Mitől biztonságos az Oracle felhő, a Cloud at Customer és az Autonomous Database?

Sárecz Lajos
Business Development Manager
EMEA
2022 május 17.

Agenda

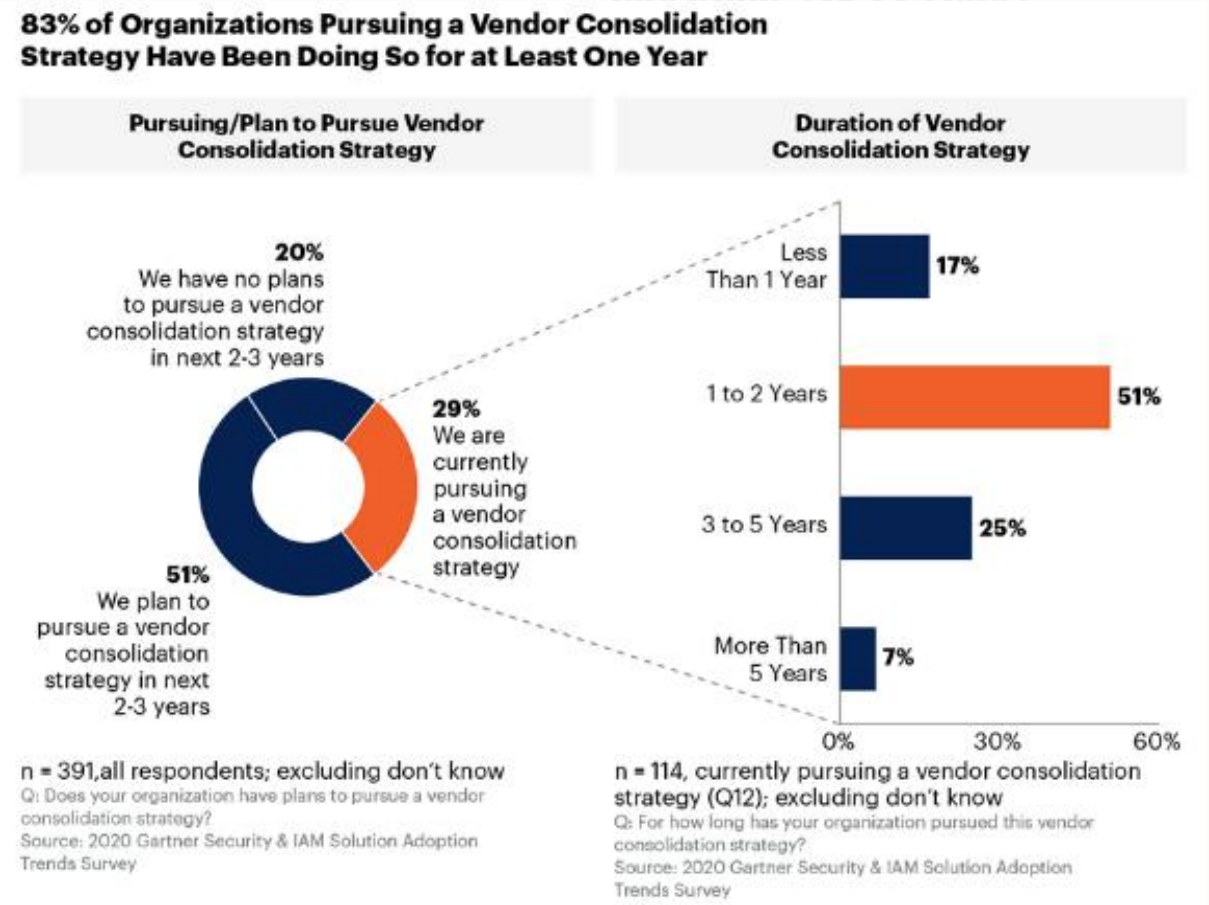
1. Security of the cloud
2. Exadata Cloud at Customer Security
3. Self Securing Autonomous Database

What Does it take to Secure your Infrastructure Today?

78 percent of organizations use more than 50 discrete cybersecurity products to address security issues

37 percent use more than 100 cybersecurity products.

- The large number of security products used by organizations drives up complexity and integration costs.
- Organizations want vendor consolidation to simplify operations and reduce overall costs.



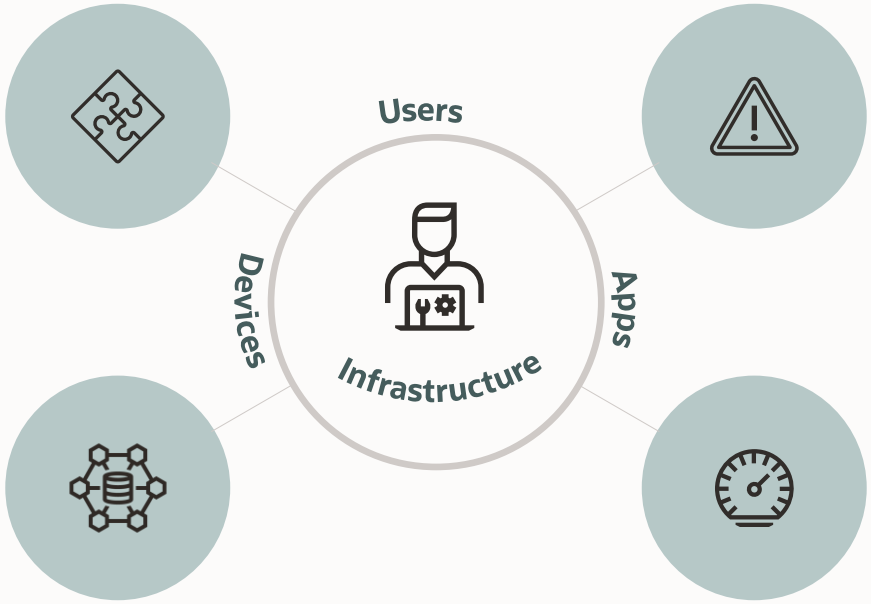
Sources:
Oracle and KPMG Cloud Threat Report 2020
Gartner: Top Security and Risk Management Trends 2021

Will More Tools Result in Better Security?

Customers don't get breached because they don't have the tools. They get breached because the tools are too complex

