Oracle Cloud Platform Security: Built for Enterprise

Yuecel Karabulut, Ph.D.
Director of Product Management
IaaS Security & Compliance

ORACLE

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, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.


Could We Design Software
Like We Design Bridges?

Diesel

Hybrid

Electric

Cloud is **unbeatable** and **unstoppable** from a power, cost and efficiency standpoint.

ORACLE

Cloud is also **unbeatable** from a security standpoint!

Nearly 60% of organizations agreed that Cloud Service Providers provide **better security** than their own IT organizations.

Source: IDC 2013 U.S. Cloud Security Survey, doc #242836, September 2013

ORACLE

Major Drivers to Consider Public Cloud

1. Reduce capital expenses
2. Explosive data growth
3. Reduce administrative costs
4. Better security

Talk About Three Things

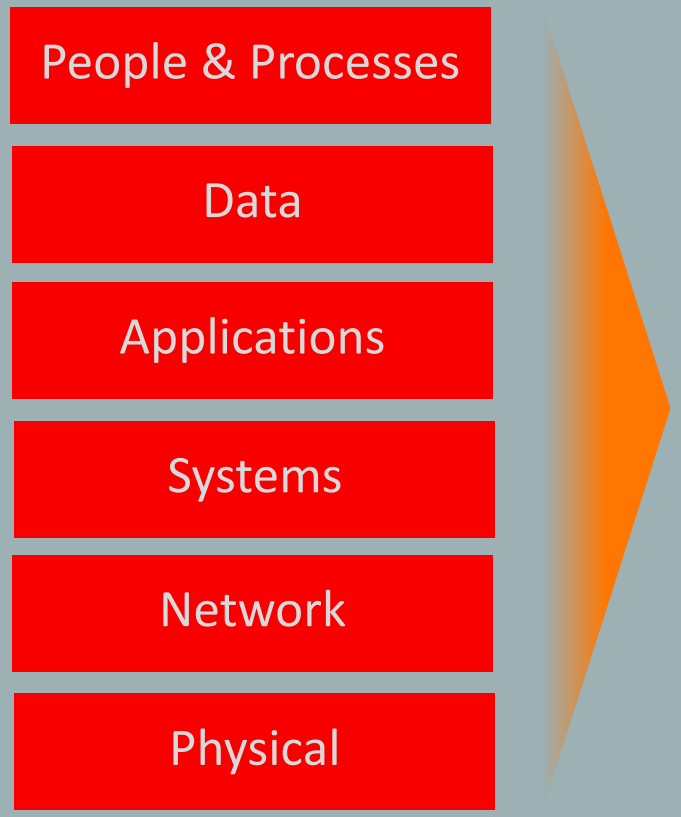
1. **Taking the Mystery out of Cloud Security**
2. **What Trusted Cloud Platform Means to Customers**
3. **Oracle Cloud Platform Security Capabilities and Best Practices**

ORACLE

Cloud Security is still a **mystery** to many enterprises!

ORACLE

How is Cloud Security Different than On-Premises Security?



On-Premises

- **100%** your responsibility
- You spend most of your security budget for network, systems and physical security.
- If security fails badly
  - You fire and hire.
  - You buy more security software
  - Your IT organization survives and continues to operate.

Cloud (IaaS and PaaS)

- Security is a **shared responsibility**.
- You focus on workload security.
- If security fails badly
  - The cloud provider would go out of business.
- Same security for all enterprises.

ORACLE

Cloud Security

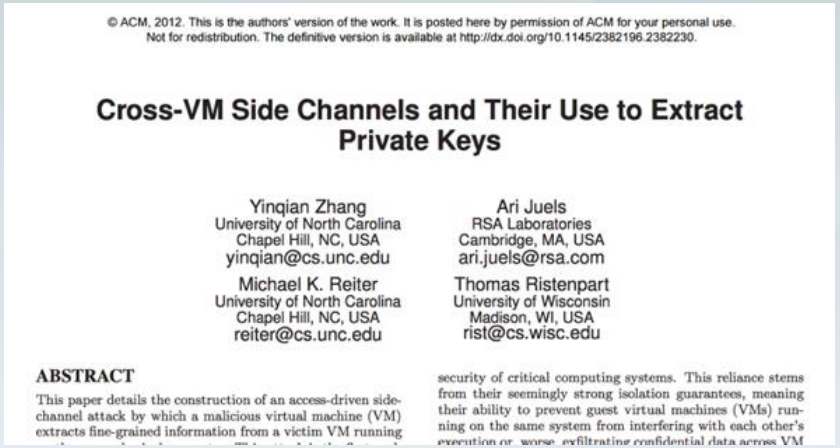
What is **fact**? What is **fiction**?

ORACLE

Conventional Wisdom vs. Real (Cloud) Security Challenges

Fiction: VM Escape

- VM escape (guest-to-host attacks)
- Side-channel attacks
- Private cloud is more secure



Cross-VM Side Channels and Their Use to Extract Private Keys

Yinqian Zhang
University of North Carolina
Chapel Hill, NC, USA
yinqian@cs.unc.edu

Ari Juels
RSA Laboratories
Cambridge, MA, USA
ari.juels@rsa.com

Michael K. Reiter
University of North Carolina
Chapel Hill, NC, USA
reiter@cs.unc.edu

Thomas Ristenpart
University of Wisconsin
Madison, WI, USA
rist@cs.wisc.edu

ABSTRACT

This paper details the construction of an access-driven side-channel attack by which a malicious virtual machine (VM) extracts fine-grained information from a victim VM running

security of critical computing systems. This reliance stems from their seemingly strong isolation guarantees, meaning their ability to prevent guest virtual machines (VMs) running on the same system from interfering with each other's

Fact: Poor Security Ops

- Threats and adversaries are not well understood
- Loss of credentials
- Least privilege is NOT widely adopted
- Patching is not a priority

