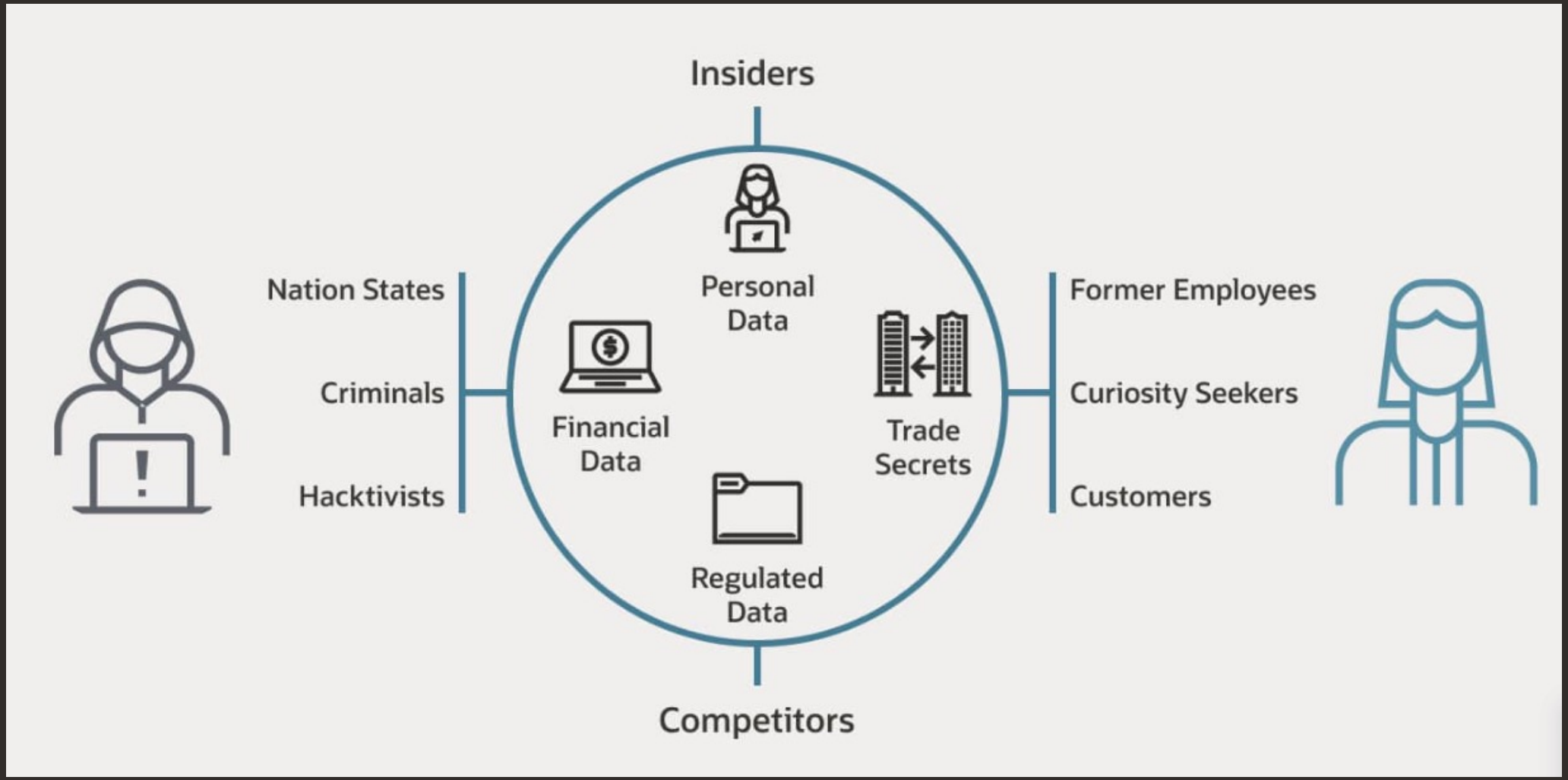
ORACLE DevLive | Level Up | MySQL Summit

