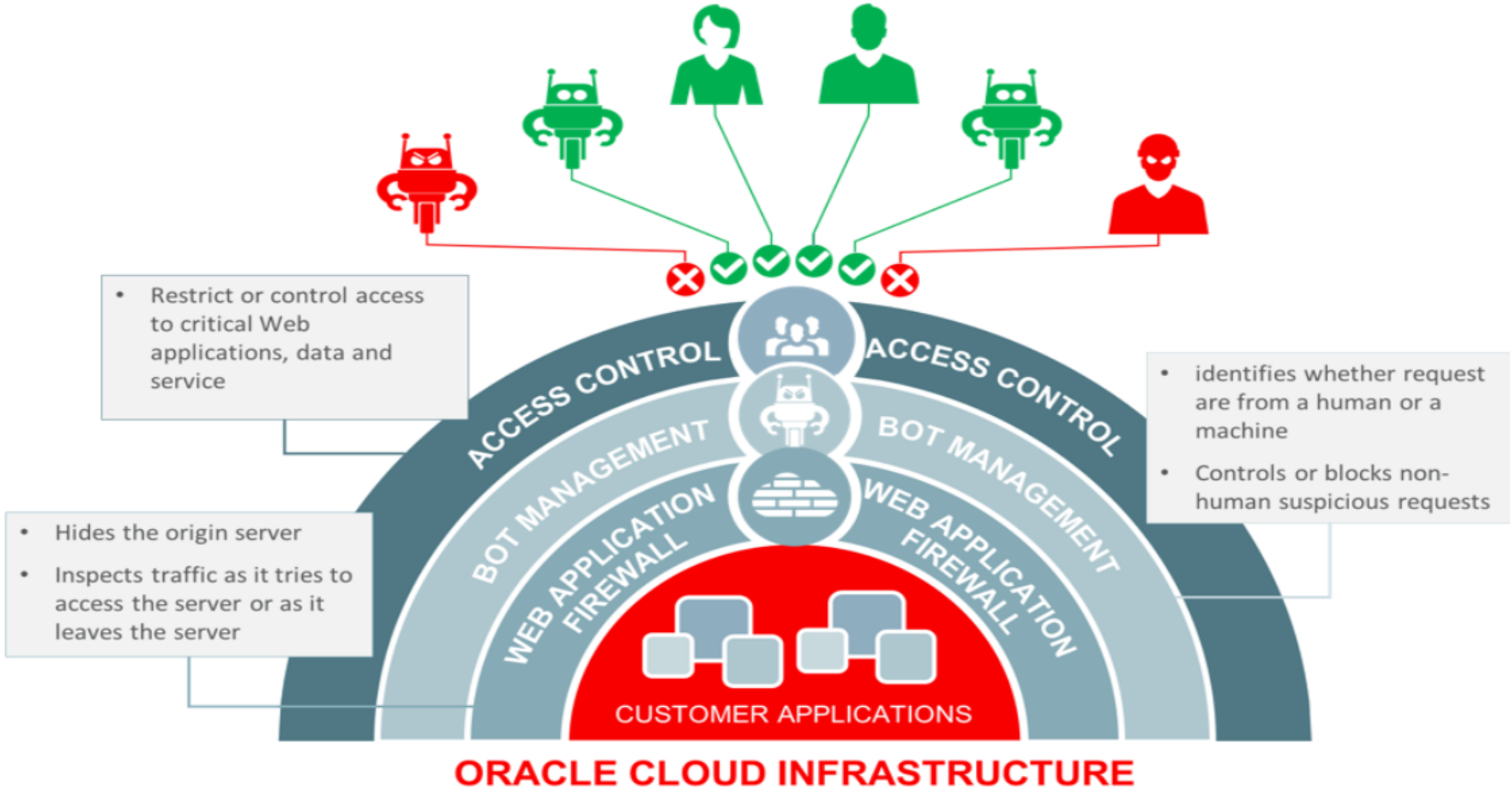
Security Lists (VCN and Subnet)



Web Access Firewall

- Designed to protect internet-facing web applications
- Uses a layered approach to protect web applications against cyberattacks
- Over 250 predefined Open Web Access Security Project (OWASP), application, and compliance-specific rules
- Administrators can add their own access controls based on geolocation, whitelisted and blacklisted IP addresses, and HTTP URL and Header characteristics
- Bot management provides a more advanced set of challenges, including JavaScript acceptance, CAPTCHA, device fingerprinting, and human interaction algorithms

Web Access Firewall



Visibility

Audit

- API calls are logged and made available to customers
  - Includes calls made via the Console, CLI, and SDKs
- API for listing audit events
  - New events available within 15 minutes. 90 days of history by default
  - Configurable up to 365 days (affects all regions and compartments)
- Searchable via the Console

Data Integrity Checks

Internal integrity checks ensure event data is read-only and any tampering can be detected for your compliance and security needs.

Maintain Traceability

Automatically record API calls made from the console or SDK. Each event can be used to identify the action, actor, target, and outcome.

Visibility into Infrastructure

Support for all Oracle Cloud Infrastructure services including Compute, Networking, Block Volumes, and Load Balancing.

Oracle CASB Cloud Service

CASBs are software that help enterprises enforce security, compliance and governance policies for their usage of applications in the cloud.

