ORACLE

Tudjuk adatainkat biztonságban

a Zero Trust megközelítés fényében konvergens adatbázissal

Fekete Zoltán
Vezető műszaki tanácsadó
Principal Solution Engineer
Oracle Hungary

2022. május 17.

Threat Landscape as per ENISA Top 9 (October 2021)

1. **Ransomware**
2. Malware
3. Cryptojacking
4. E-mail related threats
5. **Threats against data** (this category encompasses data breaches/leaks)
6. Threats against availability and integrity
7. Disinformation – misinformation
8. **Non-malicious threats**
   (mostly based on human errors and system misconfigurations)
9. Supply-chain attacks

Source: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Ki akarják megszerezni az adatainkat?

Belsősök

Nemzetállamok

Kilépett dolgozók

Személyes
Pénzügyi
Nemzeti
adatvagyon
Szellemi termék
Egészségügyi
Üzleti titkok

Bűnözők

Kalandkeresők

Hacktivisták

Ügyfelek

Versenytársak

„**Zero Trust**:
stratégiai kezdeményezés,
segít megelőzni a sikeres adatbiztonsági visszaéléseket
a bizalom koncepciójának eltörlésével”

Zero Trust is not about making a system trusted,
but instead about eliminating trust.

John Kindervag
SVP, Cybersecurity Strategy, ON2IT Cybersecurity
Originator of the Zero Trust security model

„**A Zero Trust modell**:
kikényszeríti, hogy **kizárólag**
a jogosult személyek és erőforrások legyenek jogosultak
az adatok és erőforrások elérésére,
csak a megfelelő eszközökről,
csak a megfelelő körülmények között..”

Bill Harrod
Chief Technology Officer, MobileIron

zero trust … fókuszál:
az erőforrások biztonságos elérésére,
függetlenül a hálózati helytől, tárgytól és eszközöktől,
kikényszerítve a kockázatalapú hozzáférés szabályozását,
folyamatosan vizsgálva, monitorozva és rögzítve (log) az eseményeket.

Implementing a Zero Trust Architecture
National Cybersecurity Center of Excellence

Zero Trust architektúra által kezelt veszélyek

1. Szolgáltatás kiesése, lassítása
2. Munkamenetek eredményének befolyásolása
3. Ellopott credentials
4. Belső fenyegetések

Biztonsági zónák: több megközelítés együtt működik!

Felmérés, értékelés

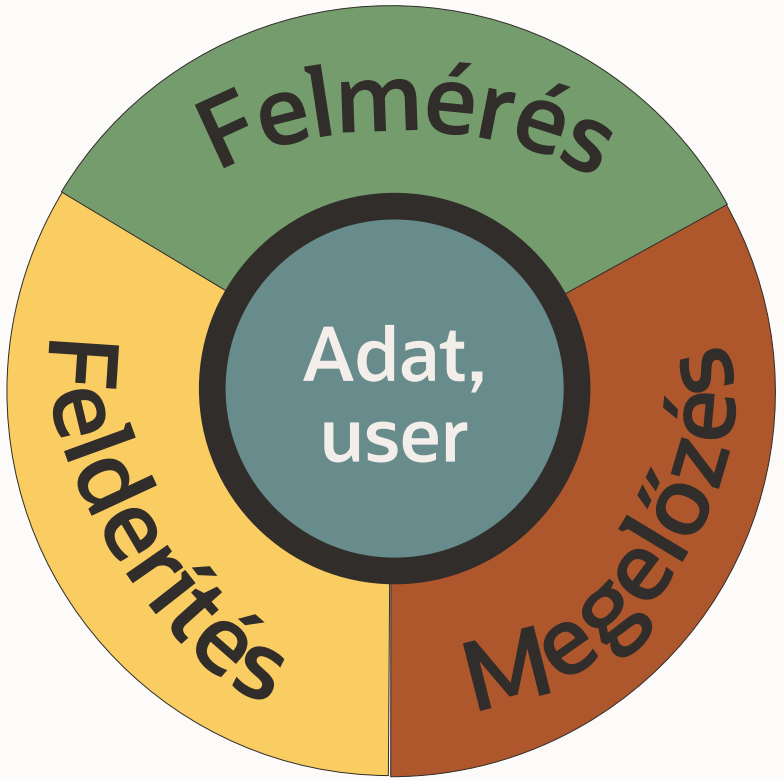
Az adatbázis aktuális állapotának felmérése.

