Secure your data: Security is no longer only for experts

Protecting your most valuable assets from ransomware

Bruno Reis da Silva

ORACLE

- Brazilian who lived in Hungary and based in Sweden since a few years ago.
- Master's in Software Engineering - Blekinge Institute of Technology in Sweden
- Master's in Data Science - Luleå University of Technology in Sweden
- Master's in Informatics (Privacy, Information Security and Cyber Security) - University of Skövde in Sweden - (pursuing status)
- I have more than a decade of experience in Oracle technologies at companies such as IBM and Playtech.
- Nowadays Technology Account Engineer at Oracle.
- First Oracle ACE associate in Hungary and second Oracle ACE Sweden.

ORACLE ACE A ALUM

https://www.linkedin.com/in/brunoreisdasilva/

https://www.techdatabasket.com/ Bruno.reis.da.silva@oracle.com

Oracle ACE

450+ technical experts helping peers globally

The **Oracle ACE Program** recognizes and rewards community members for their technical and community contributions to the Oracle community

3 membership tiers

Oracle ACE Director

Oracle ACE Pro

Oracle ACE Associate

For more details on Oracle ACE Program:
ace.oracle.com

Oracle ACE

Nominate
yourself or someone you know:
ace.oracle.com/nominate

Connect: **aceprogram_ww@oracle.com** Facebook.com/OracleACEs @oracleace Oracle ACE Program Group

Ransomware: One of the Most Dangerous Cybersecurity Threats

Over 4,000 attacks daily (source: FBI)

24-days average downtime in Q2 2022, whereas in Q4 2021 it was 20-days (source: Statista)

Multi-billion dollar economic impact on the U.S. in 2023 (source: Emsisoft)

Average total cost of remediating $1.85M (source: Sophos)

Ransomware Attack Vectors

- Phishing
- Watering hole sites
- Fuzzed URLs for common services
- Unpatched systems
- Open Remote Desktop Protocol
- Compromised accounts

Remote Desktop Connection

Remote Desktop **Connection**

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

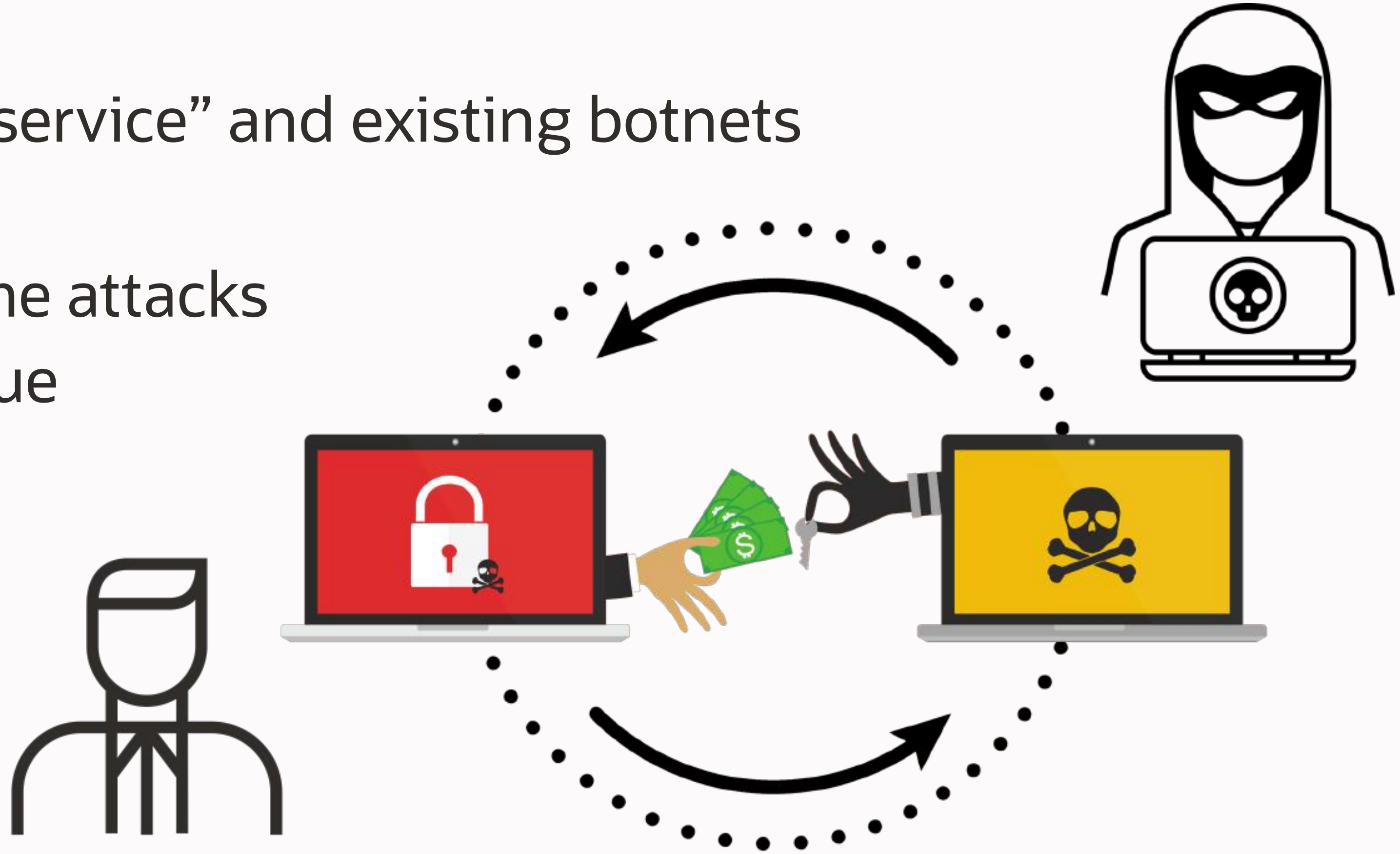
Anatomy of a Ransomware Attack

Ransomware attacks are seldom targeted

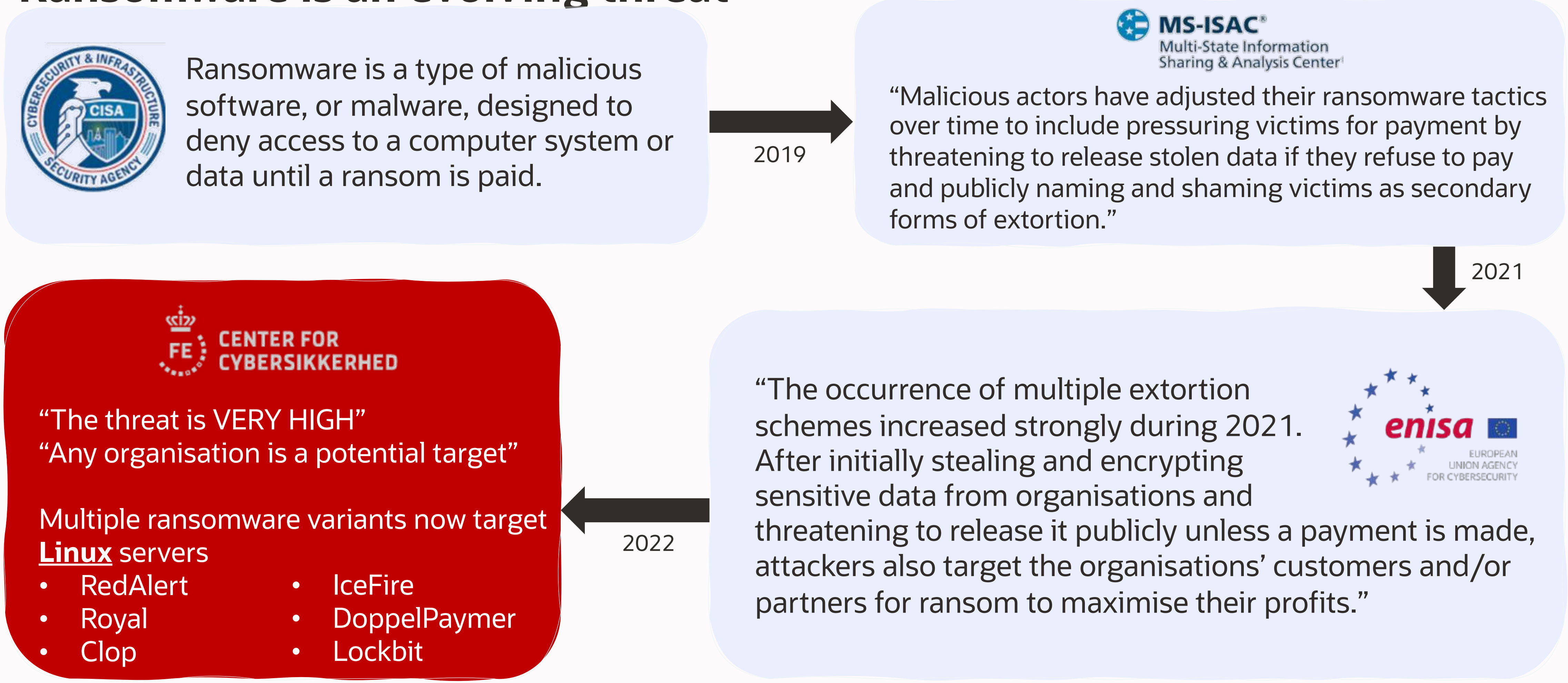
Frequently use “Malware as a service” and existing botnets

Highly automated, high-volume attacks

- Designed to generate revenue
- Transactional, business-like



Ransomware is an evolving threat



CISA

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid.