Building Secure Applications with MySQL Enterprise Edition

Mike Frank
Product Management Director
MySQL
Mar 23, 2023

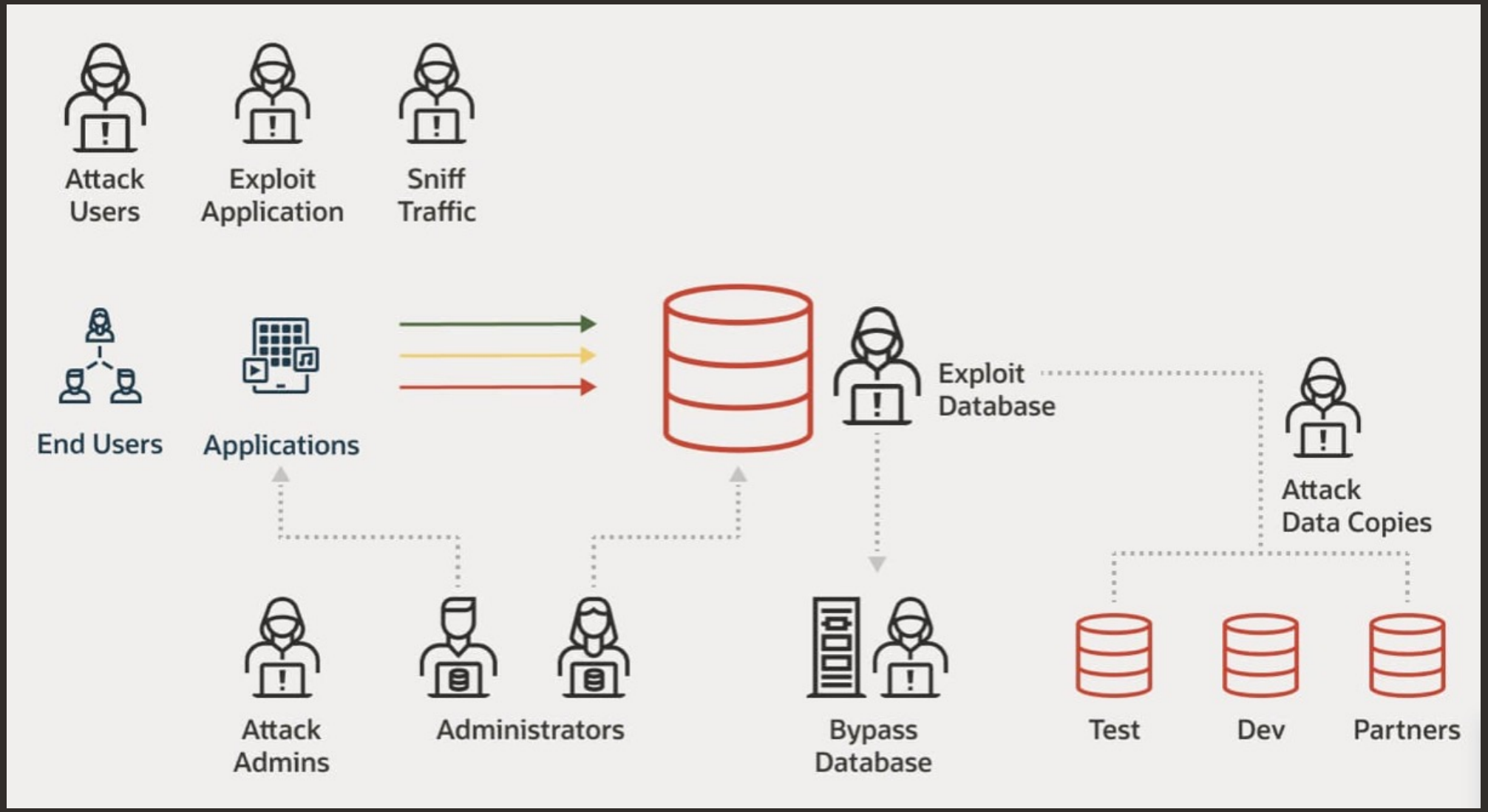
“93% of Security Breaches that are Preventable”
-- Online Trust Alliance (Internet Society)

What are the challenges of database security?



Copyright © 2023, Oracle and/or its affiliates

Where are databases attacked?



Copyright © 2023, Oracle and/or its affiliates

Database Attacks

1. SQL Injection
   - Prevention: DB Firewall, Allow List, Input Validation
2. Buffer Overflow
   - Prevention: Frequently apply Database Software updates, DB Firewall, Allow List, Input Validation
3. Insider Abuse
   - Prevention: Tight Access Controls, User specific authentication, Auditing, Monitoring, Encryption
4. Brute Force Attack
   - Prevention: lock out accounts after a defined number of incorrect attempts.
5. Network Eavesdropping
   - Prevention: Require SSL/TLS for all Connections and Transport
6. Malware
   - Prevention: Tight Access Controls, Limited Network IP access, Change default settings, Encryption

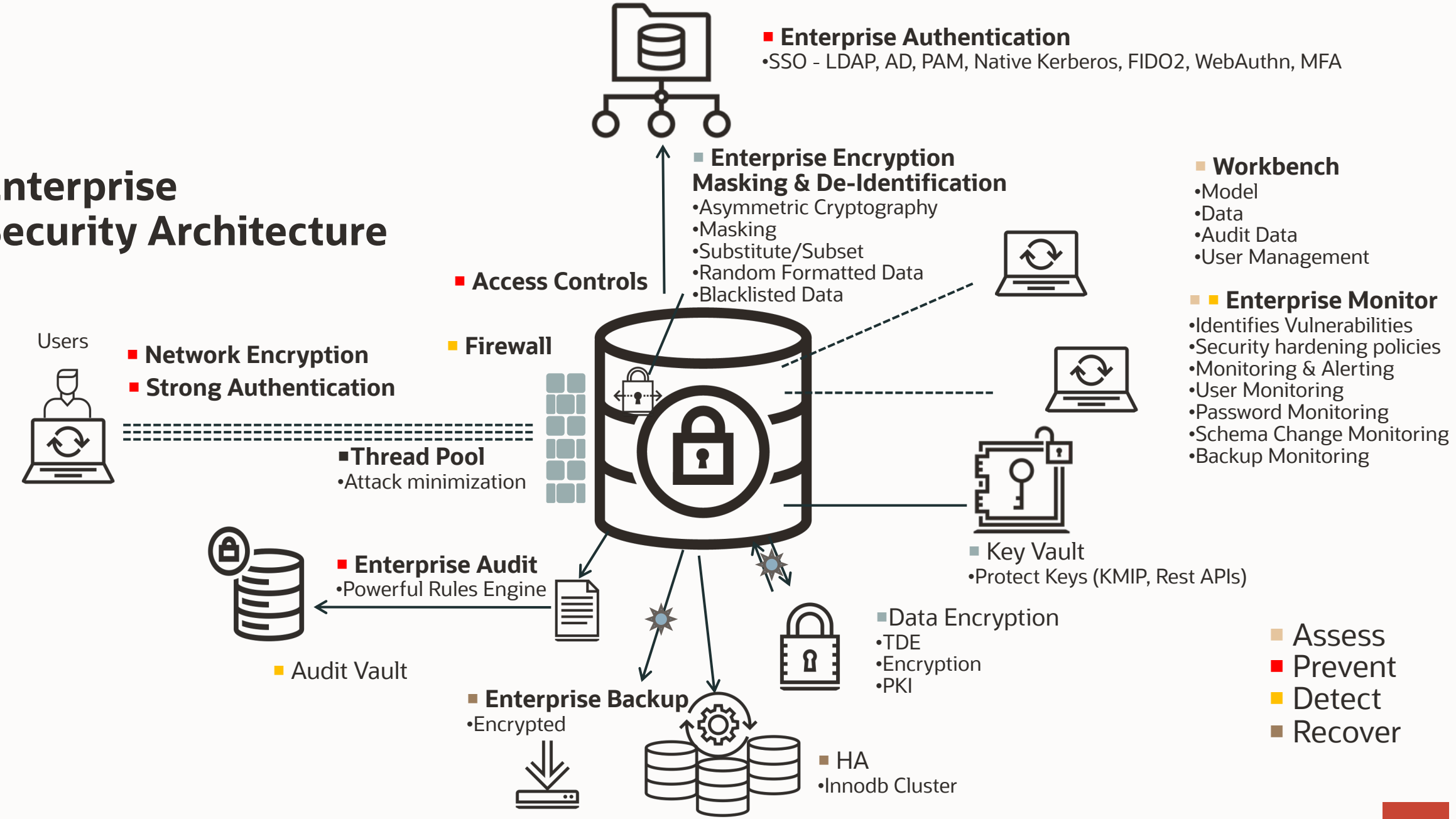
Copyright © 2023, Oracle and/or its affiliates