ORACLE

My Cloud Security Thesis

If your IT security folks do a good job

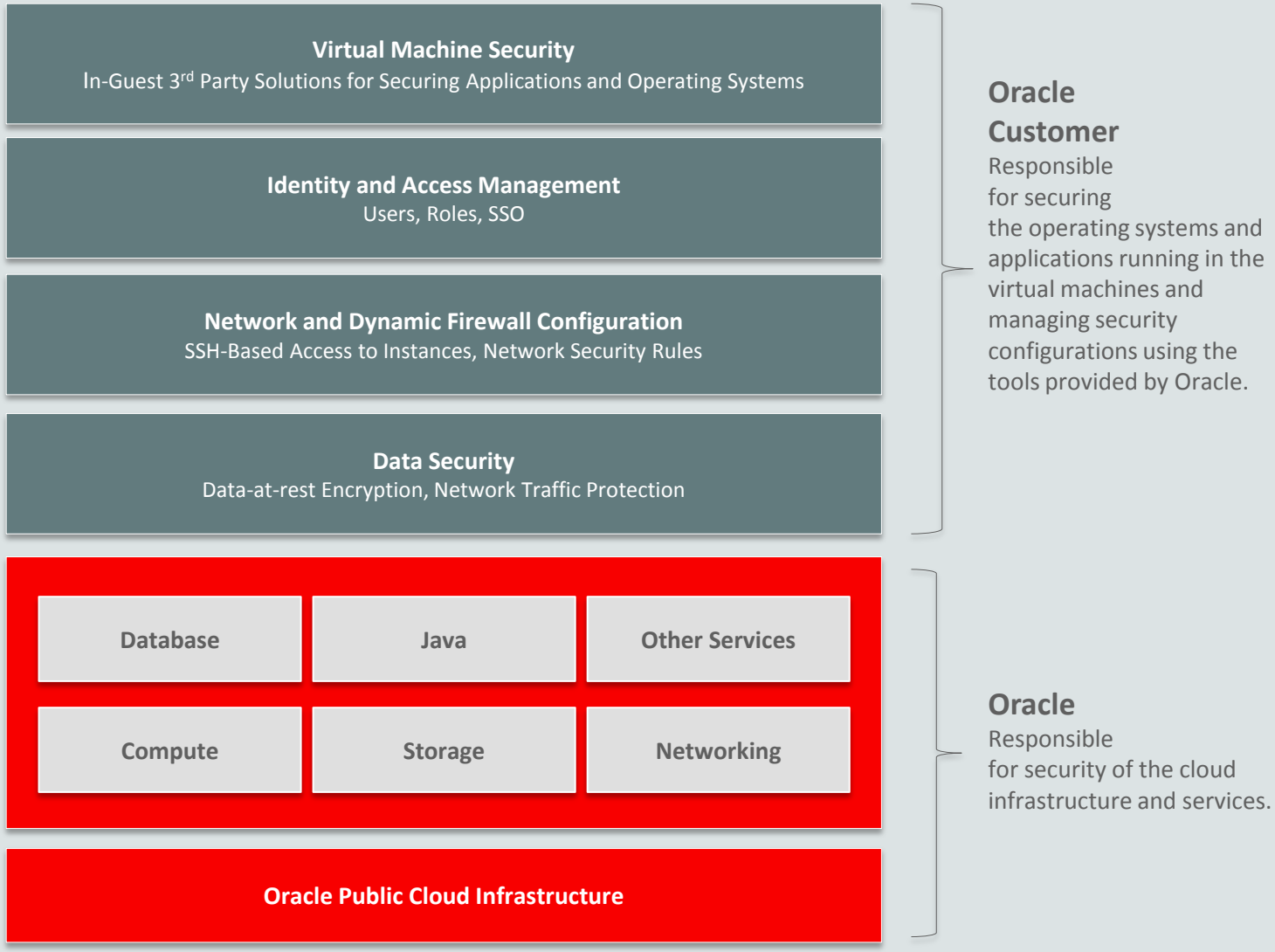
in securing your current on-premise systems,

they will do a better job in the cloud,

because they can fully “focus” on workload security due to shared responsibility model.

ORACLE

Oracle and Customers Share the Responsibility



Key Capabilities Enterprise Customers Expect from Security in the Cloud:

"I want to **constrain access** to my resources in the cloud and keep **full data ownership.**"

ORACLE

How Customers Define a Trusted Enterprise Cloud Platform

Flexible	Choose deployment option | Decide level of access control
Controllable	Constrain access | Segregate responsibilities | Control data location
Visible	Monitor what is going on with your resources
Auditable	Review 3rd party assurances | Evaluate your configuration
Hybrid Centric	Bring your users | Bring your keys | Monitor actions holistically
Security @ Core	Secure Cloud Operations | Secure Software Development

ORACLE

Oracle Combines the Best of First-gen IaaS and On-premises

First-generation IaaS (e.g. AWS, Azure)

- Adding capacity takes minutes
- Only pay for what you use

On-premises or Managed Hosting (e.g. Rackspace)

- Raw iron performance
- Dedicated hardware

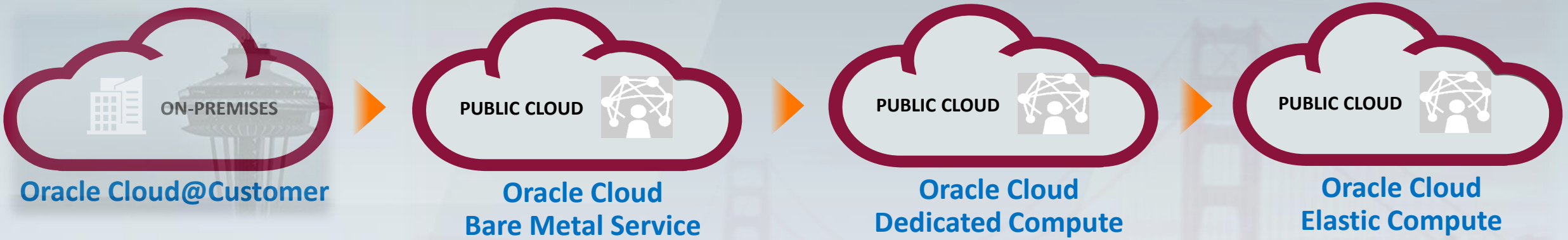
Modern Cloud Infrastructure

- Bare metal servers in minutes
- Integrated compute, storage, database services on their own private network
- All features automated, usable via console or API
- Enterprise-level security and governance