2019

MS-ISAC®
Multi-State Information Sharing & Analysis Center

“Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”

2021

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

“The occurrence of multiple extortion schemes increased strongly during 2021. After initially stealing and encrypting sensitive data from organisations and threatening to release it publicly unless a payment is made, attackers also target the organisations’ customers and/or partners for ransom to maximise their profits.”

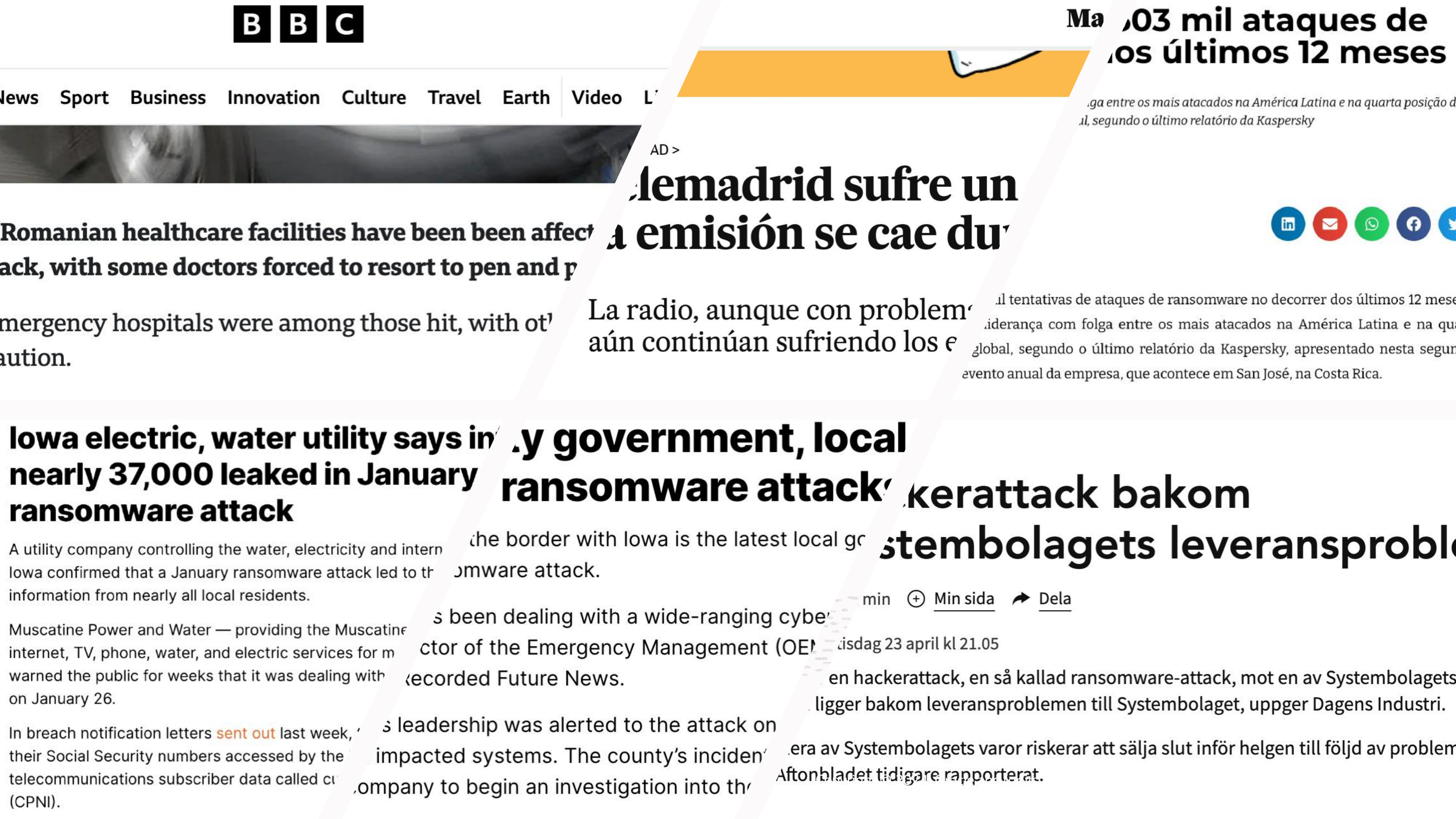
2022

FE CENTER FOR CYBERSIKKERHED

“The threat is VERY HIGH”
“Any organisation is a potential target”

Multiple ransomware variants now target **Linux** servers

- RedAlert
- Royal
- Clop
- IceFire
- DoppelPaymer
- Lockbit



BBC

News Sport Business Innovation Culture Travel Earth Video L

Romanian healthcare facilities have been been affect
ack, with some doctors forced to resort to pen and p

mergency hospitals were among those hit, with ot
aution.

AD >

lemadrid sufre un
a emisión se cae du

La radio, aunque con problem
aún continúan sufriendo los e

Ma 03 mil ataques de
os últimos 12 meses

ga entre os mais atacados na América Latina e na quarta posição d
l, segundo o último relatório da Kaspersky

l tentativas de ataques de ransomware no decorrer dos últimos 12 mese
iderança com folga entre os mais atacados na América Latina e na qu
global, segundo o último relatório da Kaspersky, apresentado nesta segun
evento anual da empresa, que acontece em San José, na Costa Rica.

Iowa electric, water utility says in nearly 37,000 leaked in January ransomware attack

A utility company controlling the water, electricity and intern
Iowa confirmed that a January ransomware attack led to th
information from nearly all local residents.

Muscatine Power and Water — providing the Muscatine
internet, TV, phone, water, and electric services for m
warned the public for weeks that it was dealing with
on January 26.

In breach notification letters sent out last week,
their Social Security numbers accessed by the
telecommunications subscriber data called cu
(CPNI).

y government, local
ransomware attack

the border with Iowa is the latest local go
omware attack.

s been dealing with a wide-ranging cybe
ctor of the Emergency Management (OEM
Recorded Future News.

s leadership was alerted to the attack on
impacted systems. The county's inciden
ompany to begin an investigation into th

kerattack bakom
stembolagets leveransprobl

min ⊕ Min sida ➦ Dela

isdag 23 april kl 21.05

en hackerattack, en så kallad ransomware-attack, mot en av Systembolagets
ligger bakom leveransproblemen till Systembolaget, uppger Dagens Industri.

era av Systembolagets varor riskerar att sälja slut inför helgen till följd av problem
Aftonbladet tidigare rapporterat.

“Security is no longer only for experts”

Ransomware Attack Breakdown

Ransomware Attack
Interactive Process, Remotely managed by Humans

Initial Attack: Hacker team starts malicious activity setting up their command & control center

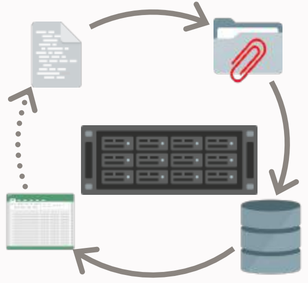
Attack Vectors : credential harvesting/stealing, phishing email, fake advertising and software upgrade

Initial Infection: once on user's PC, ransomware stays quiet for long time, while mapping the network and gathering data

Credential Theft: harvesting local, domain and network access privileged credentials

Reconnaissance: Searches for other systems and for any vulnerable locations on the network

Lateral Movement: Placing payload in any accessible storage mount point.
If the storage is backup protected, the ransomware lets the backup process commence, propagating onto the backup system.