Database Malicious Actions

1. Information Disclosure: Obtain credit card and other personal information
   - Defense: Encryption – Data and Network, Tighter Access Controls
2. Denial of Service: Run resource intensive queries
   - Defense: Resource Usage Limits – Set various limits – Max Connections, Sessions, Timeouts, …
3. Elevation of Privilege: Retrieve and use administrator credentials
   - Defense: Stronger authentication, Access Controls, Auditing
4. Spoofing: Retrieve and use other credentials
   - Defense: Stronger account and password policies
5. Tampering: Change data in the database, Delete transaction records
   - Defense: Tighter Access Controls, Auditing, Monitoring, Backups

Copyright © 2023, Oracle and/or its affiliates

Enterprise Security Architecture



Security Threat Landscape

82% of breaches leveraged either stolen and/or weak credentials

13% increase in Ransomware breaches - more than in the last 5 years combined

Evolving Security Models

Zero-trust models

Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Authentication

Integrate with Centralized Authentication Infrastructure

- Centralized Account Management
- Password Policy Management
- Groups & Roles
- Multi-Factor Authentication (up to 3)
- X509

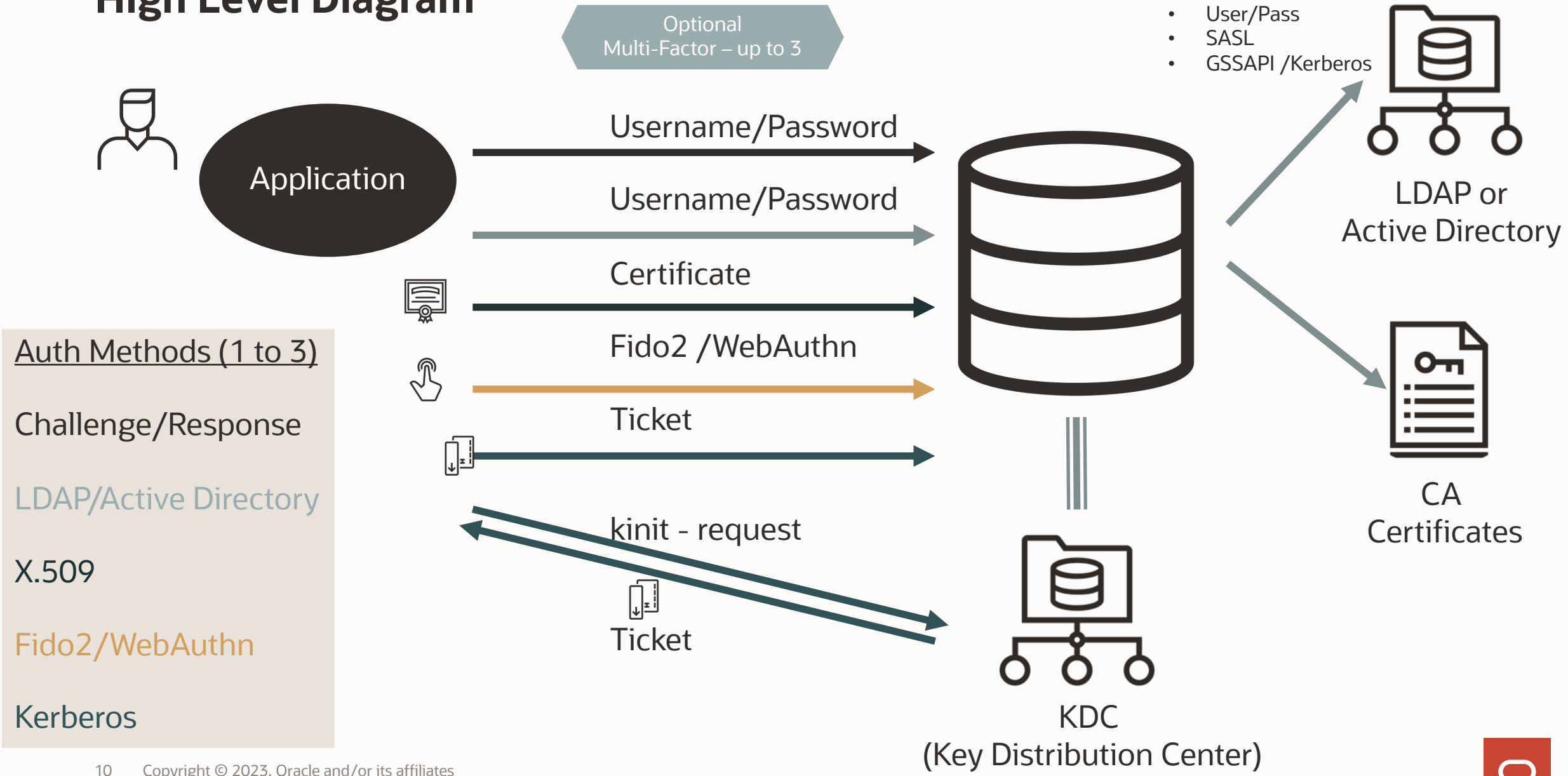
Types of Auth

- Native MySQL
  - User/Password SHA2 with configurable number of rounds (5000 default)
- Native LDAP
  - Access native LDAP service for authentication
- Native Kerberos – User/Pass, SASL, GSSAPI/Kerberos
- Windows Only - AD
  - Access native Windows service - Use to Authenticate users using Windows Active Directory or to a native host