ORACLE

- Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- Security @ Core

Oracle Cloud Offers Broadest Set of Isolation Choices



Oracle Cloud@Customer

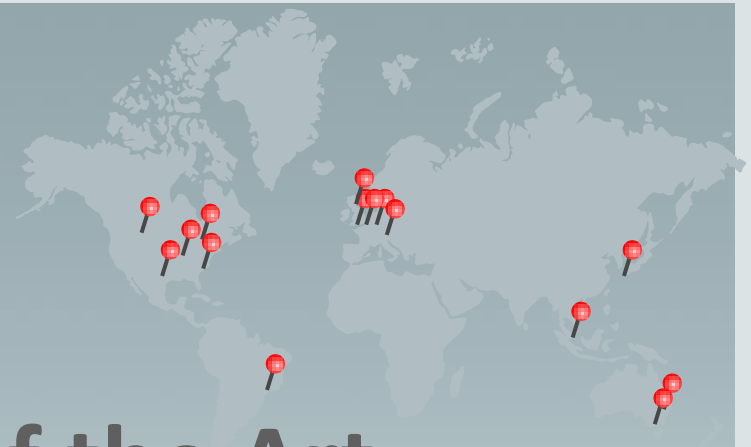
Oracle Cloud
Bare Metal Service

Oracle Cloud
Dedicated Compute

Oracle Cloud
Elastic Compute

ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- Security @ Core



Security @ Scale in 19 State of the Art "Tier IV Class" Facilities

Layered Security, Automated Security Operations

Attack Prevention, Detection, Monitoring & Response

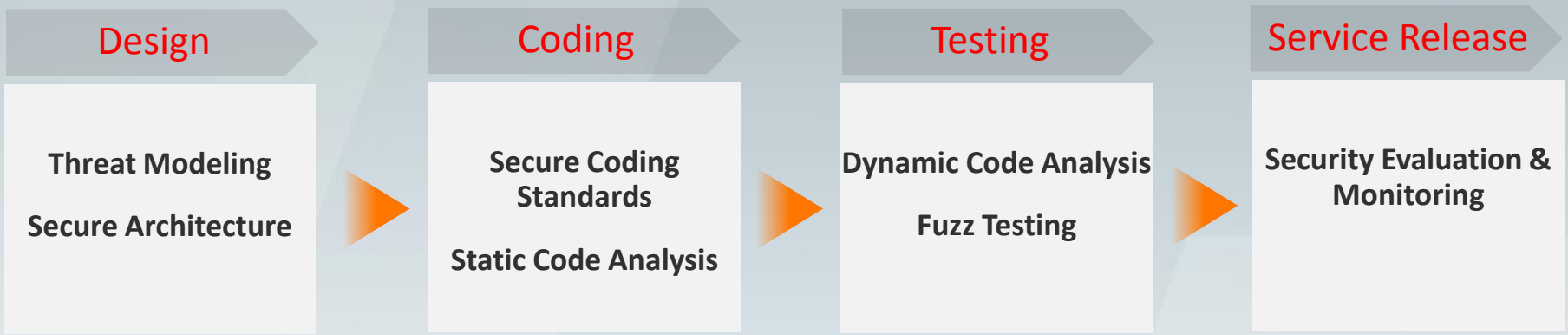
3rd party Security Testing on every major release

Auditing, Certifications and Attestations

ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- Security @ Core

Secure Design and Coding

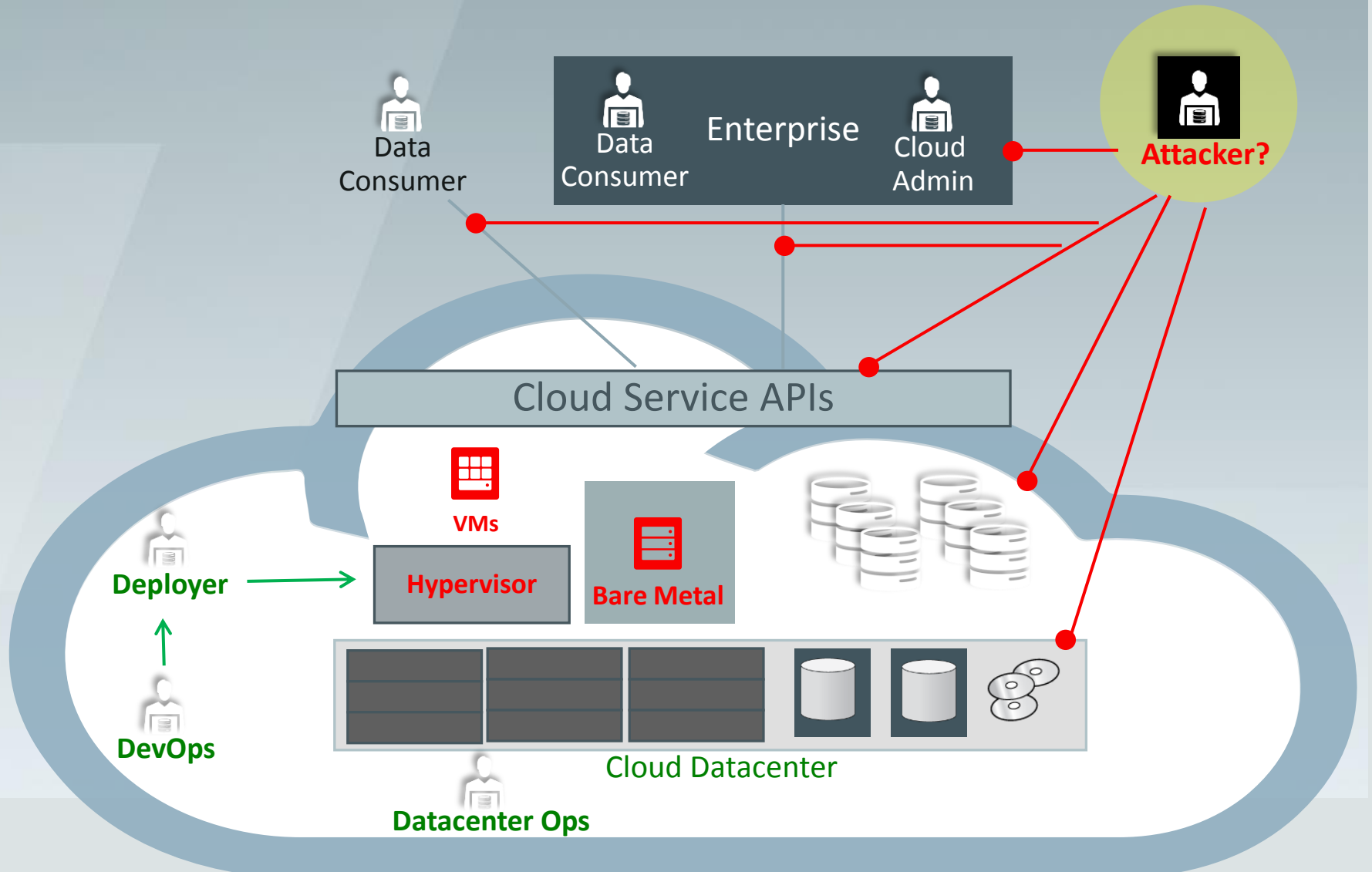


ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- Security @ Core

Threat Actors

Security is about defining trust boundaries correctly and mitigating risks.



ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Full Data Ownership

Decide where (region and availability) your data should be stored

Oracle doesn’t make any secondary use of data

ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Federated Identity and Access Management

Federated SSO using SAML 2.0

Support for AD Integration

API Authorization using OAuth 2.0

ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Fine-Grained Access Control

Users and Built-in Groups

Compartments: Isolation Between Projects and Teams

Declarative Policy Language for Fine-Grained Access Control

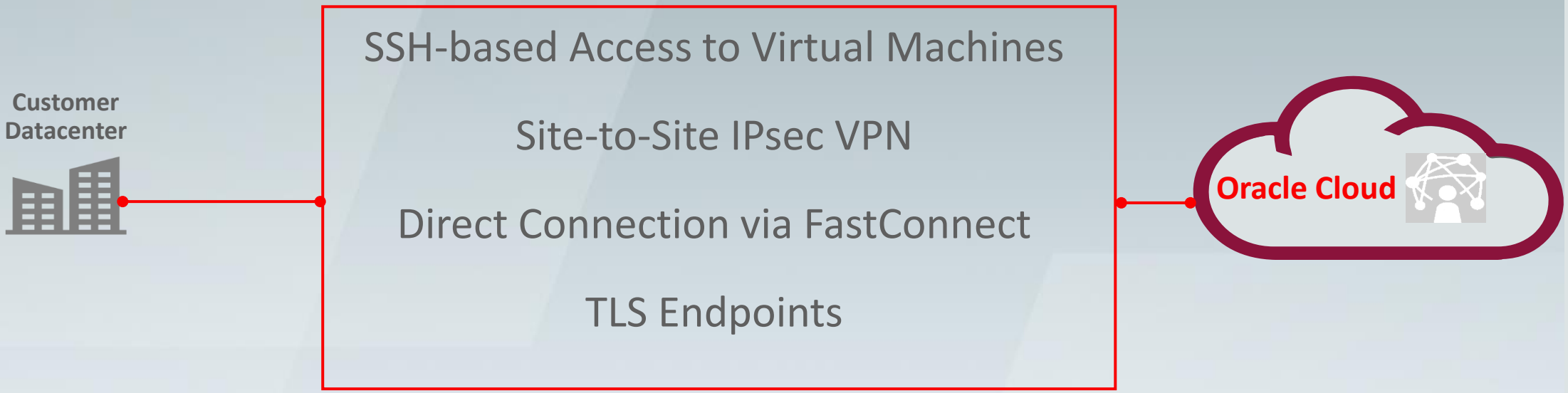
Multi-Factor Authentication (coming soon)

Instance Isolation

ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Secure Access to Cloud Resources



ORACLE

- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Virtual Cloud Network

Network Segmentation and Subnets

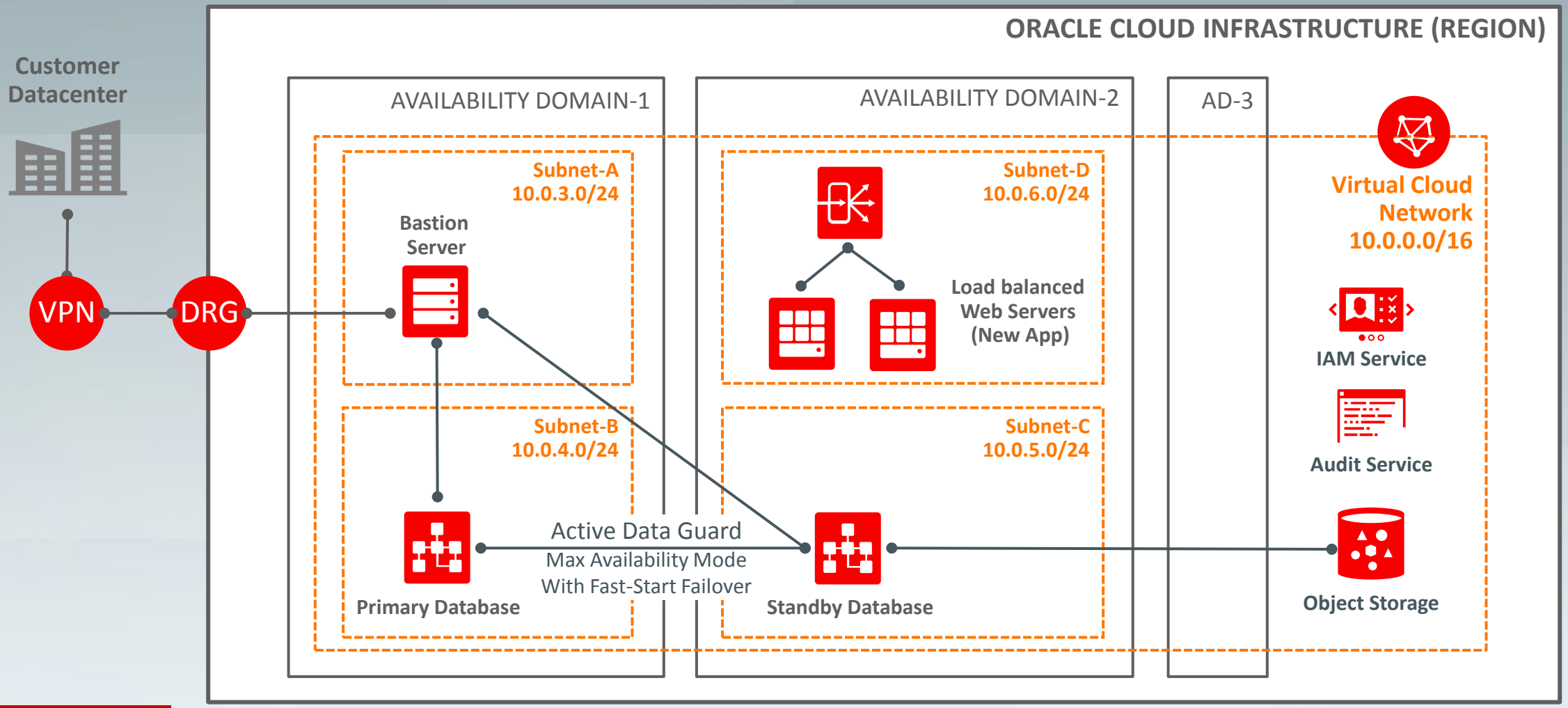
Each Customer's traffic completely isolated in Private L3 Overlay Network

