

Ograniczanie ryzyka w środowisku Autonomicznej Bazy Danych

Jak zabezpieczyć dane przed podejrzanymi użytkownikami i otoczeniem przy wykorzystaniu najnowszych opcji Autonomicznej Bazy Danych związanych z bezpieczeństwem

Witold Świerzy

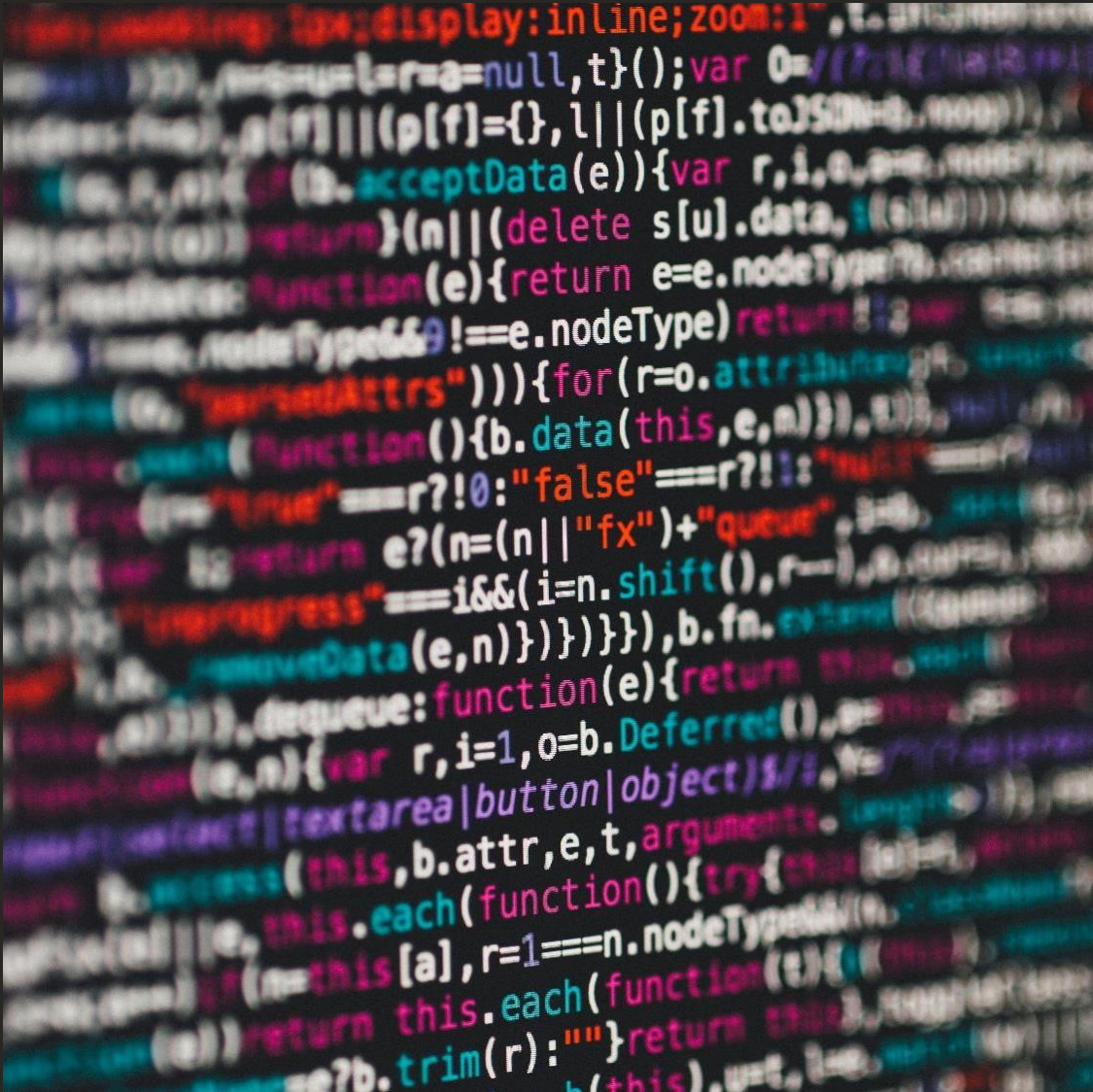
Oracle PL

Październik 22, 2019

Safe Harbor

The preceding 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.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at <http://www.oracle.com/investor>. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.