- FIDO2
- Linux PAM Standard interface

Integrates MySQL with existing security infrastructures

Copyright © 2023, Oracle and/or its affiliates

MySQL Client Authentication Options
High Level Diagram



Auth Methods (1 to 3)

Challenge/Response

LDAP/Active Directory

X.509

Fido2/WebAuthn

Kerberos

Copyright © 2023, Oracle and/or its affiliates

Applications and MySQL Authentication

Passwords

- Don’t store in clear text – use a Secrets Vault
- Rotate more often, Use Dual Password Method

Tokens

- Use Kerberos Tokens – have a TTL

Certificates

- X509 with short expiration and automated rotation

Hostname

- Limit if possible – note with VPNs etc – often no longer viable

Access grants on Application User Accounts

- Limit as much as possible

Roles

- Define multiple roles and change roles for escalated / deescalated requirements
- SET ROLE role [, role]

Copyright © 2023, Oracle and/or its affiliates

User Security

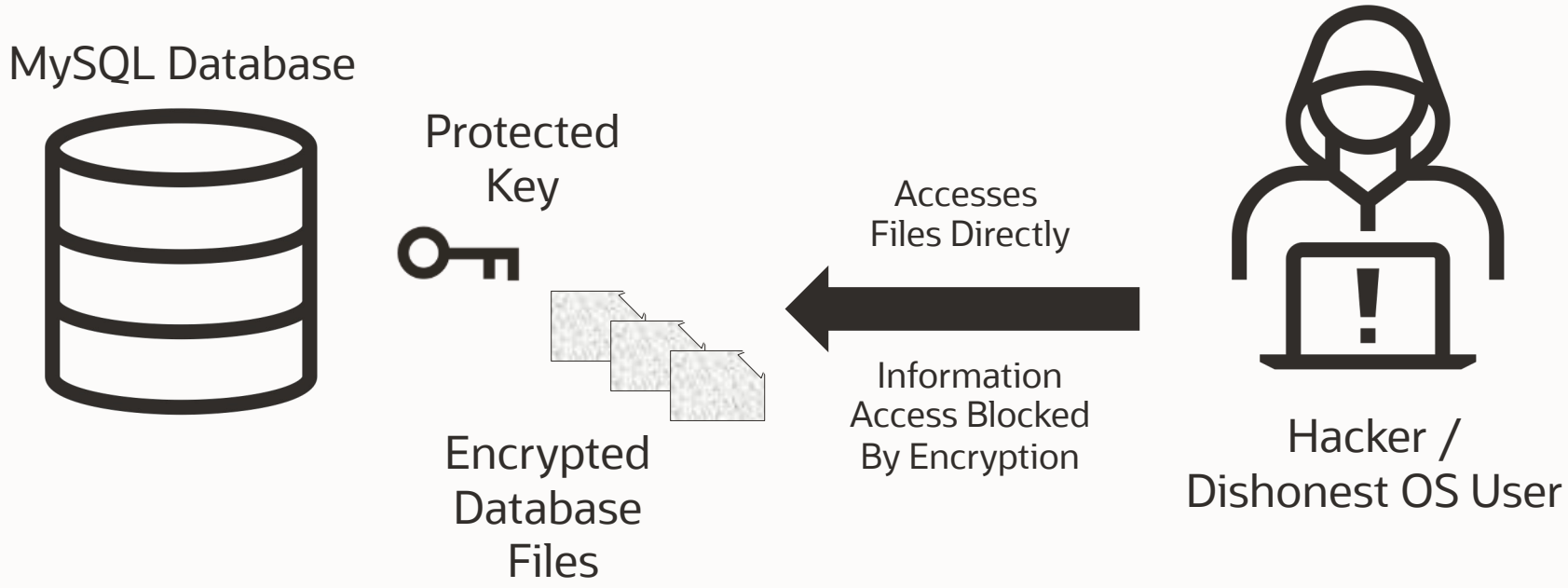
Password Management

Dual Password Change

- For each affected account, establish a new primary password on the servers, retaining the current password as the secondary password
- After the password change has propagated to all servers, modify applications that use any affected account to connect using the account primary password
- After all applications have been migrated from the secondary passwords to the primary passwords, the secondary passwords are no longer needed and can be discarded. After this change has propagated to all servers, only the primary password for each account can be used to connect
- The credential change is now complete