Visibility

- Enterprise visibility into risk posture of cloud usage

Compliance

- Out-of-the-box Reporting for audit and compliance to security best practices

Threat Protection

- Autonomous threat detection and predictive analytics using Machine Learning

Data Protection

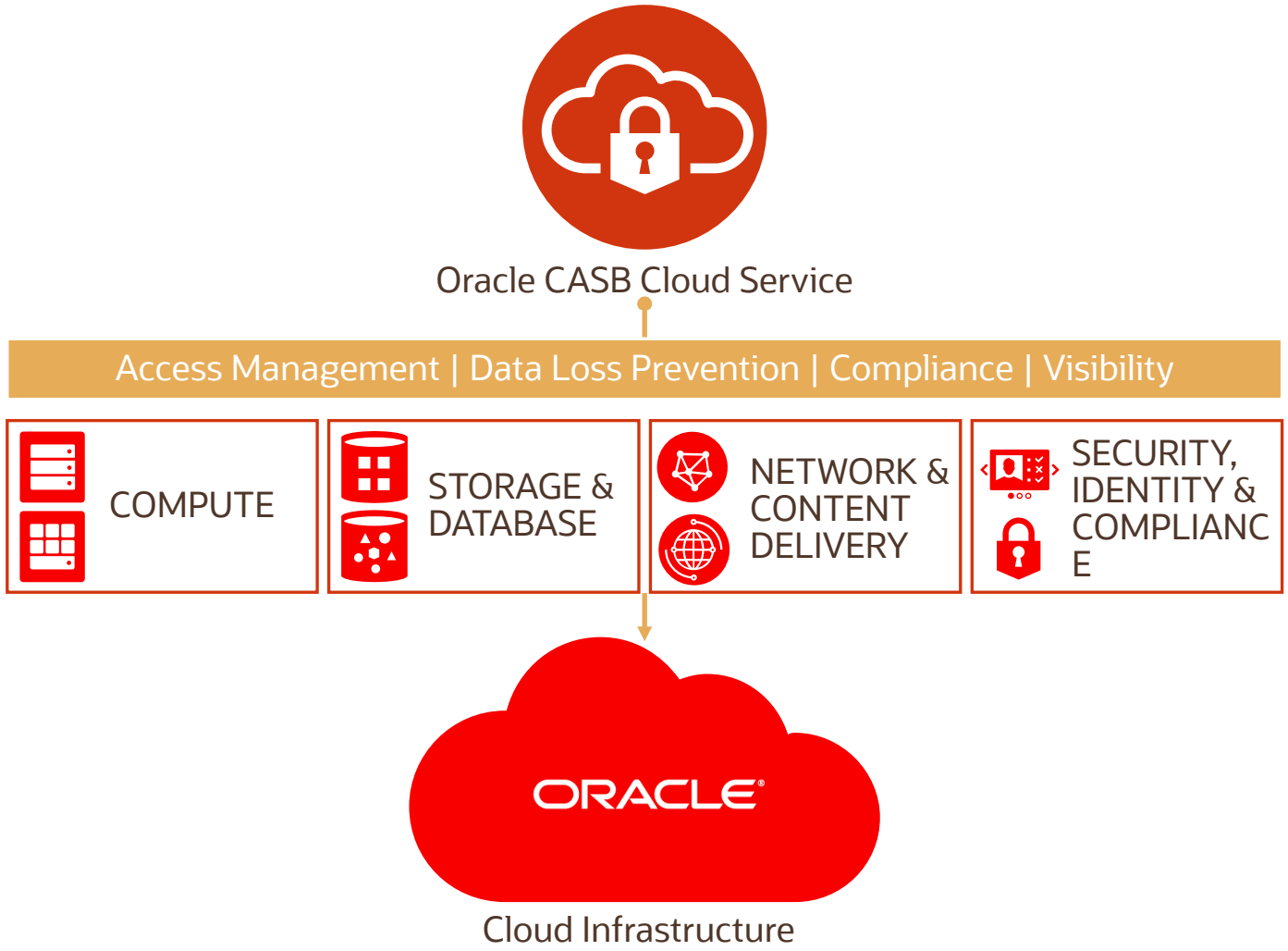
- Data classification and access control for sensitive data in the cloud

Remediation and Enterprise Integrations

- Autonomous remediation of threats and incidents with enterprise integrations

Industry's only CASB that offers proactive monitoring, threat detection and remediation for Oracle SaaS and OCI

