AOUG
Anwenderkonferenz 2024

Secure your data: Security is no longer only for experts

Protecting your most valuable assets from ransomware

Bruno Reis da Silva

- 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 as Oracle DBA at companies such as IBM and Playtech.
- Technology Software Account Engineer at Oracle.
- First Oracle ACE associate in Hungary and second Oracle ACE Sweden.

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 is an evolving threat

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

"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."

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

2022

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

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)

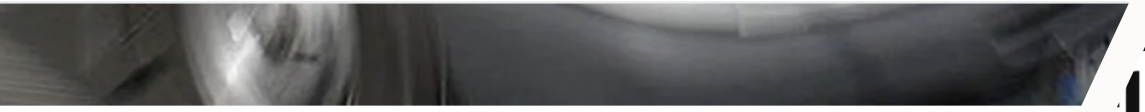
Image: Joel de Vriend via Unsplash/Photomosh

Funerals reportedly canceled due to ransomware attack on Austrian town

The municipality of Korneuburg in Austria said it was hit by a ransomware attack, leading to funerals reportedly being canceled and the town hall informing residents its staff can only be reached via telephone.

BBC

News Sport Business Innovation Culture Travel Earth Video L



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

mergency hospitals were among those hit, with ot
aution.

Ma ,03 mil ataques de os últimos 12 meses

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

AD >

lemadrid sufre un a emisión se cae du

La radio, aunque con problem
aún continúan sufriendo los e

ıl tentativas de ataques de ransomware no decorrer dos últimos 12 mese
.iderança com folga entre os mais atacados na América Latina e na qua
global, segundo o último relatório da Kaspersky, apresentado nesta segur
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

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

s been dealing with a wide-ranging cybe
ctor of the Emergency Management (OEM
ecorded 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

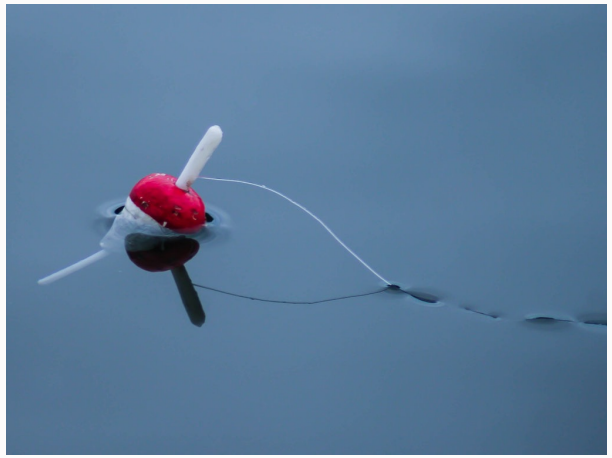
isdag 23 april kl 21.05

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

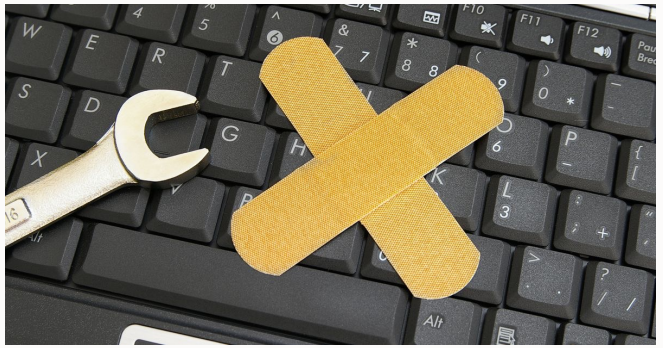
era av Systembolagets varor riskerar att sälja slut inför helgen till följd av problem
Aftonbladet tidigare rapporterat.

“Security is no longer only for experts”

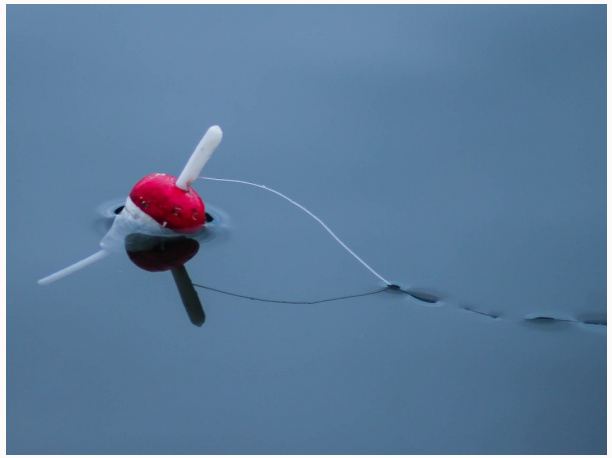
Ransomware Attack Vectors



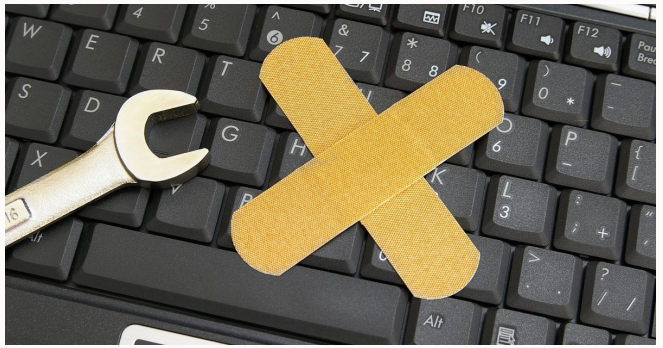
- **Phishing**
- Watering hole sites
- Fuzzed URLs for common services
- Unpatched systems
- Open Remote Desktop Protocol
- Compromised accounts



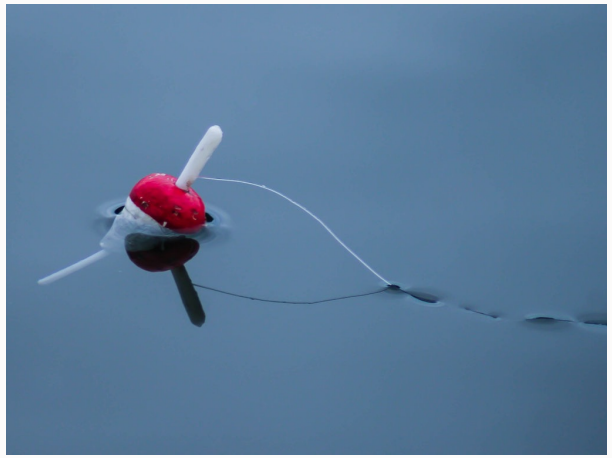
Ransomware Attack Vectors



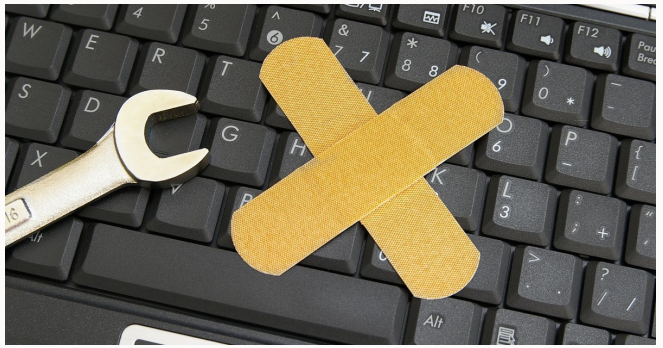
- Phishing
- **Watering hole sites**
- Fuzzed URLs for common services
- Unpatched systems
- Open Remote Desktop Protocol
- Compromised accounts



Ransomware Attack Vectors



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



DEMO

Fuzzed URLs for common services - EXAMPLE

jupyter Austrian_Oracle_User_Group_2024 Last Checkpoint: Yesterday at 11:52 AM (autosaved) Logout