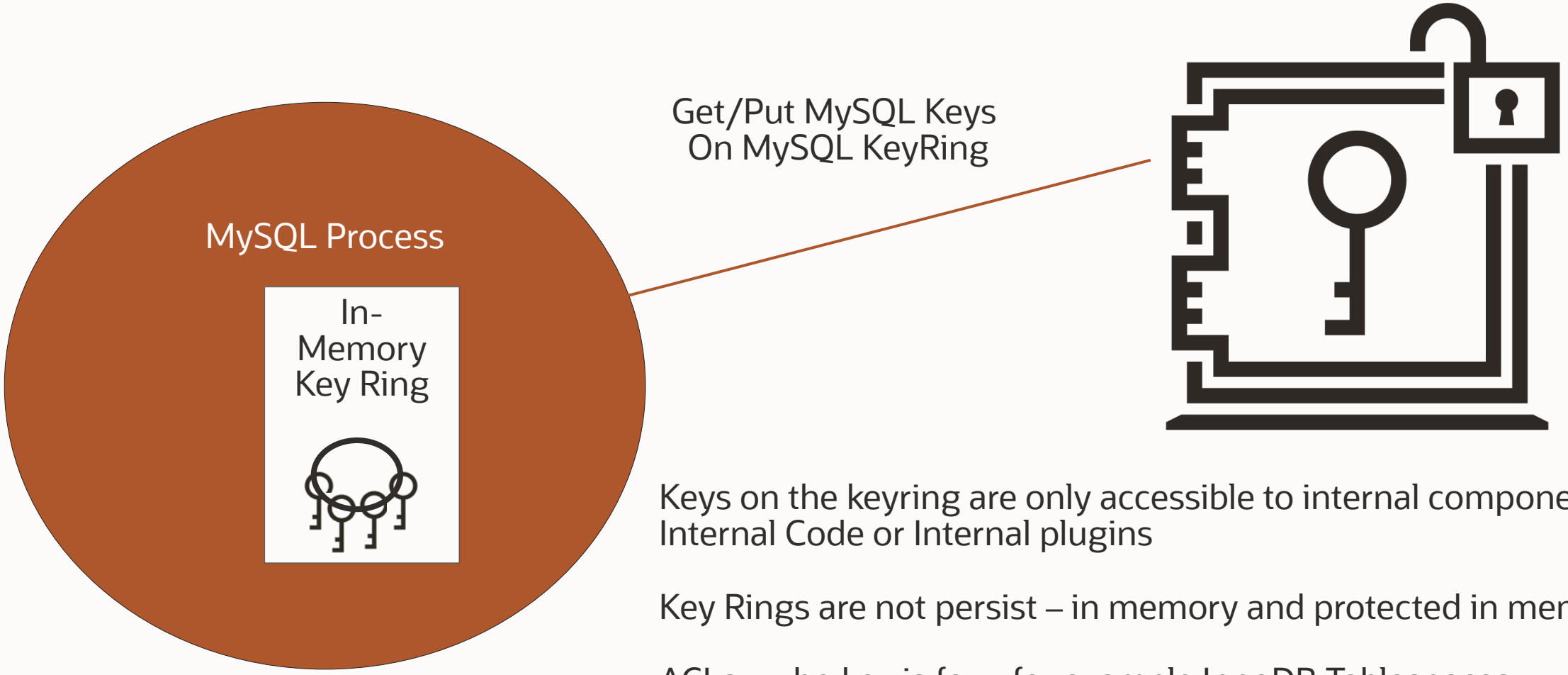
```
# Create the new password
ALTER USER 'appuser'@'localhost'IDENTIFIED BY 'newpass' RETAIN CURRENT PASSWORD;
# Wait for the password change to replicate to all slave servers
# Modify each application that uses the appuser1 account so that it connects to the
# servers using a password of 'newpass' rather than 'oldpass'
# Discard the old password
ALTER USER 'appuser'@'localhost' DISCARD OLD PASSWORD;
```

Attack on Files



Copyright © 2023, Oracle and/or its affiliates

MySQL Key Ring



Keys on the keyring are only accessible to internal components
Internal Code or Internal plugins

Key Rings are not persist – in memory and protected in memory

ACLs - who key is for – for example InnoDB Tablespaces

Copyright © 2023, Oracle and/or its affiliates

Transparent Data Encryption in MySQL

Option in CREATE TABLE

```
ENCRYPTION="Y"
```

Rotate Keys is simply

```
ALTER INSTANCE ROTATE INNODB MASTER KEY
```

Keyring plugin

- Used to retrieve keys

Component/Plugin Infrastructure

- Plugin type : keyring
- Ability to load plugin before InnoDB initialization --early-plugin-load

MySQL Files

- Support for encrypted tables, undo, redo, binlog, audit
- IMPORT/EXPORT of encrypted tables
- Support for master key rotation