Cloud Access Security Broker for SaaS *and* IaaS

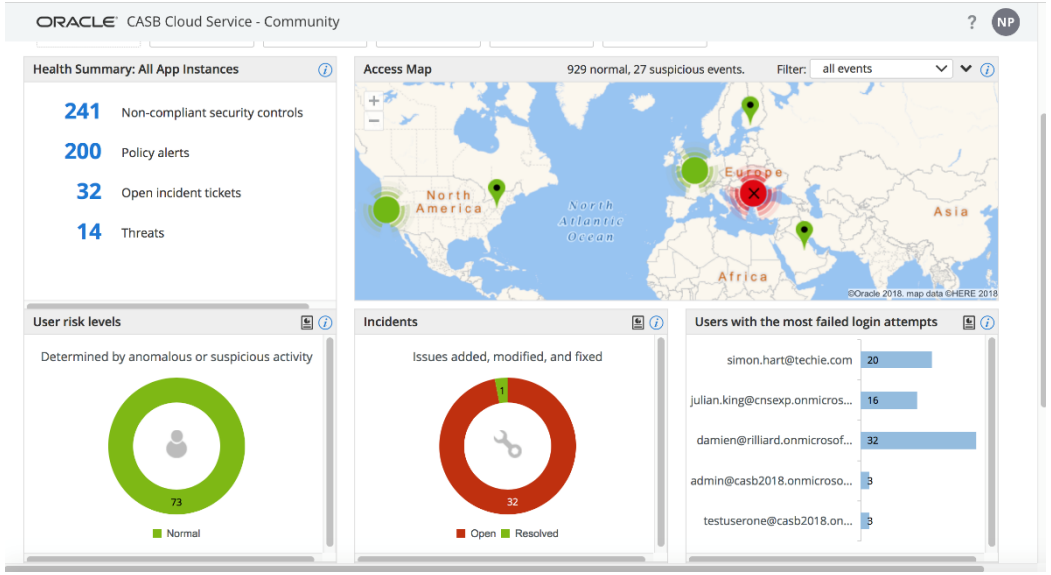


CASB Cloud Service for OCI

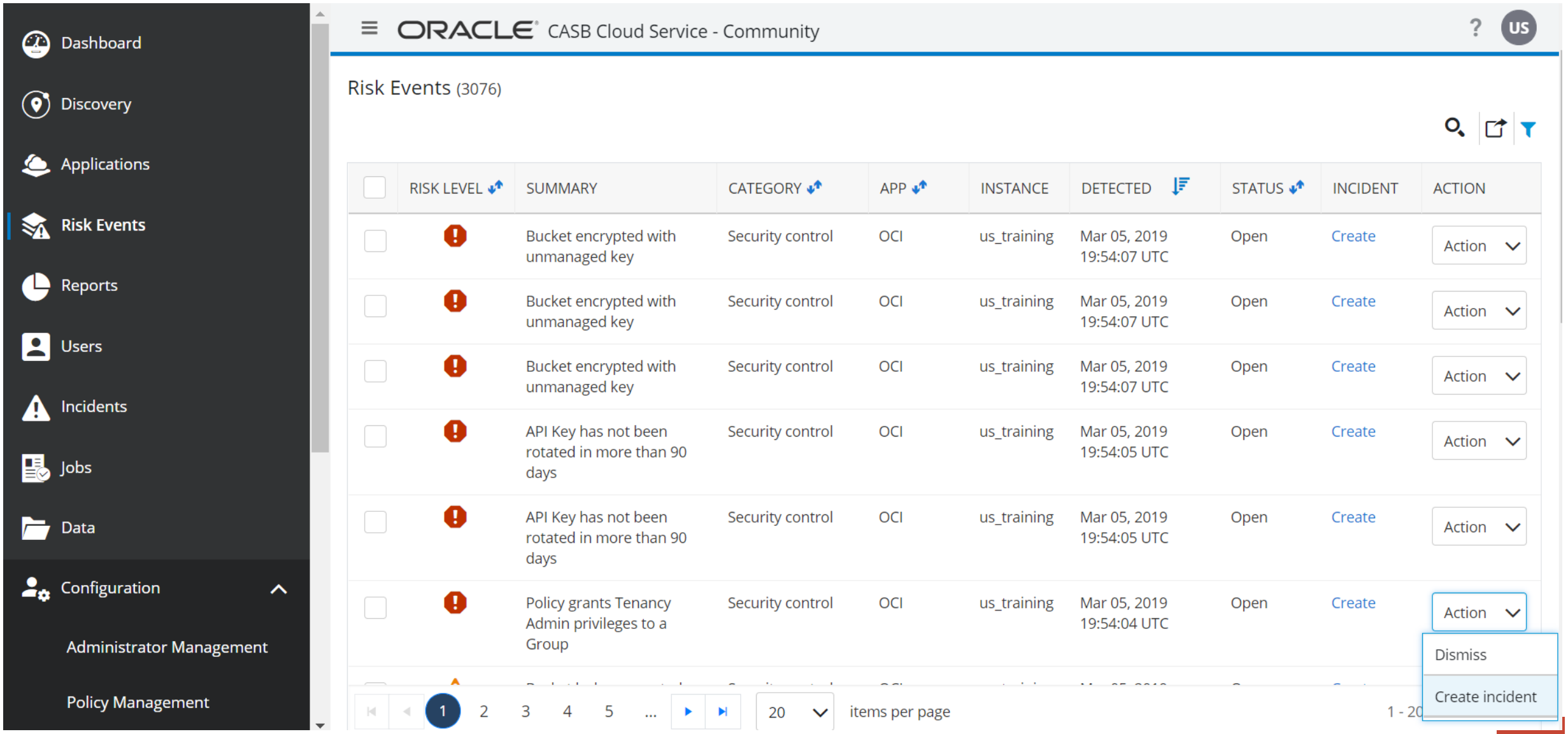
- Policy Alerts
  - ➢ *Alerting and Notifications on policy changes to resources*
- Security Controls
  - ➢ *Detection of insecure settings of OCI resources*
- Threat Detection
  - ➢ *Detection of user risks and threats using ML analytics*
- Key Security Indicator Reports
  - ➢ *Report generation for key security indicators*
- Exporting Data and Threat Remediation
  - ➢ *Enterprise Integrations with SIEM or ITSM systems*