Integration
A lot of security tools!
Many different APIs

Interoperability
Customers have to put tools together themselves



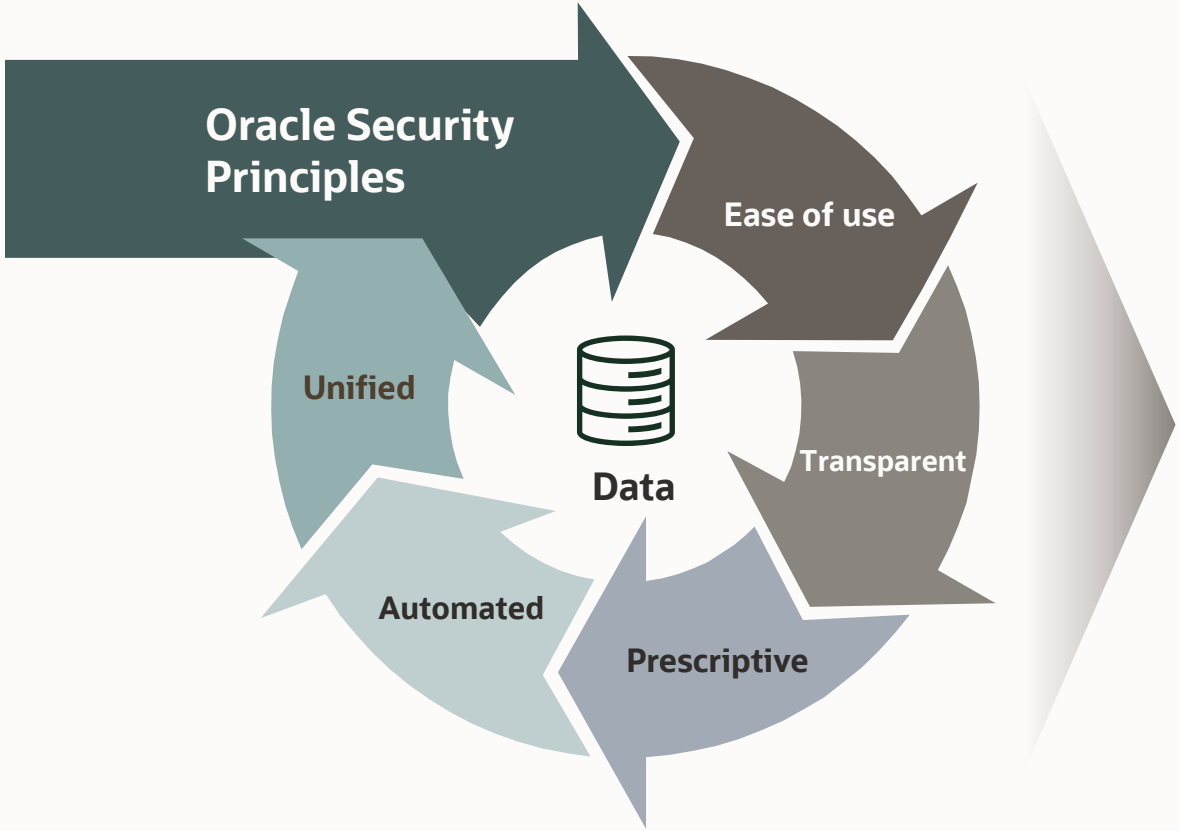
Ease-of-Use
No real instructions
Experts required

Monitoring
Multiple dashboards & workflows
Many vendors

What if there is a better way?

Oracle's Security Principles

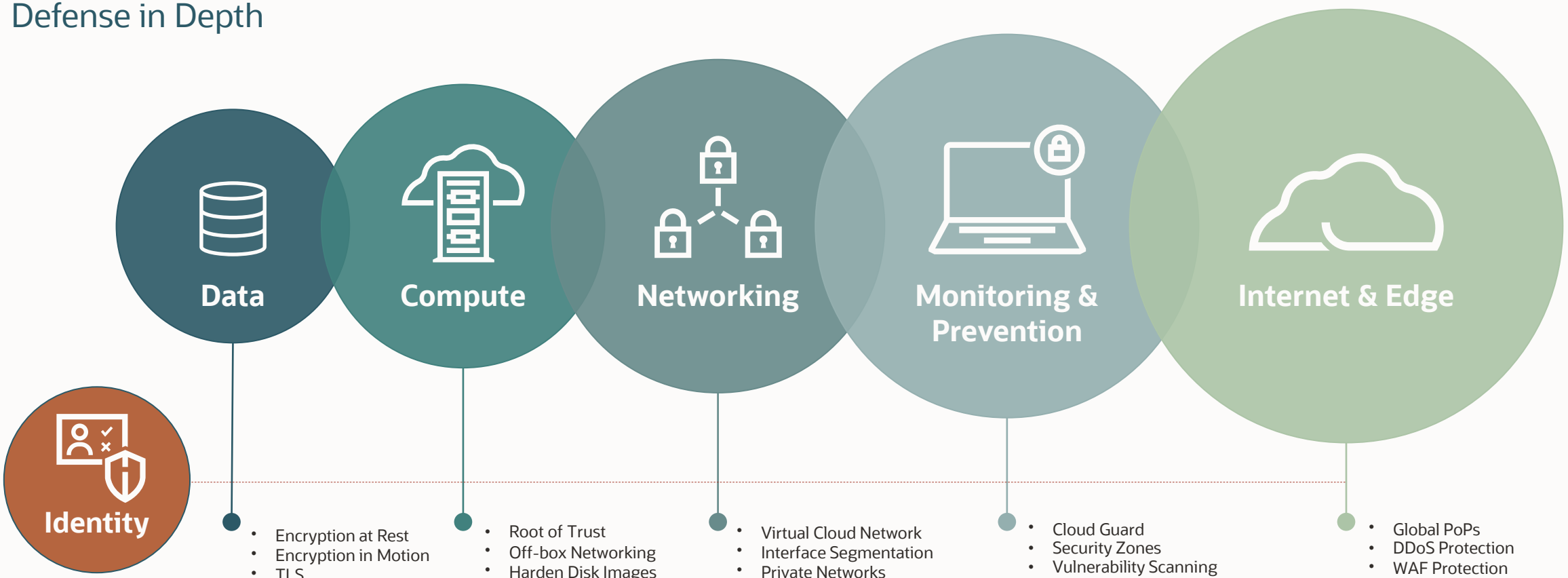
Making security Simple, Prescriptive and Integrated



- **Simple**: 'Always on' security posture. Easy defaults for developing and running apps
- **Prescriptive**: Recipes to enforce security posture, automated baseline management
- **Integrated**: Unified Security and Identity across IaaS, PaaS and SaaS
- Offer "at cost" to eliminate the cost/security tradeoff

Integrated and Automated Security from Data to Identity

Defense in Depth



Identity

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

Data

- Encryption at Rest
- Encryption in Motion
- TLS
- DataSafe
- Managed Keys
- Custom Keys
- Managed Vault
- Oracle Vault Cross Regional Replication and Asymmetric Keys

Compute

- Root of Trust
- Off-box Networking
- Harden Disk Images
- Autonomous Linux
- Certificates
- Hardware Security Modules

Networking

- Virtual Cloud Network
- Interface Segmentation
- Private Networks
- FastConnect
- Secure VPN
- Bastion
- P2P, NAT, DRG Gateways

Monitoring & Prevention

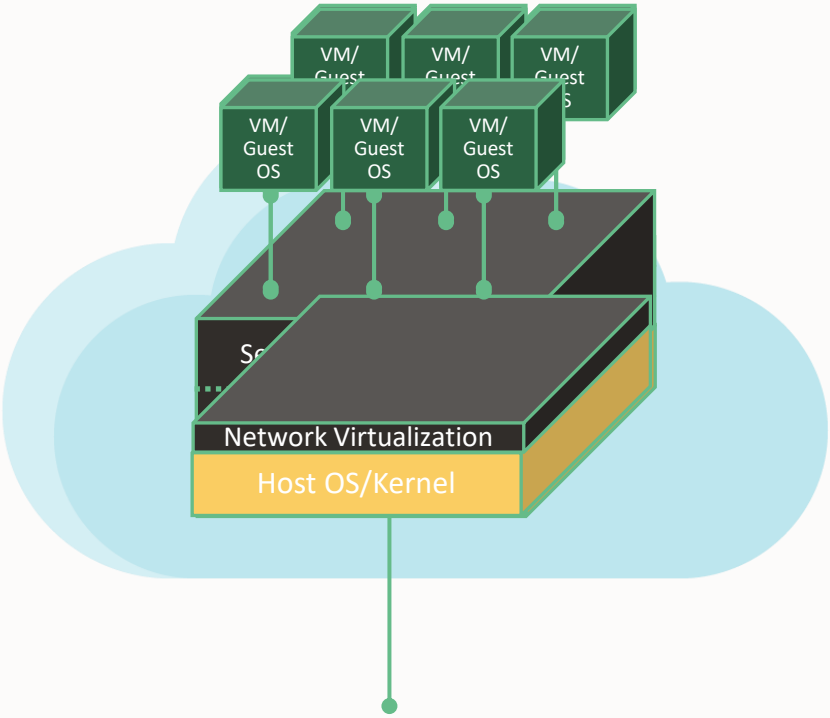
- Cloud Guard
- Security Zones
- Vulnerability Scanning
- Threat Detection
- Logging/Flows
- Governance
- Compliance