Felderítés

Az adatelérési próbálkozások felderítése, különösen a szabályoknak nem megfelelők esetében.

Megelőzés

A nem megfelelő és szabályellenes adatelérés megelőzése.



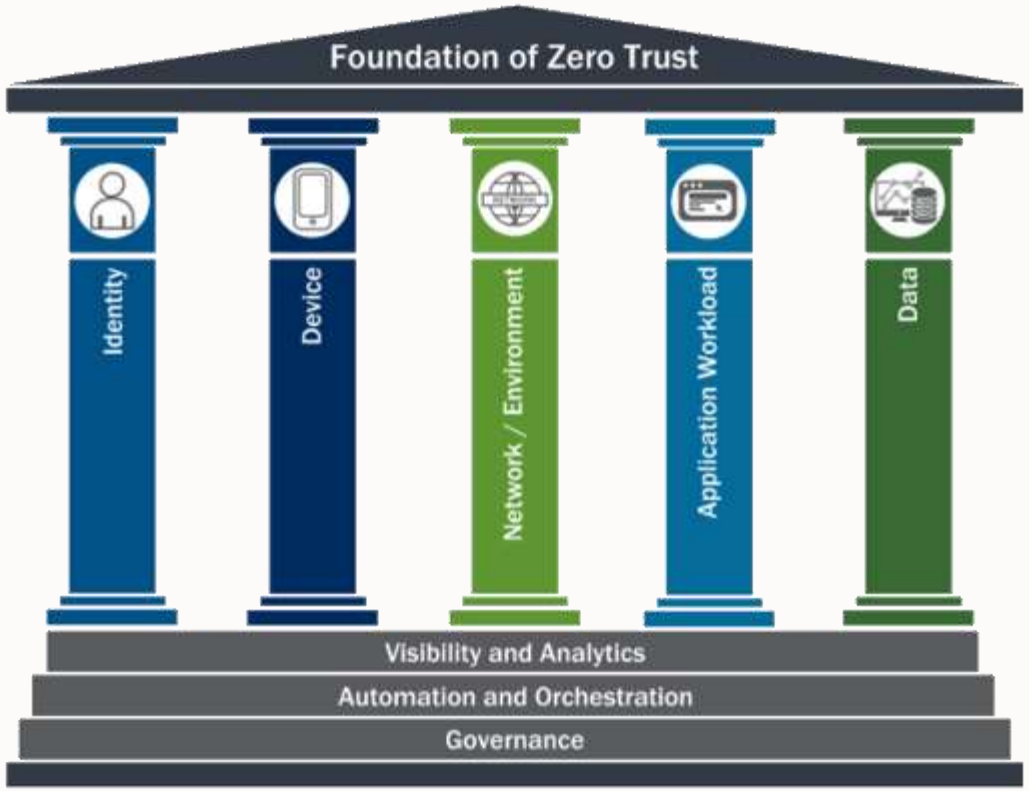
Adatok

Az adatbázisok adatai értékesek: adatvagyon, ami komoly kockázatokkal járhat..

Felhasználók

Az adatbázisokhoz felhasználók és alkalmazások kapcsolódnak, üzleti feladatok elvégzéséhez.

A Zero Trust alapjai



Source: CISA Zero Trust Maturity Model (June 2021)

5 technológiai tartóoszlop:

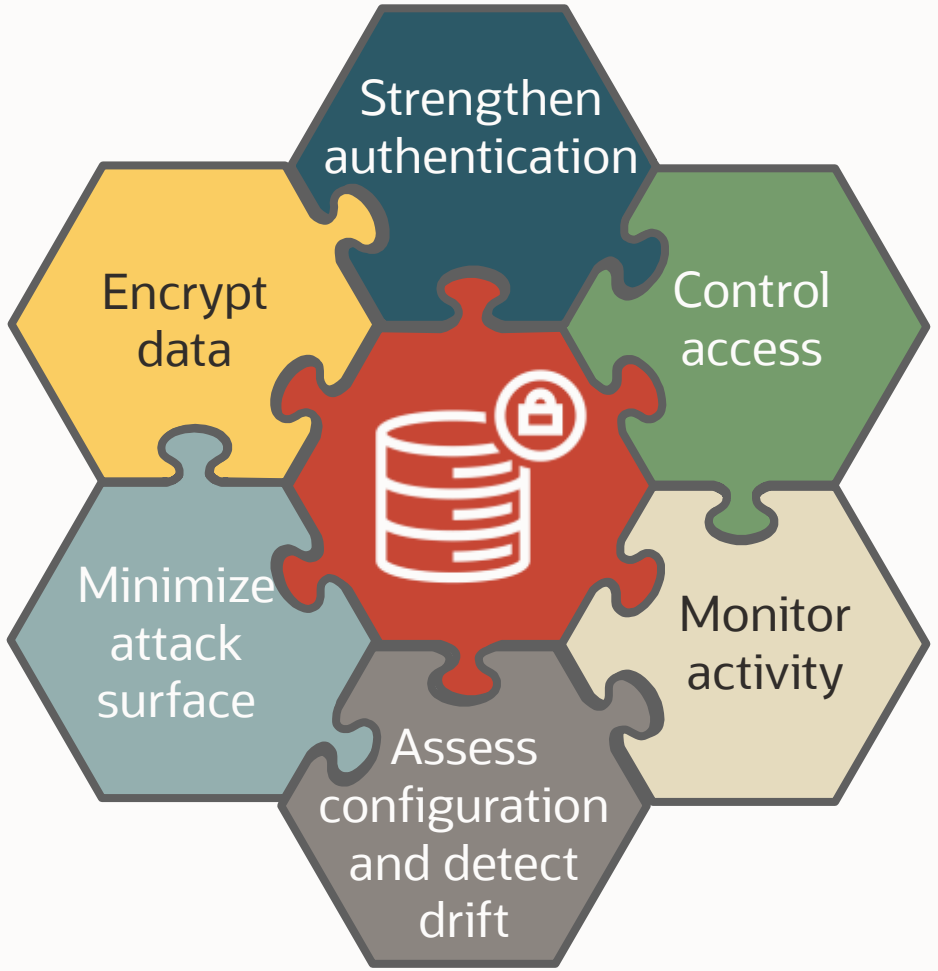
1. Identity
2. Device
3. Network/Environment
4. Application Workload
5. Data

Minden tartóoszlop támaszai:

- Láthatóság és elemzések
- Automatizálás és szervezés
- Governance

A bizalom eliminálása

Ne hagyjunk rést a pajzson!



Ne bízz abban, hogy a konfiguráció tökéletes marad!

Szabványosítás a fenntarthatóság és rendszerek számossága miatt

- Kevés (általában 2-3) különböző konfigurációs készlet: kockázat alapján
- Elfogadott, ismert szabvány alapján (CIS Benchmark, DISA STIG)

Periodikus ellenőrzés – automatizálás

Fontos Oracle eszközök és szolgáltatások:

Database Security Assessment Tool

Data Safe *Security Assessment*

Enterprise Manager Database Lifecycle Management Pack

Ne bízz abban, hogy a hálózat miatt adatbázisod biztonságos maradna!

Feltételezzzük, hogy a támadók megkerülik a szabályozást, direktben támadva az DB-t
Csökkentsük a szükséges minimálisra a jogokat, privilégiumokat
Ahol nem szükséges, ne legyen érzékeny adat

Fontos Oracle eszközök és szolgáltatások:

Teszt környezetek:

Enterprise Manager - Data Masking and Subsetting Pack

Data Safe *Masking*

felhasználókhoz:

Database Security Assessment Tool

Data Safe *User Assessment*

Audit Vault and Database Firewall *entitlement monitoring/reporting*

Database *Privilege Analysis – ingyenes a DB EE-ben*

Ne bízz abban, hogy a tároló, mentés, export védett!