Built-in Stateful Firewall

Control Subnet and VM Traffic using Ingress and Egress Security Lists

ORACLE

Virtual Cloud Network



- ✓ Flexible
- Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Encrypt Your Data The Way You Choose

Client-Side Encryption Using Your Keys You Manage

Default Block Storage Encryption Using Oracle-Managed Keys

Server-Side Encryption Using Your Keys for Object Store (coming soon)

Built-in Key Management Service (coming soon)

Tablespace-level Data Encryption

ORACLE

- ✓ Flexible
- ✓ Controllable
- Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Full Visibility of Your Resources

Completely API-driven Architecture and Console View

Full visibility of actions on your resources via log data (coming soon)

ORACLE

- ✓ Flexible
- ✓ Controllable
- ✓ Visible
- Auditable
- Hybrid Centric
- ✓ Security @ Core

Security Operations Aligned with ISO/IEC 27001

Audit reports available under NDA

Configuration Analysis using Palerra

Certifications and attestations coming soon:

SOC 1, SOC 2, ISO 27001, PCI DSS and HIPAA

ORACLE

- ✓ Flexible
- ✓ Controllable
- ✓ Visible
- ✓ Auditable

Hybrid Centric

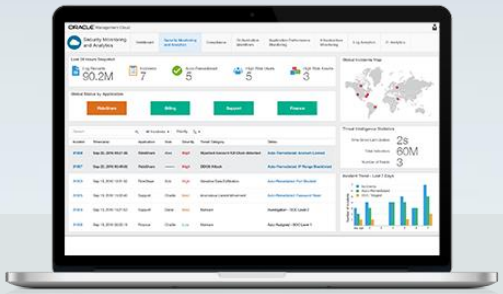
- ✓ Security @ Core

Intelligent Monitoring and Threat Detection using Oracle Identity SOC

Security automation to predict, prevent, detect, and respond to threats

Single-pane of Glass for On-Premises and Cloud

SIEM + CASB + UEBA + Identity Management



ORACLE

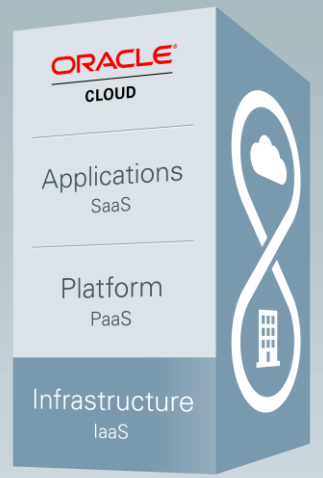
10 Oracle Cloud Security Best Practices

1. Understand the Oracle Public Cloud Shared Responsibility Model
2. Define and categorize your assets
3. Understand the Oracle Public Cloud Infrastructure
4. Design your Information Security Management System
5. Manage Cloud Account, Users and Groups and apply the “Least Privilege” principle
6. Manage OS-level Access to Compute Instances Using SSH and Built-in Firewall
7. Create subnets to define isolated network for each workload or organizational entity
8. Encrypt your data before uploading it to Oracle Storage Cloud Service
9. Monitor your workloads and protect them from Malware
10. Build Threat Protection Layers

ORACLE

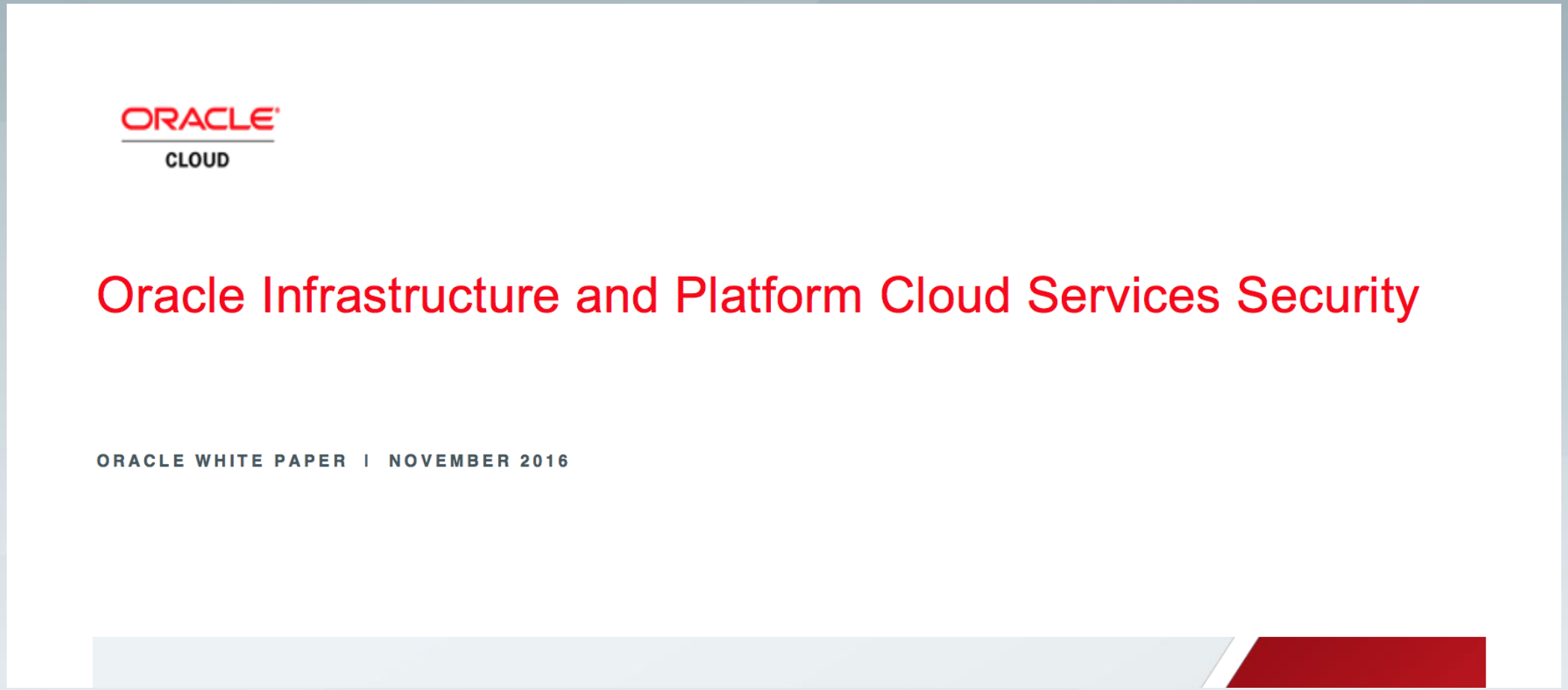
"You are **better off** in Oracle Cloud than in your environment."

