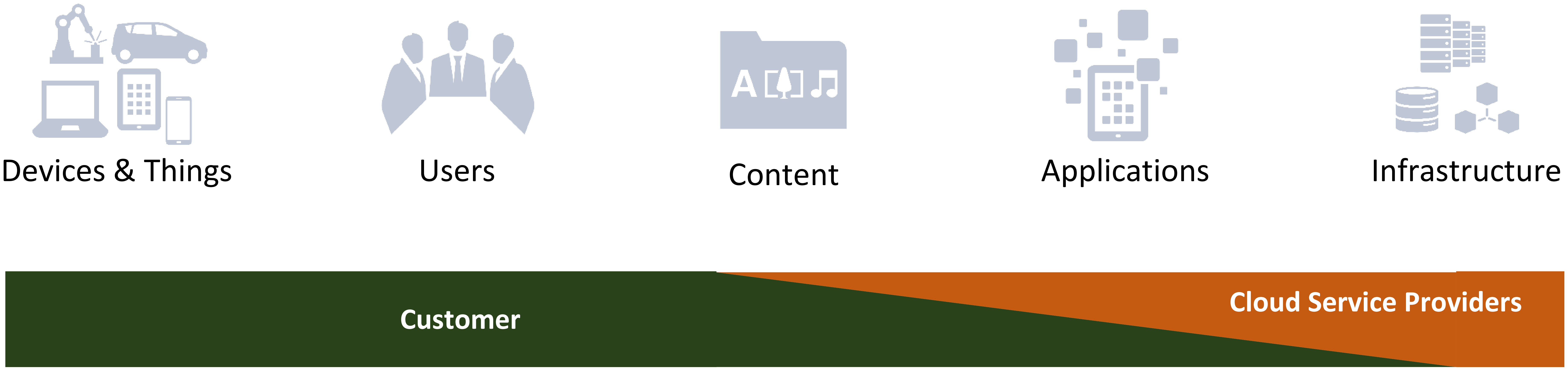
ORACLE

# Why customers in the UAE are moving regulated workloads to Oracle Cloud

**Maged Hanna**
MEA Strategic Engagements and Functional Leader

# Shared Responsibility for Security



Devices & Things

Users

Content

Applications

Infrastructure

Customer

Cloud Service Providers

**90% of CISOs are confused about their role in securing a SaaS environment versus the cloud service providers**

*Oracle and KPMG Cloud Threat Report 2020*

> “ Through 2025, **99%** of cloud security failures will be the customer’s fault.”

**Gartner, October 2019**

Source: Smarter With Gartner, Is the Cloud Secure?, October 2019, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

# Current state of the art in cloud security

**A lot of security tools**

**No real instructions**

**Customers have to put them together themselves**

What if there is a different way?

# A different take on Cloud Security

- Security is always enforced - cannot be disabled
- Not always feasible for 100% of your application

Extremely Secure Location

- Automatic problem identification
- Optional Automatic remediation

Secure Location

Continuously Monitored

# A different take on Cloud Security

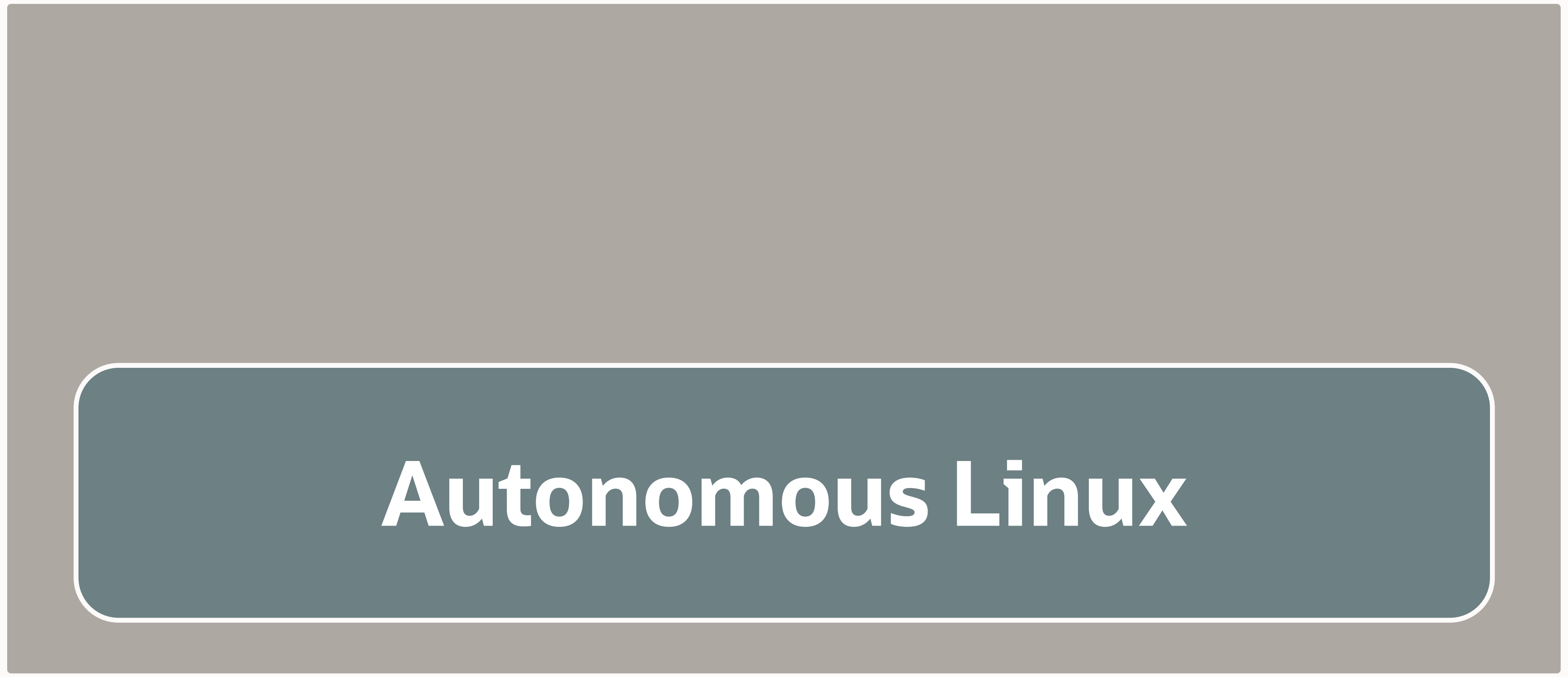
- Security is always enforced - cannot be disabled
- Not always feasible for 100% of your application