Oracle CASB Monitoring for OCI

- Performs OCI resource security configuration checks
  - ➢ Uses OCI Audit logs and OCI APIs
  - ➢ Customers creates a scoped-down OCI IAM user for CASB
- IAM user behavior analysis
  - ➢ ML based anomaly detection in user login behavior
- IP reputation analysis
  - ➢ Integration with 3rd party IP reputation feeds

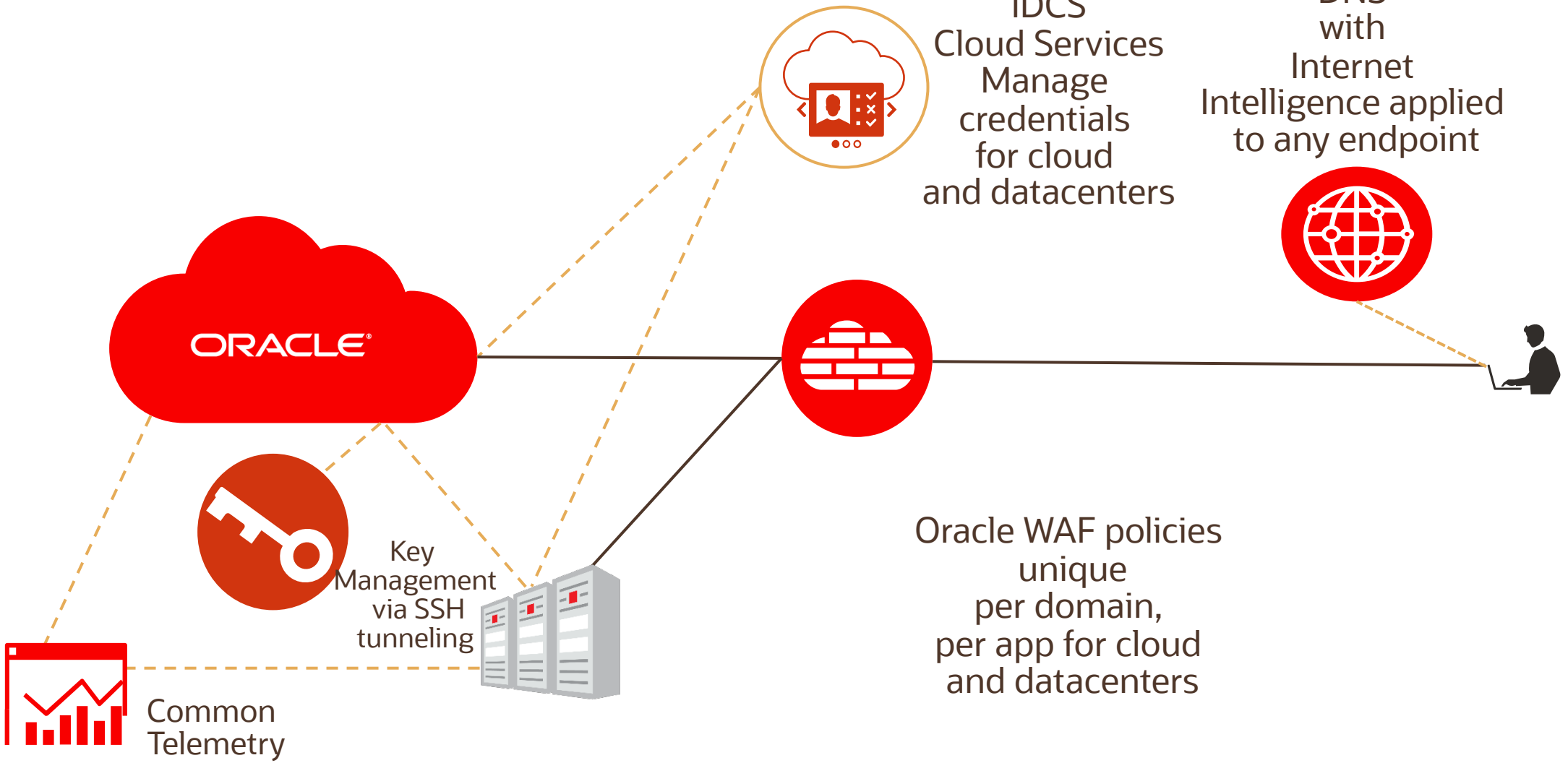


Examples of CASB OCI Security Checks

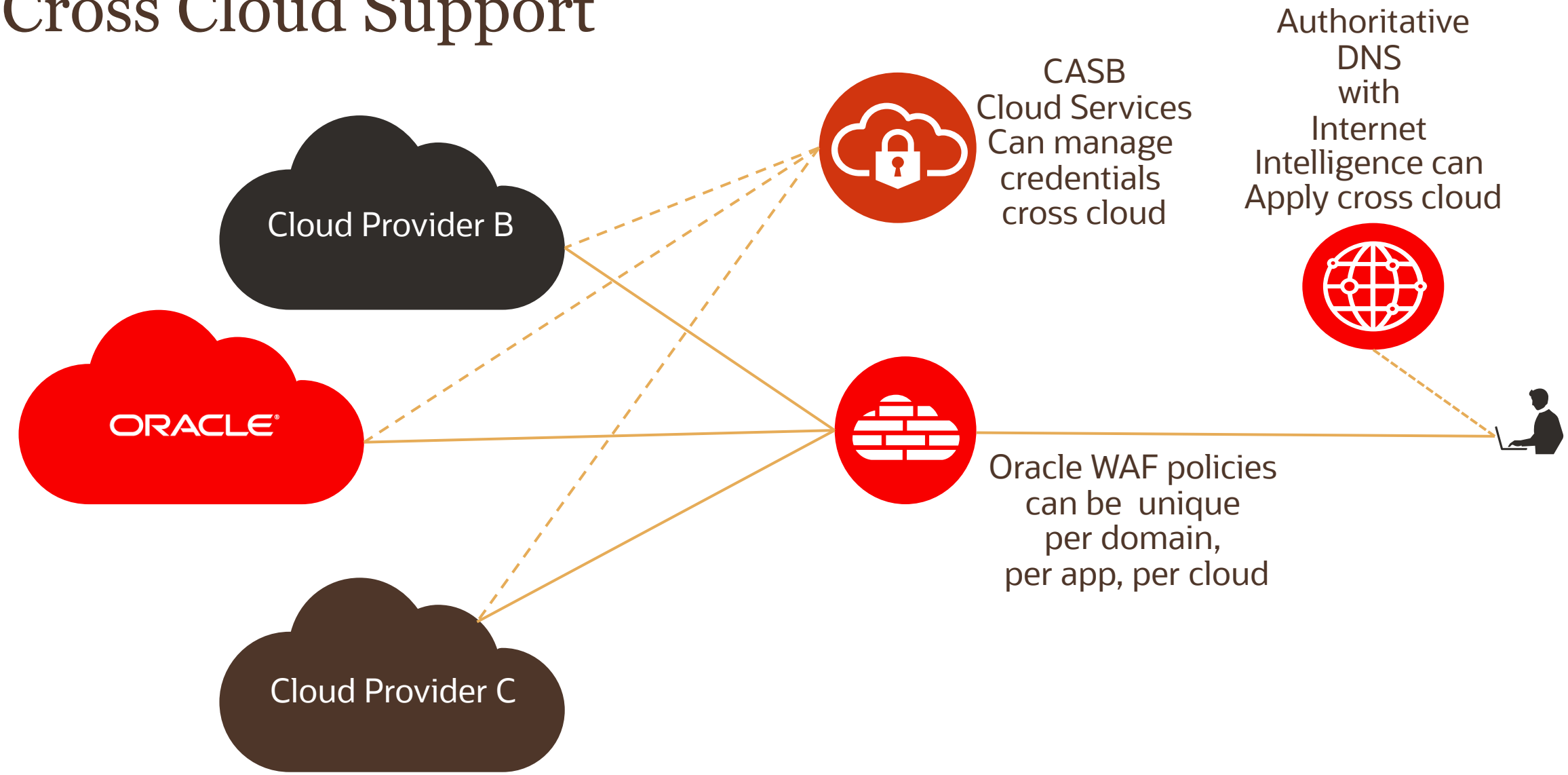


Secure Hybrid Cloud

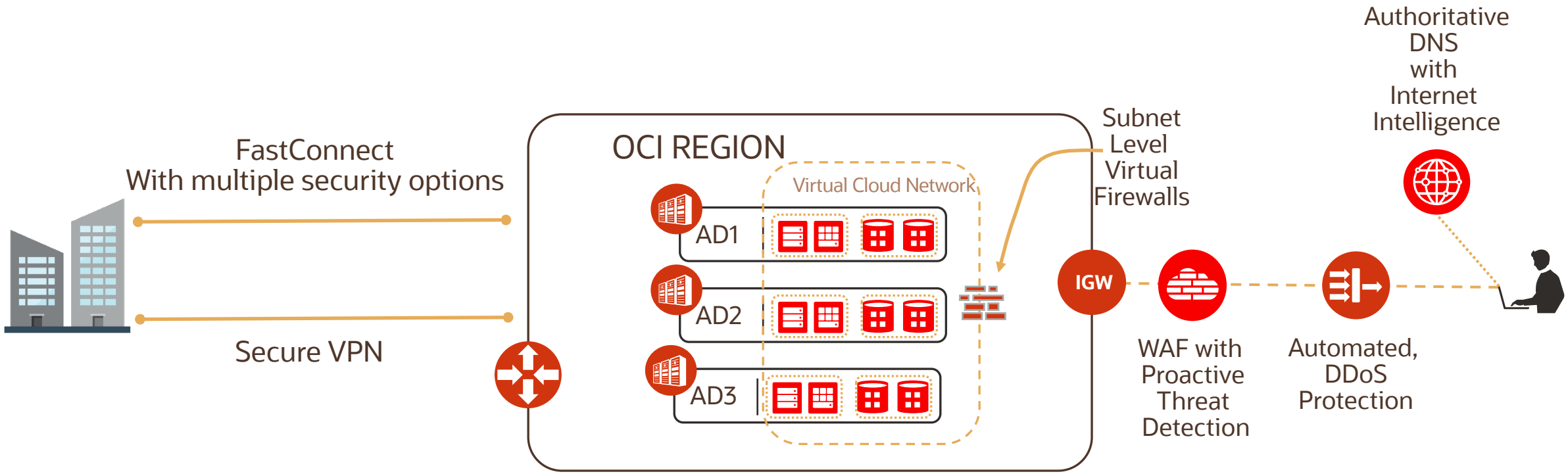
Hybrid Support



Cross Cloud Support