Copyright © 2023, Oracle and/or its affiliates

Database Auditing

Maintaining an audit trail is an essential security best practice

“Trust but verify" approach to security

- Ensure users with strong privileges don’t misuse those privileges

Business Audit – Data Validity

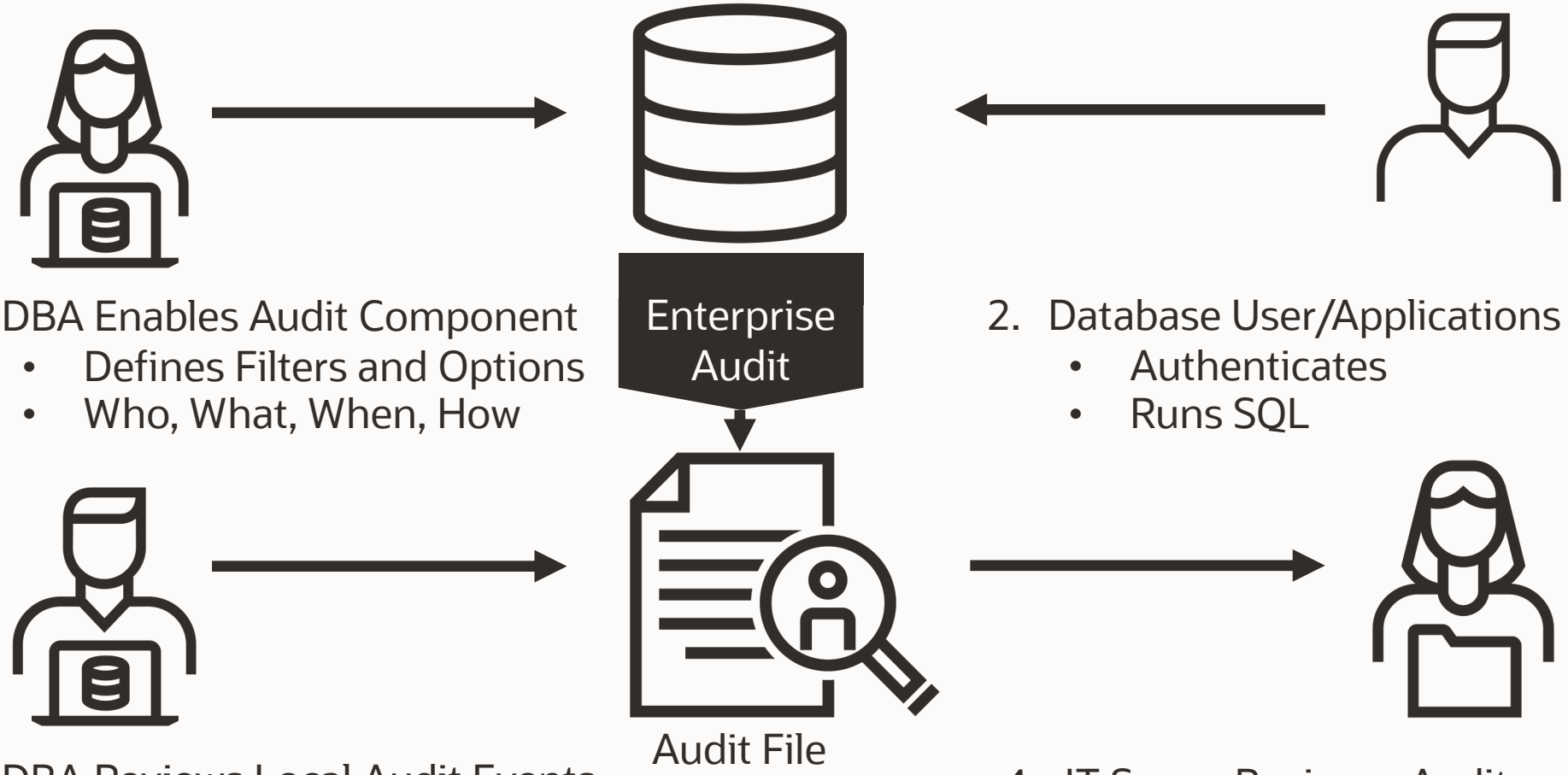
- Here’s proof my database data is accurate/correct
- Prove no tampering to data has occurred

Forensic analysis – as a component of any defense-in-depth strategy

- Proactive - Am being / Was hacked
- Reactive – How were we hacked, what was changed, taken, etc.

Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Audit - Work Flow



1. DBA Enables Audit Component
   - Defines Filters and Options
   - Who, What, When, How

2. Database User/Applications
   - Authenticates
   - Runs SQL

3. DBA Reviews Local Audit Events
   - Via SQL (with proper rights)
   - Or file if DBA can SSH to OS

4. IT Sec or Business Auditors
   - Globally evaluate Audit Trail

Copyright © 2023, Oracle and/or its affiliates

Database Firewall

SQL Injection Attacks

- #1 Web Application Vulnerability
- 77% of Web Sites had vulnerabilities

MySQL Enterprise Firewall

- Monitor database statements in real-time
- Automatic Allow List “rules” generation for any application
- Define blocking Firewall Rules
- Block SQL Injection Attacks
- Intrusion Detection System

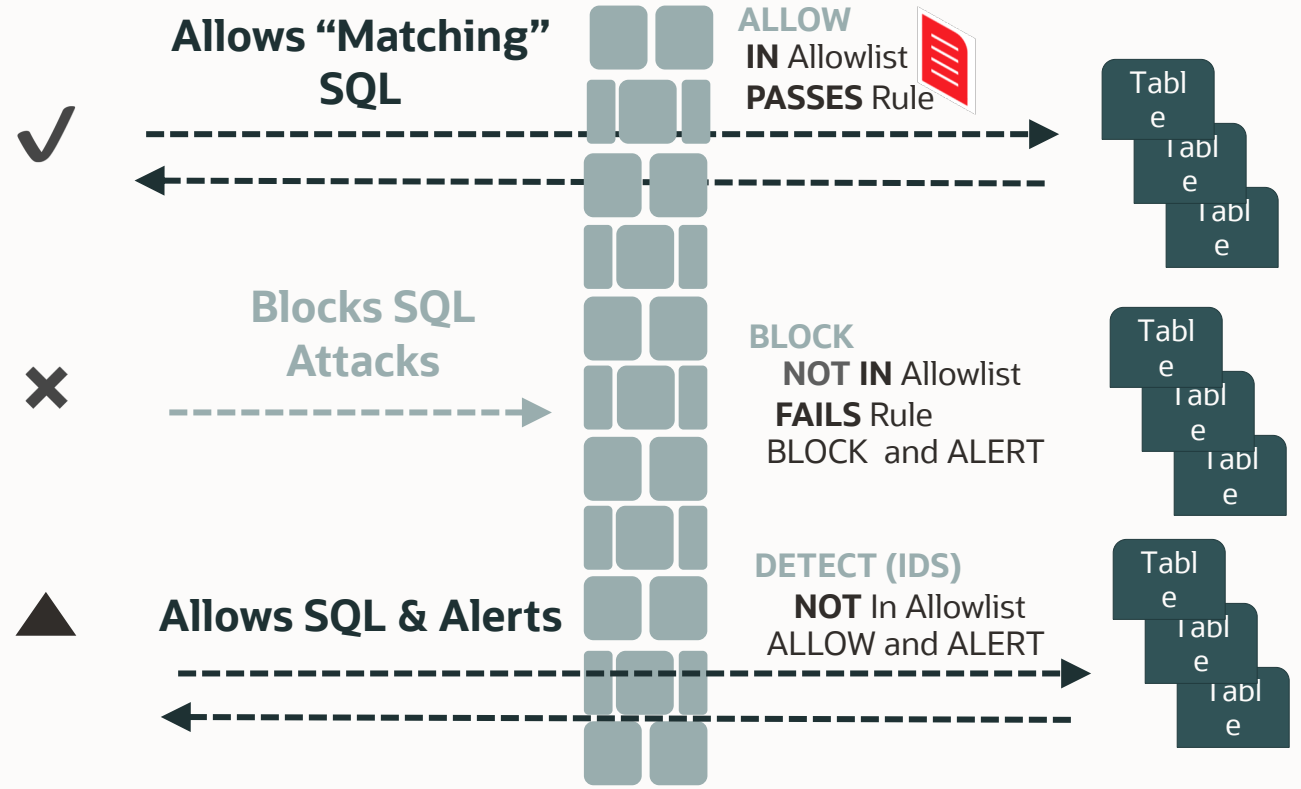
Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Firewall: Operating Modes