- **Flexible**
- **Controllable**
- **Visible**
- **Auditable**
- **Hybrid Centric**
- **Security @ Core**



ORACLE

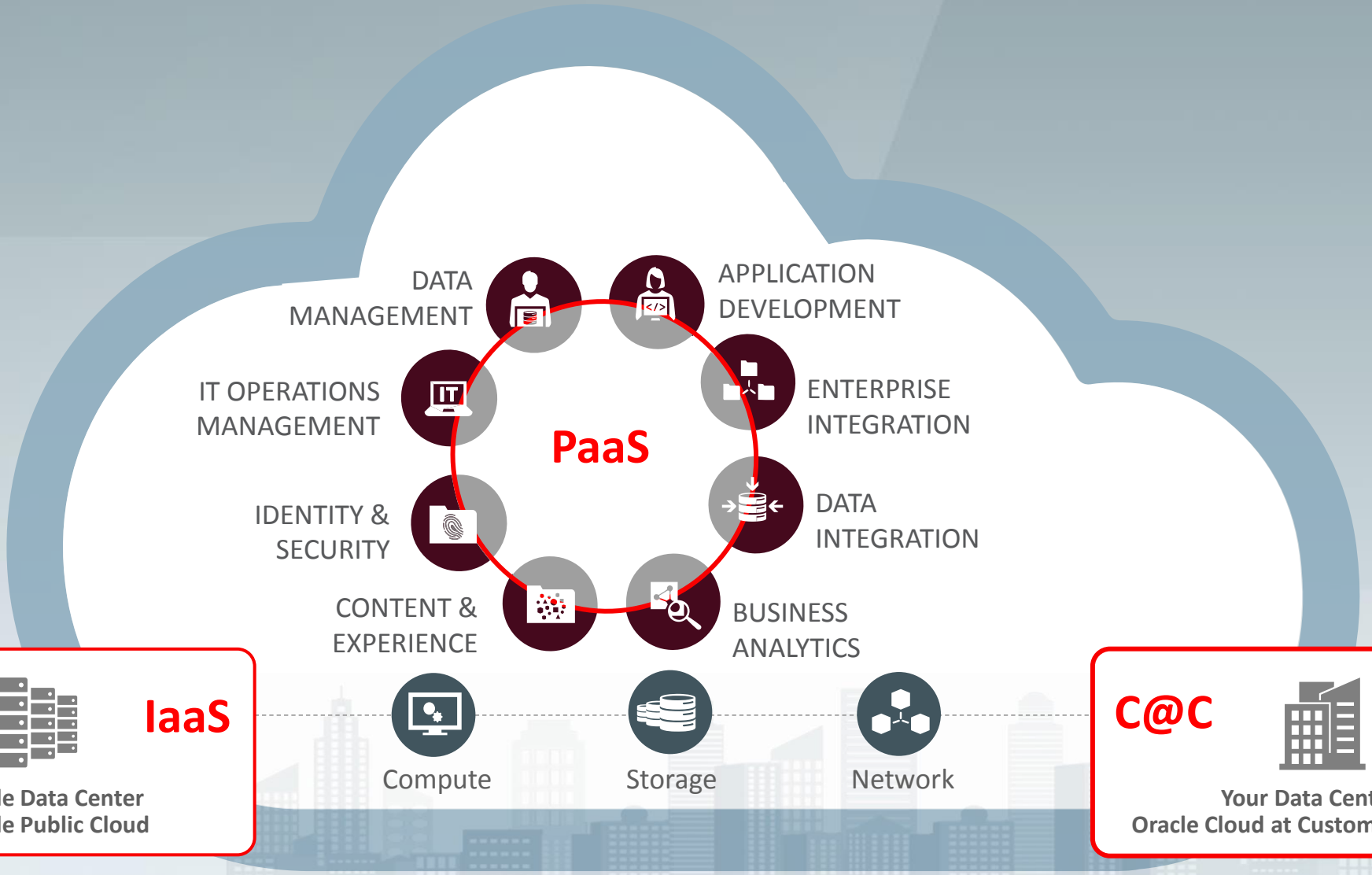
Oracle Cloud Security White Paper



ORACLE


ORACLE®

Oracle Cloud Platform: Secure Cloud for Any Workload



- Hybrid Cloud
- Comprehensive
- Integrated
- Open

IaaS

Oracle Data Center
Oracle Public Cloud

C@C

Your Data Center
Oracle Cloud at Customer

ORACLE

Holistic Cloud Security Requires More Than IaaS Security

Oracle Identity SOC

3

2

PaaS Security Controls

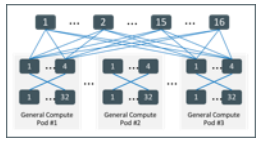
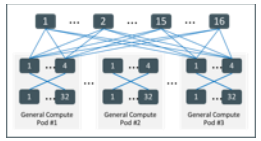
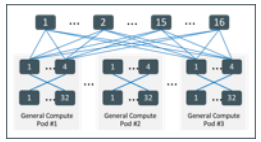
ORACLE

EVALUATE	PREVENT	DETECT
Security Configuration	Encryption & Redaction	Auditing
Sensitive Data Discovery	Masking & Subsetting	Activity Monitoring
Least Privilege Use	DBA & Operational Controls	Alerting & Reporting