### Extremely Secure Location

Autonomous Database

- Automatic problem identification
- Optional Automatic remediation

### Secure Location Continuously Monitored



Autonomous Linux

# A different take on Cloud Security

- Security is always enforced - cannot be disabled
- Not always feasible for 100% of your application

**Extremely Secure Location**

**Maximum Security Zone**

**Autonomous Database**

- Automatic problem identification
- Optional Automatic remediation

**Secure Location Continuously Monitored**

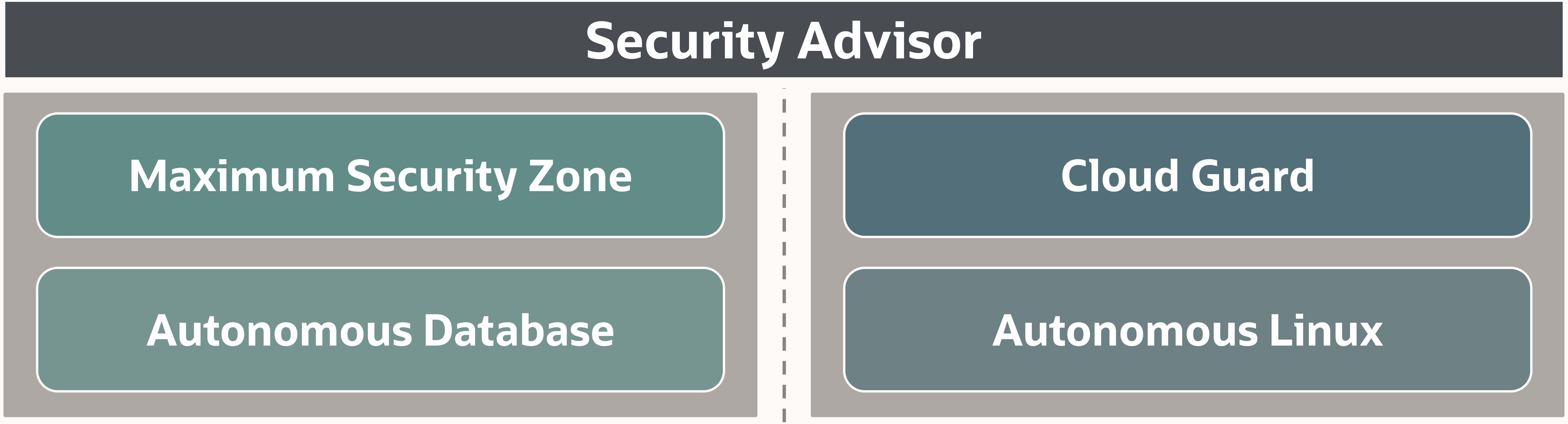
**Cloud Guard**

**Autonomous Linux**

# A different take on Cloud Security

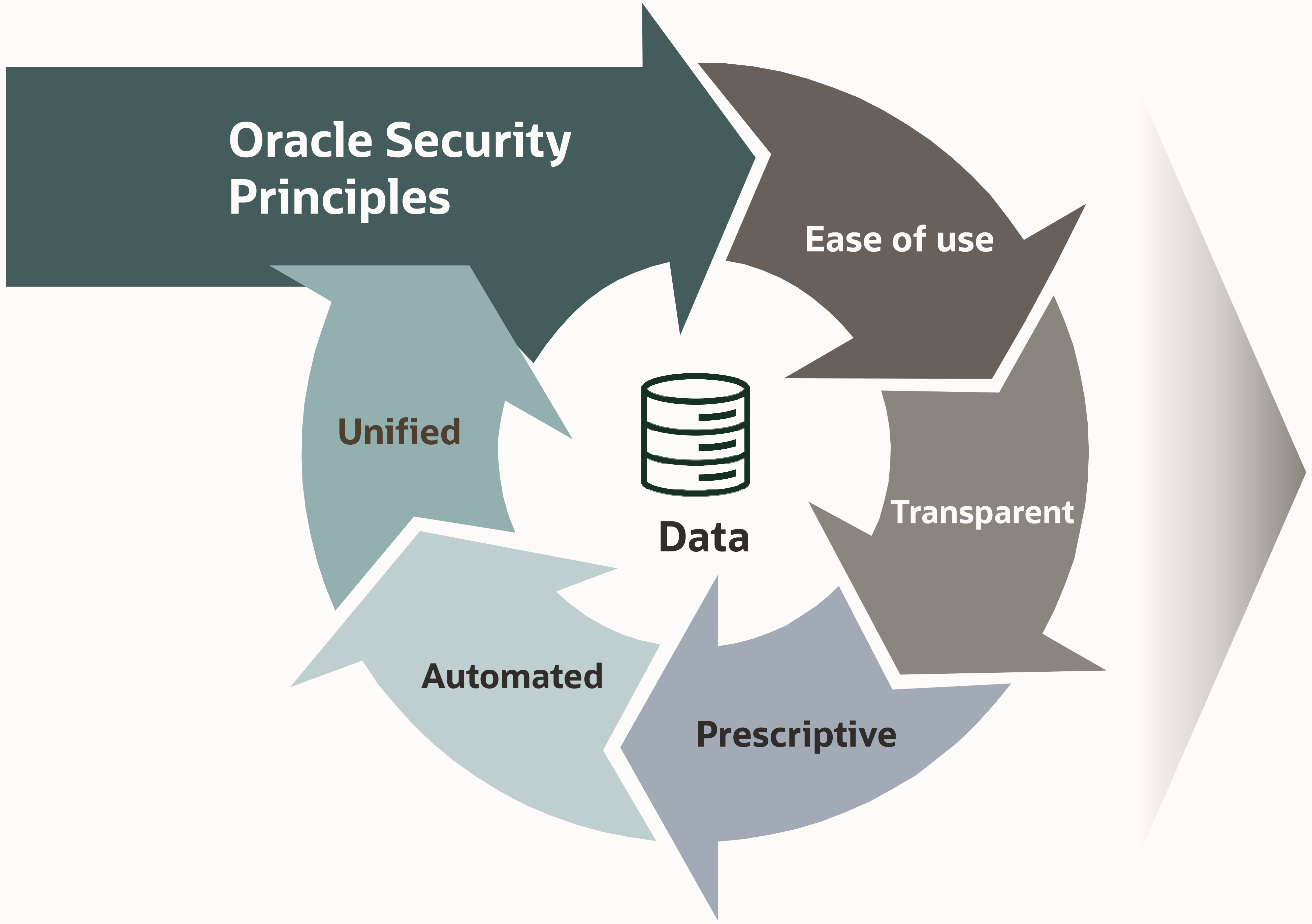
- Security is always enforced - cannot be disabled
- Not always feasible for 100% of your application