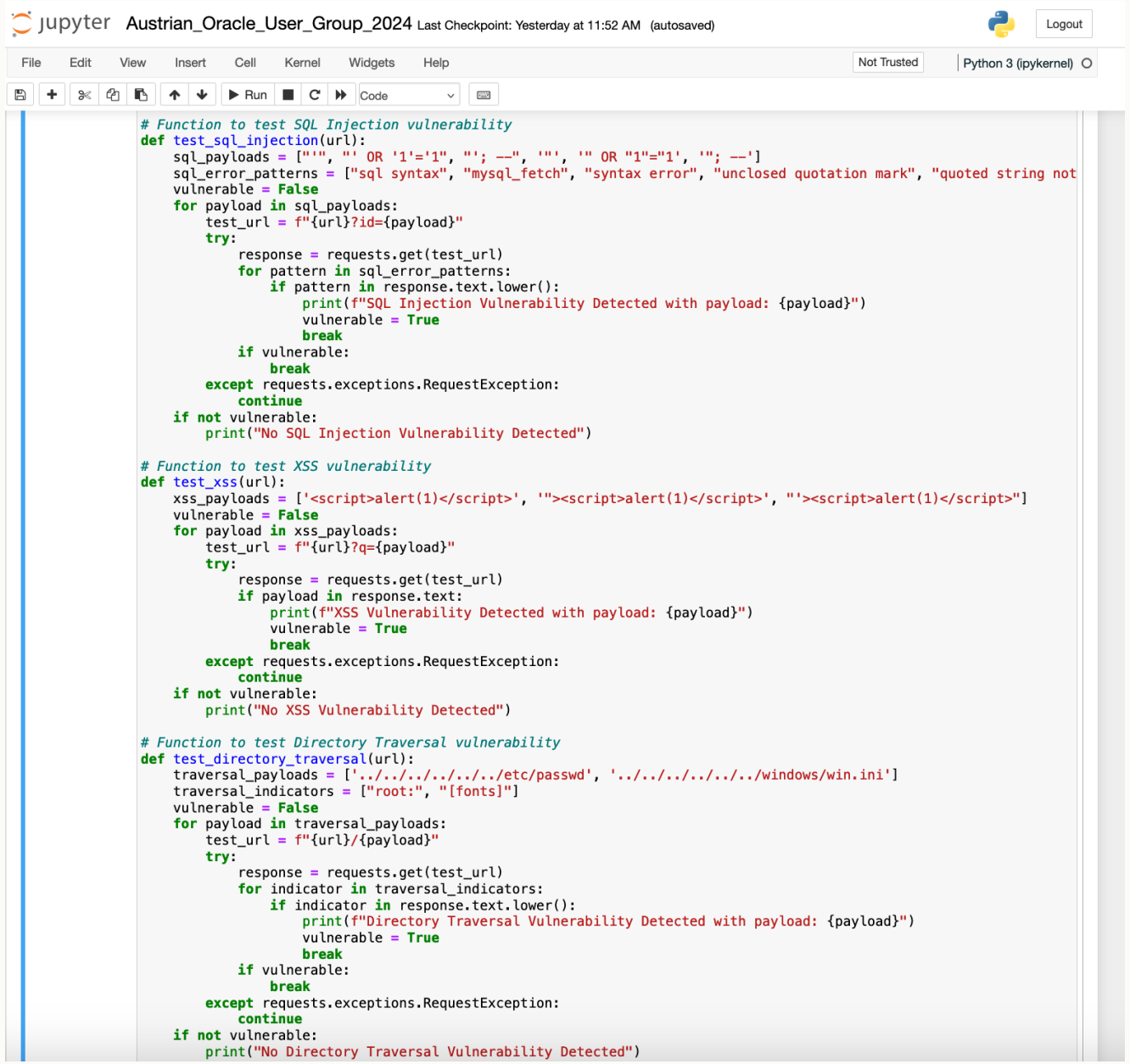
File Edit View Insert Cell Kernel Widgets Help Not Trusted Python 3 (ipykernel)

Run Code

In [ ]:

```
# Import necessary libraries
import requests
from pprint import pprint

# Function to check the status of a given URL and handle 200 responses
def check_url_status(url):
    try:
        response = requests.get(url)
        if response.status_code == 200:
            print(f"\nURL: {url} - Status Code: 200 (OK)")
            # Print additional details
            print("Headers:")
            headers = dict(response.headers)
            pprint(headers)
            print(f"Content Length: {len(response.content)} bytes")
            print(f"Content Type: {headers.get('Content-Type', 'Unknown')}")

            # Print a larger snippet of the content or handle as needed
            content_snippet = response.text[:1000]  # Print first 1000 characters of content
            print("Content Snippet:")
            print(content_snippet)

            # Basic vulnerability checks
            check_for_vulnerabilities(url, headers, response.text)
        else:
            print(f"\nURL: {url} - Status Code: {response.status_code}")
    except requests.exceptions.RequestException as e:
        print(f"\nURL: {url} - Exception: {e}")

# Function to perform basic vulnerability checks
def check_for_vulnerabilities(url, headers, content):
    print("\nPotential Vulnerabilities:")

    # Check for missing security headers
    security_headers = ['Content-Security-Policy', 'Strict-Transport-Security', 'X-Content-Type-Options', 'X-Frame-O
    missing_headers = [header for header in security_headers if header not in headers]
    if missing_headers:
        print(f"Missing Security Headers: {missing_headers}")

    # Check for server and technology disclosures
    if 'Server' in headers:
        print(f"Server Disclosure: {headers['Server']}")
    if 'X-Powered-By' in headers:
        print(f"Technology Disclosure (X-Powered-By): {headers['X-Powered-By']}")

    # Check for SQL Injection vulnerability
    test_sql_injection(url)

    # Check for XSS vulnerability
    test_xss(url)

    # Check for Directory Traversal vulnerability
    test_directory_traversal(url)
```

Fuzzed URLs for common services - EXAMPLE

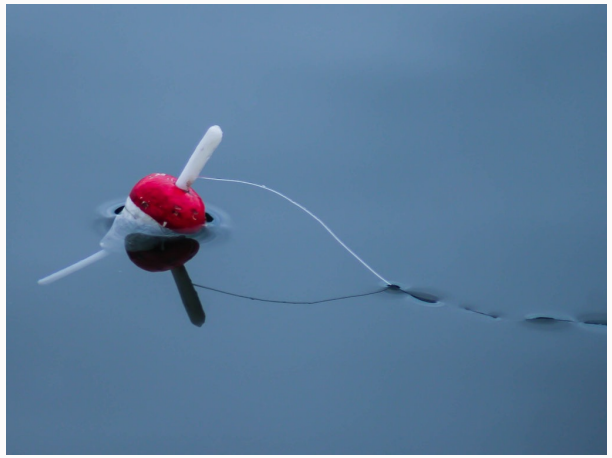



```python
# Function to test SQL Injection vulnerability
def test_sql_injection(url):
    sql_payloads = ["'", "' OR '1'='1", "'; --", '"', '" OR "1"="1', '"; --']
    sql_error_patterns = ["sql syntax", "mysql_fetch", "syntax error", "unclosed quotation mark", "quoted string not
    vulnerable = False
    for payload in sql_payloads:
        test_url = f"{url}?id={payload}"
        try:
            response = requests.get(test_url)
            for pattern in sql_error_patterns:
                if pattern in response.text.lower():
                    print(f"SQL Injection Vulnerability Detected with payload: {payload}")
                    vulnerable = True
                    break
            if vulnerable:
                break
        except requests.exceptions.RequestException:
            continue
    if not vulnerable:
        print("No SQL Injection Vulnerability Detected")

# Function to test XSS vulnerability
def test_xss(url):
    xss_payloads = ['<script>alert(1)</script>', '"><script>alert(1)</script>', "'><script>alert(1)</script>"]
    vulnerable = False
    for payload in xss_payloads:
        test_url = f"{url}?q={payload}"
        try:
            response = requests.get(test_url)
            if payload in response.text:
                print(f"XSS Vulnerability Detected with payload: {payload}")
                vulnerable = True
                break
        except requests.exceptions.RequestException:
            continue
    if not vulnerable:
        print("No XSS Vulnerability Detected")

# Function to test Directory Traversal vulnerability
def test_directory_traversal(url):
    traversal_payloads = ['../../../../../../etc/passwd', '../../../../../../windows/win.ini']
    traversal_indicators = ["root:", "[fonts]"]
    vulnerable = False
    for payload in traversal_payloads:
        test_url = f"{url}/{payload}"
        try:
            response = requests.get(test_url)
            for indicator in traversal_indicators:
                if indicator in response.text.lower():
                    print(f"Directory Traversal Vulnerability Detected with payload: {payload}")
                    vulnerable = True
                    break
            if vulnerable:
                break
        except requests.exceptions.RequestException:
            continue
    if not vulnerable:
        print("No Directory Traversal Vulnerability Detected")
```