Fast Connect and IPSEC VPN



Support for Existing Customer Security Assets

- Identity Federation
  - SAML 2.0 Federation via IDCS and Microsoft Active Directory Federation Service (ADFS) and any SAML 2.0 compliance identity provider
- Oracle is collaborating with various third-party security vendors to make their solutions accessible on Oracle Cloud Infrastructure to enable customers to use their existing security tools when securing data and applications in the cloud
- See the Oracle Cloud Marketplace for a list of partners who have been successfully tested on Oracle Cloud Infrastructure

Customer Penetration and Vulnerability Testing

- Customers can perform penetration and vulnerability testing on Customer Components such as VMs
- Customers can schedule Penetration and Vulnerability testing via “My Services” dashboard.

High Availability

Redundancy and DDoS Protections

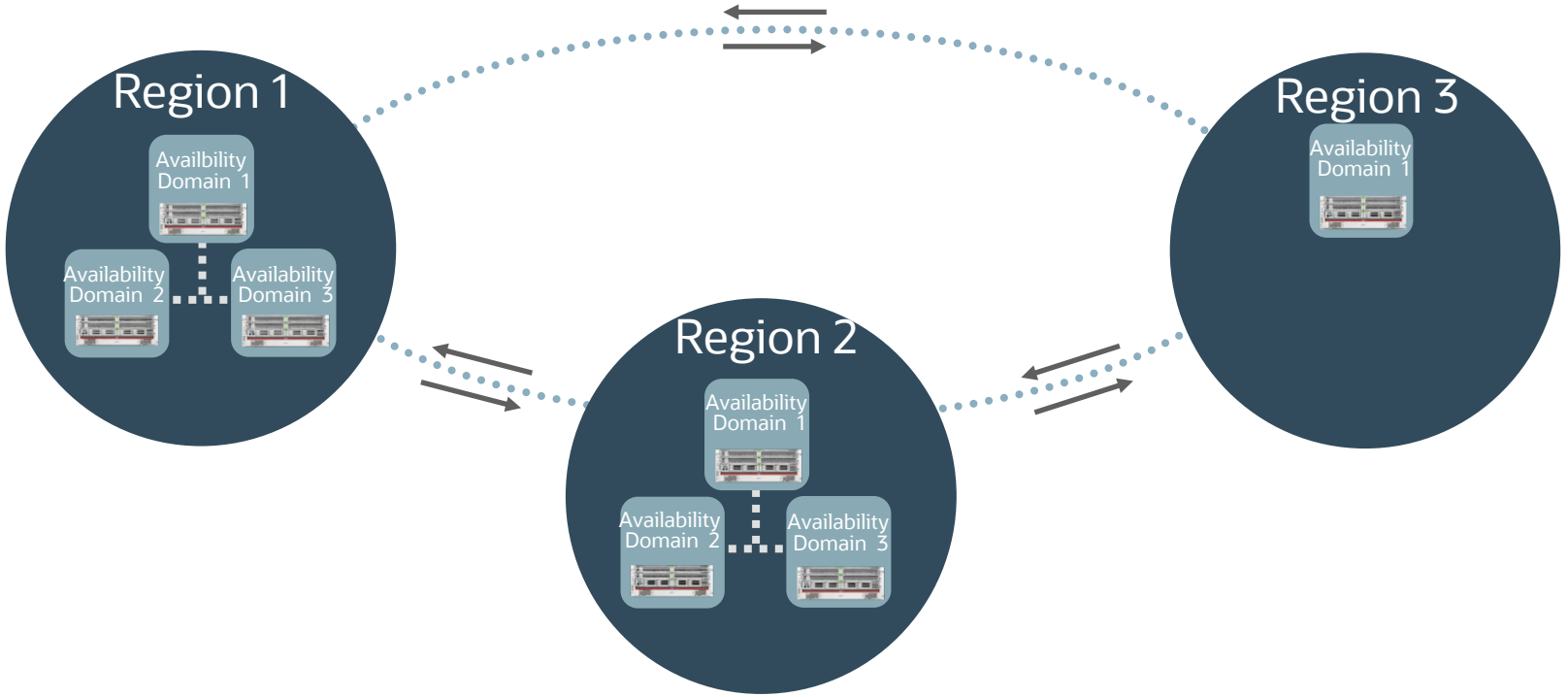
Protecting Enterprises for More than 40 Years

- 14+ Regions
- Distinct geo security profiles
- Automated global edge protection
- 2000+ cloud security personnel
- 24/7 monitoring
- Trillions of signals collected daily
- Internet and Cloud Intelligence