Internet & Edge

- Global PoPs
- DDoS Protection
- WAF Protection
- SD-WAN

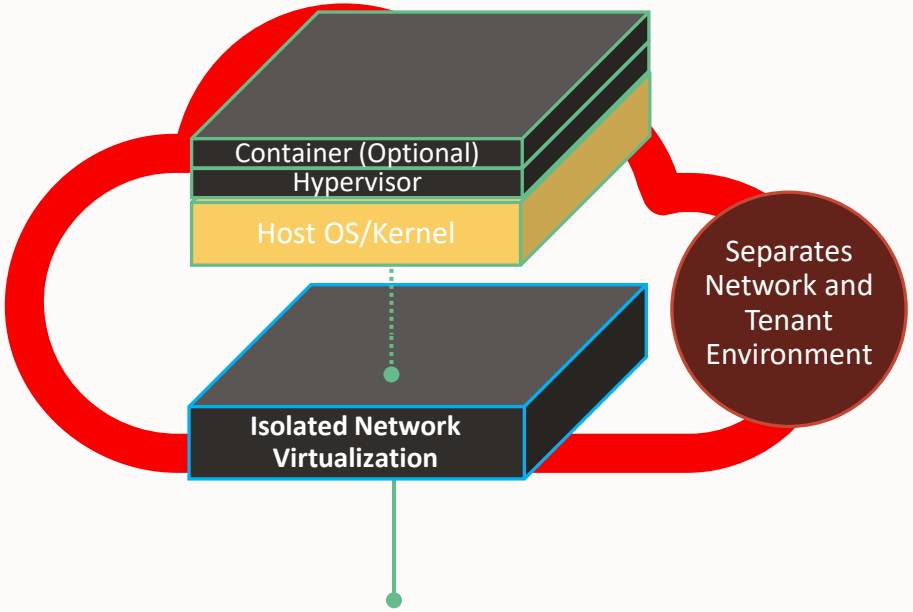
A Tale of Two Clouds:
Better Protection Through Built-In Isolated Network Virtualization

1st Generation Clouds:
Most Prevalent Today



To / From Other Tenants

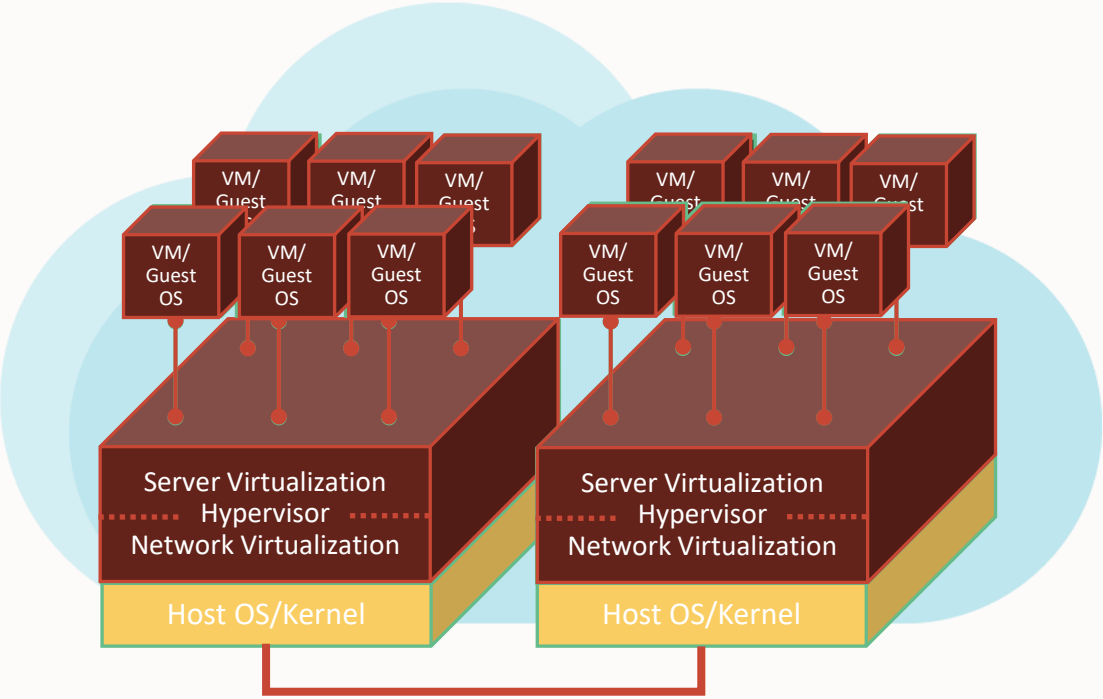
2nd Generation Cloud:
Oracle Cloud Infrastructure Wide