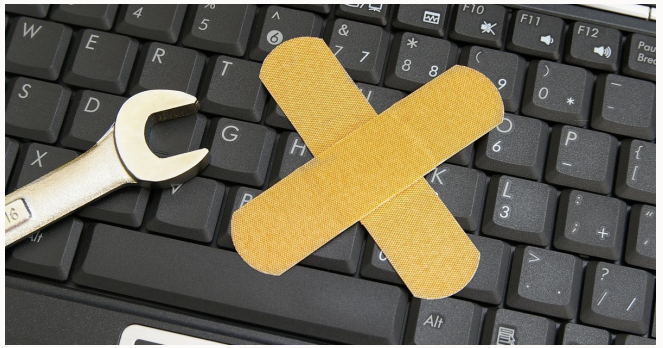
Fuzzed URLs for common services - EXAMPLE

```
# List of URLs to check
common_services = [
    "https://martinhistory.home.blog/2019/09/30/database-and-word-cloud/",
    "https://www.enterprisedb.com/postgres-tutorials/how-deploy-wordpress-highly-available-postgresql",
    "https://medium.com/@shoaibhassan_/install-wordpress-with-postgresql-using-apache-in-5-min-a26078d496fb",
    "https://themeforest.net/item/cuisine-wordpress-blog-recipe-theme/20095034",
    "https://arpegi.wordpress.com/"
]

# Check the status of each URL
for service in common_services:
    check_url_status(service)
```

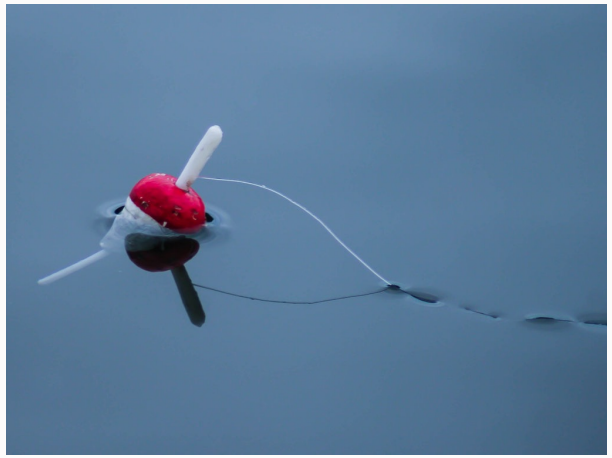
Ransomware Attack Vectors



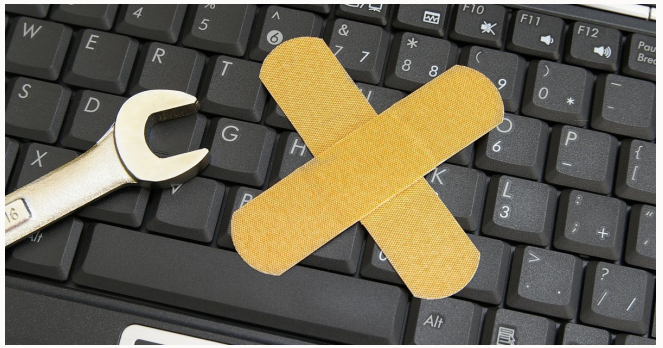
- Phishing
- Watering hole sites
- Fuzzed URLs for common services
- **Unpatched systems**
- Open Remote Desktop Protocol
- Compromised accounts



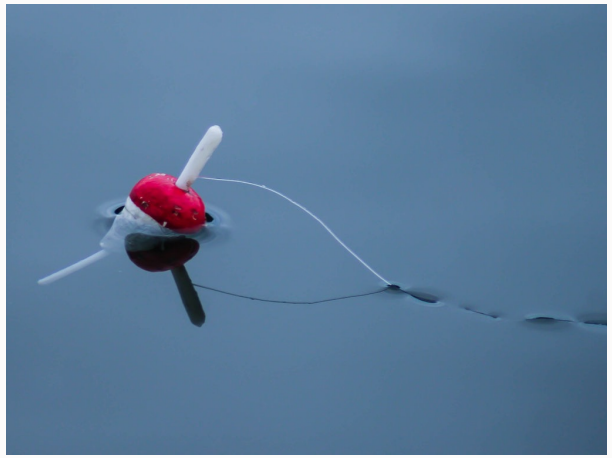
Ransomware Attack Vectors



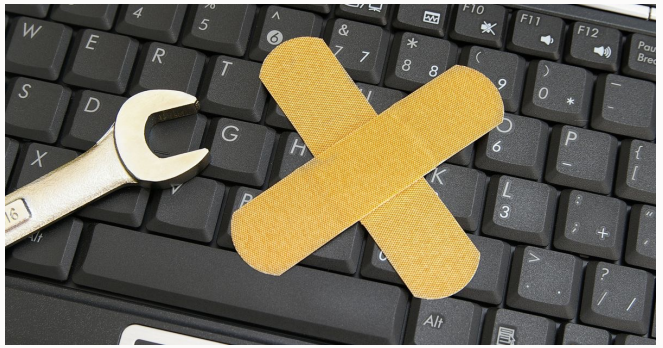
- Phishing
- Watering hole sites
- Fuzzed URLs for common services
- Unpatched systems
- **Open Remote Desktop Protocol**
- Compromised accounts



