ORACLE

DB Cloud Spotlight Series:
Zero Trust and Oracle Database Cloud Services

Alexandre Fagundes

Cloud Architect, Oracle Latin America

Top Government Security Concerns

- Ransomware
- Security Complexity
- Human Error
- Supply Chain Vulnerabilities
- Cybersecurity Talent Shortage
- Hybrid Work Environment
- Geopolitical Risks
- Fraud
- Dispersed SaaS Services
- Compliance Requirements

What is “Zero Trust”?

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following zero trust and ZTA operative definition:

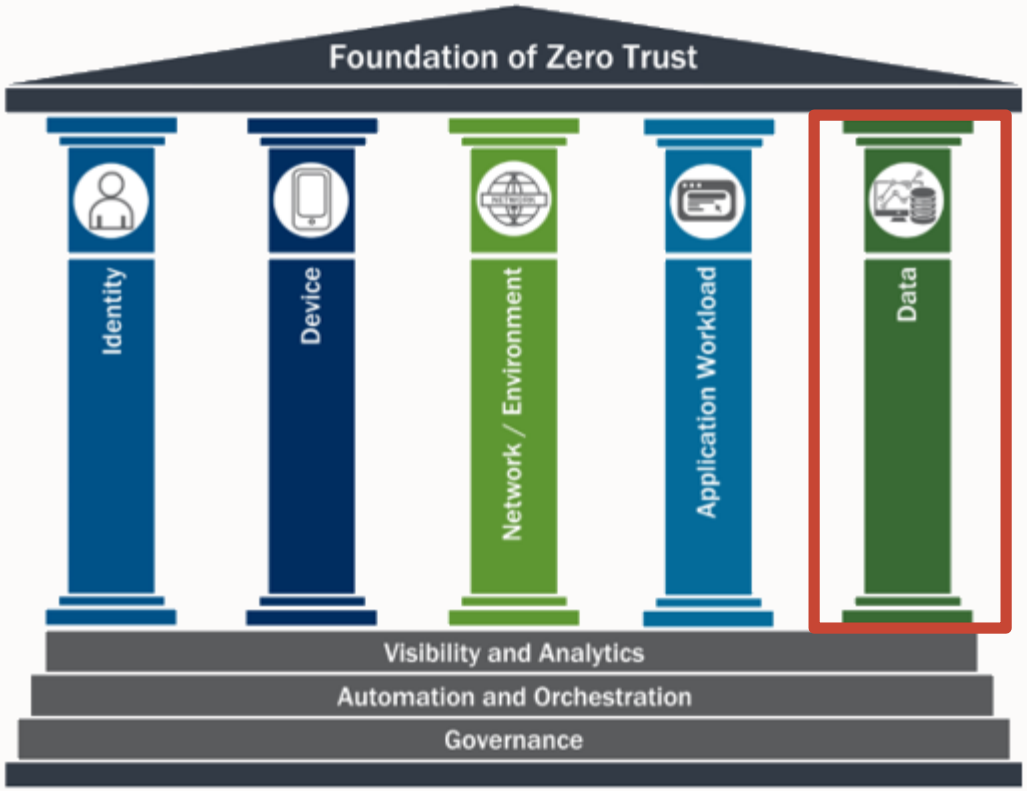
> ***Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. ZTA is an enterprise’s cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.****

SP 800-207 emphasizes that the goal of ZT is to **“prevent unauthorized access to *data* and *services* coupled with making the access control enforcement as granular as possible.”** Similarly, the National Security Telecommunications Advisory Committee (NSTAC) describes Zero Trust as **“a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified**.”

* NIST SP 800-207: Zero Trust Architecture. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

What is the “Zero Trust Maturity Model”?