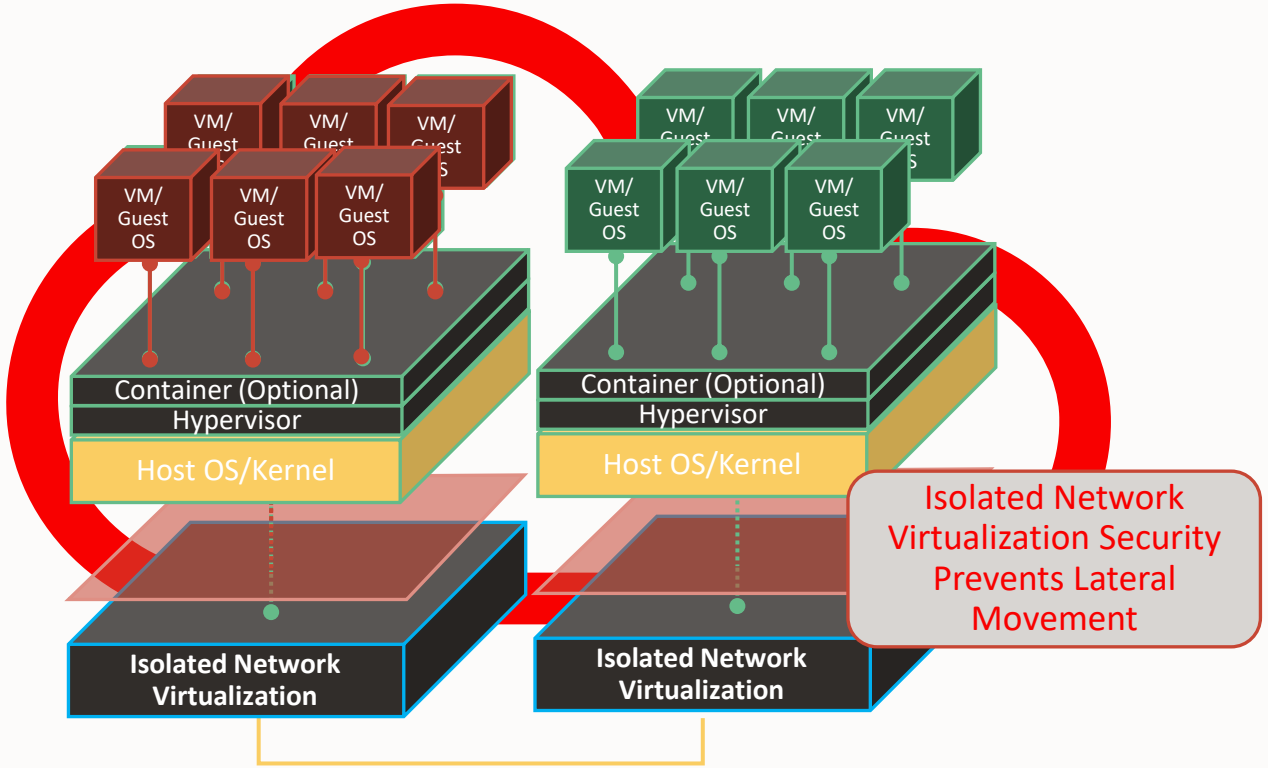
To / From Other Tenants

Isolation: Threat Containment & Reduced Risk Built Into the Architecture

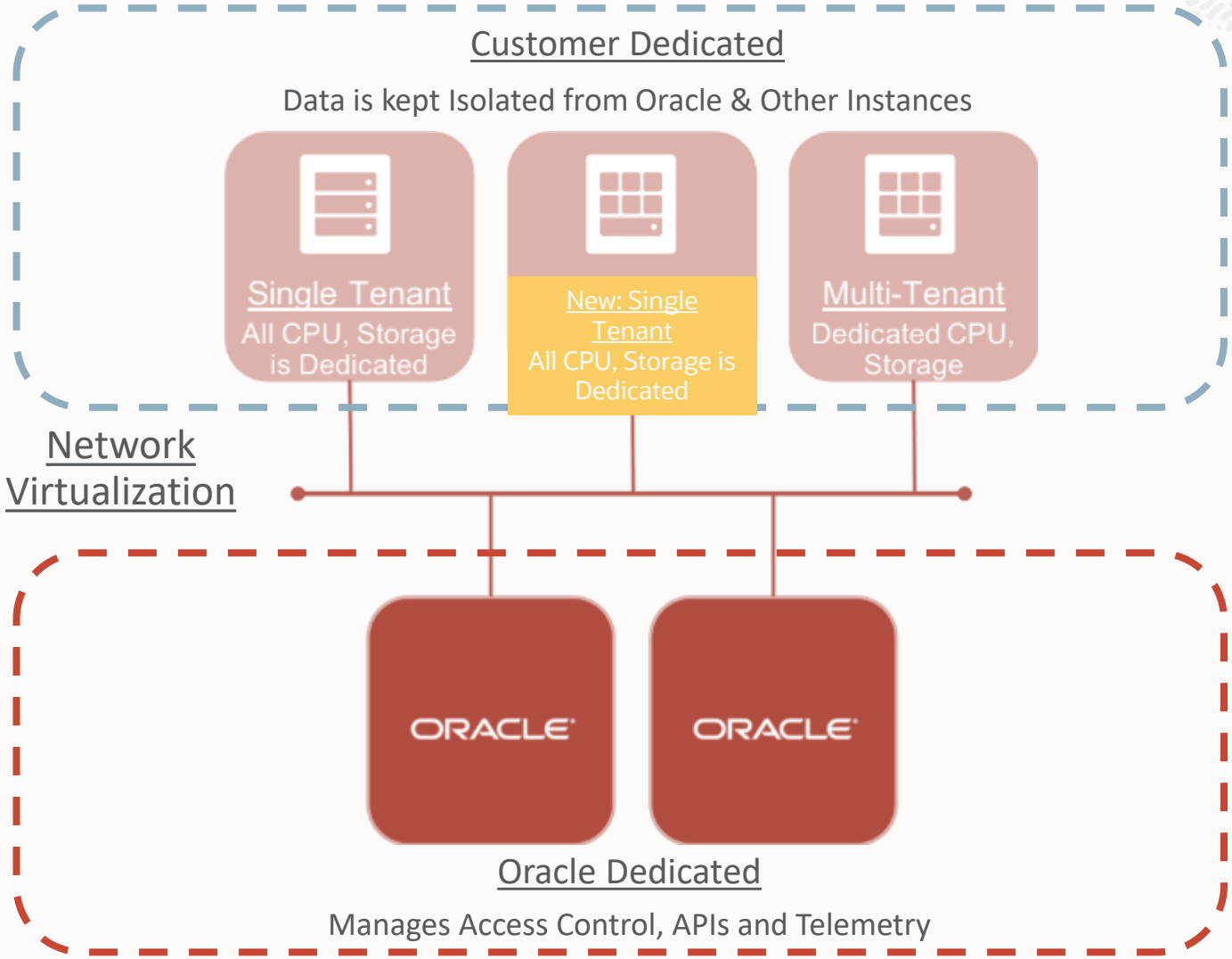
1st Generation Cloud



Oracle 2nd Generation Cloud



Advanced Control: Bare Metal & Dedicated VM Options



- Choice of Bare Metal or VM
- No Oracle code on BM
- Customer controls host entirely
- Oracle personnel have no access to Host
- Provides utmost data privacy

But not every organization or workload can easily use the public cloud

Data Residency and Security

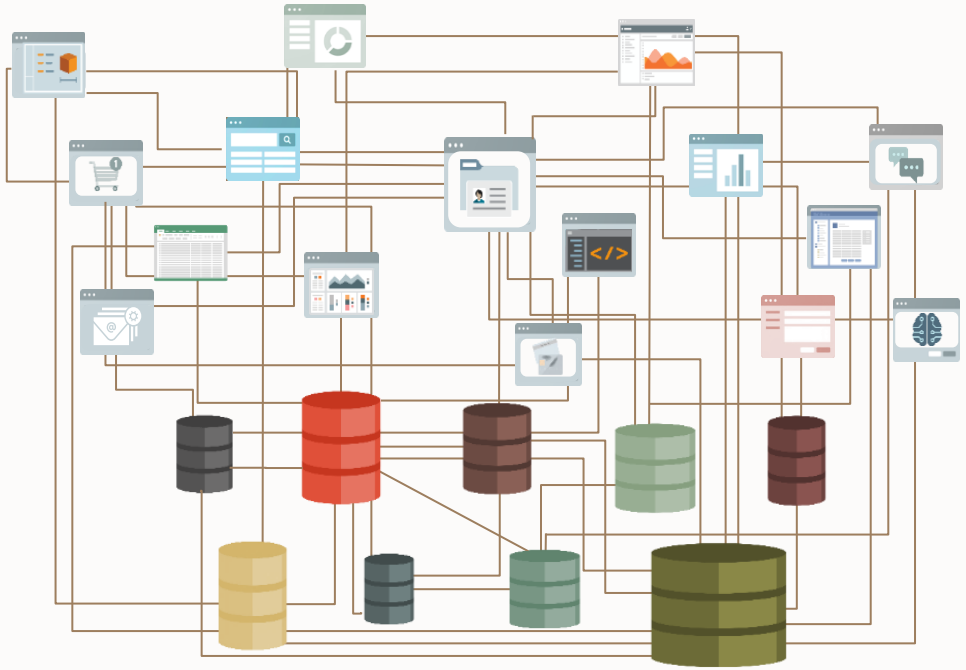
- Regulations or policies require data to be local
- Requirements to protect data in specific ways

Response Time

- Real-world systems require low latency
- Hard to disentangle one system from others

Perceived Risk

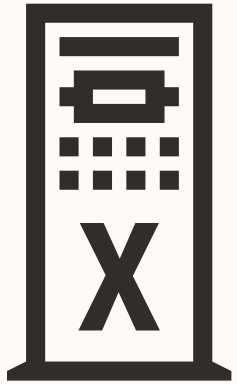
- Concerns about multi-tenant cloud
- Concerns about cloud provider access to data



Simplest for Deploying Mission-Critical Databases Where You Need Them

Traditional On-Premises

Exadata Database Machine



Customer Data Center
Purchased
Customer Managed

Public Cloud or Dedicated Region

Exadata Cloud Infrastructure

Oracle Cloud
Subscription
Oracle Managed

Cloud@Customer

Exadata Cloud@Customer

Customer Data Center
Subscription
Oracle Managed

Operator Access Control (OpCtl)