Lateral Movement : Backup System Infected, backup files canceled, backup devices made inoperable by DDoS attack

Data Exfiltration: scraped data from infected systems and copy to external command and control systems

Last stage: Encryption
Make as much of the target's environment as possible unusable until the have the decryption key

Request ransom payment

HELLO!

YOUR STORAGE WAS COMPROMISED.
YOUR FILES ARE IN OUR POSSESSION.

FOR THE MOMENT ALL YOUR FILES AND FOLDERS ARE SAFE. THEY HAVE BEEN MOVED TO OUR SECURE SERVERS AND ENCRYPTED. IF YOU WANT YOUR FILES BACK OR DO NOT WANT THEM LEAKED PLEASE SEND 3.5 BITCOIN TO THIS BITCOIN WALLET: 1DHtv7TPk1VoGchJJs21dzKfLxRtTTFNGf

YOU HAVE UNTIL THE 3rd of JULY 2024 TO MAKE THE PAYMENT OR YOUR FILES WILL BE AUTO-DELETED FROM OUR SERVERS, LEAKED OR SOLD.
YOUR UNIQUE ID IS: 148.71.84.153
PLEASE EMAIL US YOUR ID AND PAYMENT CONFIRMATION TO:
cloud@mail2pay.com
AFTER THE PAYMENT CONFIRMATION YOU WILL RECEIVE INSTRUCTIONS ON HOW TO DOWNLOAD ALL YOUR FILES BACK.

How to obtain Bitcoin:
The easiest way to buy bitcoin is the LocalBitcoins site.
https://localbitcoins.com/buy_bitcoins
!!! ATTENTION !!!
Even if all your files are backups and you have a copy of them, do not disregard this message.
Considering the huge amount of sensitive and private information we harvested, we reserve the right to LEAK or SELL all your data, if no payment is made.

THANK YOU FOR YOUR COOPERATION.
Cl0ud SecuritY

HELLO!

YOUR STORAGE WAS COMPROMISED.
YOUR FILES ARE IN OUR POSSESSION.

FOR THE MOMENT ALL YOUR FILES AND FOLDERS ARE SAFE. THEY HAVE BEEN MOVED TO OUR SECURE SERVERS AND ENCRYPTED. IF YOU WANT YOUR FILES BACK OR DO NOT WANT THEM LEAKED PLEASE SEND 3.5 BITCOIN TO THIS BITCOIN WALLET: 1DHtv7TPk1VoGchJJs21dzKfLxRtTTFNGf

YOU HAVE UNTIL THE 3rd of JULY 2024 TO MAKE THE PAYMENT OR YOUR FILES WILL BE AUTO-DELETED FROM OUR SERVERS, LEAKED OR SOLD.
YOUR UNIQUE ID IS: 148.71.84.153
PLEASE EMAIL US YOUR ID AND PAYMENT CONFIRMATION TO:
cloud@mail2pay.com
AFTER THE PAYMENT CONFIRMATION YOU WILL RECEIVE INSTRUCTIONS ON HOW TO DOWNLOAD ALL YOUR FILES BACK.

How to obtain Bitcoin:
The easiest way to buy bitcoin is the LocalBitcoins site.
https://localbitcoins.com/buy_bitcoins
!!! ATTENTION !!!
Even if all your files are backups and you have a copy of them, do not disregard this message.
Considering the huge amount of sensitive and private information we harvested, we reserve the right to LEAK or SELL all your data, if no payment is made.

THANK YOU FOR YOUR COOPERATION.
Cl0ud SecuritY

Typical Results

Pay the ransom

- Possibly get the decryption key and get your data back
- Law enforcement may be able to recover some of the ransom

Don’t pay the ransom

- Rebuild your systems from backup

Recommended Defense Against Database Destruction

Immutable offline backup

Good
Offline backup to storage media like magnetic tape

Better
Oracle Database Cloud Backup Service

Best
Zero Data Loss Recovery Appliance

A peek inside the Hacker's tool chest

THE
DIRTY
DOZEN

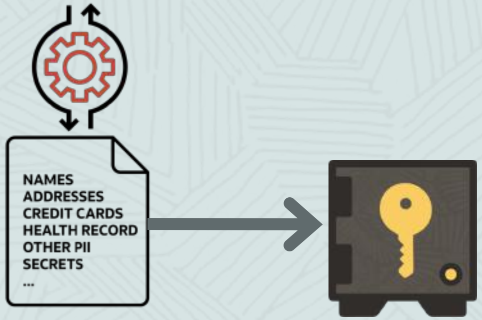
1. Insecure configuration and configuration drift
2. Unpatched and out-of-date systems
3. Lack of a consistently enforced security policy
4. Lack of visibility into sensitive data placement and quantity
5. Overprivileged database users and administrators
6. Weak authentication and shared accounts
7. SQL Injection vulnerabilities and insecure application design
8. Trusting vulnerable networks
9. Insufficient or inefficient monitoring and auditing
10. Sensitive data proliferation to non-production databases
11. Unprotected servers and database backups
12. Insecure encryption keys and secrets

How do you protect the database?

Implement a secure configuration and monitor for configuration drift

- Ensure your database configuration follows policy
- Monitor for configuration drift

Encrypt the data and protect the encryption keys



- Encrypt data in motion and at rest
- Protect against network sniffing attacks
- Protect against data scraping attacks (eg: ransomware)

Control access to the data

- Enforce least privilege
- Control privileged user access to data
- Enforce separation of duties
- Establish and enforce a trusted path to data

Monitor access to the data

- Use native auditing capabilities to capture high-value activity
- Use network-based monitoring to examine ALL activity

Recommended Defense Against Database Destruction

Zero Data Loss Recovery Appliance

Zero Data Loss

- Real-time Transaction Protection

Best Database Recovery

- End-to-End Recovery Validation
- Fast Restore to any Point-in-Time
- Resilient Ransomware Recovery

Minimal Impact Backups

- Incremental Forever
- Backup Processing Offloaded

Cloud-Scale Protection

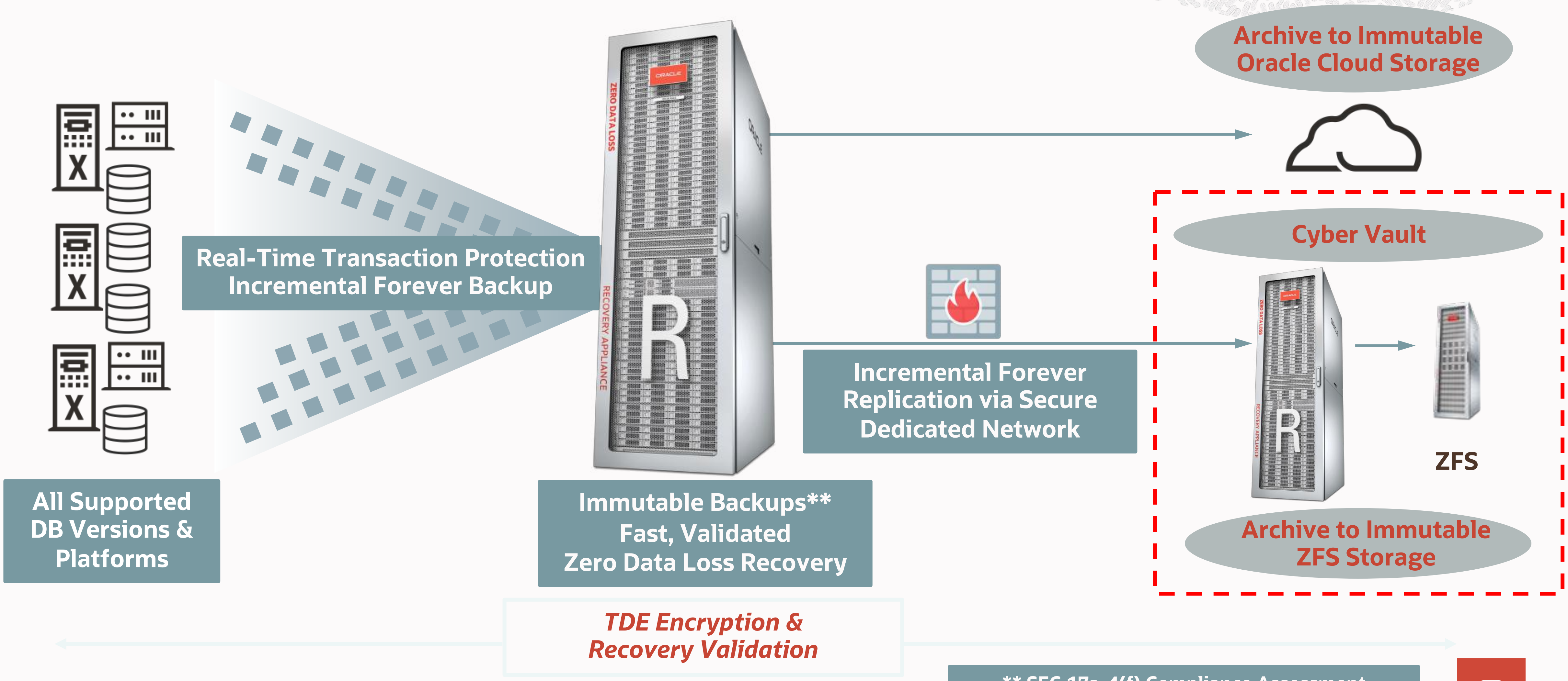
- Enterprise Scale-Out Platform
- Unlimited Cloud Archive Tier