Ransomware Attack Vectors



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



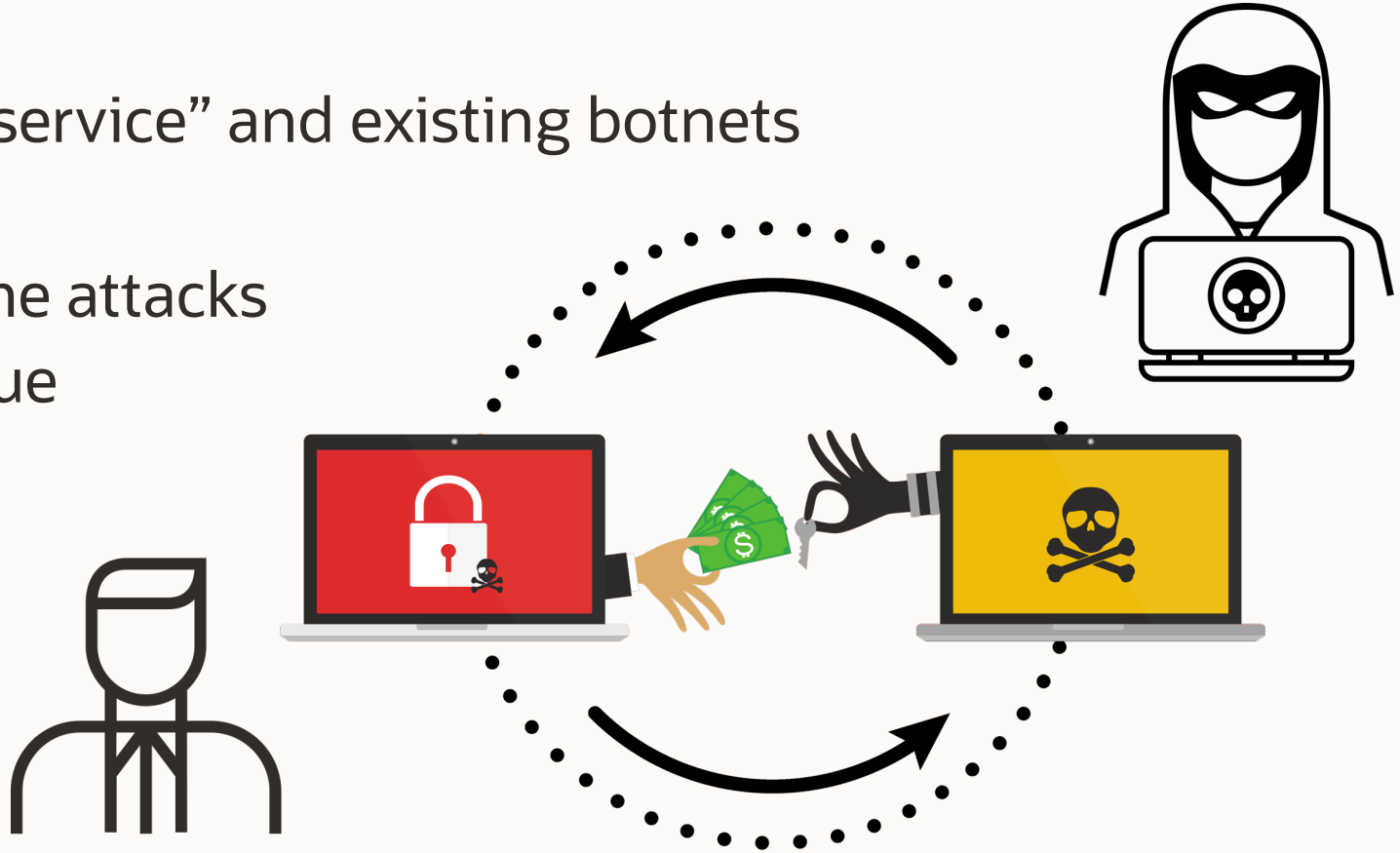
Anatomy of a Ransomware Attack

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 Attack Breakdown

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

Request ransom payment

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

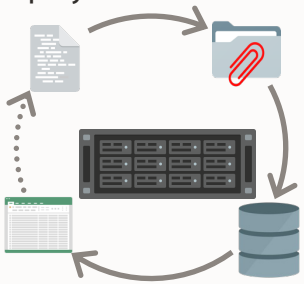
Attack Vectors : credential harvesting/stealing, phishing email, fake advertising and software upgrade

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.



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

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

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

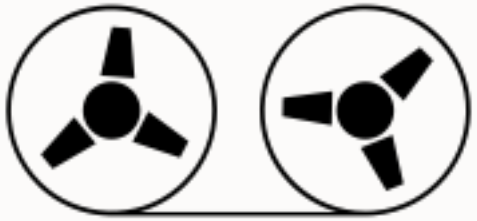
- Rebuild your systems from backup

Recommended Defense Against Database Destruction

Immutable offline backup

Good

Offline backup to storage media like magnetic tape

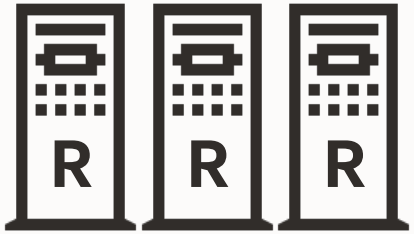


Better

Oracle Database Cloud Backup Service

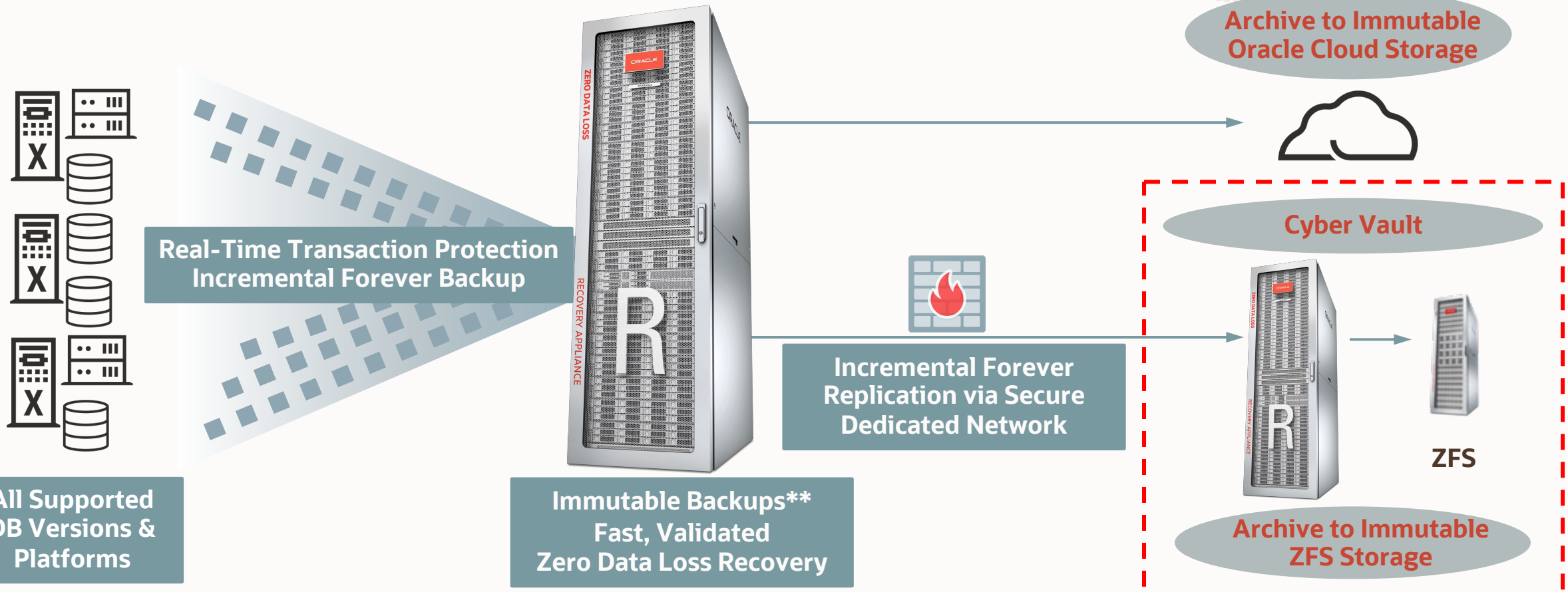
Best

Zero Data Loss Recovery Appliance



Recovery Appliance: Engineered for Cyber Resiliency

Transaction Protection + Resilient Recovery + Cyber Vault + Cloud Archive

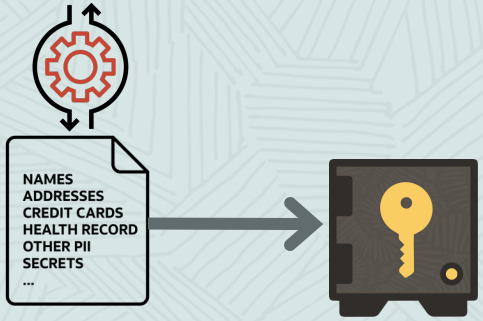


How do you protect the database?