Data – The Fuel for Digital Businesses

Every business relies on digital data

Creation rates exploding with innovative applications

Significant driver of revenue and value creation

Data can increase business risk

Data — The Holy Grail for Attackers

175 Zettabytes

Global data by 2025

4.1 Billion

Records breached 1H2019

\$700 Million

Largest fine by FTC for data breach

40%

Annual growth in company data

885 Million

Largest single breach (so far) for 2019

\$230 Million

Largest GDPR fine to date

Security Challenges

Technology Stack

- Multi-vendor security stack
- Complexity in systems and configs
- Mobile, cloud, IoT, containers...

Shortage of Expertise

- Inability to find qualified staff
- Misuse/underuse of security products
- Inability to innovate, short staffed

Keeping Up

- Patching and maintaining systems
- Consistency across infrastructure
- New attack methods and techniques



66%

CxOs cite security as
biggest benefit of
cloud

Dependency on Cloud Services Compounding Cybersecurity Challenges



Shortage of Skills

- **53%** - Cybersecurity skills
- **38%** - IT architecture / planning
- **35%** - Artificial Intelligence / Machine Learning (AI / ML)



53%

Are using Machine Learning for cybersecurity purposes

Source: [Oracle and KPMG Cloud Threat Report 2019](#)

The Future Is Autonomous Database



CUSTOMER PERSPECTIVE

“We are at the dawn of the intelligent, autonomous age and having a self-driving database is a natural progression... I feel that autonomous databases will become ubiquitous in the future.”

Clark A. Kho , Senior Technology Architect, Accenture

Source: [Oracle and KPMG Cloud Threat Report 2019](#)

Traditional Shared Responsibility Model

On-Premises	IaaS Infrastructure-as-a-Service	PaaS Platform-as-a-Service	SaaS Software-as-a-Service
User Access / Identity	User Access / Identity	User Access / Identity	User Access / Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Service Consumer Responsibility

Service Provider Responsibility

Autonomous Database Shared Responsibility Model

DBaaS (PaaS) Database-as-a-Service	Autonomous Database
User Access / Identity	User Access / Identity
Data	Data
Database	Database
Guest OS	Guest OS
Virtualization	Virtualization
Network	Network
Infrastructure	Infrastructure
Physical	Physical

Service Consumer Responsibility

Service Provider Responsibility



Autonomous DBaaS
shifts closer to a SaaS
Responsibility Model

Oracle Autonomous Database



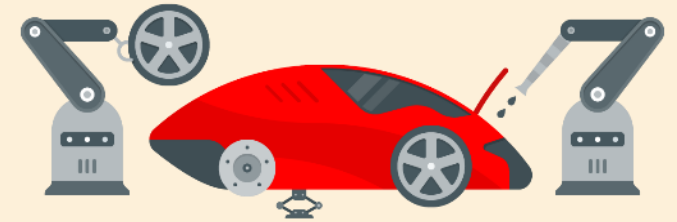
Self-Driving

Reduces
human labor



Self-Securing

Protects itself
from attacks



Self-Repairing

Keeps business up
and running

World's First Autonomous Database

A New Industry Category

Under the hood of Self-Securing



Benefits

- Secure configuration with full database encryption
- Automatically applies security updates online
- Sensitive data hidden from Oracle or customer admins
- Protects from both external and malicious internal threats

Oracle Technology

Monitors threats, applies security **updates online**, stops admin snooping with **DB Vault**, **encrypts** all data