- Automatic problem identification
- Optional Automatic remediation



# Oracle’s Security Principles

Making security Simple, Prescriptive and Integrated



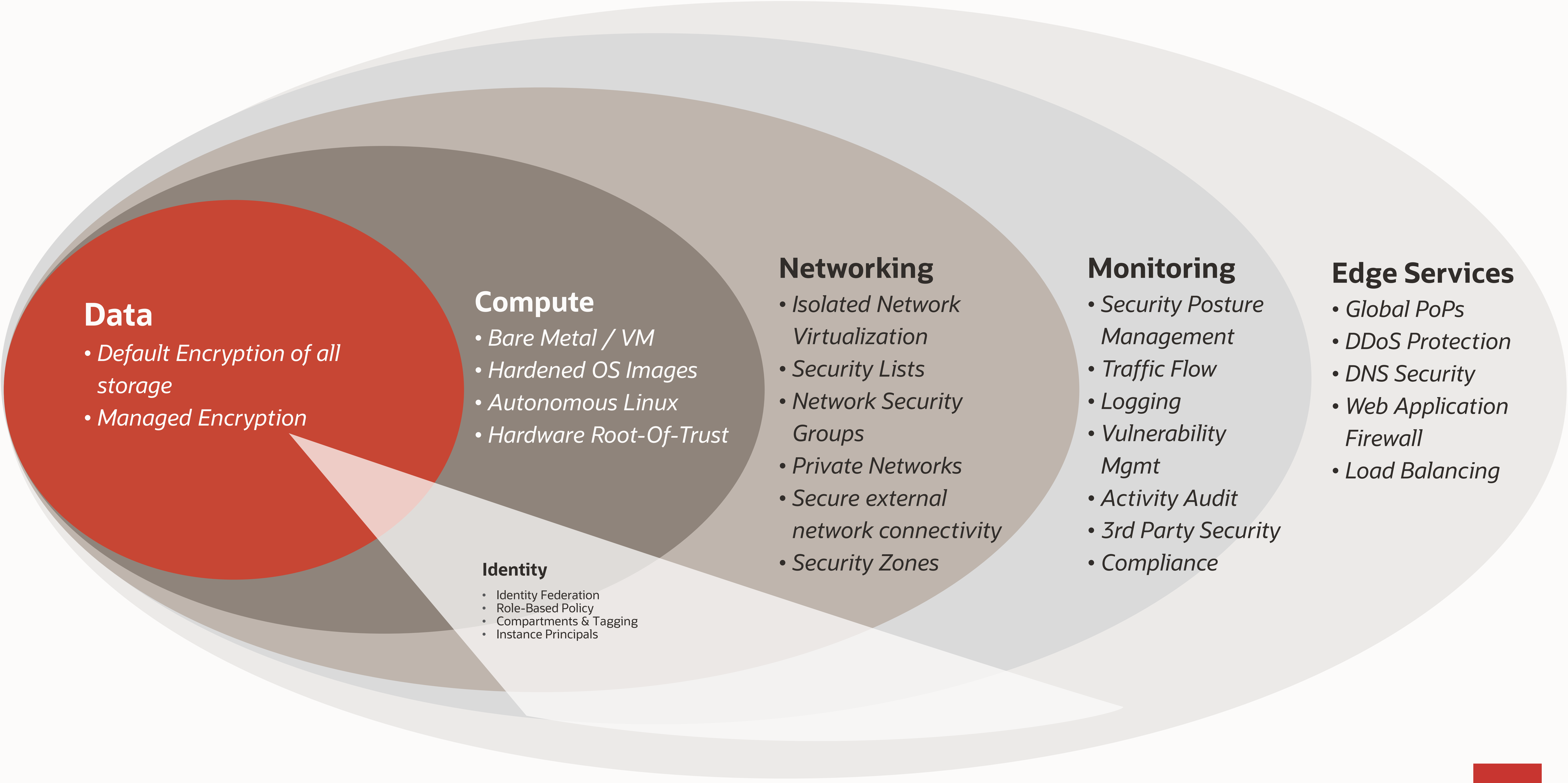
## Principles and Customer Benefit:

- Simple: Reduces learning curve
- Transparent: ‘Always on’ security posture
- Prescriptive: Guardrails minimize errors
- Automated: Reduce workload and human error
- Unified: Full stack view across platform tool

## Results:

- Shift the security burden from the Customer
- Eliminate cost versus security trade-offs

# OCI Next Gen Architecture Designed from the Ground Up To Be Secure



**Data**

- *Default Encryption of all storage*
- *Managed Encryption*

**Compute**

- *Bare Metal / VM*
- *Hardened OS Images*
- *Autonomous Linux*
- *Hardware Root-Of-Trust*

**Networking**

- *Isolated Network Virtualization*
- *Security Lists*
- *Network Security Groups*
- *Private Networks*
- *Secure external network connectivity*
- *Security Zones*

**Monitoring**

- *Security Posture Management*
- *Traffic Flow*
- *Logging*
- *Vulnerability Mgmt*
- *Activity Audit*
- *3rd Party Security*
- *Compliance*

**Edge Services**

- *Global PoPs*
- *DDoS Protection*
- *DNS Security*
- *Web Application Firewall*
- *Load Balancing*

**Identity**

- Identity Federation
- Role-Based Policy
- Compartments & Tagging
- Instance Principals

# Oracle Compliance Programs

# OCI Compliance Programs

## Expansive list of independent assessments across industries and regions

### REGIONAL

- GDPR [EU]
- PIPEDA [Canada]
- ENS [Spain]
- BSI C5 [Germany]
- K-ISMS [Korea]
- NISC [Japan]
- CITC [Saudi Arabia]
- Cyber Essentials Plus [UK]
- Cloud Security Principles [UK]
- مركز دبي للأمن الإلكتروني DUBAI ELECTRONIC SECURITY CENTER
- TRA هيئة تنظيم الاتصالات TELECOMMUNICATIONS REGULATORY AUTHORITY
- مركز أبوظبي للأنظمة الإلكترونية والمعلومات ABU DHABI SYSTEMS & INFORMATION CENTRE

### 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

https://www.oracle.com/cloud/cloud-infrastructure-compliance/

# UAE Compliance Programs

## Global

Compliance programs Obtained

- SOC/ HIPAA/ C5/ CSA STAR/PCI/
- ISO 20000-1
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701

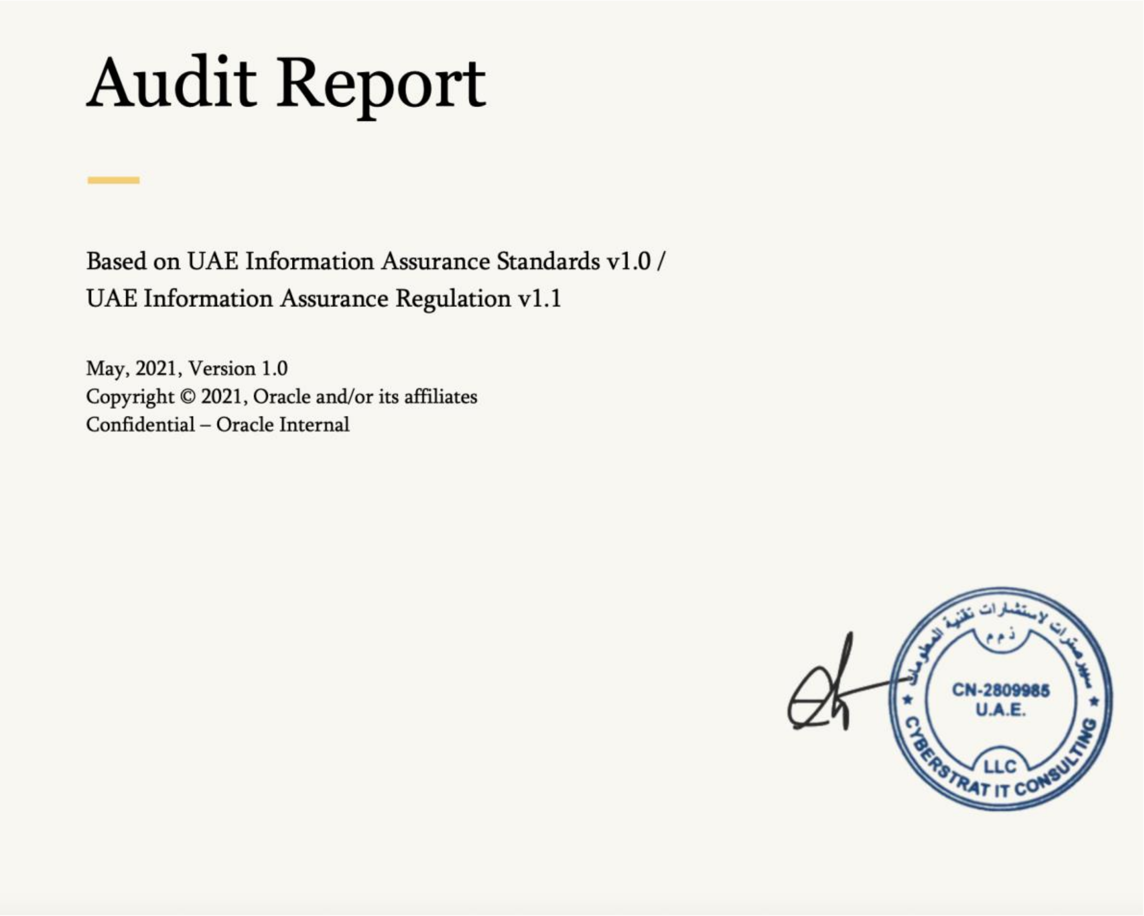
## Regional

| Certification Body | Industry / Gov | Standards /Controls | Outcome | Status |
|---|---|---|---|---|
| TRA Telecommunications Regulatory Authority | Fed Gov / FSI / Telcos | UAE IAR (Formerly NESA) | SoA & Audit Report | Obtained |
| ADISS AD Information Security Standards | AD PS | AD ISR V2 | Audit Report | Obtained |
| DESC Dubai Electronic Cyber Security Center | Dubai PS | ISR V2 | Certification | CY2022 |
| UAE Health Data Law | Fed Gov / Health care | The UAE Federal Law No. 2 of 2019 | White Paper | White Paper |