Mozgásban

- Throughput korlátozások – a hálózat legalacsonyabb szintjén védve
- Értsd meg a különbségeket: native network encryption and TLS – működtetésben is

Helyben

- Titkosítani az exportokat is – gyakran kockázatos nem titkosítani
- Figyelj a mentések titkosítására

Fontos Oracle eszközök és szolgáltatások:

Database *Native Network Encryption*

Database *TLS Network Encryption*

Advanced Security *Transparent Data Encryption*

Key Vault

Ne bízz kizárólag a jelszavakban!

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

Fontos Oracle eszközök és szolgáltatások:

Database *Password Profiles*

Database *Gradual Database Password Rollover*

Database *Centrally Managed Users*

Database *Strong Authentication*

Oracle Radius Adapter

Ne bízz a felhasználók jó szándékában!

Részísítsük előnyben a megelőző technika védelmet, ne csak a process/policy-k

Védjük meg az érzékeny adatokat a hozzáférés szükséges minimalizálásával

Fontos Oracle eszközök és szolgáltatások::

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

Ne bízz a megelőzés 100% hatékonyságában!

Auditing és network-based monitoring:

- Anomáliák elemzése: gyanús eseményeket felderíthetünk
- Vizsgálatok, megfelelőségi elemzések

Audit:

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

Fontos Oracle eszközök és szolgáltatások:

Database *Unified Auditing*

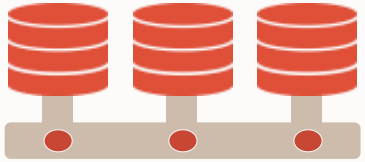
Audit Vault and Database Firewall

Data Safe *Auditing*

Adatvezérelt szervezetek és alkalmazások

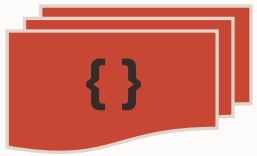
Sok külön adatbázis vagy „converged database” kulcsmutatók, predikciók, egyszerű szabályozott hozzáférés