1. ALLOW – Execute SQL
   - SQL Matches Allowlist
   - SQL Passes Rule

2. BLOCK – Block the request
   - Not in Allowlist
   - SQL FAILs Rule
   - In Block Mode

3. DETECT – Execute SQL & Alert
   - Not in Allowlist
   - SQL FAILs Rule
   - In Alert Mode



Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Masking and De-Identification

De-identify, Anonymize Sensitive Data

"Data Masking is a method to hide sensitive information by replacing real values with substitutes."

Employee Table

ID	Last	First	SSN
1111	Smith	John	555-12-5555
1112	Templeton	Richard	444-12-4444

Random Data Generation

Masked View

ID	Last	First	SSN
2874	Smith	John	XXX-XX-5555
3281	Templeton	Richard	XXX-XX-4444

Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Masking and De-Identification

Data Masking and Random Data Generation

Data Masking

- String masking
- Dictionary based replacement
- Specific masking
  - SSN
  - Payment card : Strict/Relaxed

Random Data Generators

- Random number within a range
- Email
- Payment card (Luhn check compliant)
- SSN
- Dictionary based generation

Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Masking and De-Identification

String data masking

- Mask a substring within a string : ArthXXXXnt
- Mask substrings at the beginning and at the end :
  - XXthurDeXX

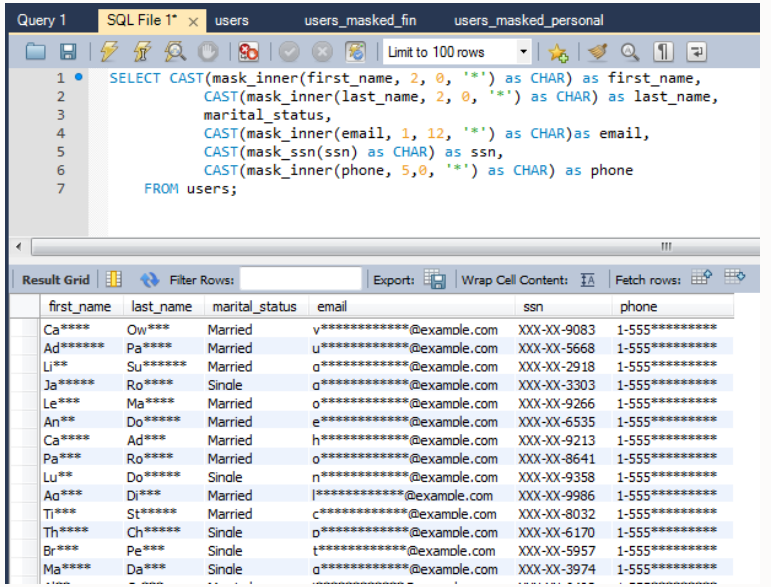
SSN masking : XXXX-XX-1234

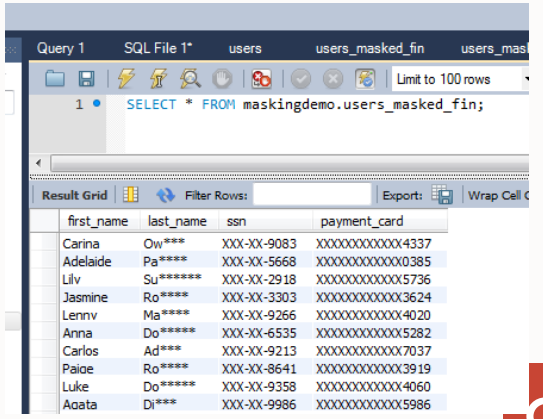
Payment Card masking

- Strict: XXXXXXXXXXXXXX7395, Relaxed: 493812XXXXXXXXX7395

Dictionary based masking

- gen_blocklist(“007”, “00designations”, “Cover_identity”) => Universal Exports





Copyright © 2023, Oracle and/or its affiliates

MySQL Enterprise Masking and De-Identification

Random Data Generation

Random data within range

- gen_rnd(10000, 20000) => 12503

Email : kajsm.hamskdk@example.com

Payment card : 7389026626032990

- Configurable length : 12 to 19 digits

SSN : 915-63-3858

US Phone number : 1-555-3456-332

```
UPDATE users SET designation = CAST(gen_dictionary("Designations") as CHAR) where id >  0 ;
UPDATE users SET ssn = CAST(gen_rnd_ssn() as CHAR) where id >  0;
UPDATE users SET salary = gen_range(40000, 55000) WHERE designation in ('Developer') and id >  0
UPDATE users SET salary = gen_range(60000, 70000) WHERE designation in ('Senior Developer') and
UPDATE users SET salary = gen_range(75000, 90000) WHERE designation in ('Principal Developer', '
UPDATE users SET salary = gen_range(95000, 120000) WHERE designation in ('Architect', 'Senior Ma
UPDATE users SET salary = gen_range(125000, 150000) WHERE designation in ('Director') and id >
UPDATE users SET salary = gen_range(160000, 200000) WHERE designation in ('Senior Director') and
UPDATE users SET salary = gen_range(220000, 250000) WHERE designation in ('Vice President') and
UPDATE users SET email = gen_rnd_email() where id >  0;
UPDATE users SET phone = gen_rnd_us_phone() where id >  0;