# UAE IAR & ADISS Audit Reports and HDL advisory white Paper

## Applicable for UAE 1 & 2 Regions

UAE IAR



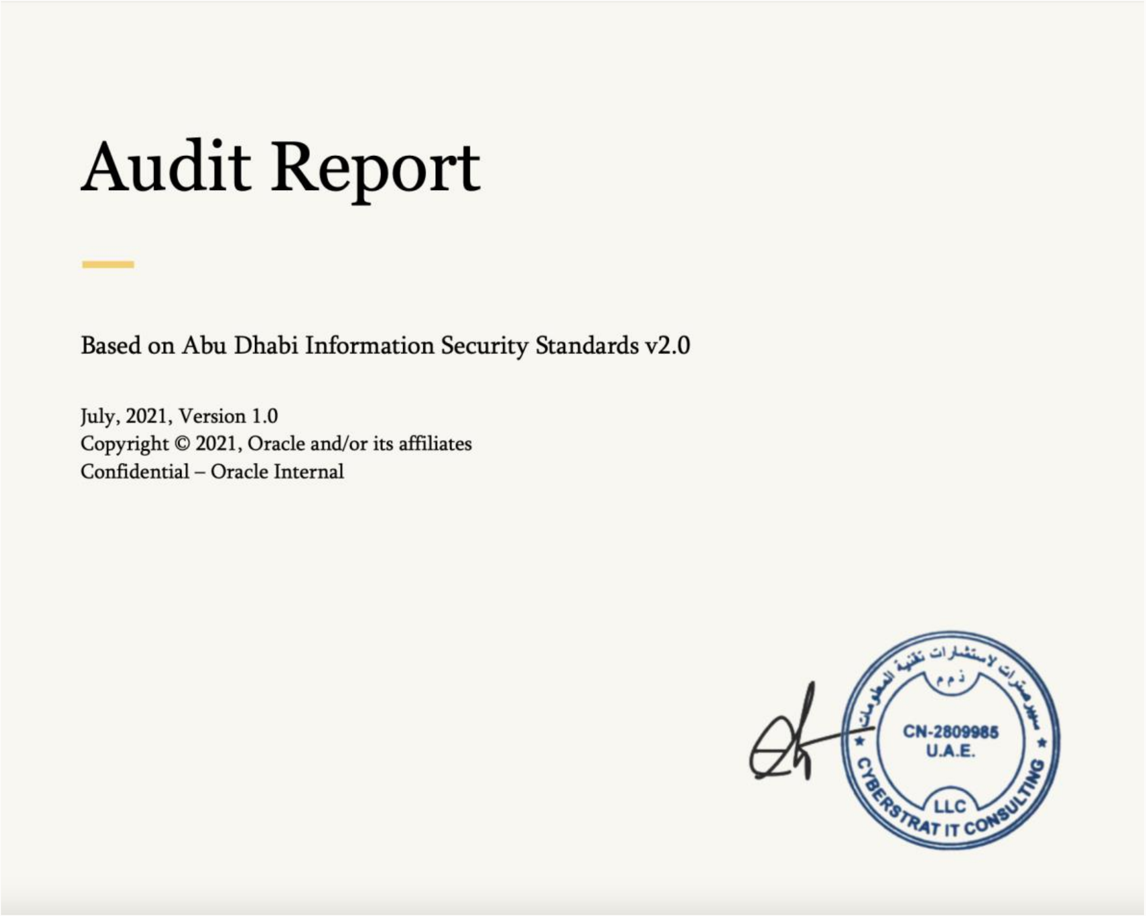
# Audit Report

Based on UAE Information Assurance Standards v1.0 /
UAE Information Assurance Regulation v1.1

May, 2021, Version 1.0
Copyright © 2021, Oracle and/or its affiliates
Confidential – Oracle Internal

سيبرسترات لاستشارات تقنية المعلومات
ذ م م
CN-2809985
U.A.E.
LLC
CYBERSTRAT IT CONSULTING

ADISS



# Audit Report

Based on Abu Dhabi Information Security Standards v2.0

July, 2021, Version 1.0
Copyright © 2021, Oracle and/or its affiliates
Confidential – Oracle Internal

سيبرسترات لاستشارات تقنية المعلومات
ذ م م
CN-2809985
U.A.E.
LLC
CYBERSTRAT IT CONSULTING

HDL

# Advisory: Oracle Cloud Services and the United Arab Emirates Health Data Law

Description of Oracle Cloud Services in the Context of the United Arab Emirates (UAE) Federal Law No. 2 of 2019 on the use of Information and Communication Technology (ICT) in Health Fields

July 2021, Version 1.0
Copyright © 2021, Oracle and/or its affiliates
Public

# UAE IAR Audit Report Summary

- **Background:**
  - Oracle contracted with an independent certification assessor to assess the Oracle Cloud Infrastructure system and related practices against the Information Assurance Regulation (IAR).
  - Cyberstrat IT Consulting, LLC (Cyberstrat) assessed the compliance of Oracle's Information Security Management System (ISMS) with the United Arab Emirates (UAE) compliance framework issued by National Electronic Security Authority (**NESA**) **UAE Information Assurance Standards (IAS) v1.0**, superseded with identical content by the **UAE Information Assurance Regulation (IAR) v1.1** issued by Telecommunications Regulatory Authority (**TRA**)
- **Scope:**
  - Scope is OCI (**42** services) and Oracle SaaS (**8** services) offering in the UAE East Region, including Dubai.
  - The compliance assessment included all of the UAE IAS v1.0 / UAE IAR v1.1 management and technical domains, controls, and sub-controls.
- **Outcome:**
  - All of the **188** controls consisting of **699** sub-controls are applicable to OCI, Oracle SaaS or other Oracle corporate functions. Overall compliance with NESA UAE IAS v1.0 / UAE IAR v1.1 controls is **100%**.