Foundation of Zero Trust



Source: CISA Zero Trust Maturity Model (June 2021)

There are five zero trust technology pillars

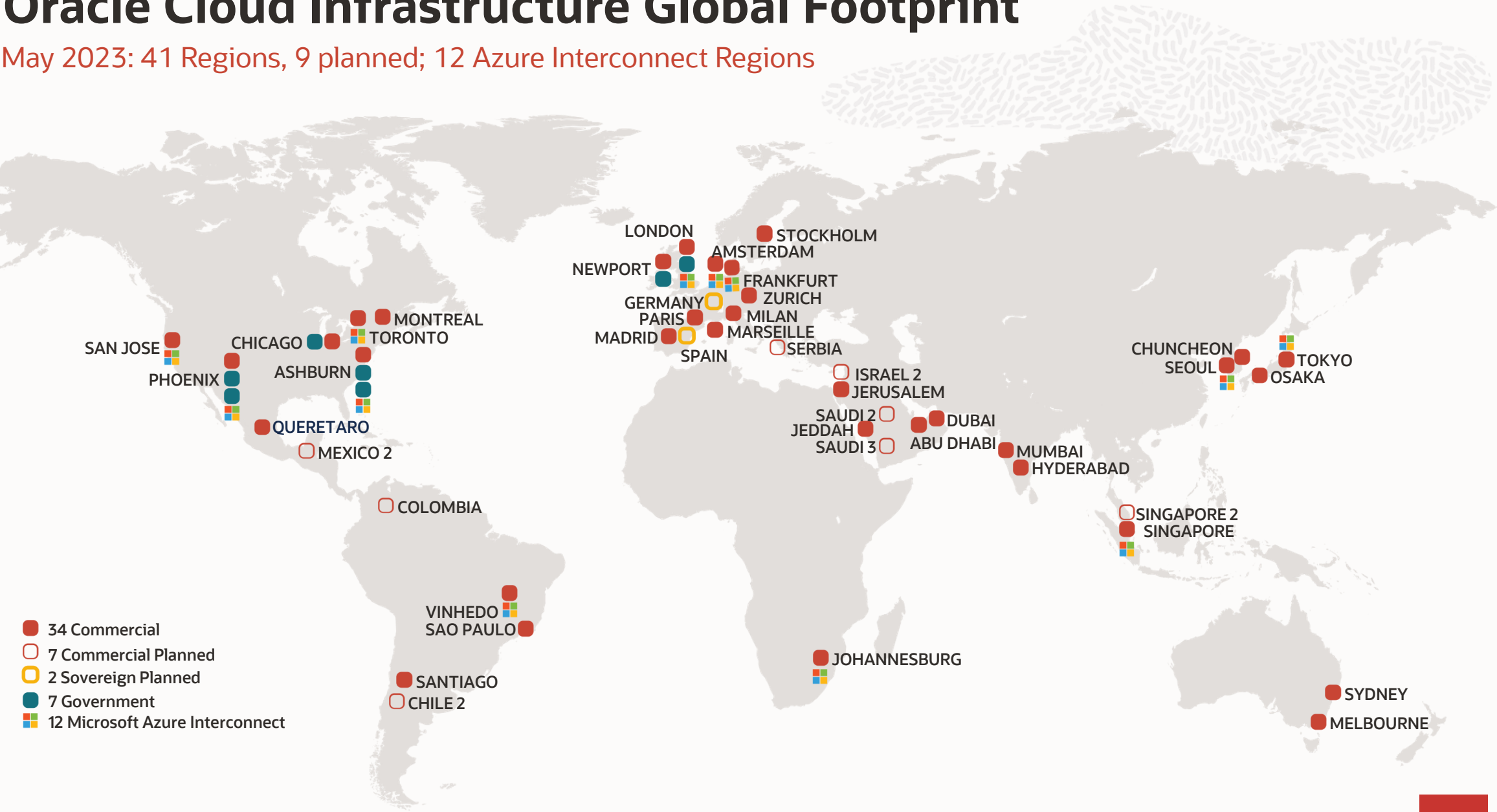
1. **Identity**
2. **Device**
3. **Network/Environment**
4. **Application Workload**
5. ***Data***

Each pillar is supported by:

- **Visibility and analytics**
- **Automation and Orchestration**
- **Governance**

Oracle Cloud Infrastructure Global Footprint

May 2023: 41 Regions, 9 planned; 12 Azure Interconnect Regions



100% renewable energy by 2025

Oracle Cloud Infrastructure Security

Build Confidence with Simple, Prescriptive, and Integrated Security

Easy to Use, Deploy, and Operate Cloud Security

Increase the confidence in your ability to detect and respond to emerging risks from possible security errors with simple, built-in security that is turned on by default.