UPDATE users SET payment_card = gen_rnd_pan() where id >  0;
```


Copyright © 2023, Oracle and/or its affiliates

Run MySQL Security Assessments

- Upgrades and Patches to software
  - MySQL
  - Development Frameworks and ORMs
  - Application Libraries
- HA, DR, Security, and Backups go hand in had – Use Cluster, Replica Set, Cluster Set, Run Backups
- Regularly check and re-check MySQL Security
- Monitor and review changes
- Review audit data for suspect activity
- Review application code
  - Configuration
    - How do they connect
    - Where is that information
  - Data validation – do they check inputs for data type, length, etc
  - Use of prepared statements, binding data versus dynamic

Copyright © 2023, Oracle and/or its affiliates

Security Guidelines

CIS Benchmark for MySQL 8.0 EE

- https://www.cisecurity.org/benchmark/oracle_mysql/

CIS recommendations are recognized as a secure configuration standard by the DoD Cloud Computing Security Recommendation Guide (SRG), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and the National Institute of Standards and Technology (NIST).

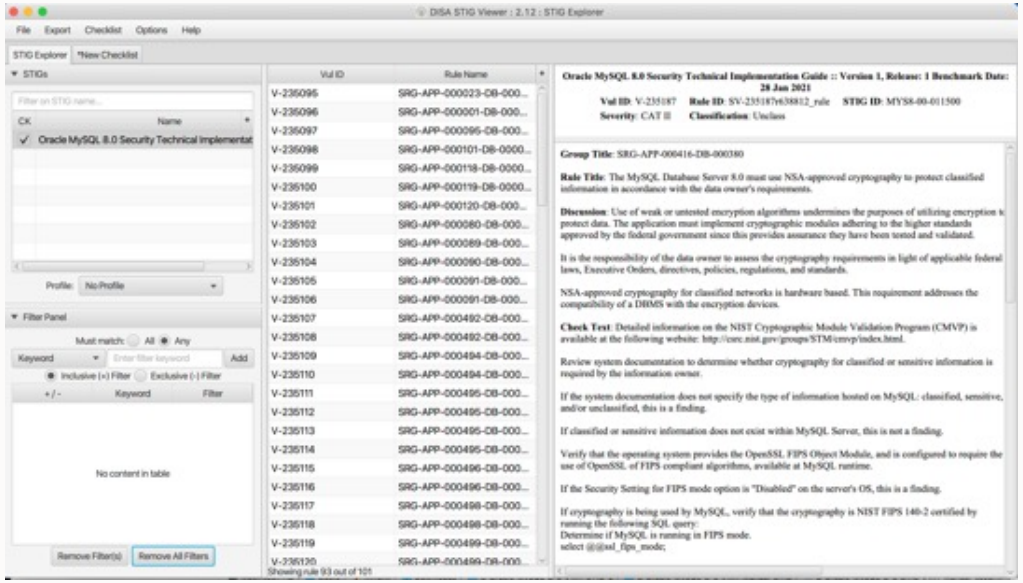
Copyright © 2023 Oracle and/or its affiliates.

Security Guidelines

- DISA STIG (Security Technical Implementation Guidelines) for MySQL 8.0 EE

https://www.mysql.com/products/enterprise/stig.html

https://public.cyber.mil/stigs/



Copyright © 2023 Oracle and/or its affiliates.

Oracle Secure Processes

- Oracle Corporate Security Practices
  - Critical Patch Updates, Security Alerts, Bulletins
  - Handling of sensitive “private/personal” information during support
  - Source Code protection
  - Secure Coding Standards
  - Security Analysis and Testing
  - Employee Screening and Education
  - Architectural Security Reviews
  - Trusted installation package repositories
- MySQL Security Guide
- MySQL Support KBs on security

Oracle Support, Security, and Compliance References

Oracle's corporate security

- https://www.oracle.com/corporate/security-practices/

Oracle's cloud compliance

- https://www.oracle.com/cloud/compliance/

The Critical Patch Updates and Security Alerts Page

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

Instructions on how to report security vulnerabilities

- https://www.oracle.com/corporate/security-practices/assurance/vulnerability/reporting.html

Oracle Software Technical Support Policies

- https://www.oracle.com/us/assets/057419.pdf

The agreements for Oracle Cloud (including the Data Processing Agreement for Oracle Services)
http://www.oracle.com/corporate/contracts/cloud-services/index.html

Copyright © 2023, Oracle and/or its affiliates

Mike Frank
mike.frank@oracle.com

Copyright © 2023, Oracle and/or its affiliates

ORACLE DevLive | Level Up

Please rate this session.

Session ID – MS13

Copyright © 2023, Oracle and/or its affiliates