Enhanced security for regulated industries

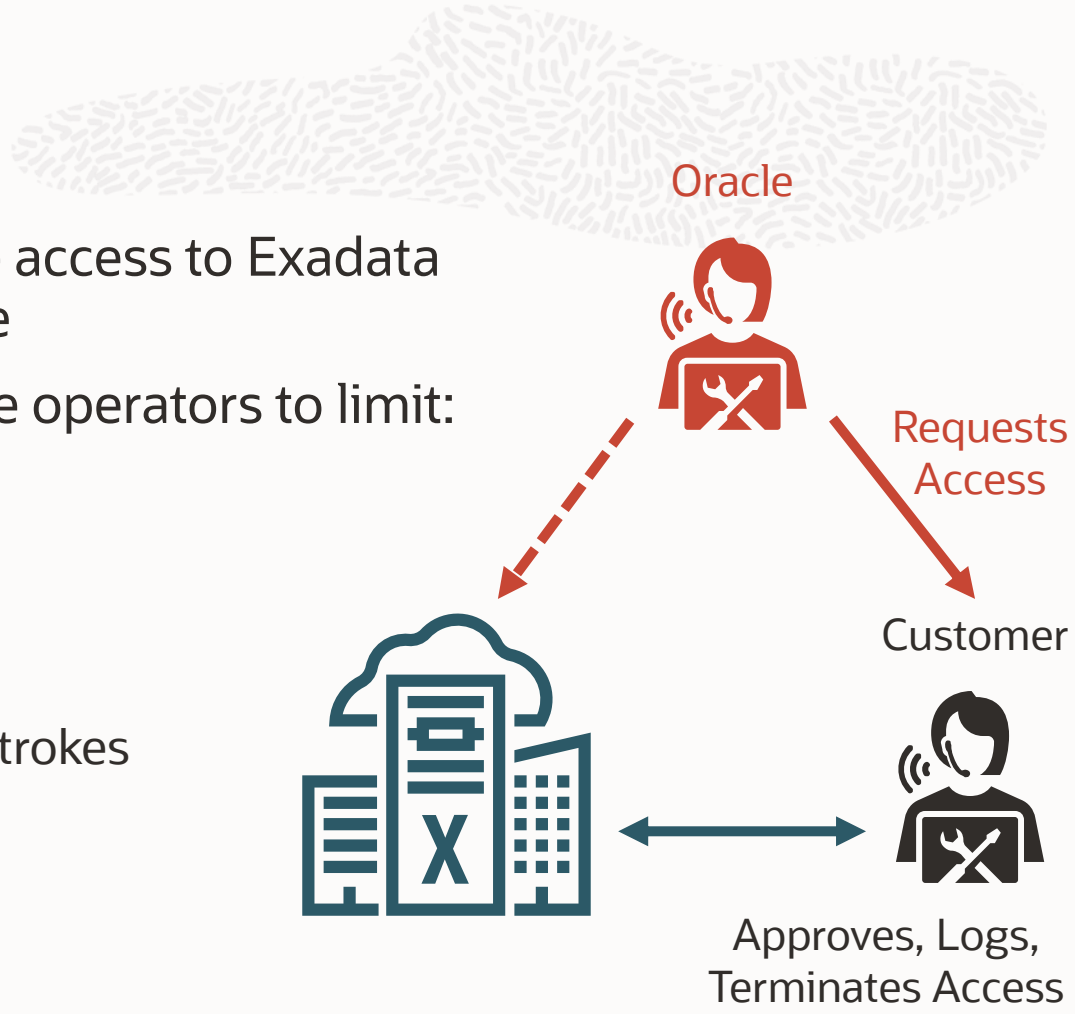
OpCtl enables customers to grant, audit, and revoke access to Exadata Cloud@Customer infrastructure managed by Oracle

Customers control access to infrastructure by Oracle operators to limit:

- when they have access
- components they can access
- commands they can execute

Observe and record Oracle operator commands and keystrokes that Oracle staff execute

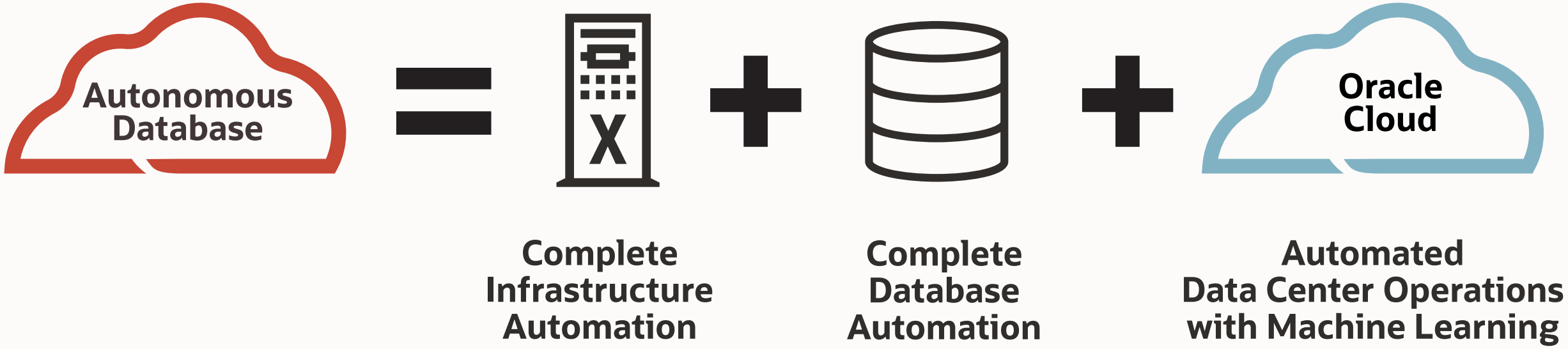
Terminate Oracle operator connections at discretion



Significantly more control than other cloud vendors

Oracle Autonomous Database on Exadata Cloud@Customer

Automates the entire database stack



Autonomous Database on Exadata Cloud@Customer

Multi-VM autonomous clusters Improve database consolidation efficiency and cloud economics

Autonomous Database Service

and

Exadata Database Service

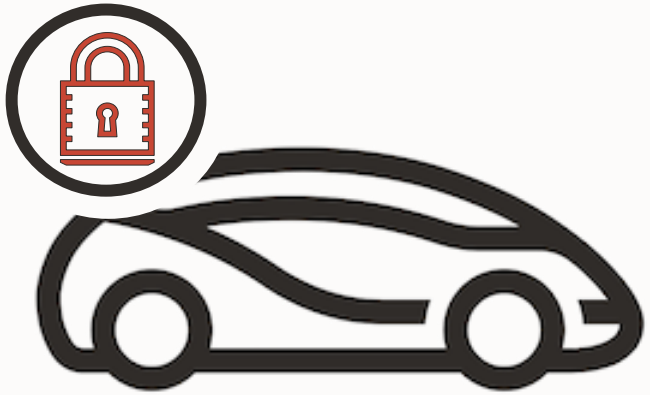
run concurrently

on the same infrastructure

Autonomous Database is Self-Securing

Only Databases are exposed to users – SQL access only

- No highly privileged access – no SYSDBA access
- No login allowed to CDB - only login to PDB
- No callouts to OS allowed



Database Vault's Automatic protects customer data from Oracle operations staff

Oracle automatically applies security updates for the entire stack

Self-Securing | Encryption by Default

Secure by default

Encryption for Data at Rest

- Automatically configured
- All application data is encrypted within the database at the tablespace level
- Database Backups are also encrypted