47

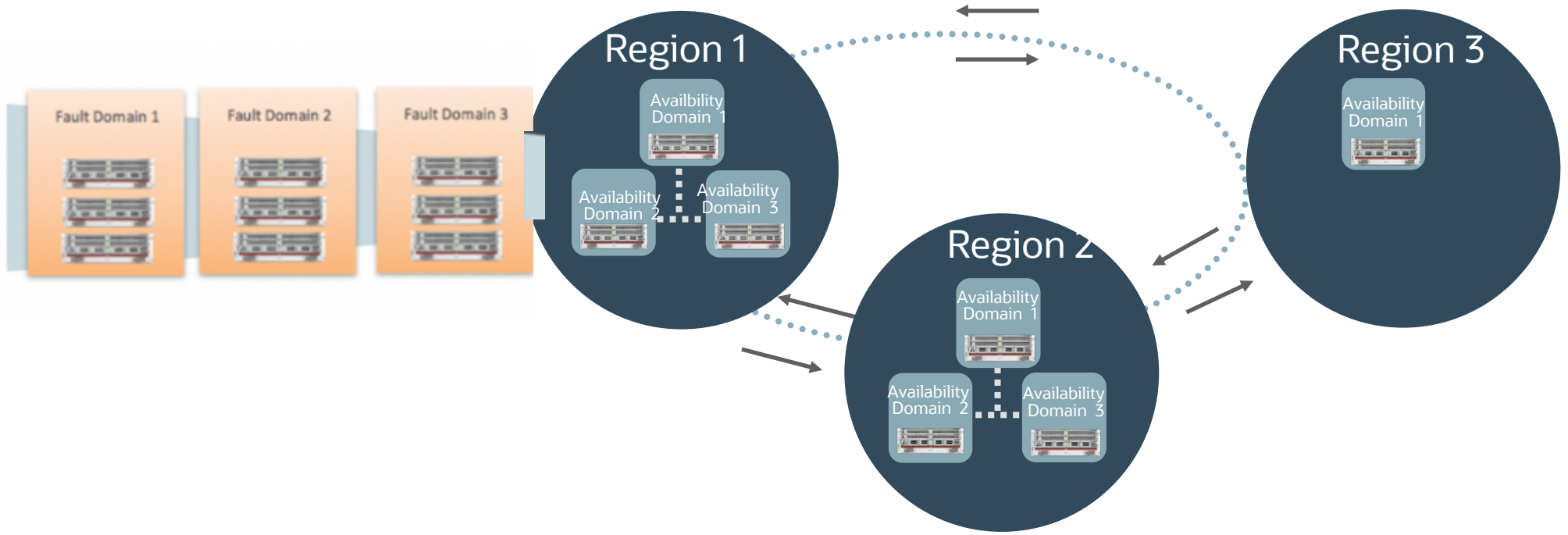
Availability Domains (ADs): Multiple Fault-Decorrelated Independent Data Centers

- Fault-independent availability
- Remote disaster recovery
- Predictable low latency and high speed, encrypted interconnect between ADs



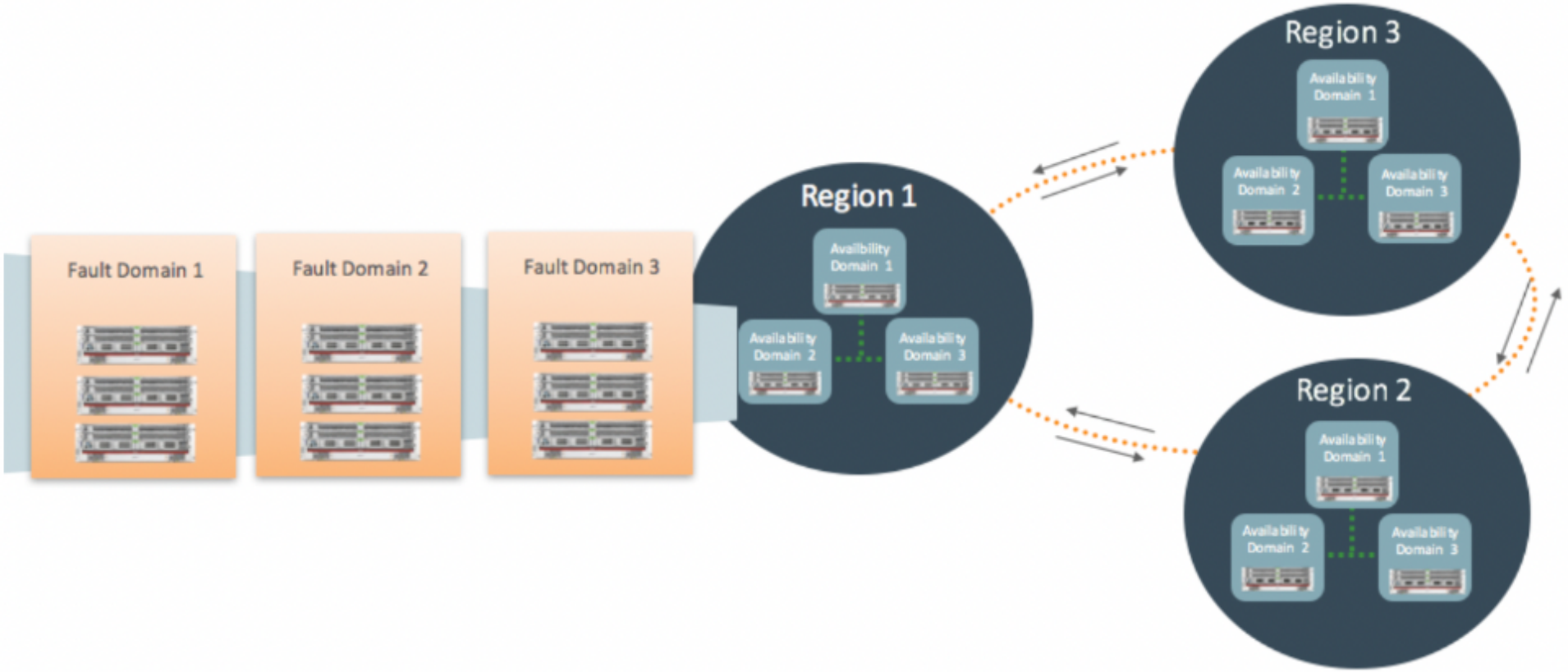
Availability Domains (ADs): Multiple Fault-Decorrelated Independent Data Centers