Autonomous Database Capabilities

Gen 2 Infrastructure Foundation

Denial of Service Attack

Self Patching and Configuration

Encryption by Default

Separation of Duties

Auditing

Data Safe*

Available on Dedicated Infrastructure*

** = Now available in Fall 2019*

Self-Securing | Patching and Configuration

Quarterly patching of all components
(on-demand for critical security issue)

- Firmware, OS, Hypervisor, Clusterware, Database
- Installs prebuilt Gold Image of patched database executables rather than directly applying patches

Patching is automatically scheduled

- Customer can adjust timing within a time range

Patches applied rolling across RAC nodes and
Exadata storage servers

- Database is continuously available to application
- Applications using Application Continuity best practices run without interruption

Self-Securing | Data Encryption by Default



Encryption for Data at Rest

- Automatically configured – all application data is encrypted within the database
- 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)

Autonomous Database

Dedicated Infrastructure

Private Reserved Infrastructure in Public Cloud

- Single Tenant
- Dedicated Exadata Infrastructure
 - **Databases of any size**, scale, or criticality

Highest Security **Secure Isolation Zone**

- **Perimeter Control Computers:** Impenetrable Barrier
- Highest protection from other tenants
- Container Databases for intra-company isolation

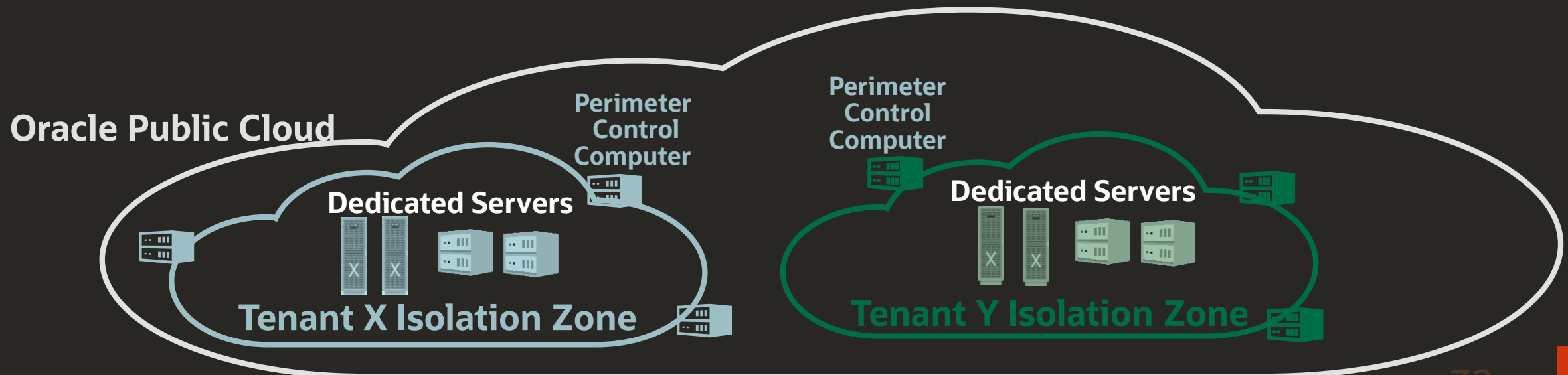
Customizable **Operational Policies**

- Control of provisioning, updates, availability, density



Gen2 Oracle Cloud Security Hardware: **Secure Isolation Zones**

- **Dedicated Servers** inside tenant's isolation zone run tenant's VMs and DBs
 - Dedicated Servers protects from security exploits at the VM, OS, and other software levels
- Perimeter Control Computers filter all incoming network packets
 - Perimeter Control Computers not visible on the network
 - Immune from software and zero-day exploits



Common Reasons for Database Breaches

- Unencrypted data
- Security patches not applied
- Administrator Snooping
- Malware / Viruses
- Poor Network Isolation

Security configuration drift
Unmanaged privileged users
Unaudited users
Untracked sensitive data
Sensitive data in open