2000+ PB Protected Databases

Leading Financial Services, Semiconductor, Insurance, Utilities Transportation, Manufacturing, and Government organizations

Recovery Appliance: Engineered for Cyber Resiliency

Transaction Protection + Resilient Recovery + Cyber Vault + Cloud Archive



Archive to Immutable Oracle Cloud Storage

Real-Time Transaction Protection
Incremental Forever Backup

Cyber Vault

Incremental Forever Replication via Secure Dedicated Network

ZFS

All Supported DB Versions & Platforms

Immutable Backups**
Fast, Validated
Zero Data Loss Recovery

Archive to Immutable ZFS Storage

TDE Encryption &
Recovery Validation

** SEC 17a-4(f) Compliance Assessment

How Oracle look at Database Security

Assess

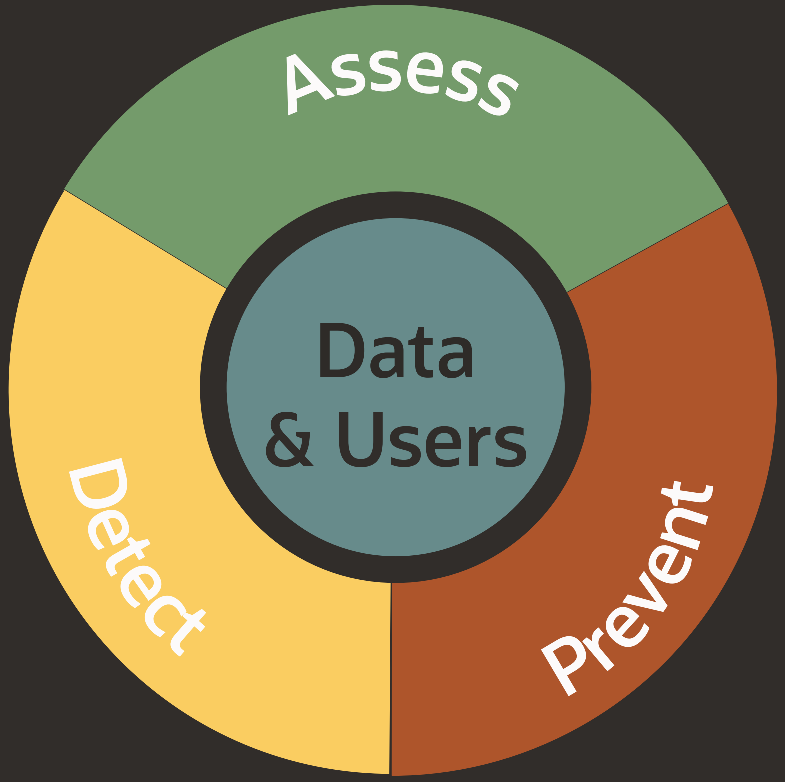
Assess the current state of security for the database

Detect

Detect attempts to access data, especially attempts that violate policy

Prevent

Prevent unauthorized or out-of-policy access to data



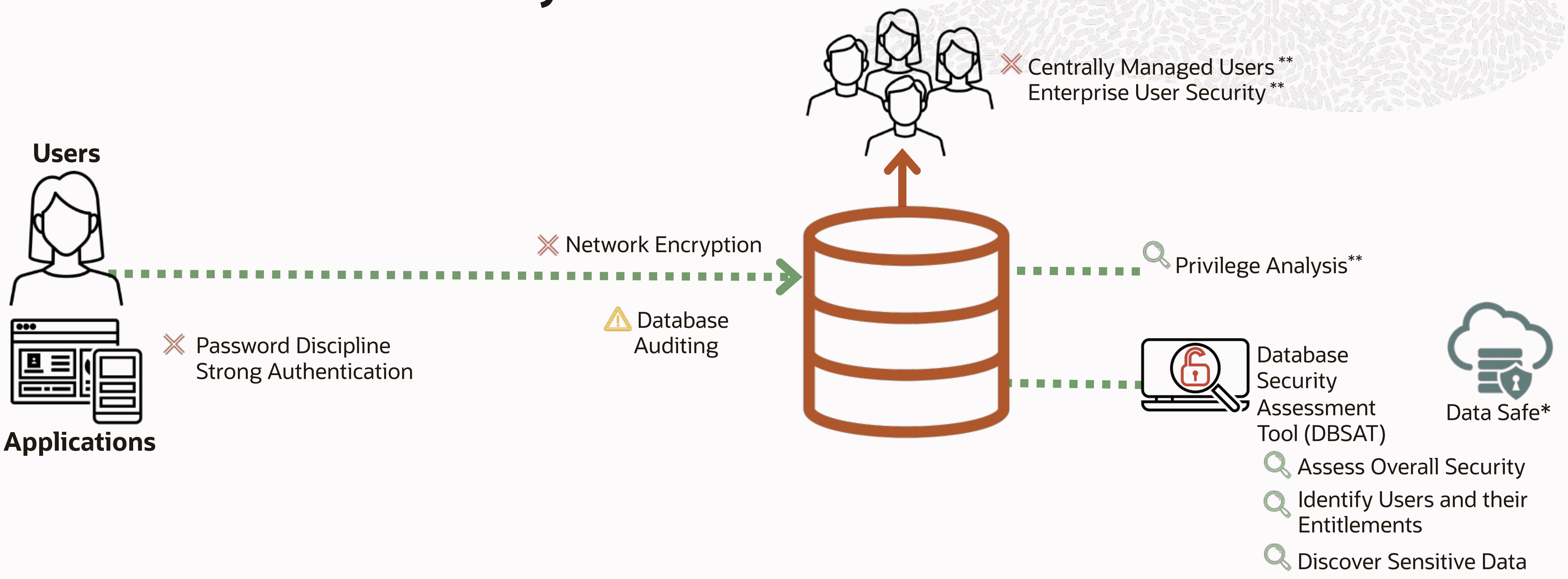
Data

Data stored in a database is your organization's most valuable asset, but also a source of significant risk.

Users

Users and applications connecting to your database are prime targets

Database Baseline Security



Users

Applications

✕ Password Discipline
Strong Authentication

✕ Network Encryption

⚠ Database
Auditing

✕ Centrally Managed Users**
Enterprise User Security**

Privilege Analysis**

Database
Security
Assessment
Tool (DBSAT)

Data Safe*

- Assess Overall Security
- Identify Users and their Entitlements
- Discover Sensitive Data

* Included with Database Cloud, additional cost on-premises
** Only available with Enterprise Edition

Key to Database Security Controls

Assess ✕ **Prevent** ⚠ **Detect**

Let DBSAT help assess your security profile

Understand how (in)secure is your database

- Database securely configured
- Identify privileged users and risks you carry
- Discover your sensitive data for regulations