Agilis



Multitenant

Rugalmas

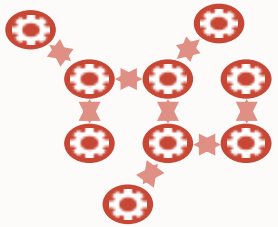


JSON

Biztonságos

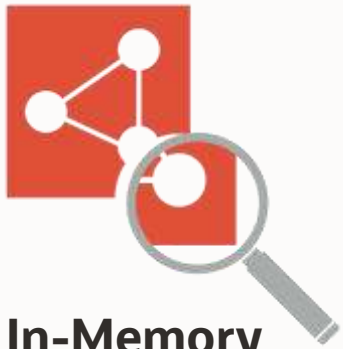
Blockchain

Adaptálódó



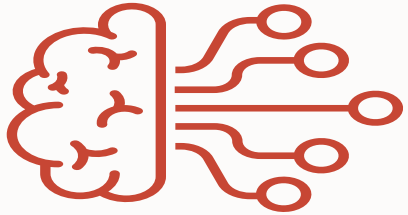
Microservices

Elemző



In-Memory

Prediktív

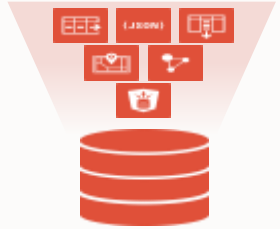


Machine Learning

Kiterjeszthető

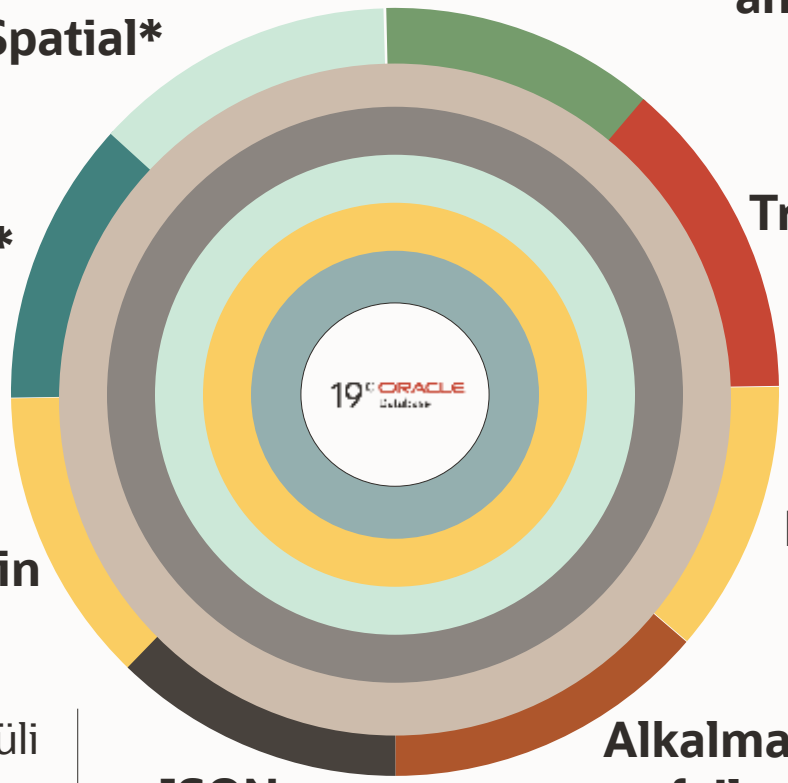
Data Lake

Egyszerű



Converged Database

Oracle Database – konvergensre tervezve:
multi-tenant, -model, -workload



Gépi tanulás* & analitika
30+ in-database Machine Learning algoritmus

100+ térképi funkció
Spatial*

50+ gráf elemzési algoritmus
Graph*

Transactions
Tranzakciós esemény queue-k

Biztonságos blockchain táblák
Blockchain

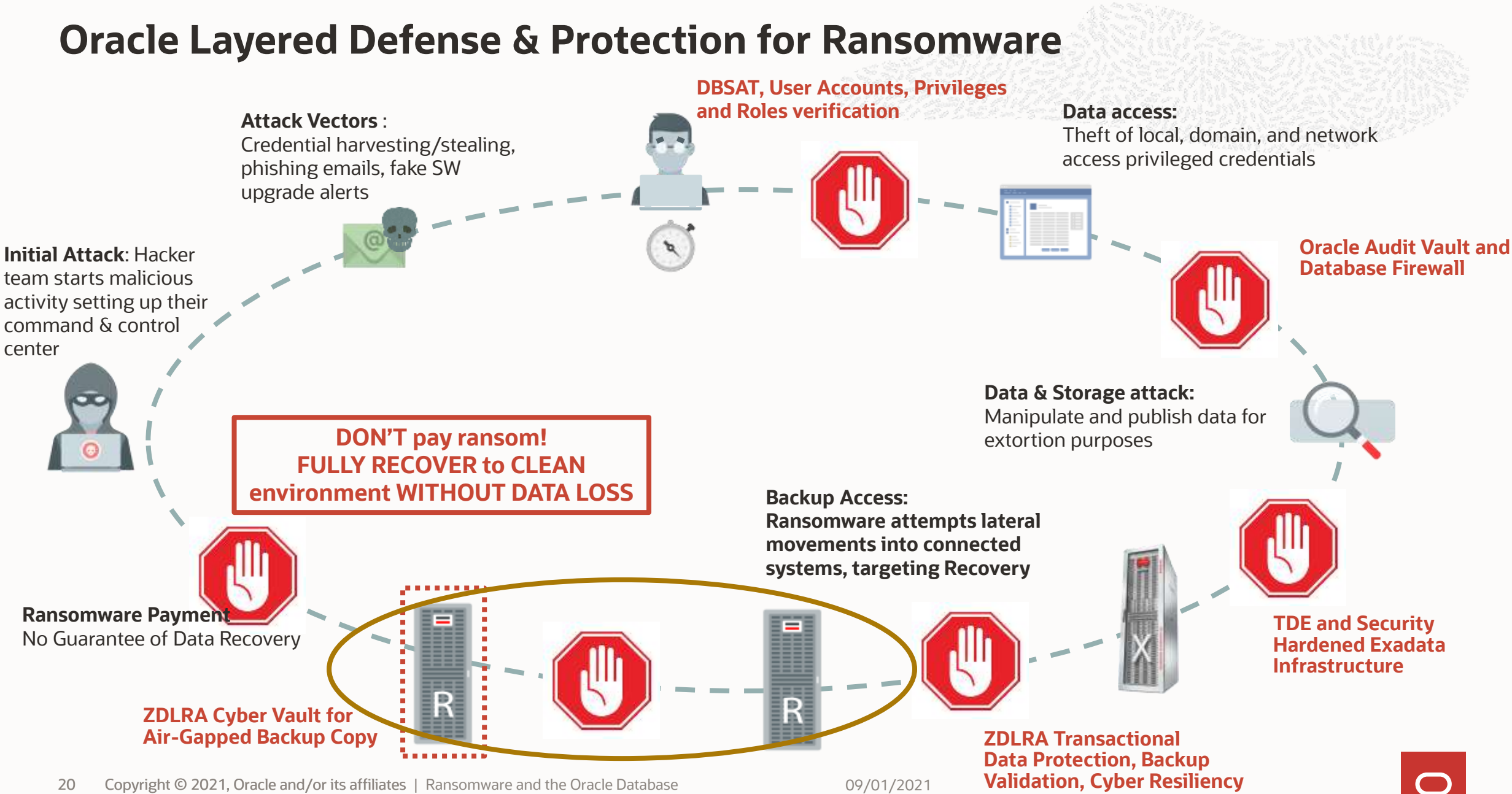
IoT
IoT streaming (valós idejű analitika)