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

How Oracle look at Database Security

Assess

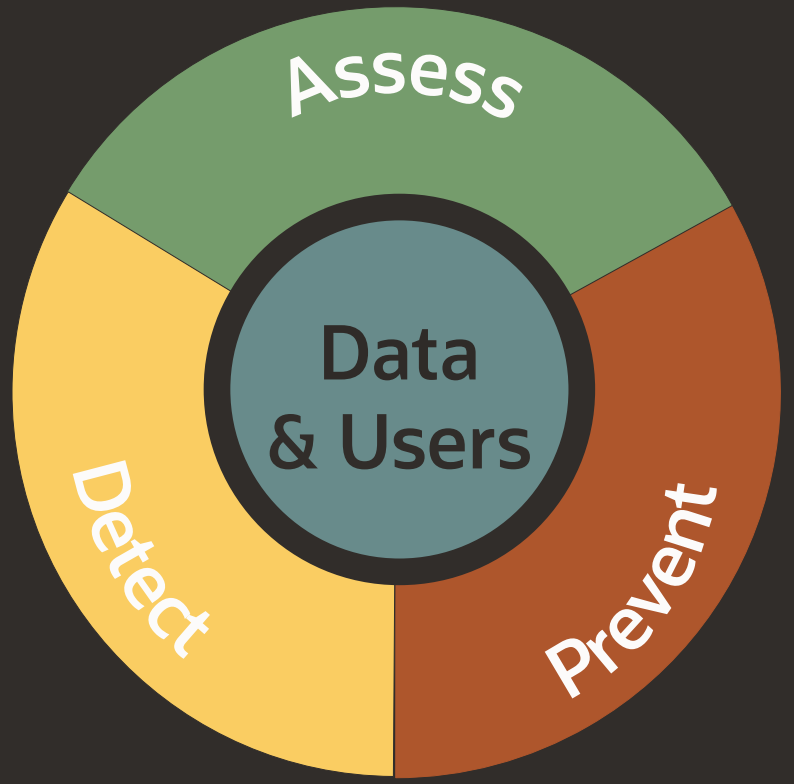
Assess the current state of security for the database