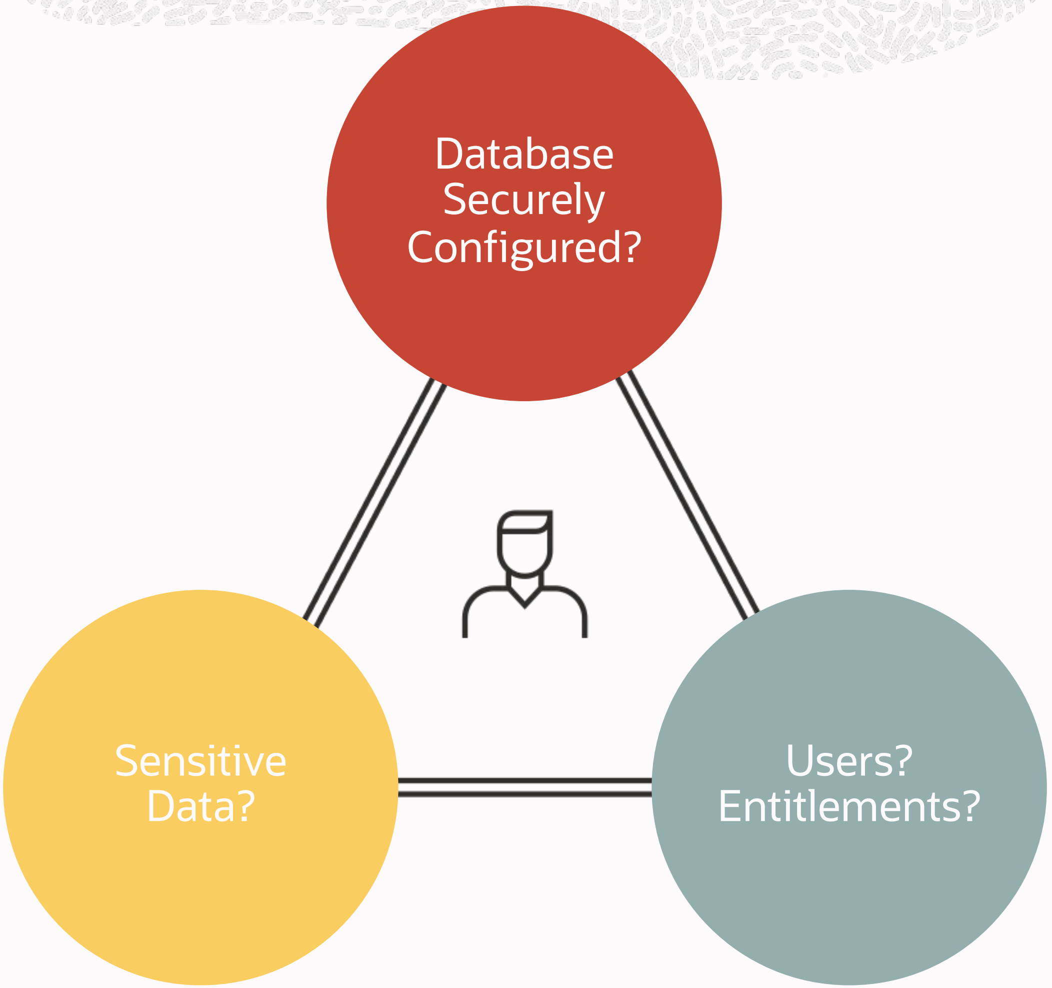
Actionable Reports

- Summary and detailed reports
- Prioritized recommendations
- CIS, STIG, GDPR findings

Analyze Oracle Database 11g and later

Stand-alone tool: Quick, Easy

FREE to current Oracle customers



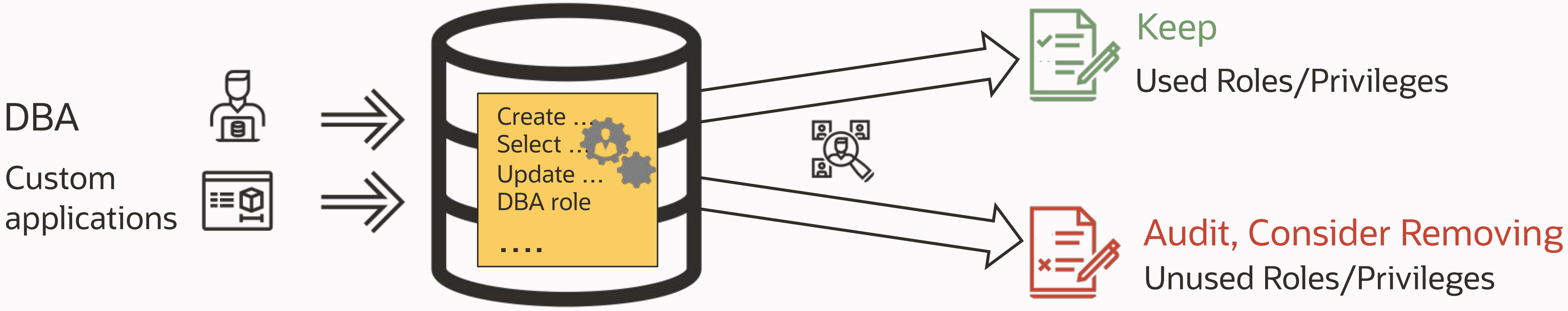
Easy to install and run

Download DBSAT 3.1 today from https://www.oracle.com/security/database-security/assessment-tool/

Collect security config data by running ‘dbsat collect’ on the target Run ‘dbsat report’ to generate security assessment report

Run ‘dbsat discover’ to generate sensitive data report

Privilege Analysis



Track privilege/role usage by a database user for a period of time

Identify and consider removing unused privileges

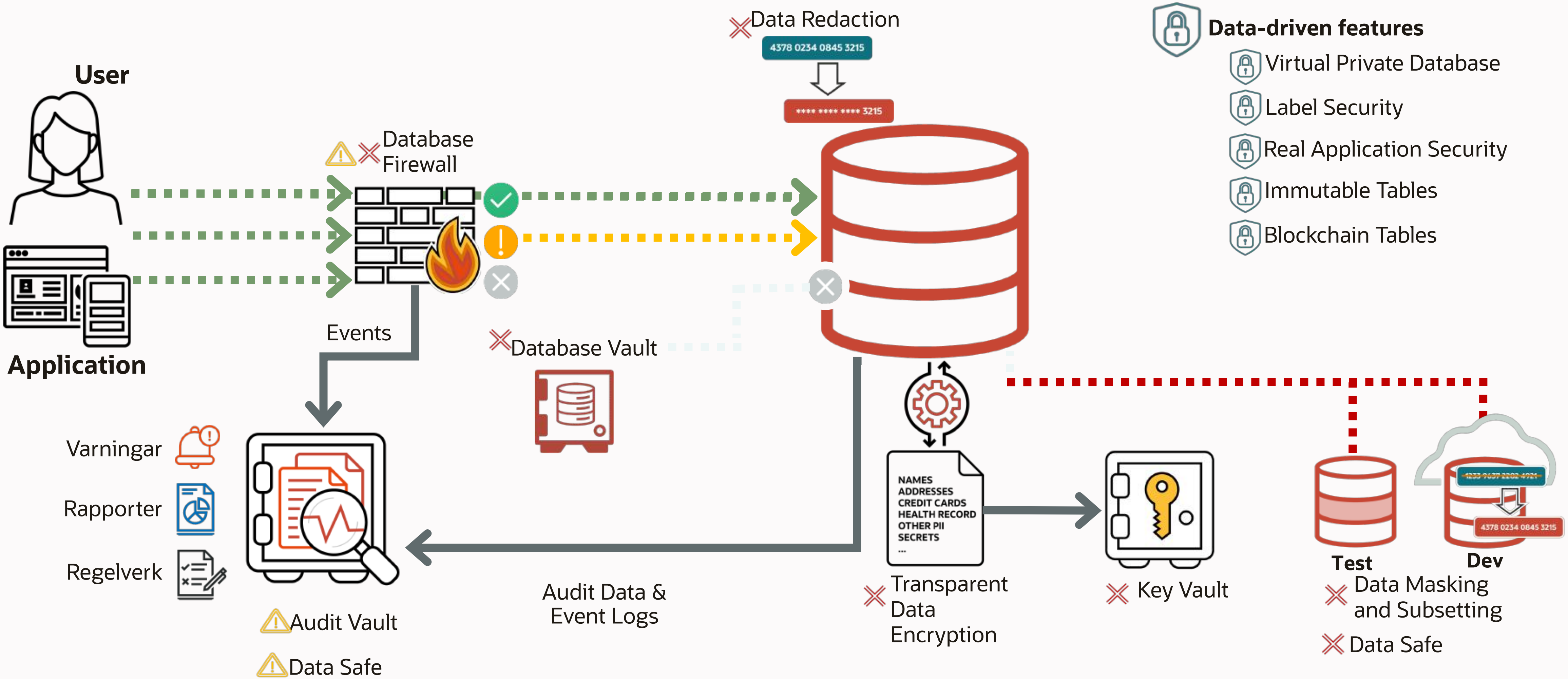
Minimal performance impact – processing done during report generation

Moved to core database in 2019. No dependency on Database Vault Licensing.