Séma nélküli alkalmazás-fejlesztés
JSON

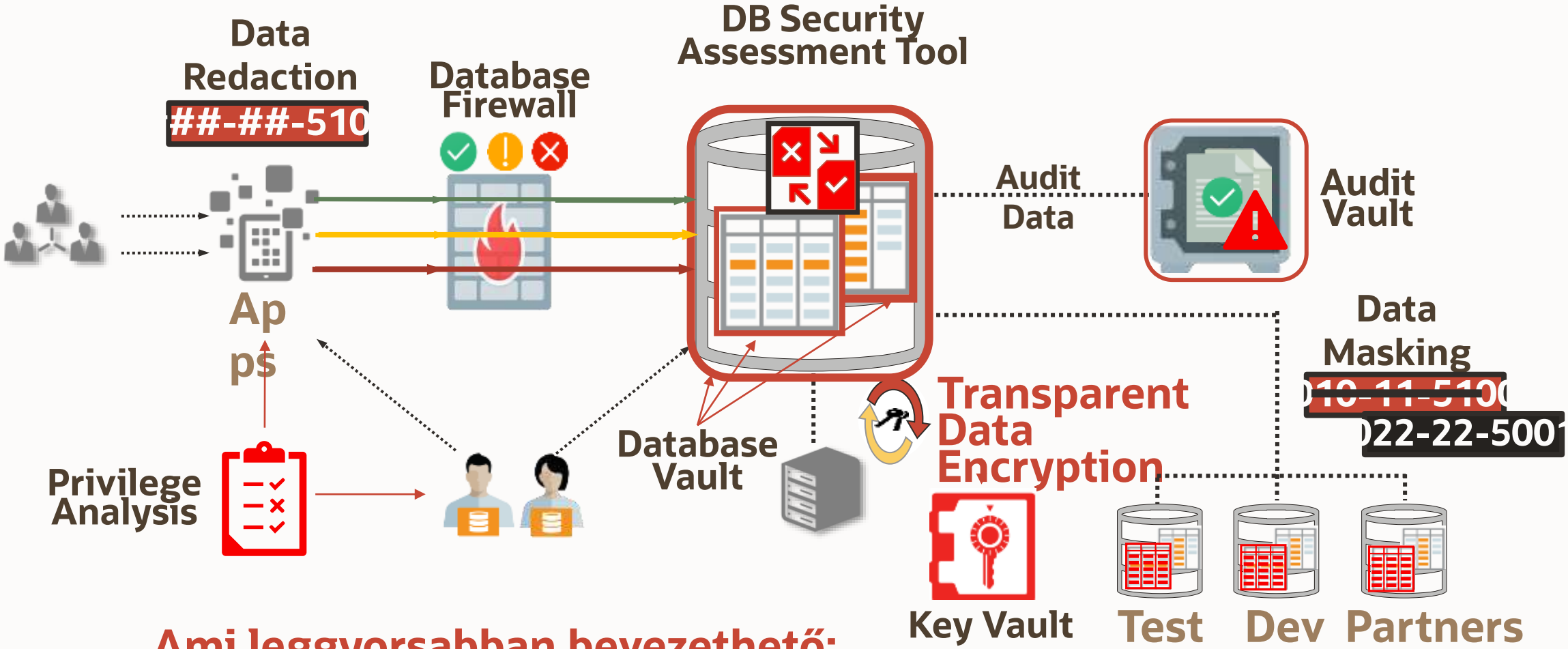
Alkalmazás-fejlesztés
APEX kódolásmentes fejlesztési platform