# ADISS Audit Report Summary

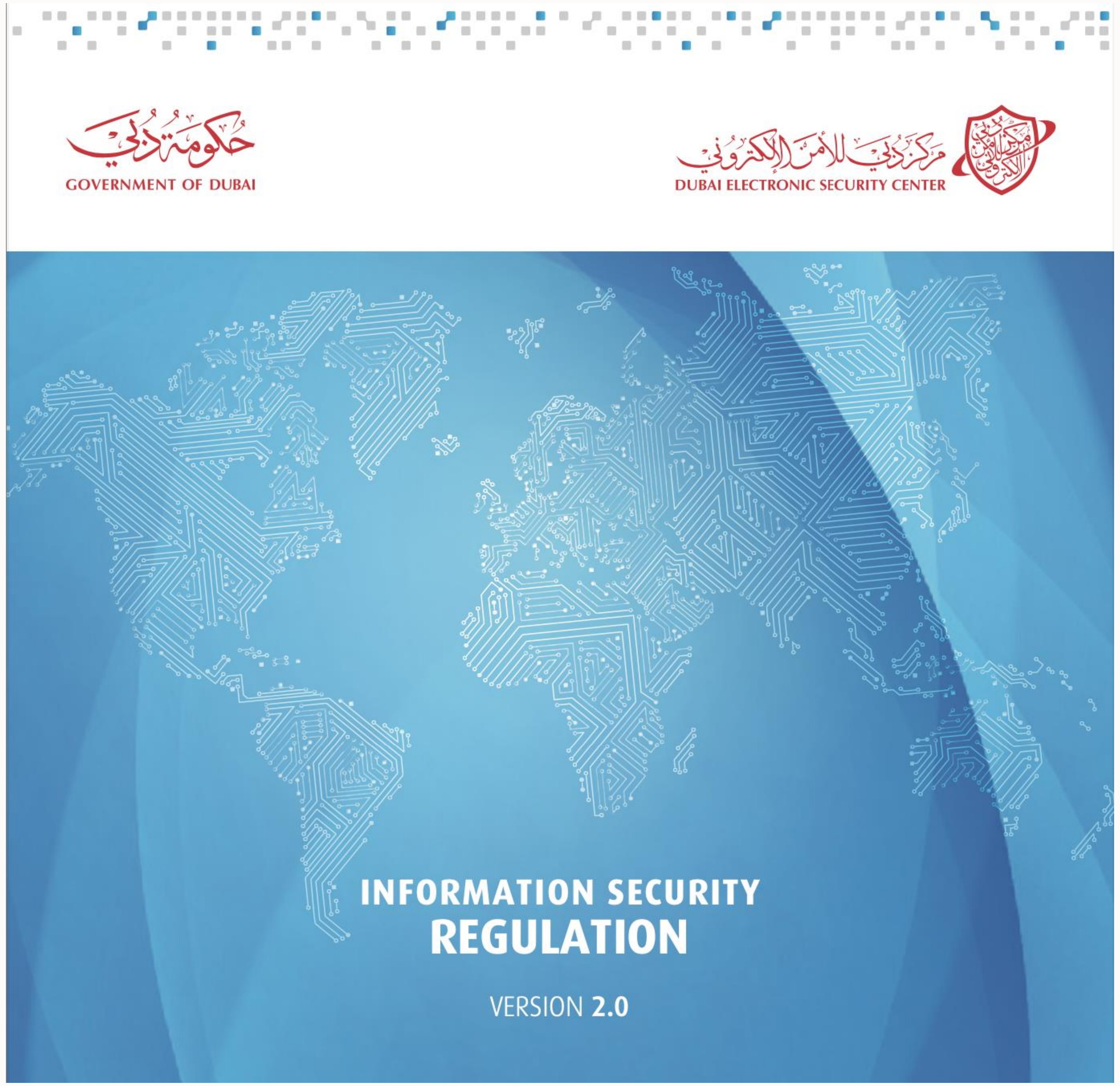
مـركز أبـوظبي للأنـظمة
الإلكترونية والمعلومات
ABU DHABI SYSTEMS &
INFORMATION CENTRE

- **Background:**
  - Oracle contracted with an independent certification assessor to assess the Oracle Cloud Infrastructure system and related practices against Abu Dhabi Information Security Standard (ADISS)
  - IT Consulting, LLC (Cyberstrat) assessed the compliance of Oracle's Information Security Management System (ISMS) with the United Arab Emirates (UAE) framework **Abu Dhabi Information Security Standards (ADISS) v2.0** issued by Abu Dhabi Systems & Information Center (**ADSIC**)
- **Scope:**
  - Scope is OCI (**42** services) and Oracle SaaS (**8** services) offering in the UAE East Region, including Dubai.
  - The compliance assessment included all of the ADISS v2.0 primary controls, main controls (99) and sub-controls (**1,274**)
- **Outcome:**
  - The applicability of the **1,274** sub-controls is as follows: **895** are Mandatory, **256** are Recommended (in scope), **121** are Suggested (in scope), and **2** are Not Applicable (out of scope) for they are Government specific. Overall compliance with all ADISS v2.0 is **100%.**