1

IaaS Security Controls

IAM | Encryption | Network Isolation | Secure Access

Secure IaaS

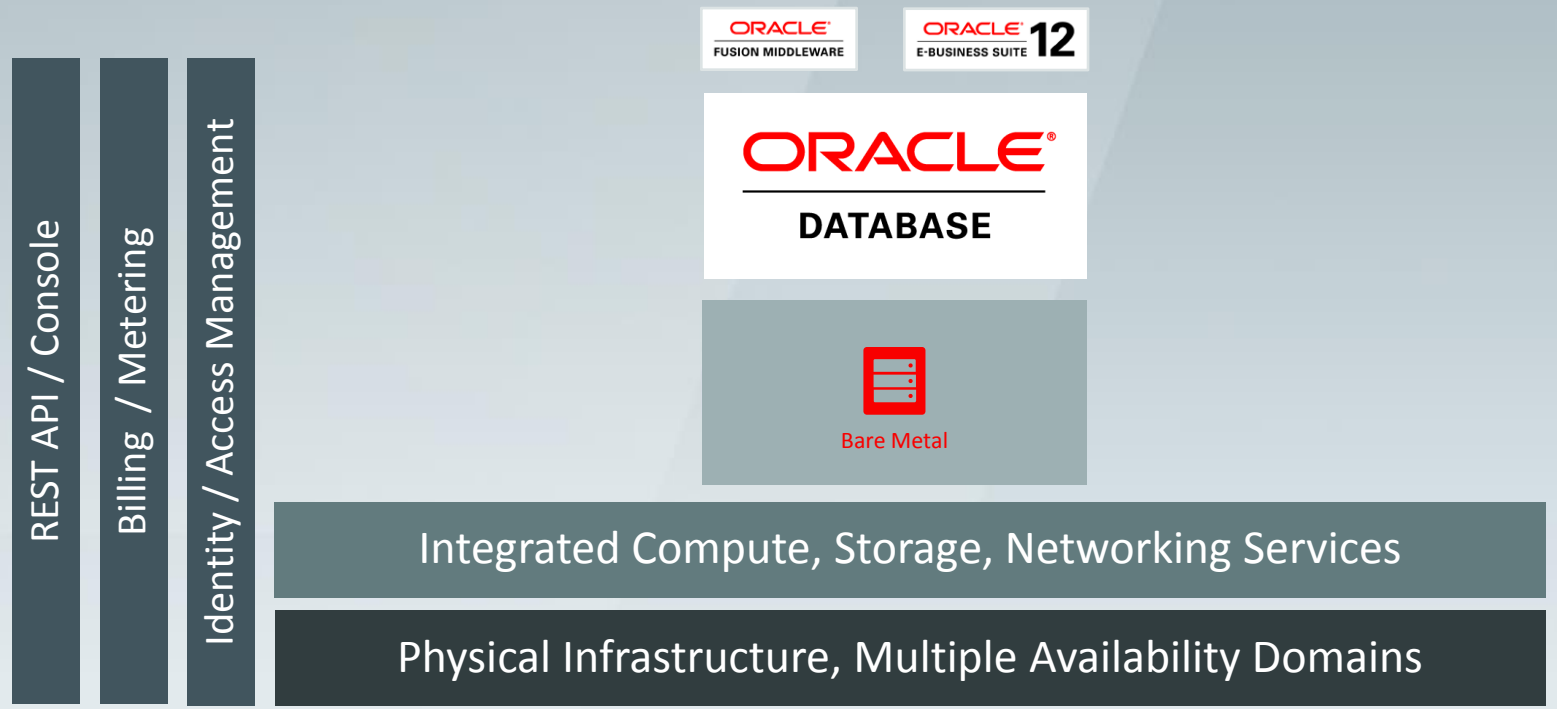
3rd Party Security Solutions

4

ORACLE

PaaS Security

Bare Metal Database Service Security



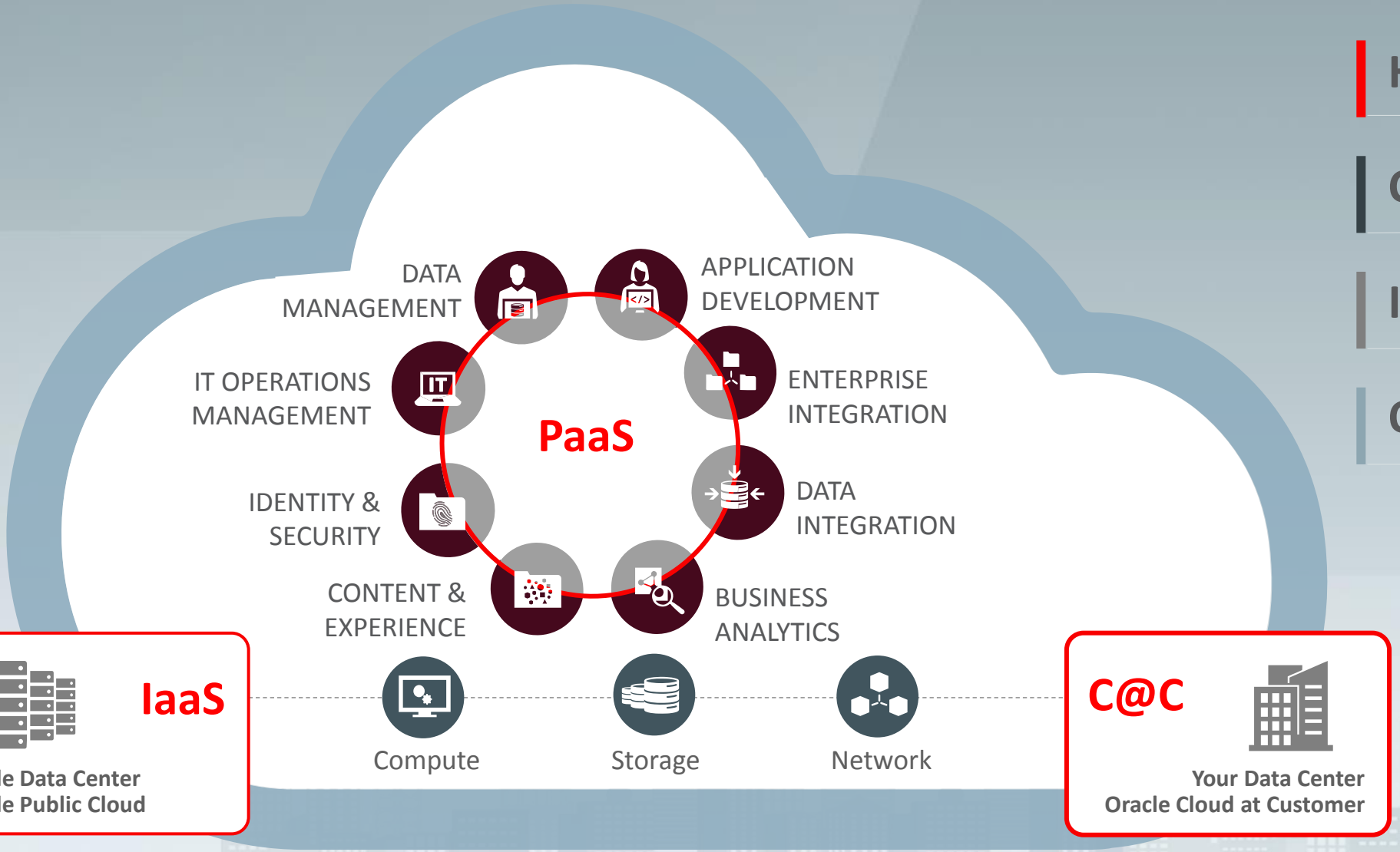
- Databases **configured with Auto TDE** by default
- Deploy databases into **a private network** (VCN) with **triple-redundant VPN** access
- Configure **Security Lists (Inbound/Outbound)** to secure your databases
- Setup **Identity policies to control management access** only to your DBAs
- **3-way or 2-way mirroring** on Local NVMe flash drives on all instances in DataGuard setup