- Isolated Network Virtualization
- Least privilege access
- Oracle Threat Intelligence
- OCI Network Firewall
- OCI WAF for Fusion Applications

Breadth of Security Integrated for a Zero Trust Architecture

Security services are integrated across the cloud infrastructure and applications to avoid misconfigurations and streamline security.

- OCI Bastion
- Oracle Cloud Guard Fusion Applications Detector
- OCI Identity and Access Management
- OCI Vault
- OCI WAF

Prescriptive Guidance Which Requires Less Expertise

Adopt guardrails to help consistently apply Oracle security best practices with reduced dependency on costly security experts.

- Oracle Security Zones
- Oracle Cloud Guard
- Oracle Cloud Guard Threat Detector
- OCI Vulnerability Scanning Service

Oracle Database Security

Reduce the risk of a data breach and simplify compliance

Identify Security Posture

Discover sensitive and personal data, assess how securely database is configured, and get recommendations on improving security posture

- Oracle Data Safe
- Oracle Database Security Assessment Tool (DBSAT)

Prevent Unauthorized Access to Data

Enforce least privilege and mitigate exposure to stolen credentials and compromised accounts with solutions that offer separation of duties and multifactor authentication

- Oracle Data Safe
- Oracle Database Vault
- Oracle Label Security

Secure Private Information

Meet global compliance requirements, data governance, regulatory mandates, and industry requirements while addressing local needs for data sovereignty, privacy, and transparency

- Oracle Advanced Security
- Oracle Data Masking and Subsetting
- Oracle Data Safe
- Oracle Key Vault

Monitor for Threats

Identify risky user behavior, detect and block threats, and simplify and accelerate compliance reporting

- Oracle Audit Vault & Database Firewall
- Oracle Data Safe

“the Zero Trust model enforces that only the right people or resources have the right access to the right data and services, from the right device, under the right circumstances.”

Bill Harrod
Chief Technology Officer, MobileIron

Threats addressed by a Zero Trust Architecture

1. Denial of service or workload disruption
2. Workload corruption
3. Stolen credentials
4. Insider threat

What should you expect?

Increased emphasis on fundamental security practices

Stronger network segmentation enforced by newer (more powerful) firewalls

Bastion hosts/jump servers

Use of privilege account managers and other identity management technologies

Device management

Encryption

Increased emphasis on data catalogs, sensitive data inventory

To know what to protect, you need to know:

- What types of data you have
- How much data you have
- Where that data is located

Data minimization efforts typically follow data inventory

- Reduce your risk by reducing the number of repositories, amount of sensitive data

Expect a special focus on test and development environments

Increased emphasis on access controls, least privilege

A basic tenet of Zero Trust is that an organization protects resources by limiting access to only what is needed

Access should be periodically reviewed

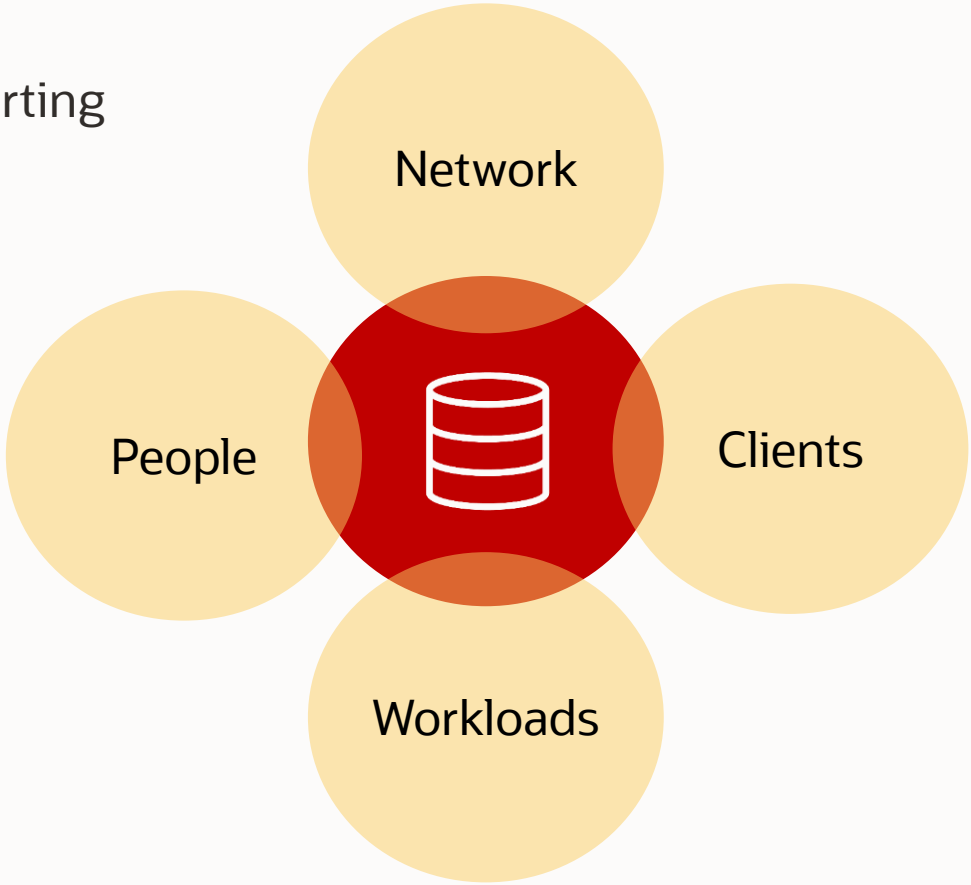
Access to data should be dynamically determined by evaluating the observable state of the client identity