Közös rendelkezésre állás, teljesítmény, biztonság, párhuzamosság, üzemeltetés

Oracle Layered Defense & Protection for Ransomware



Oracle Database Maximum Security Architecture



Ami leggyorsabban bevezethető:
az alkalmazkodó informatikához

Oracle Data Safe

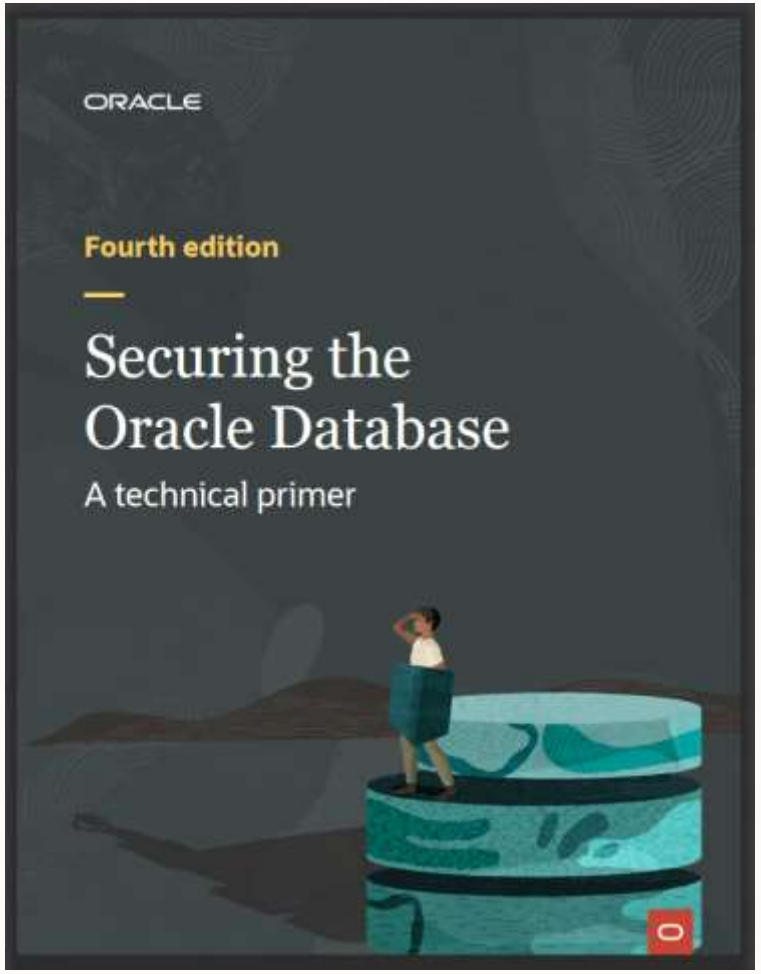
Egységes, ingyenes* adatbázis-biztonsági konzol a felhőben

- Egységes DB Security Control Center
  - Security Assessment
  - User Assessment
  - User Activity Auditing
  - Sensitive Data Discovery
  - Sensitive Data Masking
- Kezeli a DB-biztonsági kockázatokat
- Időt takarít meg
- Mélységi védelem
- Nincs szükség szakértői tudásra
- On prem és felhő

**** A legtöbb funkció ingyenes***

Securing the Oracle Database

Ingyenes DB security könyv, negyedik kiadás.
https://oracle.com/securingthedatabase



Database Security Office Hours

Database Security PM

Minden hónap 2. csütörtökén,

URL: http://bit.ly/asktomdbsec
„AskTom Database Security Office Hours”