- **Enable you to distribute your** compute instances so that they are not on the same physical hardware within a single Availability Domain



Fault Domain(FDs):

- Enable you to distribute your compute instances so that they are not on the same physical hardware within a single Availability Domain



Verifiably Secure Infrastructure

Third-Party Audit, Certifications and Attestations

- ISO 27001
  - Regions: Phoenix (Arizona), Ashburn (Virginia), London (United Kingdom), and Frankfurt (Germany)
  - Services covered: Compute, Block Volumes, Object Storage, Networking, Database, Governance, and Load Balancing
- SOC 1, SOC 2 and SOC 3
  - Regions: Phoenix (Arizona), Ashburn (Virginia), and Frankfurt (Germany)
  - Services covered: Compute, Block Volumes, Object Storage, Networking, Database, Governance, and Load Balancing
- PCI DSS Attestation of Compliance
  - Services covered: Compute, Networking, Load Balancing, Block Volumes, Object Storage, Archive Storage, File Storage, Data Transfer Service, Database, Exadata, Container Engine for Kubernetes, Registry, FastConnect, and Governance.

Third-Party Audit, Certifications and Attestations

- HIPAA Attestation
  - Services covered: Compute, Networking, Load Balancing, Block Volumes, Object Storage, Archive Storage, File Storage, Data Transfer, Database, Exadata, FastConnect, and Governance Services.
- Strong security controls to meet GDPR requirements
- For a complete list of compliance certifications and attestations, visit https://www.oracle.com/cloud/cloud-infrastructure-compliance/

Meet GDPR Requirements

Lawfully, Fairly, Transparently

Purpose Limitation

Accuracy

Integrity and Confidentiality

- Data breach notification within 24 hours
- Oracle Services Privacy Policy gives transparency about Oracle's data handling as a processor
- Customers data stay in the home region chosen by the customer for their tenancy.
- Audit Service logs all calls to the API.
- Compartments, VCN, and Tagging
- Object Storage, Block Volume and File Storage services for keeping accurate copies of customer data and ensuring business continuity.
- Least privilege access control, data encryption, API authentication and MFA via identity federation for integrity and confidentiality.

Physical Security

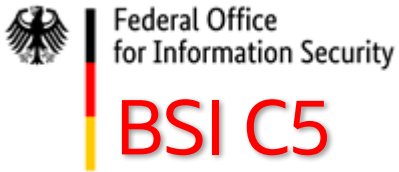
- State-of-the-art “Tier IV Class” facilities in the US and Europe
- Sufficient redundancy of critical equipment such as power sources in case of a failure or breakdown
- Layered approach to physical security
  - Perimeter barriers
  - Site-specific badges and identification
  - Smart-card based authentication
  - Least-privilege access
  - Audited access usage
  - Video surveillance
  - Isolated security zones around server and networking racks

Personnel Security

- Hire best talent with strong ethics and good judgment
- Conduct pre-employment screening
- Offer baseline and specialized security training
- Use security as a component of our team evaluation processes
- Collaborate with industry experts in specialist conferences

Compliance for ALL Regions and ALL Services

27001 : 27017 : 27018



EXTENSIVE LIST OF ACCREDIDATIONS

Basic Security Considerations

Security considerations

- Keep software up-to-date. This includes the latest product release and any patches that apply to it.
- Limit privileges as much as possible. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Learn about and use the Oracle Cloud Infrastructure security features.
- Keep up-to-date on security information. Oracle regularly issues security-related patch updates and security alerts. Install all security patches as soon as possible. Visit http://www.oracle.com/technetwork/topics/security/alerts-086861.html

ORACLE

Oracle Cloud always free tier:
oracle.com/cloud/free/

OCI training and certification:
https://www.oracle.com/cloud/iaas/training/
https://www.oracle.com/cloud/iaas/training/certification.html
education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:
ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:
youtube.com/user/OracleLearning

Thank you