Maximum Security Architecture

Keys actions for database security

Access ✕ Prevent ⚠ Detect



User

Application

⚠ ✕ Database Firewall

Events

✕ Data Redaction

✕ Database Vault

Varningar

Rapporter

Regelverk

⚠ Audit Vault

⚠ Data Safe

Audit Data & Event Logs

✕ Transparent Data Encryption

✕ Key Vault

Test

Dev

✕ Data Masking and Subsetting

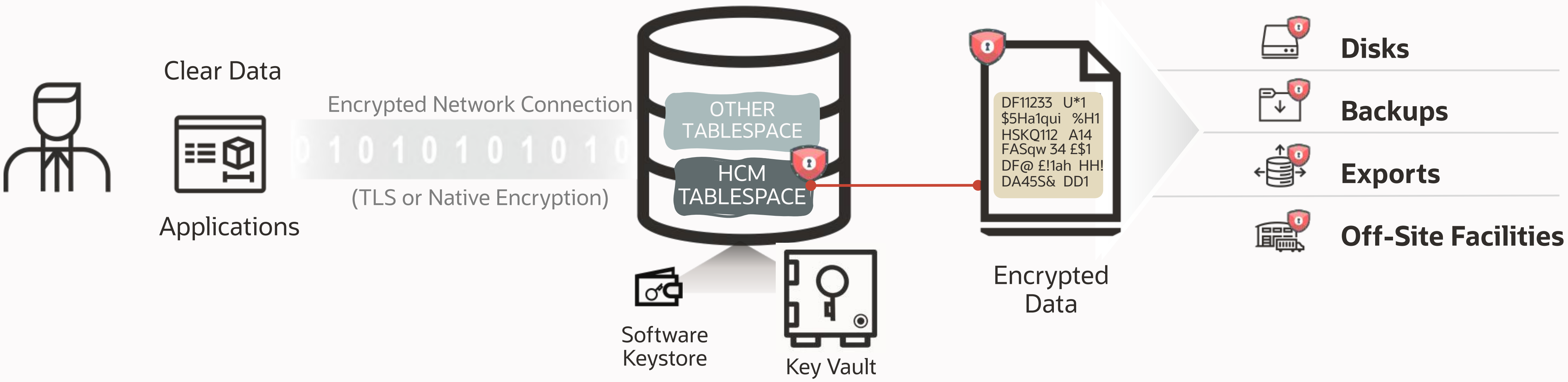
✕ Data Safe

Data-driven features

- Virtual Private Database
- Label Security
- Real Application Security
- Immutable Tables
- Blockchain Tables

Recommended Defense Against Database Exfiltration & Extortion

Oracle Transparent Data Encryption (TDE) and Oracle Key Vault



Encrypts entire application tablespaces or an application column

Protects the database files on disk and in backups

Integrated with the Oracle technology stack, no application changes required

Separate Key Vault server which removes the keys from the database server

Regulatory compliance for personal data (GDPR, CCPA), patient data (HIPAA), credit card data (PCI-DSS)

Additional ways of beating the odds for Ransomware on Oracle Databases

Known software vulnerabilities are a common vector

- Shorten your patch cycles to apply patches soon after release
- Consider using Autonomous Database, where patches are automatically applied very quickly after release

Most attacks target the Windows platform

- Consider running your database on Linux/Unix
- Consider running Exadata with a small installation footprint of Oracle Linux to reduce the attack surface

Limit and monitor access to the database

- Consider running Database Vault, Database Firewall and Audit Vault

Ransomware may not propagate to other data centers

- Consider having a Data Guard standby in another location/network

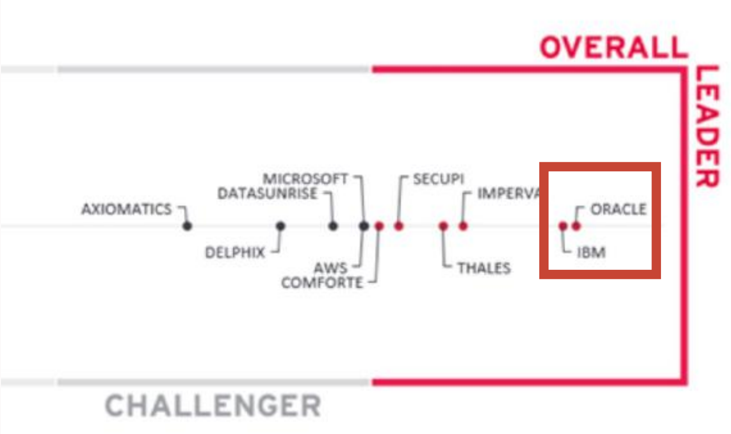
Most attacks encrypt the attached file system

- Consider Oracle ASM for storage. Because ASM is a raw file system it is difficult for malware to locate. Encrypting a raw file system AND providing a way to decrypt it is not trivial

Analysts Agree: Oracle #1

KuppingerCole Oracle #1

Overall for Database & Big Data security



Database+Big Data Security Leadership Compass, Q2 2023

https://blogs.oracle.com/datawarehousing/post/oracle-autonomous-database-named-a-leader-in-the-forrester-wave-cloud-data-warehouses-q2-2023

Forrester Oracle #1

“Security” criterion (4.5/5)

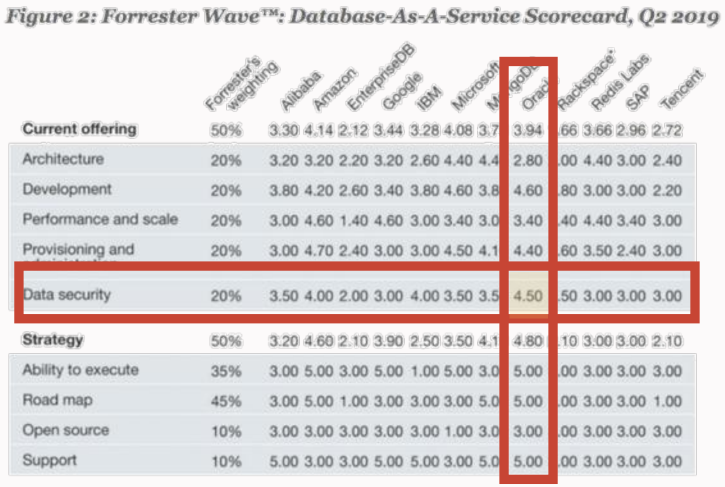


Figure 2: Forrester Wave™: Database-As-A-Service Scorecard, Q2 2019

	Forrester's weighting	Alibaba	Amazon	EnterpriseDB	Google	IBM	Microsof	MongoDB	Oracl	Rackspace*	Redis Labs	SAP	Tencent
Current offering	50%	3.30	4.14	2.12	3.44	3.28	4.08	3.7	3.94	.66	3.66	2.96	2.72
Architecture	20%	3.20	3.20	2.20	3.20	2.60	4.40	4.4	2.80	.00	4.40	3.00	2.40
Development	20%	3.80	4.20	2.60	3.40	3.80	4.60	3.8	4.60	.80	3.00	3.00	2.20
Performance and scale	20%	3.00	4.60	1.40	4.60	3.00	3.40	3.0	3.40	.40	4.40	3.40	3.00
Provisioning and	20%	3.00	4.70	2.40	3.00	3.00	4.50	4.1	4.40	.60	3.50	2.40	3.00
Data security	20%	3.50	4.00	2.00	3.00	4.00	3.50	3.5	4.50	.50	3.00	3.00	3.00
Strategy	50%	3.20	4.60	2.10	3.90	2.50	3.50	4.1	4.80	.10	3.00	3.00	2.10
Ability to execute	35%	3.00	5.00	3.00	5.00	1.00	5.00	3.0	5.00	.00	3.00	3.00	3.00
Road map	45%	3.00	5.00	1.00	3.00	3.00	3.00	5.0	5.00	.00	3.00	3.00	1.00
Open source	10%	3.00	3.00	3.00	3.00	3.00	1.00	3.0	3.00	.00	3.00	3.00	3.00
Support	10%	5.00	3.00	3.00	5.00	5.00	3.00	5.0	5.00	.00	3.00	3.00	3.00