Detect

Detect attempts to access data, especially attempts that violate policy

Prevent

Prevent unauthorized or out-of-policy access to data



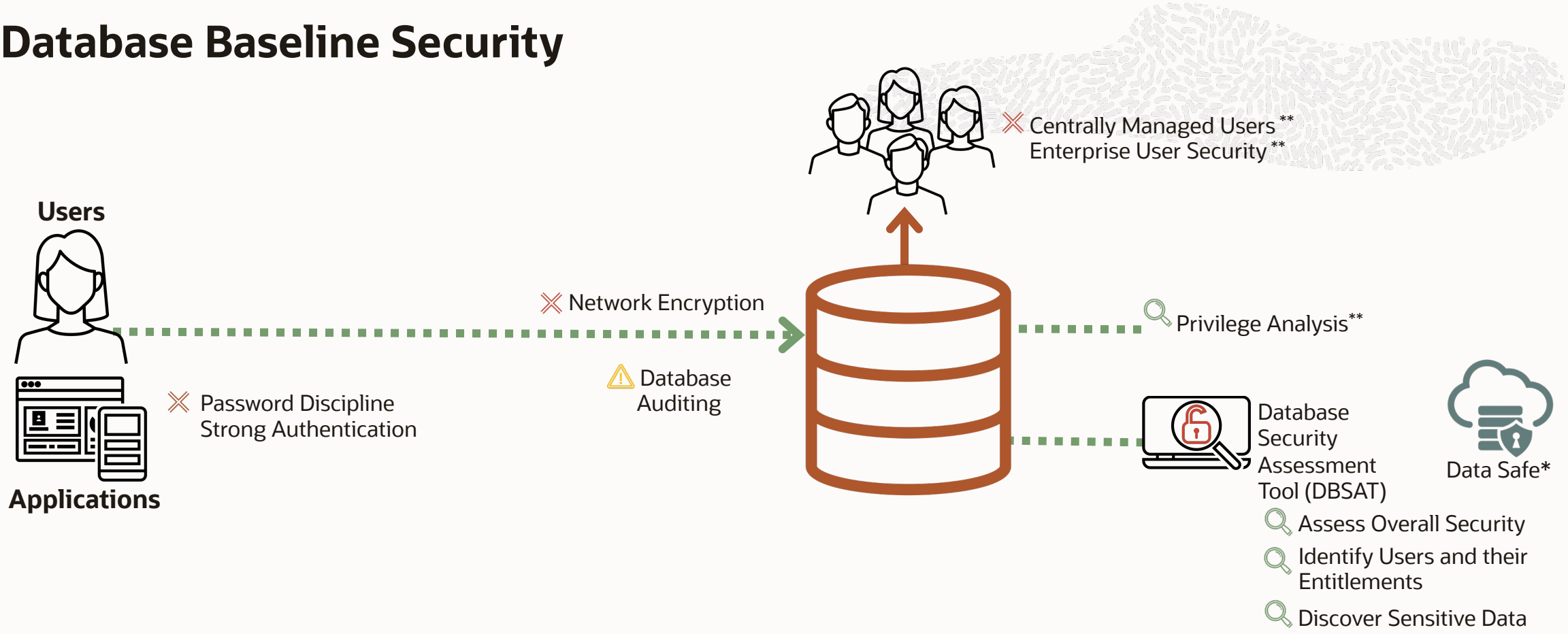
Data

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



* 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

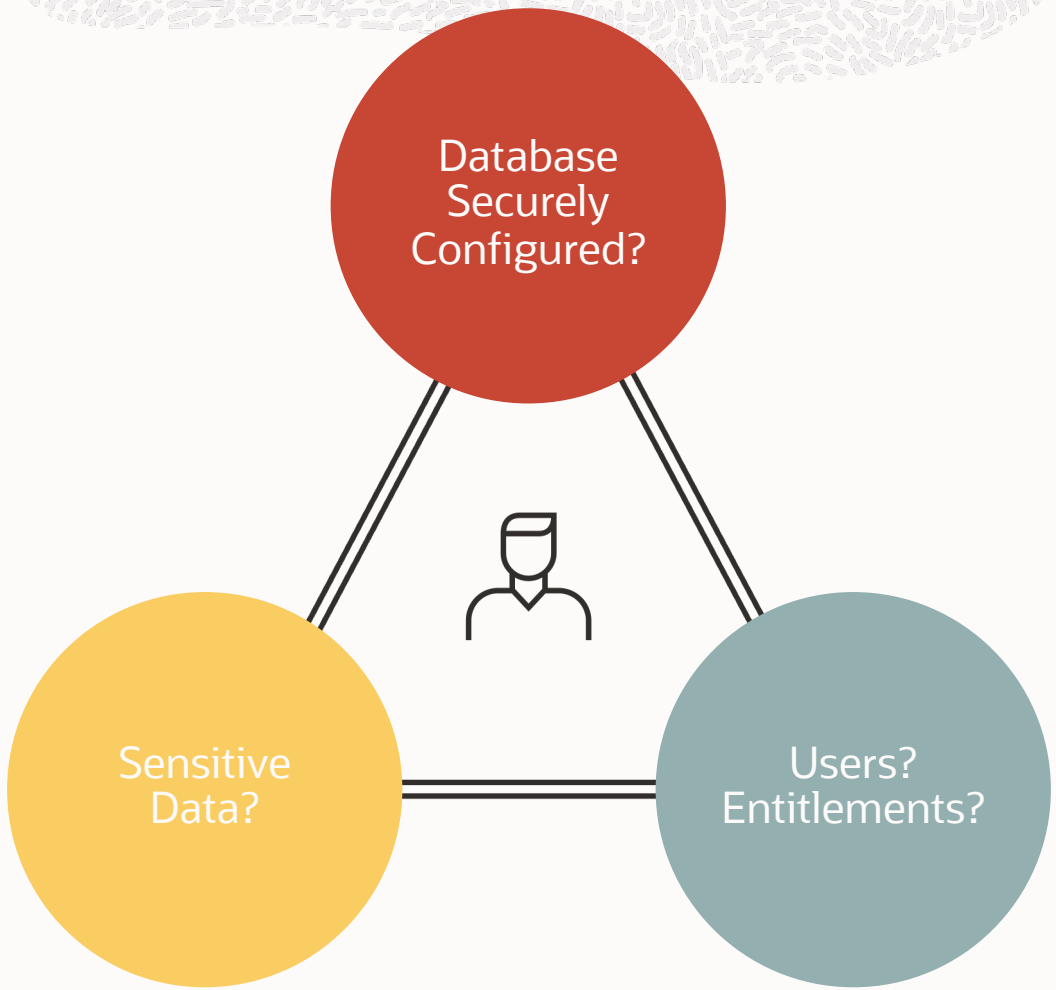
Actionable Reports

- 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



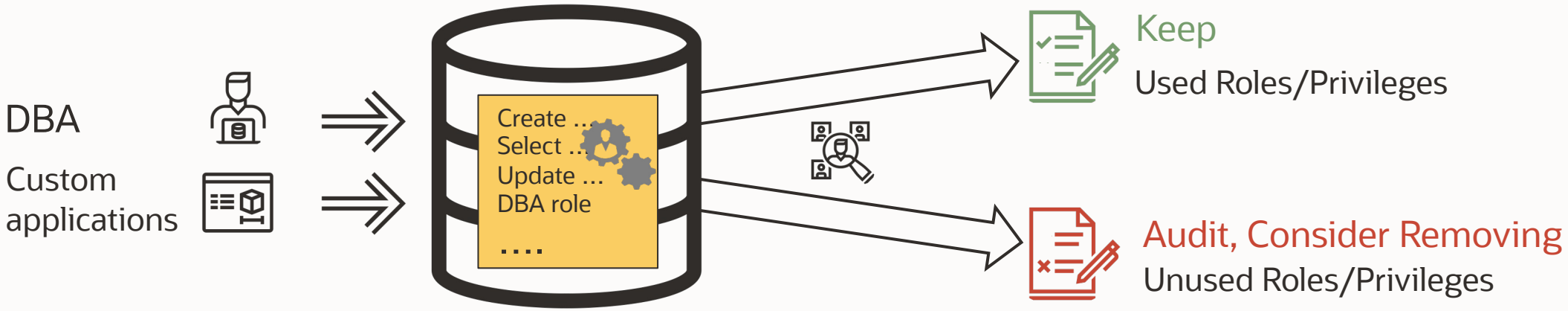
Easy to install and run

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



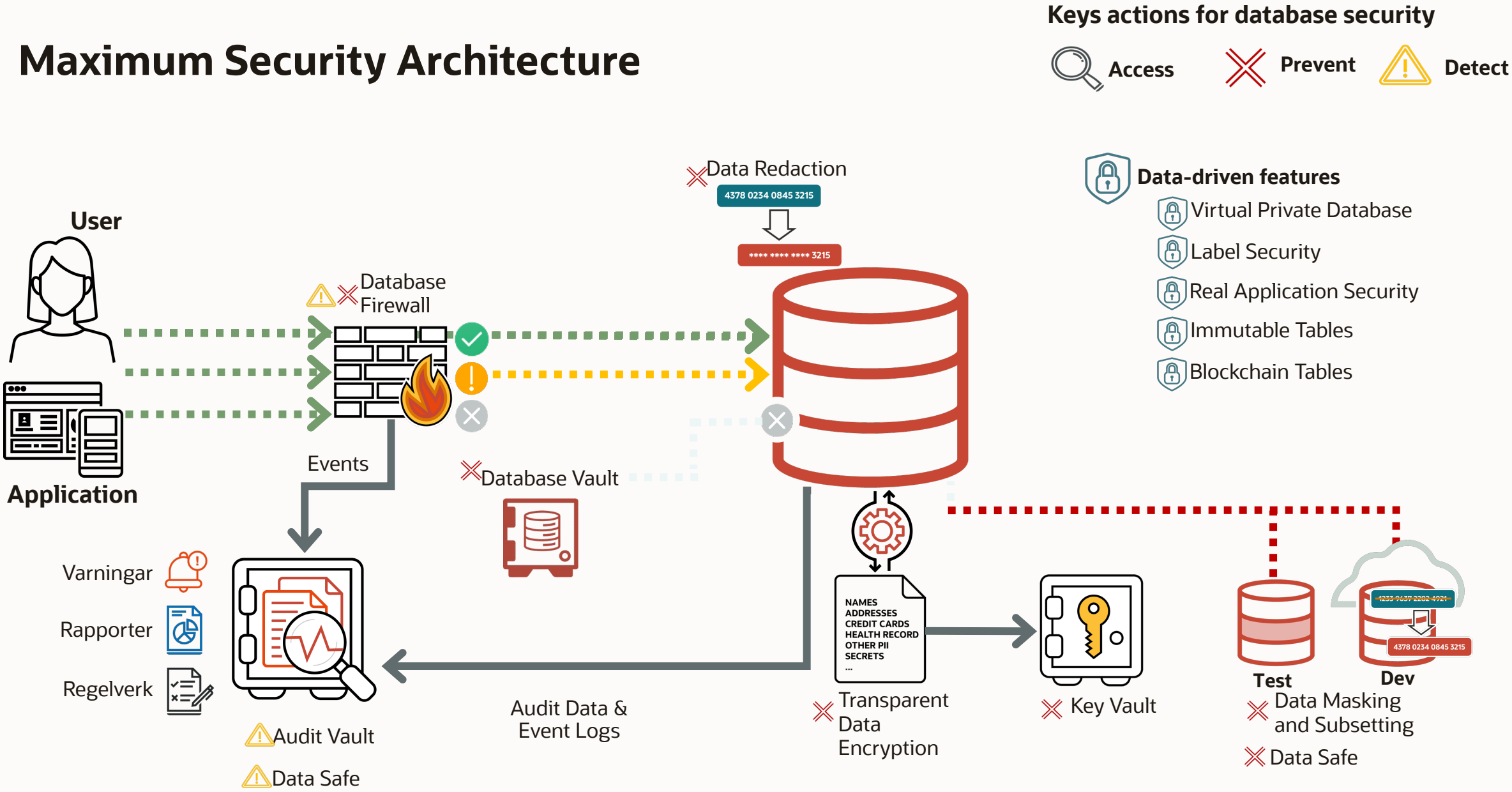
Track privilege/role usage by a database user for a period of time