Self-Securing | Encryption by Default

Secure by default

Encryption for Data at Rest

- Automatically configured
- All application data is encrypted within the database at the tablespace level
- Database Backups are also encrypted

Encryption for Data in Motion

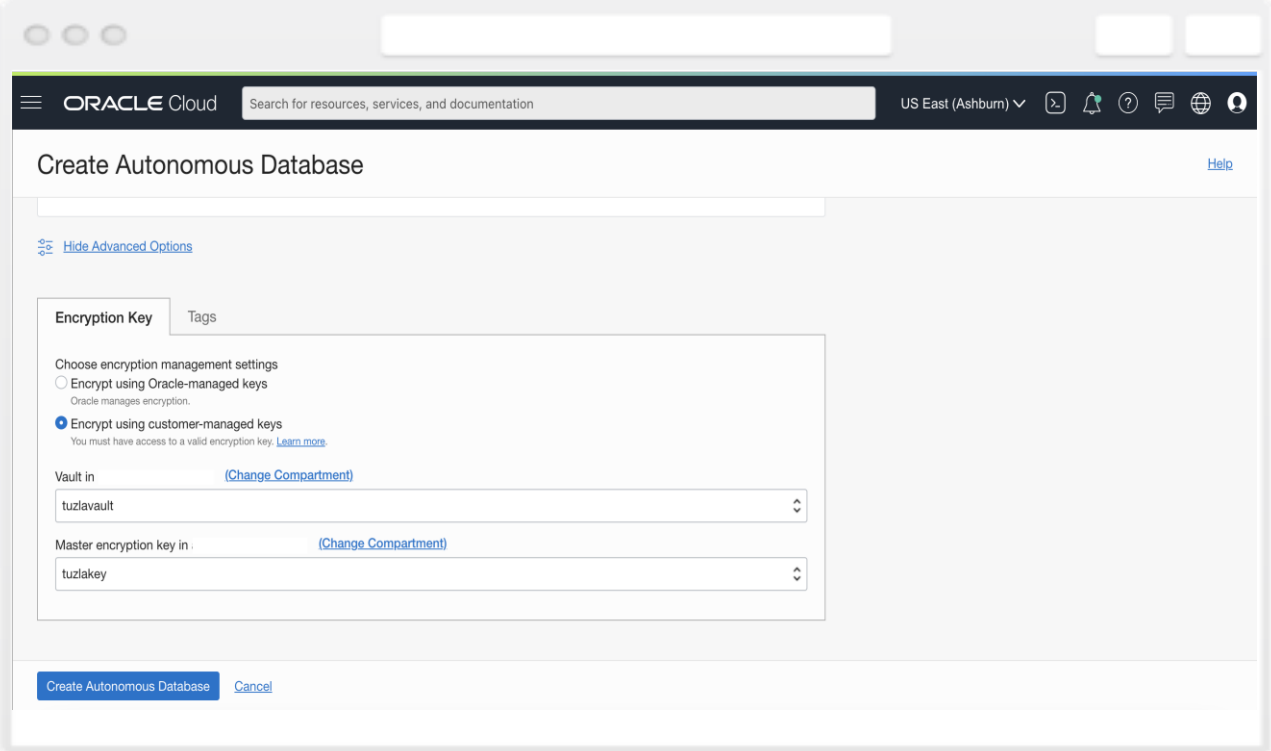
- Automatically configured
- All network access is encrypted to and from the database
- Choice of two methods
  - Oracle Native Network Encryption
  - Transport Layer Security (TLS) v1.2 (default)
- Oracle client credentials can be downloaded via encrypted wallet files

Self-Securing | Encrypting Data

Customer Managed Keys

ADB now provides two options for encrypting the data in your database:

- Oracle-managed encryption keys (default)
- Customer-managed encryption keys



Self-Securing | Encrypting Data

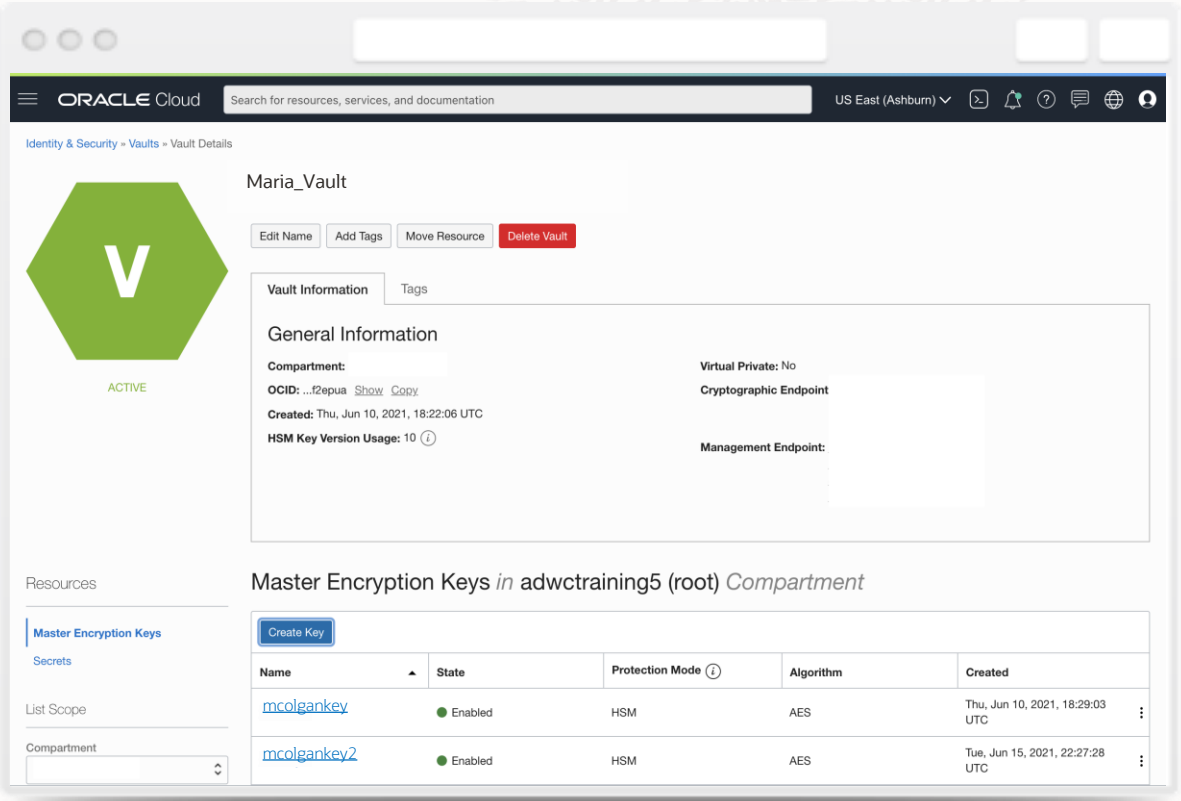
Customer Managed Keys

ADB now provides two options for encrypting the data in your database:

- Oracle-managed encryption keys (default)
- Customer-managed encryption keys

Customer managed keys integrates with Oracle Cloud Infrastructure Vault service

- Need to create an OCI Vault and a Master Encryption Key inside the vault
- Optionally, you can also import your own key



Self-Securing | Encrypting Data

Customer Managed Keys

ADB now provides two options for encrypting the data in your database:

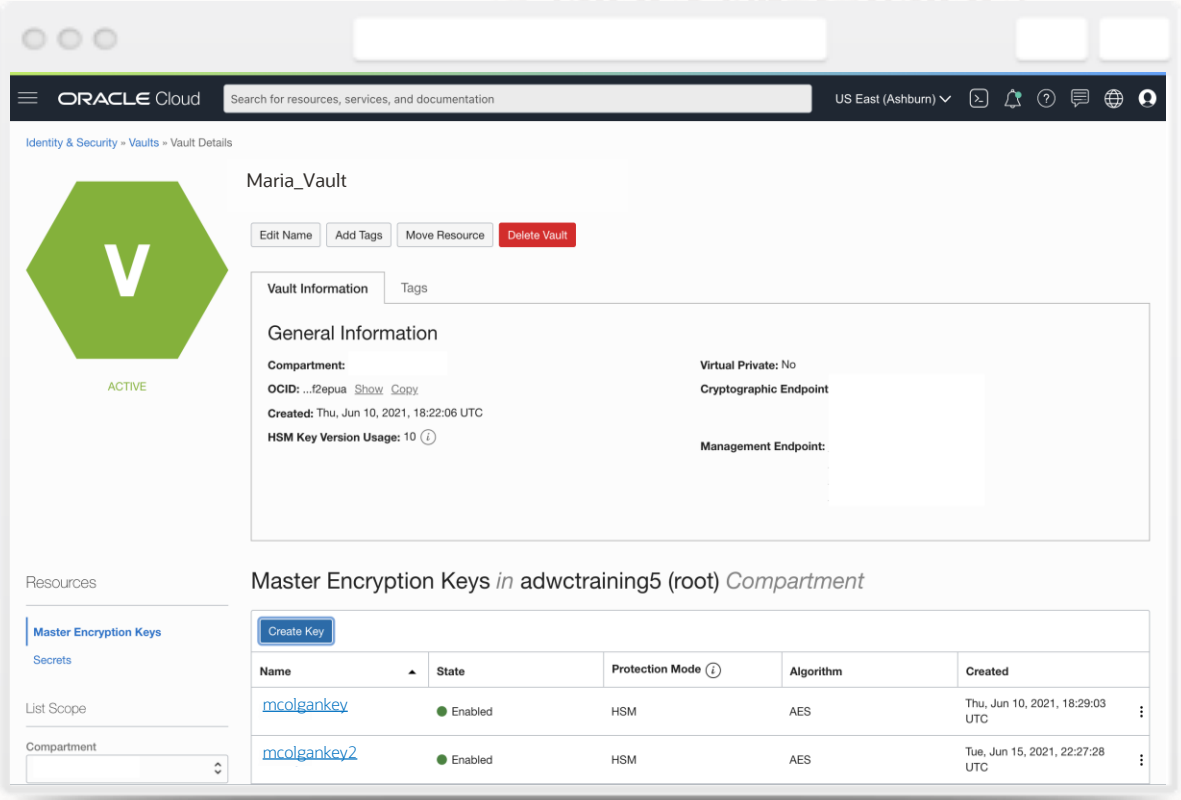
- Oracle-managed encryption keys (default)
- Customer-managed encryption keys

Customer managed keys integrates with Oracle Cloud Infrastructure Vault service

- Need to create an OCI Vault and a Master Encryption Key inside the vault
- Optionally, you can also import your own key

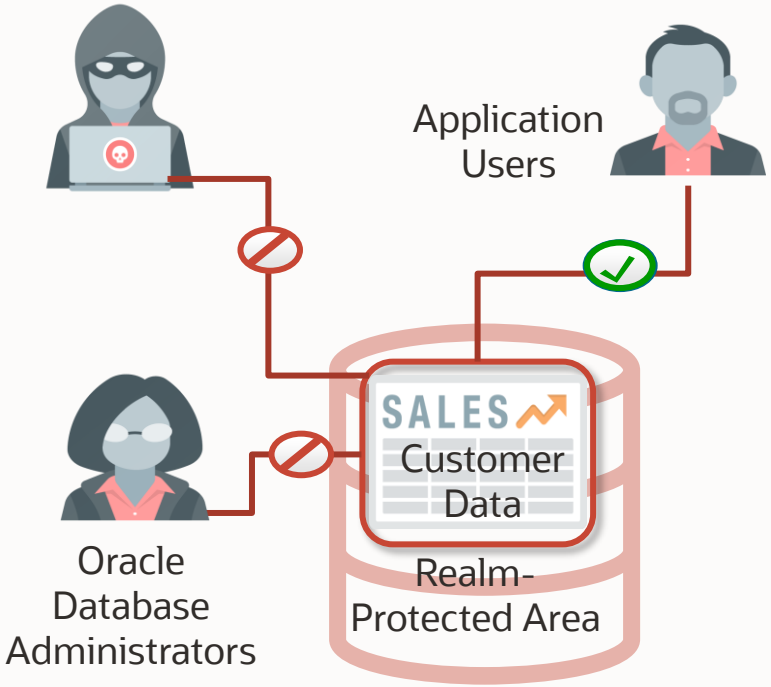
Rotating customer-managed master keys triggers ADB to generates a new TDE master key

- Operation is fast and does not require downtime



Self-Securing | Oracle Database Vault

Mitigate Risks Posed by Misuse Privileged Database Accounts



Oracle Database Vault controls privileged users' access to customer data

- All Customer data is stored in a realm-protected area
- Restricts privileged users’ access to realm-protected data
- Attempts to bypass realms are audited
- Enforces enterprise data governance, separation of duties, and least privilege

Self-Securing | Auditing

Users are unable to disable security configurations

- Autonomous Database leverages Oracle Unified Audit to capture security-relevant activity
  - Login failures
  - Changes to users, including creation of new accounts, grants of privileges or roles
  - Changes to database structures, including tables, procedures, and synonyms
- Customers have access to all audit data via the `UNIFIED_AUDIT_TRAIL` view
- The `DBMS_FGA` package can be used to add more polices

Self-Securing | Auto Patching

Automatic patching without downtime

Automatic Patching of all components (on-demand for critical security issue)

Firmware, OS, Hypervisor, Clusterware, Database

Patches applied in a rolling fashion across RAC nodes and Exadata storage servers

Database is continuously available to application

Applications using Application Continuity best practices, run without interruption

Patching is automatically scheduled

Customer can adjust patching window within a time range on Dedicated deployments

Next patching windows shown on console

Note: Early access to patches now possible on both Shared & Dedicated Infrastructure

Self-Securing | Separation of Duty

Security is a **shared** responsibility

Oracle automatically takes care of

- Data encryption by default
- Network security and monitoring
- OS and platform security
- Database patches and upgrades
- Administrative separation of duties

However, there are still areas of security that need to be managed by the customer

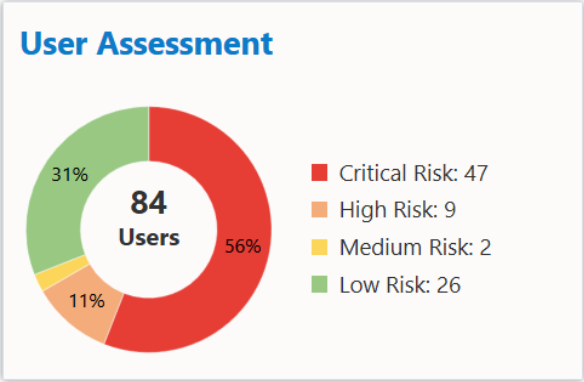
- Ongoing security assessments
- Users & Privileges
- Sensitive data discovery
- Data protection
- Activity auditing