- How was the client authenticated
- What application or program is accessing data
- Network location making the request
- Time/date of request
- Other behavioral and environmental attributes

Stronger focus on monitoring activity

Understanding data usage flows and patterns are key components of Zero Trust.

Expect more focus on audit policies, audit data analysis and reporting



“It’s a Marathon, Not a Sprint”

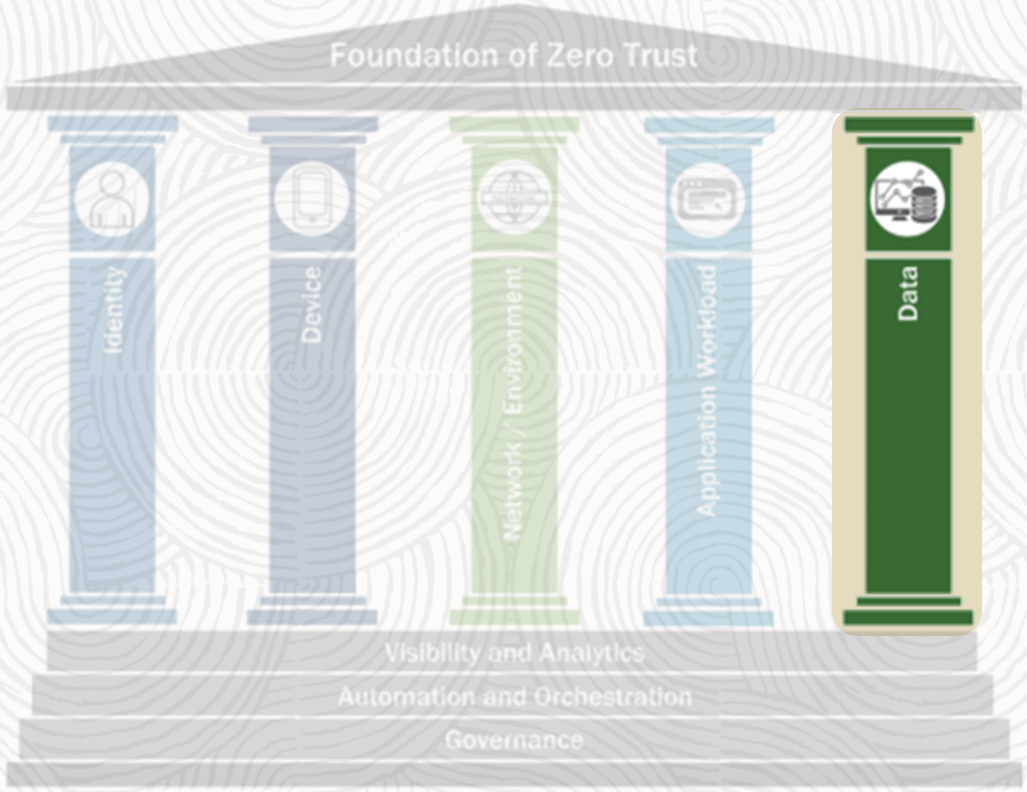
A Practical Guide to a Zero Trust Implementation