ORACLE

Oracle Cloud Platform: Cloud for Any Workload

ORACLE

Oracle Cloud Platform



Hybrid Cloud

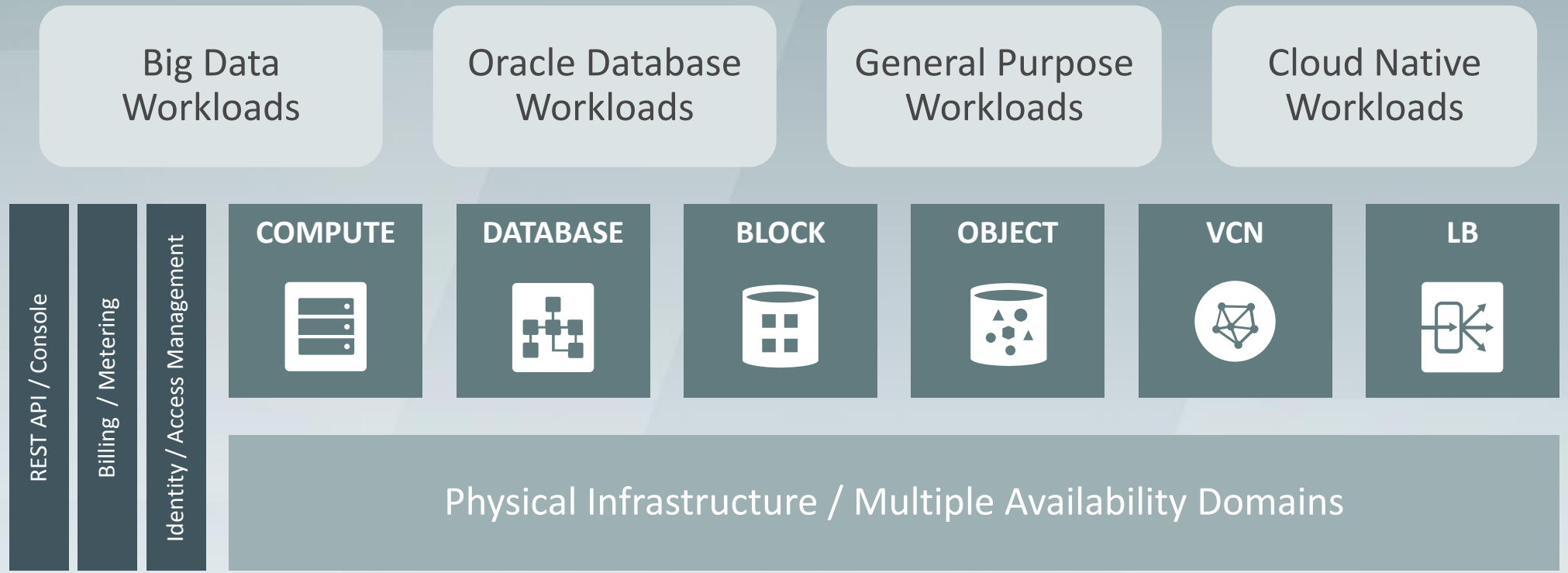
Comprehensive

Integrated

Open

ORACLE

Oracle IaaS Overview



Oracle IaaS Compute: Supports Broadest Set of Workloads

Bare Metal	Elastic Compute	Container Service	Ravello	Dedicated Compute, SPARC	Engineered Systems, C@C
Multiple OS Bare Metal, VMs	Hypervisor	MESOS Docker Registry	vmware KVM		

Hardware – Physical Servers & Storage

Core Data Center & Access Network

Data Center Regions & Availability Domains

ORACLE

Oracle IaaS Storage: Highest Performance and Durability

Local NVMe	Block	Object	Archive	File & Database Backup	Storage Cloud Software Appliance
			COMMVAULT	Symantec. COMMVAULT	POSIX NFS SMB, NAS WebDav

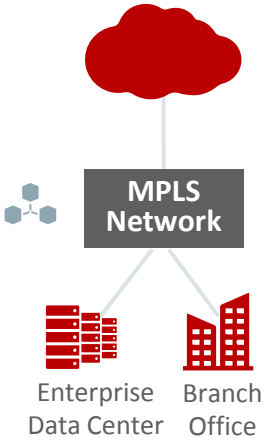
Hardware – Physical Servers & Storage

Core Data Center & Access Network

Data Center Regions & Availability Domains

ORACLE

Oracle IaaS Networking: Ultimate Control and Connectivity

VCN	IPSEC VPN	Oracle Cloud FastConnect SE	Oracle Cloud FastConnect EE
			

Hardware – Physical Servers & Storage

Core Data Center & Access Network

Data Center Regions & Availability Domains

ORACLE

Oracle Cloud@Customer

1. Oracle Cloud behind your firewall
2. Test and dev in the public cloud and production environment on your premises
3. Burst from your premises to the Oracle Cloud for flex capacity on demand
4. Same subscription and pay-as-you-go pricing

ORACLE