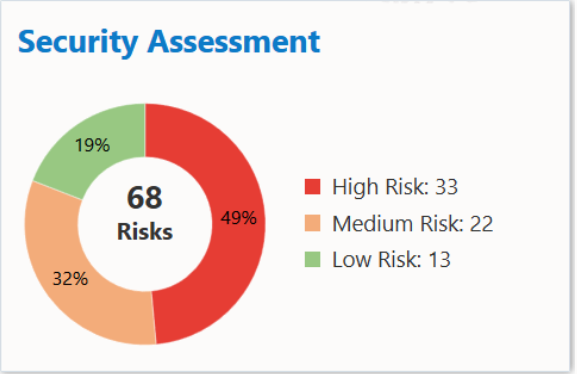
Self-Securing | Oracle Data Safe

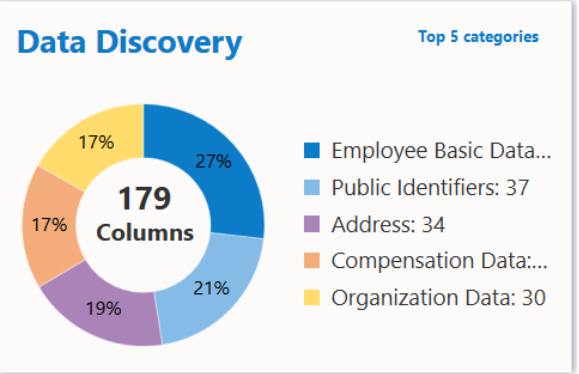
Automated Data Protection

Unified database security control center

- Security configuration assessment
- User risk assessment
- User activity auditing
- Sensitive data discovery
- Data masking







Self-Securing | Oracle Data Safe

Automated Data Protection

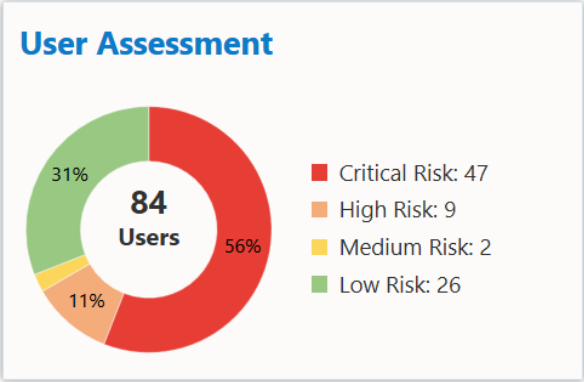
Unified database security control center

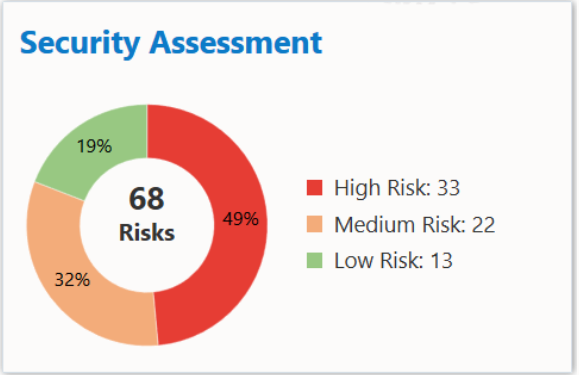
- Security configuration assessment
- User risk assessment
- User activity auditing
- Sensitive data discovery
- Data masking

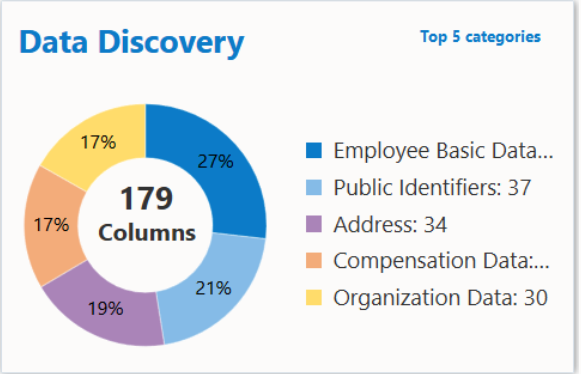
Defense in depth for all customers

- Saves time and mitigates security risks
- No special security expertise needed

Free with all Oracle Cloud Databases

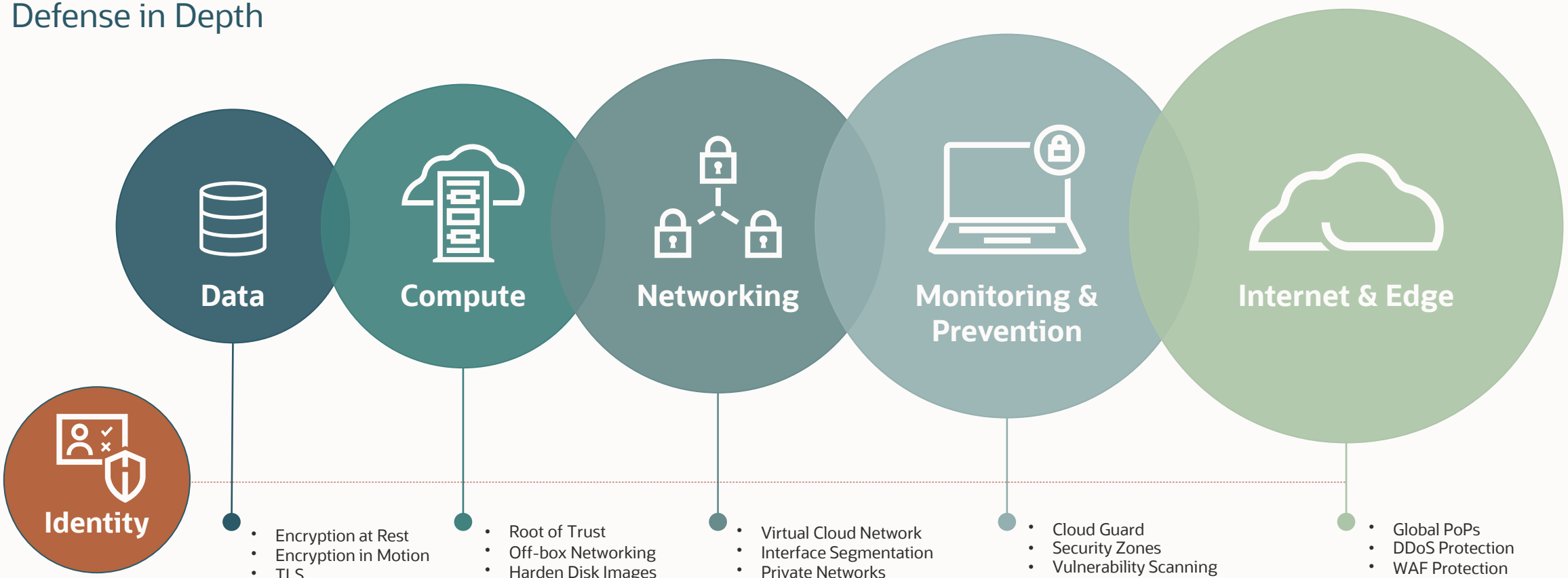






Integrated and Automated Security from Data to Identity

Defense in Depth



Identity

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

Data

- Encryption at Rest
- Encryption in Motion
- TLS
- DataSafe
- Managed Keys
- Custom Keys
- Managed Vault
- Oracle Vault Cross Regional Replication and Asymmetric Keys

Compute

- Root of Trust
- Off-box Networking
- Harden Disk Images
- Autonomous Linux
- Certificates
- Hardware Security Modules

Networking

- Virtual Cloud Network
- Interface Segmentation
- Private Networks
- FastConnect
- Secure VPN
- Bastion
- P2P, NAT, DRG Gateways

Monitoring & Prevention

- Cloud Guard
- Security Zones
- Vulnerability Scanning
- Threat Detection
- Logging/Flows
- Governance
- Compliance

Internet & Edge

- Global PoPs
- DDoS Protection
- WAF Protection
- SD-WAN

Thank you.

ORACLE