Steve Turner David Holmes, Chase Cunningham, Jinan Budge, Paul McKay, Andras Cser, Heidi Shey, and Merrit Maxim

Forrester

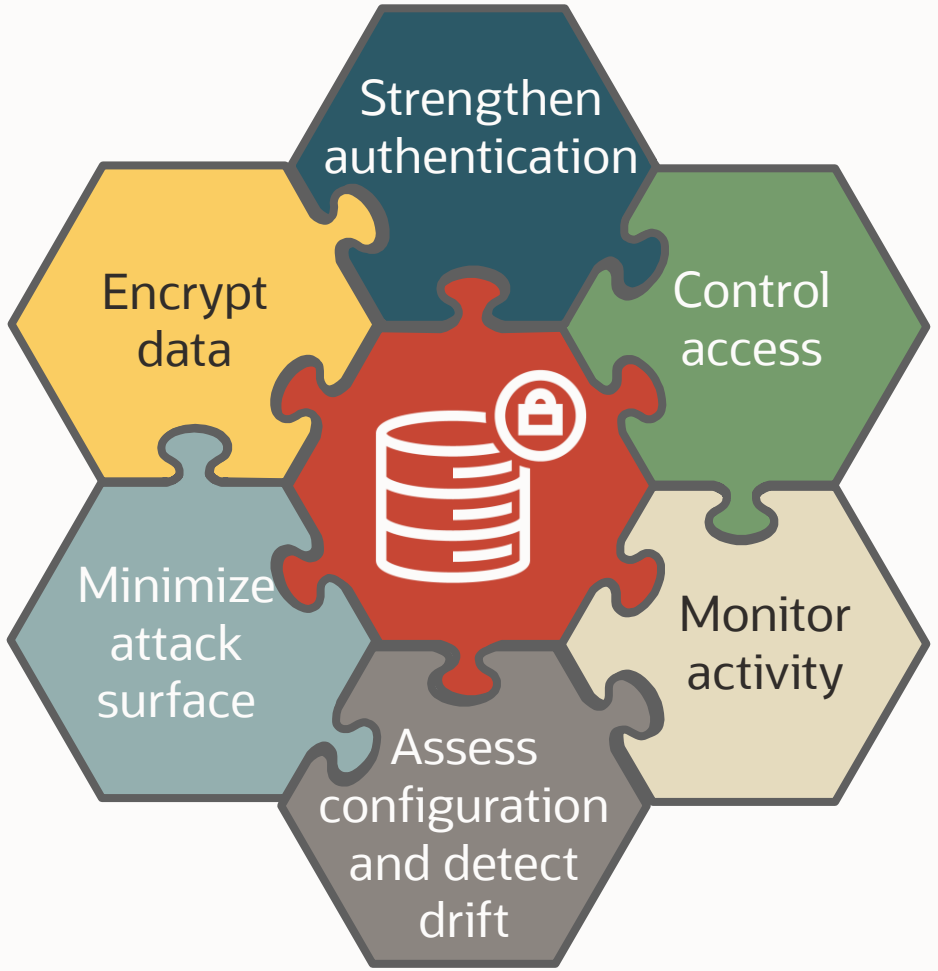
March 3, 2021

What should you do?

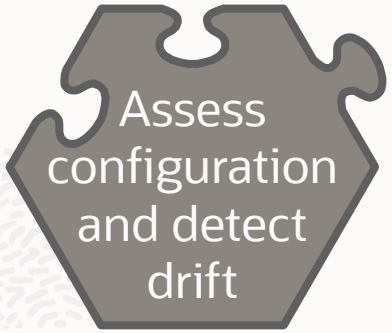


Driving out trust

Leave no gaps



Do not trust a system to remain properly configured



Standardization is crucial to sustainability and success at scale

- A few (usually two or three) different configurations based on risk
- Start with a well-known standard (eg: CIS Benchmark, DISA STIG)

Assess periodically to detect configuration drift – automation is key to success in this area

Relevant Oracle utilities, features, services, products:

- Database Security Assessment Tool
- Data Safe *Security Assessment*
- Audit Vault and Database Firewall *Security Assessment*
- Enterprise Manager Database Lifecycle Management pack