Database-as-a-Service Wave, June 2019

https://go.oracle.com/LP=82715

Gartner Oracle #1

“Operational Use Cases” criterion

Critical Capabilities for Cloud DBMS, Dec. 2023

https://www.oracle.com/news/announcement/2023-gartner-cloud-database-management-systems-2024-01-16/

SQL Injection risk continues to be hacker's favorite choice

Top 10 OWASP Web Application Security Risks

1 Broken Access Control

2 Cryptographic Failures

3 SQL Injection

4 Insecure Design

5 Security Misconfiguration

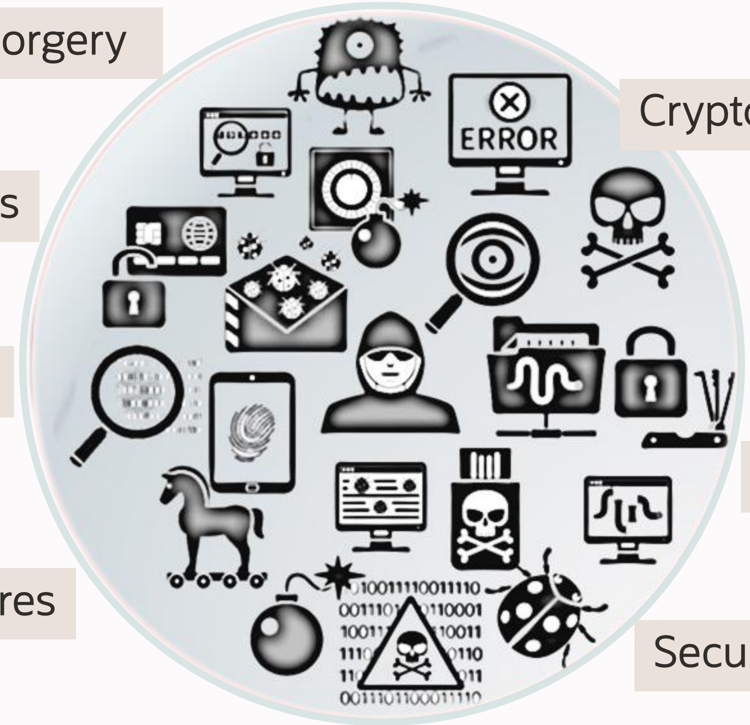
6 Vulnerable and Outdated Components

7 Identification and Authentication Failures

8 Software and Data Integrity Failures

9 Security Logging and Monitoring Failures

10 Server-Side Request Forgery

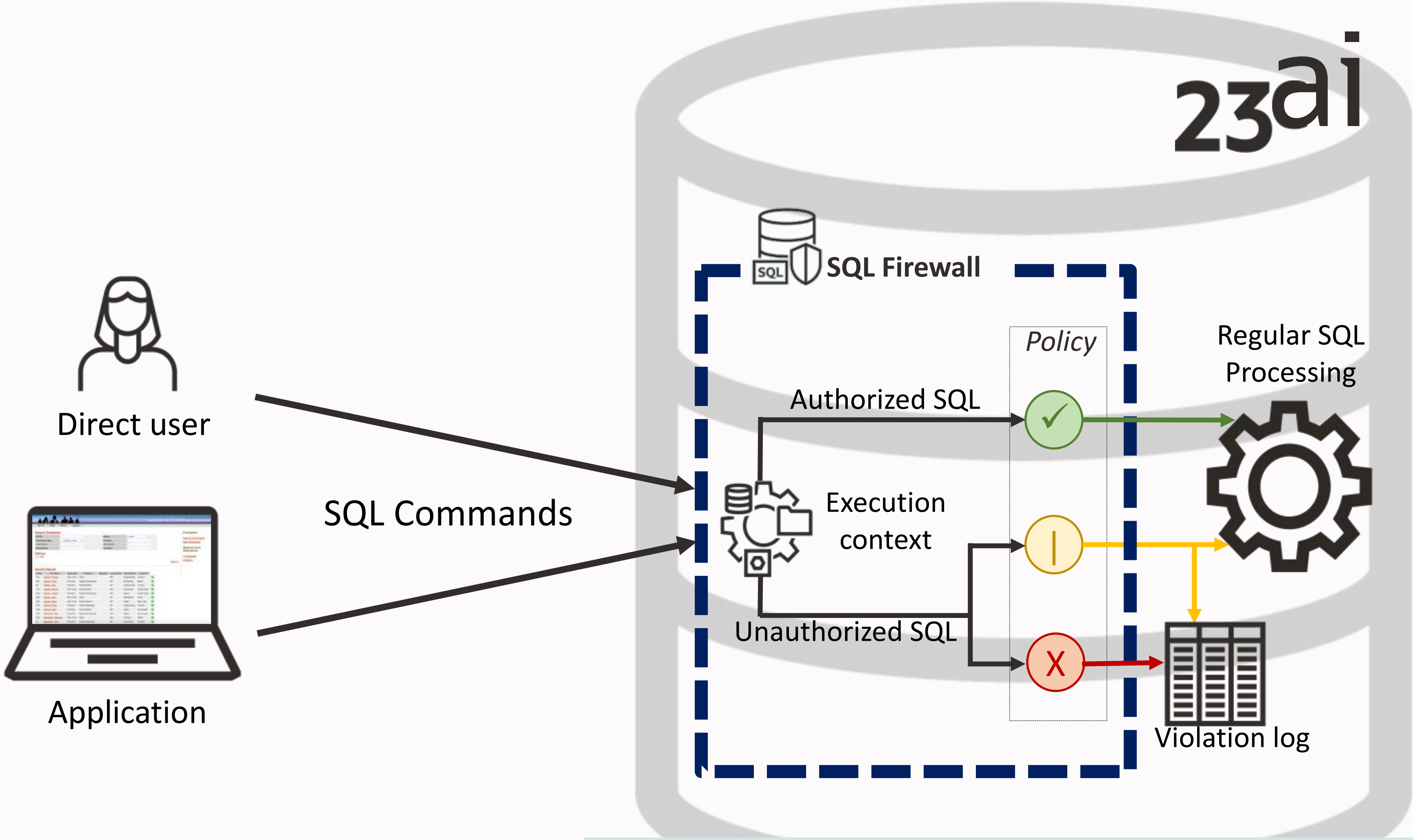


Top 3 most serious risk since 2017

Reference OWASP Top 10

SQL Injection remains the most common and dangerous database attack pattern for data-driven web applications!

Kernel-resident SQL Firewall (built into Oracle Database 23ai)



Key points to remember

- Strategically positioned
- Not possible to bypass
- No client-side configuration changes
- Quicker deployment
- Scales easily across your database estate
- Visibility into ALL SQL traffic regardless of origin

Available for Oracle Database Enterprise Edition (version 23ai and later)