Identify and consider removing unused privileges

Minimal performance impact – processing done during report generation

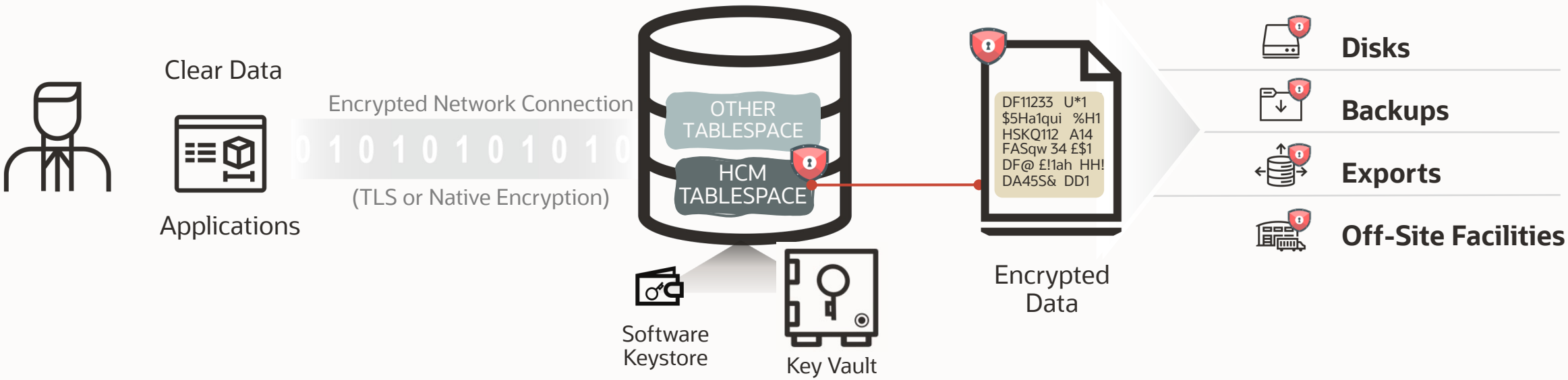
Moved to core database in 2019. No dependency on Database Vault Licensing.

Maximum Security Architecture



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

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

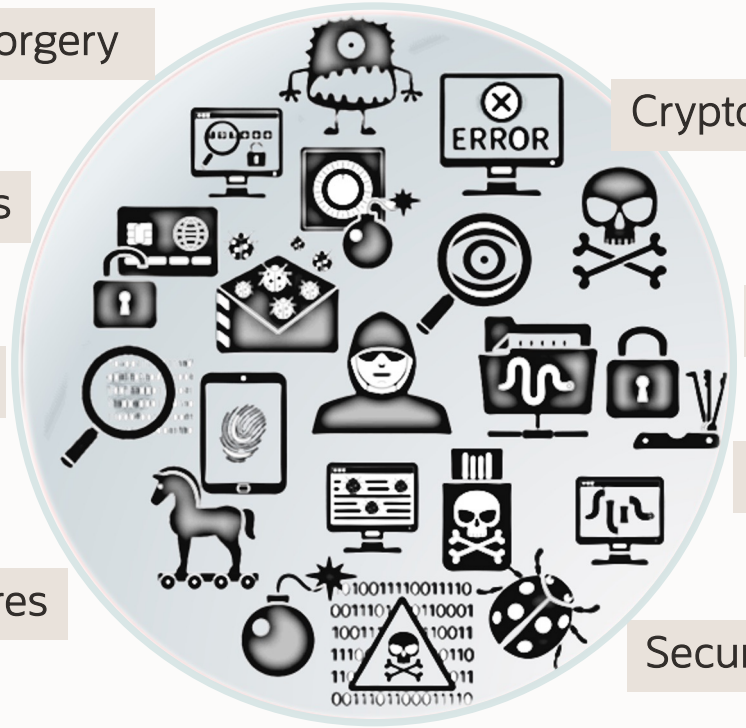
6 Vulnerable and Outdated Components

7 Identification and Authentication Failures

8 Software and Data Integrity Failures

9 Security Logging and Monitoring Failures

10 Server-Side Request Forgery

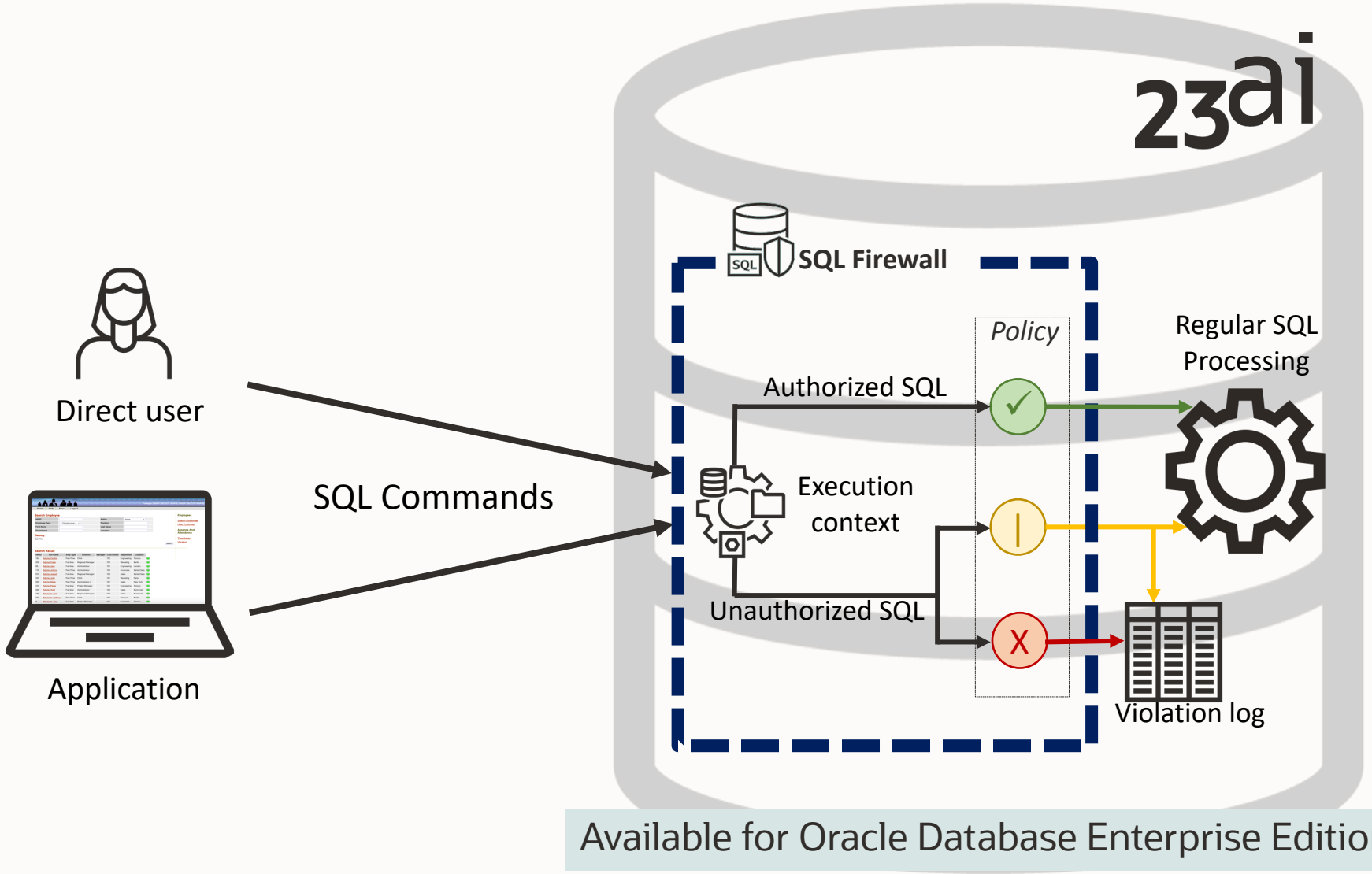


Top 3 most serious risk since 2017

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)