Do not trust the network to keep your database secure

Assume the attackers will bypass other controls to directly attack the database
Reduce user entitlements to minimum necessary for job function
Remove sensitive data from environments that do not need it

Relevant Oracle utilities, features, services, products:

Test Environments:

- Enterprise Manager Data Masking and Subsetting Pack
- Data Safe *Masking*

User entitlements:

- Database Security Assessment Tool
- Data Safe *User Assessment*
- Audit Vault and Database Firewall *entitlement monitoring/reporting*
- Database *Privilege Analysis*

Do not trust that storage, backups, and exports are protected

In-motion

- Be aware of throughput restrictions - protect at the lowest practical level of the network stack
- Understand the difference between native network encryption and TLS – including operational considerations!

At-rest

- Don’t forget to encrypt database exports – this is often your highest area of vulnerability
- Consider the impact of encryption on database backups

Relevant Oracle utilities, features, services, products:

- Database *Native Network Encryption*
- Database *TLS Network Encryption*
- Advanced Security *Transparent Data Encryption*
- Key Vault

Do not trust passwords

Separate database accounts into categories

- Superuser accounts (eg: SYSDBA, SYSKM)- Secure with Privileged Account Manager (PAM) and use infrequently
- Administration/DBA accounts - Multi-factor authentication if possible. May want to manage centrally (eg: Active Directory). May want to secure with PAM
- End users – Strong authentication (Kerberos, certificate, MFA)
- Application service accounts – frequently limited by application design. Consider using multi-factor authorization to mitigate risk of compromised accounts. Monitor logins for unusual patterns

Relevant Oracle utilities, features, services, products:

- Database *Password Profiles*
- Database *Gradual Database Password Rollover*
- Database *Centrally Managed Users*
- Database *Strong Authentication*
- Unified Audit
- Oracle Radius Adapter

Do not trust users to act in good faith

Favor technical, preventive controls over process/policy controls wherever practical

Lock down sensitive data so that access is minimized

Relevant Oracle utilities, features, services, products:

- Database *Privilege and role grants, including secure application roles*
- Database Vault *Privileged User Controls*, *Trusted Path Enforcement*
- Database *Blockchain and immutable tables*
- Database *Virtual Private Database, Real Application Security*
- Label Security
- Advanced Security *Data Redaction*

Do not trust your preventive controls to be 100% effective

Use a combination of auditing and network-based monitoring to:

- Identify anomalies that may indicate malicious/unauthorized activity
- Support investigations and compliance activities

Audit:

- Data Definition and Data Control Language (DDL, DCL)
- Privileged user activity
- Access to sensitive data from outside of applications

Relevant Oracle utilities, features, services, products:

- Database *Unified Auditing*
- Audit Vault and Database Firewall
- Data Safe *Auditing*
- SQL Firewall *new in Database 23c*

What next?

Recommended reading on Zero Trust

Read NIST SP 800-207 (*Zero Trust Architecture*) – https://crsc.nist.gov

National Cybersecurity Center of Excellence *Implementing a Zero Trust Architecture (draft/legacy)* – https://nccoe.nist.gov