Ask Tom
Database Security

Learn more

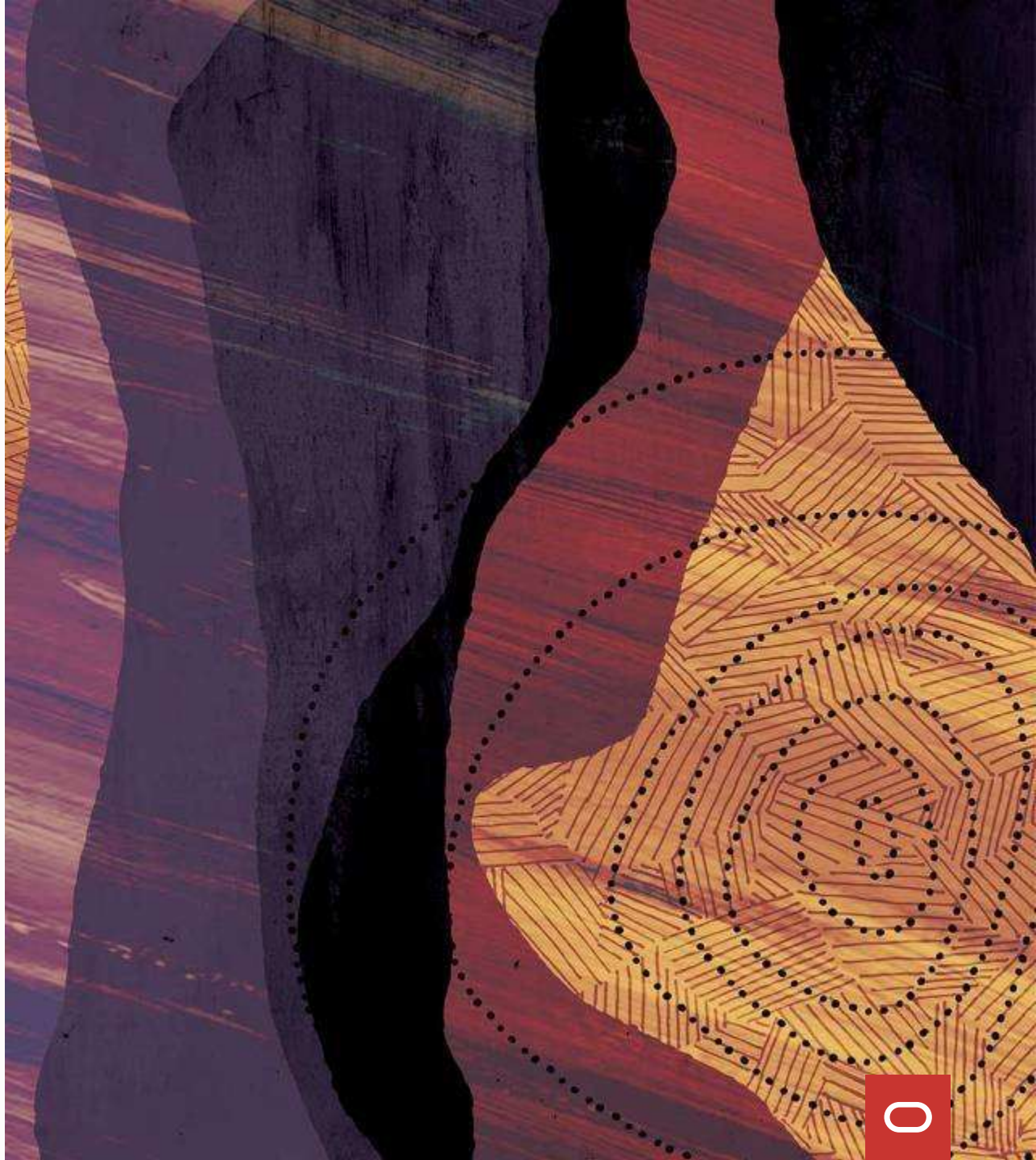
Read NIST SP 800-207 (*Zero Trust Architecture*) – https://crsc.nist.gov

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*

Köszönjük!




ORACLE