SQL Firewall – Protect from SQL injection and unauthorized access

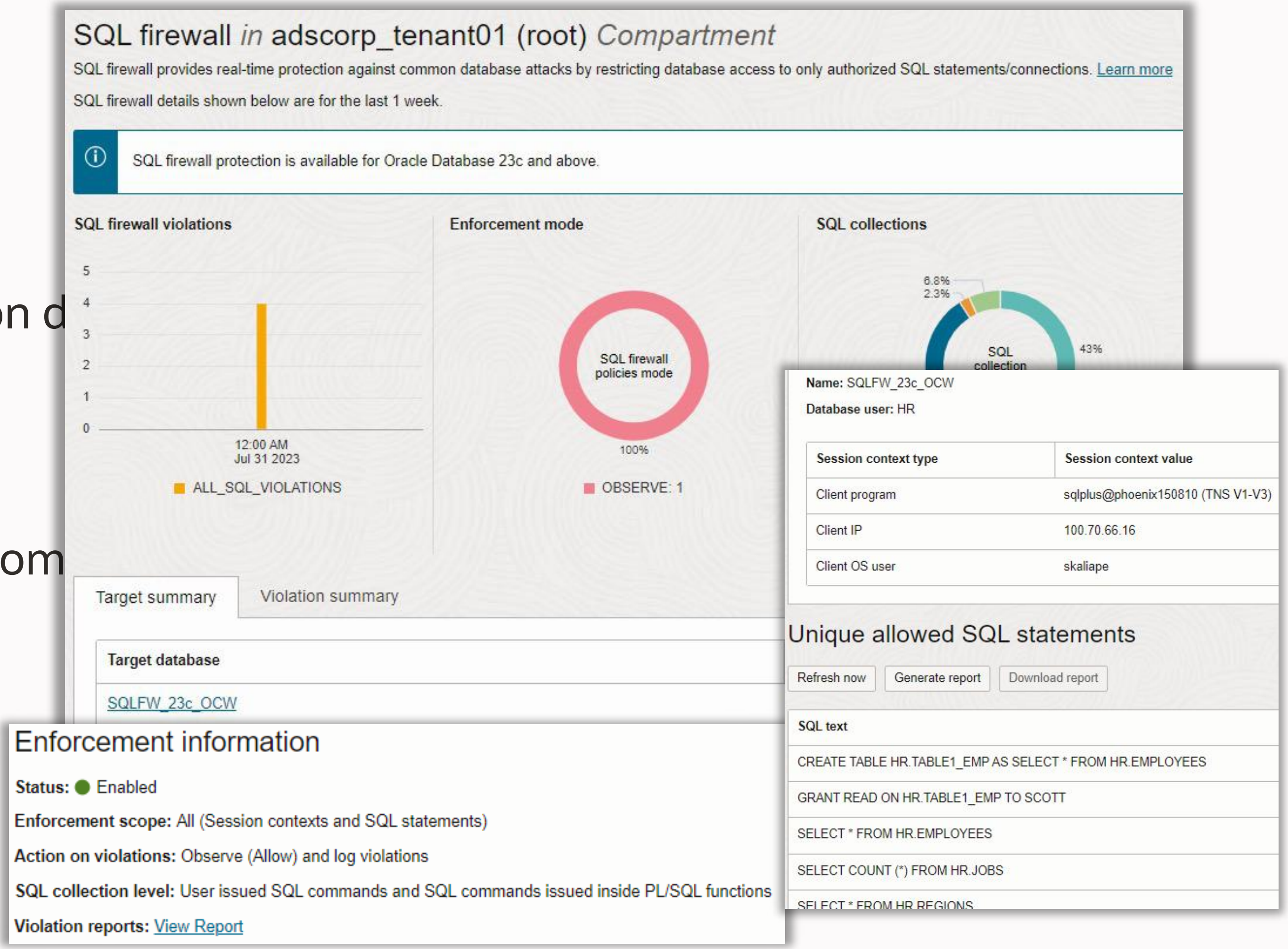
Provides real-time protection against common d

- authorized connections
- authorized SQL statements

Block or monitor any violations

Mitigates risks from SQL injection attacks, anom

Available for 23ai databases only



SQL firewall *in* adscorp_tenant01 (root) *Compartment*

SQL firewall provides real-time protection against common database attacks by restricting database access to only authorized SQL statements/connections. Learn more

SQL firewall details shown below are for the last 1 week.

ⓘ SQL firewall protection is available for Oracle Database 23c and above.

Name: SQLFW_23c_OCW

Database user: HR

Session context type	Session context value
Client program	sqlplus@phoenix150810 (TNS V1-V3)
Client IP	100.70.66.16
Client OS user	skaliape

Unique allowed SQL statements

SQL text
CREATE TABLE HR.TABLE1_EMP AS SELECT * FROM HR.EMPLOYEES
GRANT READ ON HR.TABLE1_EMP TO SCOTT
SELECT * FROM HR.EMPLOYEES
SELECT COUNT (*) FROM HR.JOBS
SELECT * FROM HR.REGIONS

Enforcement information

Status: ● Enabled

Enforcement scope: All (Session contexts and SQL statements)

Action on violations: Observe (Allow) and log violations

SQL collection level: User issued SQL commands and SQL commands issued inside PL/SQL functions

Violation reports: View Report

Oracle database security helps protect against attacks

Built-in capabilities and cloud-native services

Attack

Configuration drift

Lateral movement and data access

Data theft

Compromised backups from ransomware

Limit attack spread

Identity and Access Management (IAM)

Seamless identity integration with OCI IAM helps decrease the risk of attacks with multi-factor authentication and role-based access control

Data Safe / DB SAT

Continuously assess your configuration and users with Data Safe and database security assessment tool

Audit Vault Database Firewall (AVDF)

Detect suspicious activity with Audit Vault and Database Firewall (AVDF)

Advanced Security and Key Vault

Encrypt the data and protect encryption keys with Advanced Security and Key Vault

Zero Data Loss services

Recover up to the last transaction with immutable backups ZDLRA (zero data lose recovery appliance) and ZFS

Isolated network virtualization

Separates virtualization layer from the network layer to protect customer instances

Database security product portfolio

ORACLE
Advanced Security

ORACLE
Key Vault

ORACLE
Database Vault

ORACLE
Data Masking
and Subsetting

ORACLE
Audit Vault and
Database Firewall

ORACLE
Label Security

Try Everything...for FREE

free-oracle.github.io

cloud.oracle.com/free

bit.ly/ADB_free

developer.oracle.com/livelabs

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

Learn more

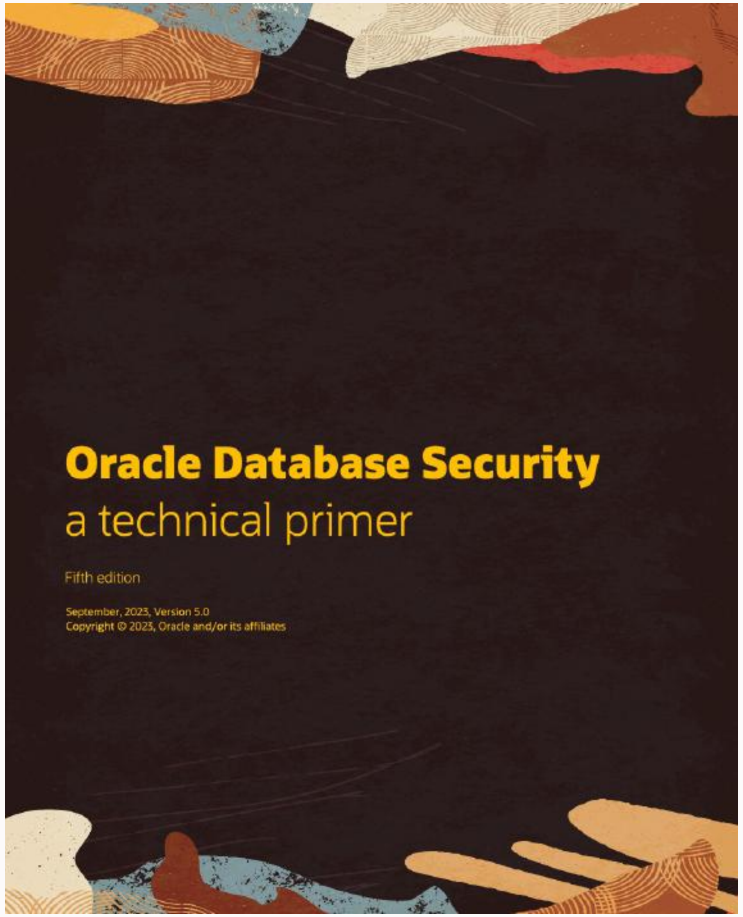
OTN: www.oracle.com/database/technologies/security.html

Blog: http://blogs.oracle.com/cloudsecurity/db-sec

NEW: eBook 5th Edition: https://download.oracle.com/database/oracle-database-security-primer.pdf

Oracle LiveLabs - Try it yourself:

- DBSAT: https://bit.ly/3w1wwVy
- All Database Security: https://bit.ly/3tTZ6XQ



Oracle Database Security

a technical primer

Fifth edition

September, 2023, Version 5.0
Copyright © 2023, Oracle and/or its affiliates

Additional Resources

Oracle Database Security

- https://www.oracle.com/security/database-security/

Oracle Live Labs

- https://apexapps.oracle.com/pls/apex/dbpm/r/livelabs/livelabs-workshop-cards?p100_focus_area=43

Oracle Exadata Database Machine - Maximum Security Architecture

- https://www.oracle.com/a/tech/docs/exadata-maximum-security-architecture.pdf

Recovery Appliance Product Central

- https://www.oracle.com/engineered-systems/zero-data-loss-recovery-appliance/

Database Cyber-Attack Protection with Zero Data Loss Recovery Appliance (blog)

- https://tinyurl.com/zdlracyberblog

Maximum Availability Architecture (MAA) Blogs

- https://blogs.oracle.com/maa/

Maximum Availability Architecture (MAA) Website

- https://www.oracle.com/database/technologies/high-availability/maa.html

Q & A

Thank you

Bruno Reis

Bruno.reis.da.silva@oracle.com

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

ORACLE