Forrester *Zero-Trust Playbook*

Forrester *Practical Guide to a Zero Trust Implementation*

Secure Architecture

CIS Landing Zones

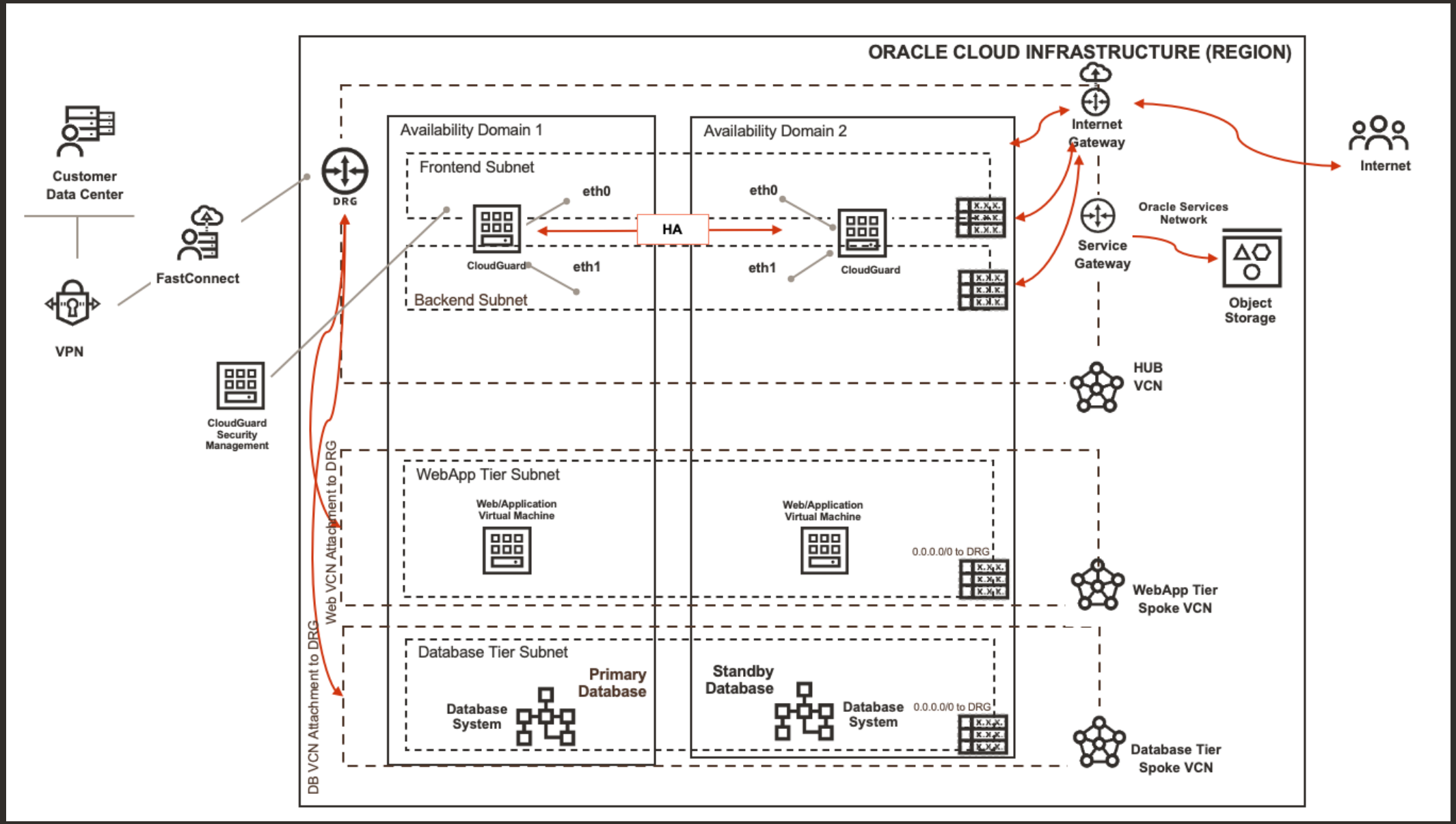
Terraform configuration for tenancy creation → CIS Benchmark for OCI +Architecture Best Practices

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



Want to learn more about database security?

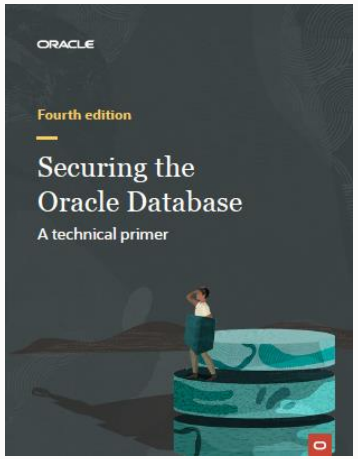
Free hands-on labs that help you learn how to use the different security features and options

bit.ly/golivelabsdbsec

Database Security office hours – second Wednesday of each month

bit.ly/asktomdbsec

Securing the Oracle Database – a technical primer (fourth edition)



oracle.com/securingthedatabase

Summary

1. Oracle gives you the flexibility to reduce risk (and trust) to a level you are comfortable with

2. Almost any control objective should be achievable within your Oracle technology stack

3. The threat is real – start addressing it by assessing your current database security state

Our mission is to help people see data in new ways, discover insights, unlock endless possibilities.