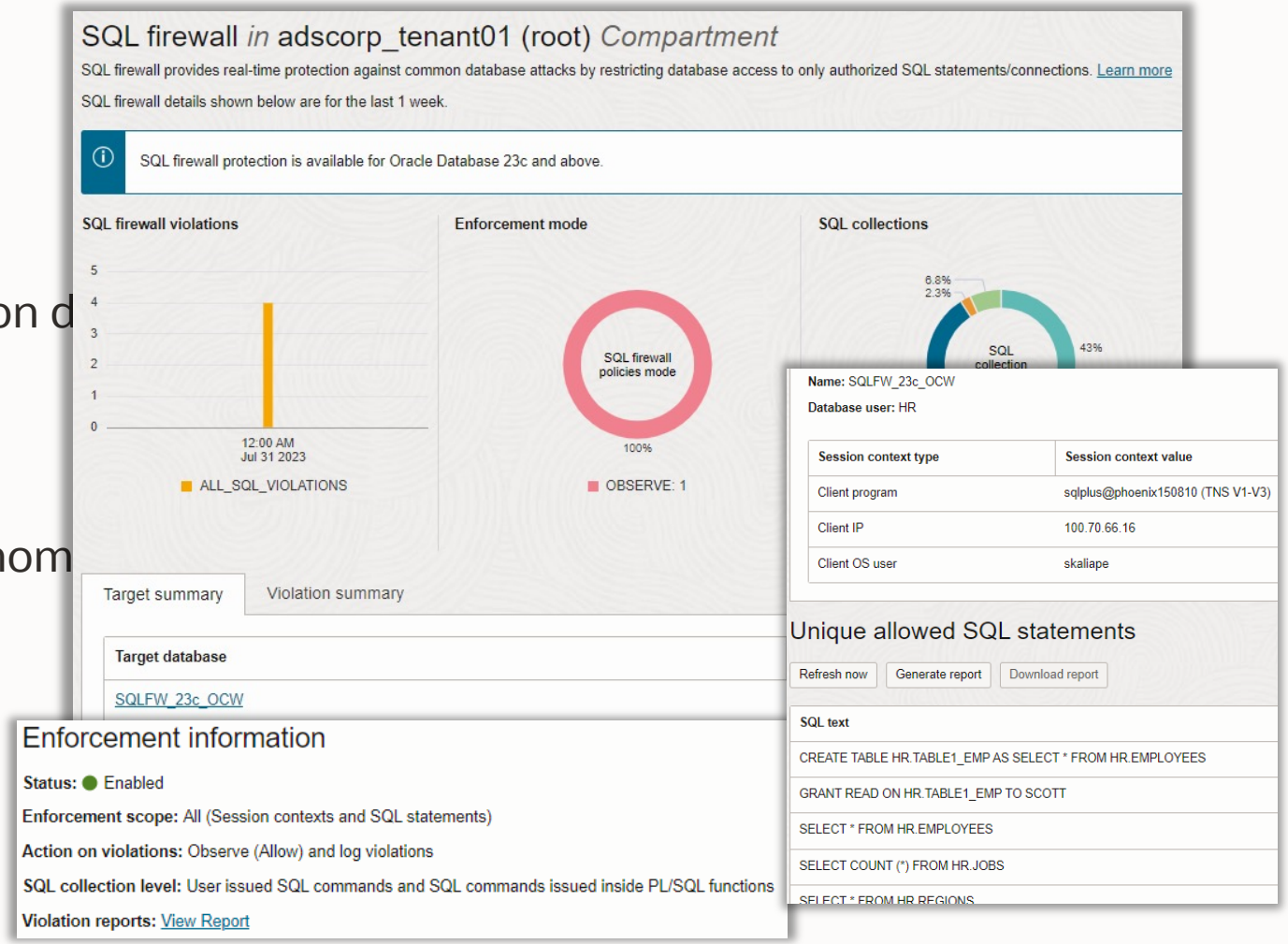
SQL Firewall – Protect from SQL injection and unauthorized access

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



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

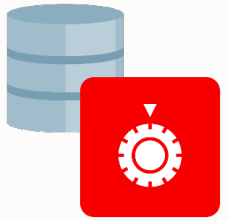
Separates virtualization layer from the network layer to protect customer instances

Database security product portfolio

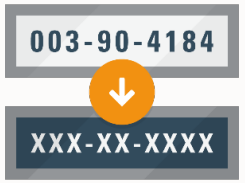
ORACLE Advanced Security

ORACLE Key Vault

ORACLE Database Vault



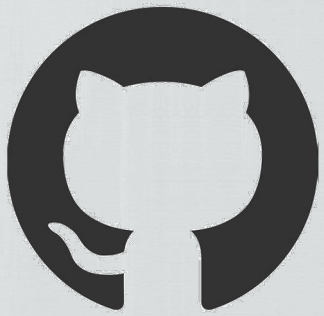
ORACLE Data Masking and Subsetting



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

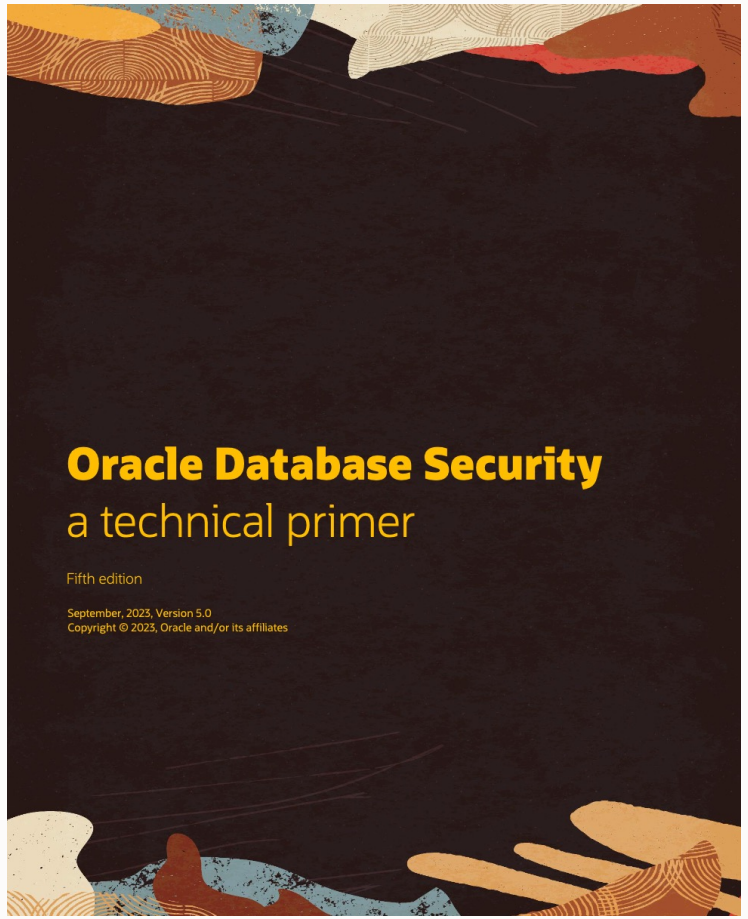
OTN: www.oracle.com/database/technologies/security.html

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



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