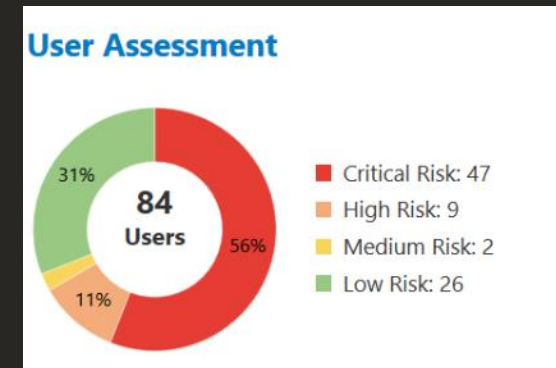
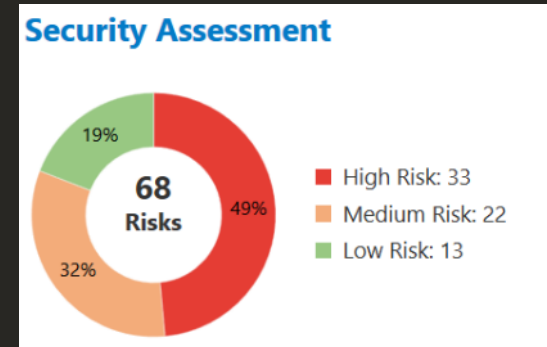
Addressed by
OCI/Autonomous Database

Currently
Customer Responsibility

Announcing | Oracle Data Safe

Autonomous Database | Now even more Secure

- Unified Database Security Control Center
 - Security Assessment
 - User Assessment
 - User Activity Auditing
 - Sensitive Data Discovery
 - Sensitive Data Masking
- Saves time and mitigates security risks
- Defense in Depth for all customers
- No special security expertise needed



Available with Oracle Cloud Databases at no additional cost



Comparing Security Services for Cloud Databases

Functionality	Amazon AWS	Microsoft Azure	Google Cloud	Oracle
Database Encryption	Available	Included	Included	INCLUDED with Cloud Databases
Strong Separation of Duty				INCLUDED with Autonomous Databases and Enterprise editions
Security Patching				INCLUDED with Autonomous Databases
Security Assessment	-	SQL Adv. Threat Protection	-	Data Safe
Data Discovery	-	SQL Adv. Threat Protection		Data Safe
Data Masking	-	-		Data Safe
User Assessment	-	-	-	Data Safe
User Activity Auditing	CloudTrail, CloudWatch, GuardDuty	SQL Adv. Threat Protection	Stack Driver Logging	Data Safe
Pricing	Fine grained	\$15/mo/target	Fine grained	FREE

Always Free Oracle Autonomous Database



- **Always Free: Two Databases per Cloud Tenancy** ⁺
 - Each Database gets 1 OCPU and 20 GB storage
- **Free Tools** for Application Development
 - APEX for low-code, web-based app development
 - SQL Developer Web for database development
 - SQL Notebooks for Machine Learning
 - Automatic REST for easy access and publishing of DB data
 - Drivers for all popular programming languages

⁺ Free Oracle Autonomous Database does not include Data Safe



Only Oracle Provides the First Fully Autonomous Database

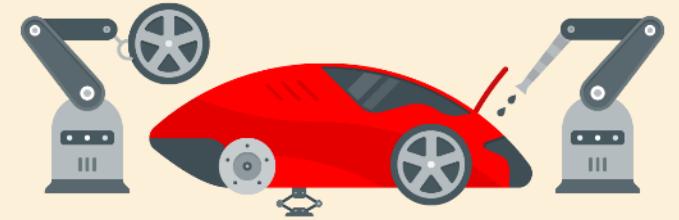


Self-Driving



Self-Securing

- Gen 2 Infrastructure Foundation
- Denial of Service Attack
- Self Patching and Configuration
- Encryption by Default
- Separation of Duties
- Auditing
- Data Safe
- Available on Dedicated Infrastructure



Self-Repairing

Thank You