DUBAI ELECTRONIC SECURITY CENTER

# DESC - WiP

## Exemption Request -> ISR@desc.gov.ae

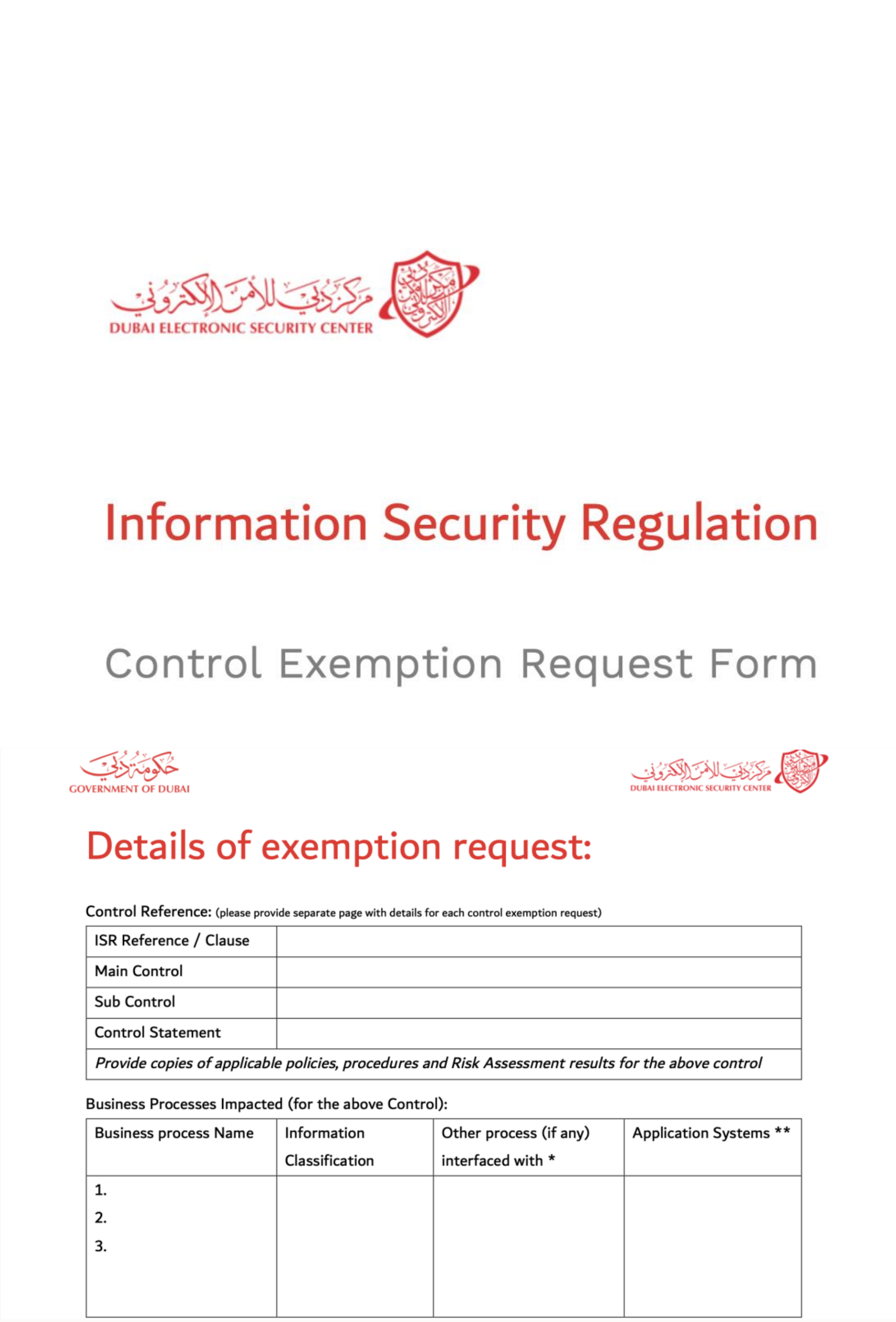


GOVERNMENT OF DUBAI

DUBAI ELECTRONIC SECURITY CENTER

INFORMATION SECURITY
REGULATION

VERSION 2.0



DUBAI ELECTRONIC SECURITY CENTER

Information Security Regulation

Control Exemption Request Form

GOVERNMENT OF DUBAI

DUBAI ELECTRONIC SECURITY CENTER

Details of exemption request:

Control Reference: (please provide separate page with details for each control exemption request)

| | |
|---|---|
| ISR Reference / Clause | |
| Main Control | |
| Sub Control | |
| Control Statement | |
| *Provide copies of applicable policies, procedures and Risk Assessment results for the above control* | |

Business Processes Impacted (for the above Control):

| Business process Name | Information Classification | Other process (if any) interfaced with * | Application Systems ** |
|---|---|---|---|
| 1.<br>2.<br>3. | | | |

ORACLE

# US Cloud ACT

# What is the CLOUD Act?

CLOUD is an acronym, and stands for **C**larifying **L**awful **O**verseas **U**se of **D**ata Act.

The summary purpose of the CLOUD Act is to enable **law enforcement agencies** to deter and **fight international criminal and terrorist activities**. It does not allow free reign of the US Law enforcement agencies free access to data stored in the cloud.

It is a clarification of existing practices of legal cooperation between countries in place since the 1980s.

# Common Questions Answered

1. Does the CLOUD Act **allow unfettered access** to data in Cloud Providers?
   A. No. It provides a **mechanism** whereby Law enforcement agencies can **request da**ta, in support of a well defined **legal pursuit**. (Rigourous requirements including the acquisition of a warrant from an independent Judge concluding reasonable grounds to request the information.

2. Does the CLOUD Act impact **only US companies**?
   A. No. It applies to **all organisations globally** whose services may be used by **US citizens**, whether operating within the US or not.

3. Is the CLOUD Act **limited** to Cloud Providers?
   A. No. The CLOUD Act applies to **any** organisation storing data on the internet, where US citizens are using that service. This includes, **Email**, **Telecom companies**, **Social Media** etc…

# Common Questions Answered

4. Does the CLOUD Act take **precedence** over **local** country law?
    A. No. The CLOUD Act specifically **makes provision for recognising** the right for service providers to **dispute a request** that **conflicts** with local law. The CLOUD Act simply applies clarity for US Law enforcement, concerning the mechanism by which information can be requested from organisations holding data beyond US borders.

5. Will the CLOUD Act compel Oracle to **de-crypt** customer data in response to a lawful request?
    A. No. Oracle offers encryption capabilities for customer data both at rest and in transit. Customers are able to utilise **FIPS 140-level 3 compliant HSMs** for Encryption Keys and store their keys offline in their premises or using Key Vault. Oracle holds no keys for these encryptions and therefore is not able to de-crypt customer data in response to such a request. Furthermore, Oracle uses security features of it's software to ensure the privacy of customer data, such as data vault, to ensure that even administrative staff within the customer organisation are not able to access customer data, without the proper privilege.

# Proven hard and soft cost savings in the UAE

### ACCELAERO ISA

- UAE Based travel system serving **26** airlines and **275 million** passengers
- Moved mission critical reservation app to OCI to **scale** on demand
- **12X** performance increase compared to **AWS Aurora** for 1ms response time
- **40%** performance improvement compared to **on-prem** and less costs

### LANDMARK GROUP

- It took under 12 months to move **80%** of business solutions to move to Oracle Cloud
- **20%** In Cost Reduction & Performance Improvements
- Improved Business Processes & Omni-channel experience.

### desert adventures

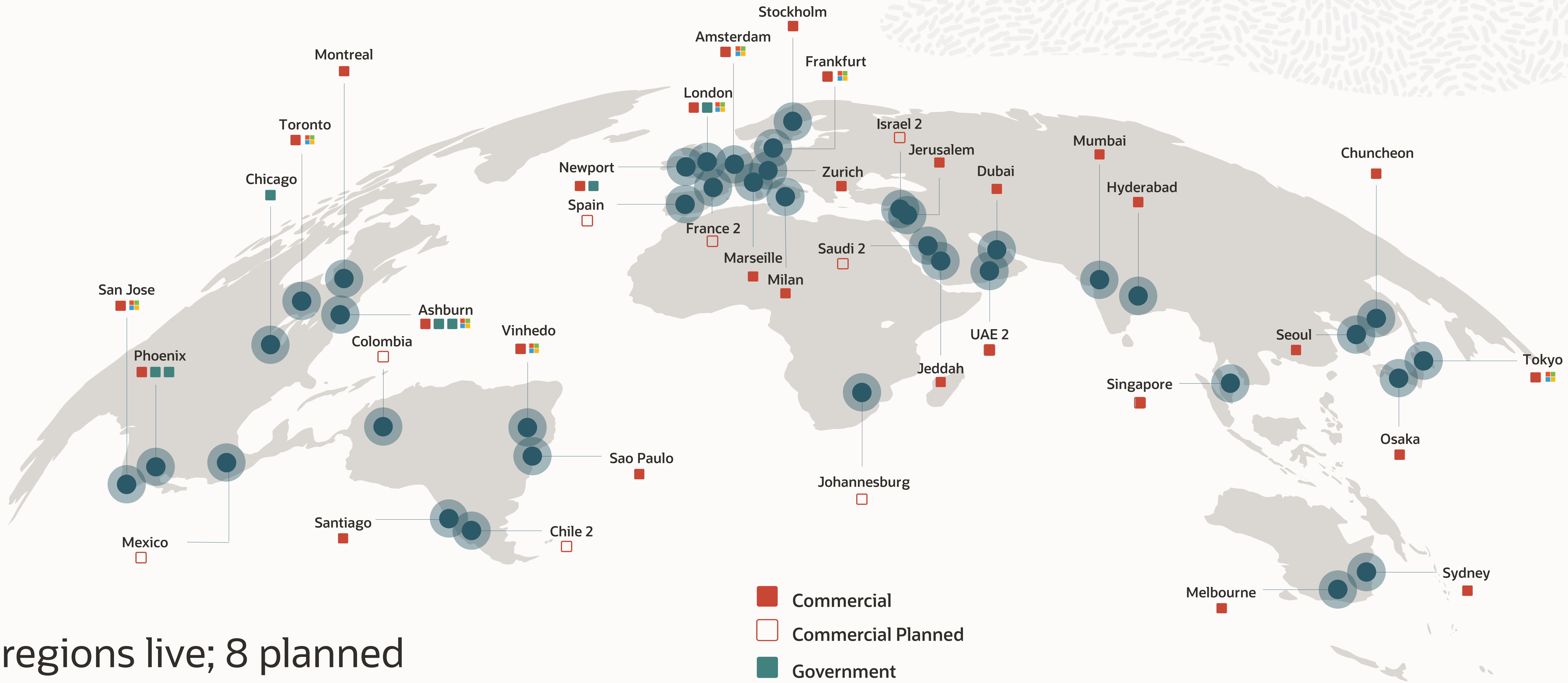
- **30%** Cost savings compared to previous On-Prem Deployment
- **20%** to **30%** Cost savings compared to AWS
- Scalability, Reliability, better security Posture and compliance with GDPR
- Migration to OCI is projected to yield a **$1M** benefit over the next 2 years

### JOPACC

WE INNOVATE & CONNECT DIGITAL PAYMENTS

- Migrated mission critical **24X7** payment systems and digital wallet on OCI leveraging fast connect and DB systems
- **First Fast Connect** Customer in Jordan
- **Stronger security** Posture
- Better **Performance**
- Better **Business Continuity** Plan

# OCI offers cloud regions and multicloud around the world



🟥 Commercial

□ Commercial Planned

🟩 Government

⊞ Oracle Cloud and Microsoft Azure Interconnect

**36** regions live; 8 planned

**8** Azure Interconnect Regions

# Thank you