ORACLE®

MySQL Enterprise Edition
Security - Transparent Data Encryption

Mike Frank Product Management Director

April, 2016

ORACLE

Safe Harbor Statement

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, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Program Agenda

1. Introduction to Transparent Data Encryption in MySQL
2. Demo
3. Server Startup and Configuration
4. Questions

Mega Breaches

552 Million identities exposed in 2013. 493% increase over previous year

77%

Web sites with vulnerabilities. 1-in-8 of all websites had a critical vulnerability.

8

Breaches that exposed more than 10 million records in 2013.

Total Breaches increased 62% in 2013

Source: Internet Security Threat Report 2014, Symantec

Regulatory Drivers

- Regulations
  - PCI – DSS: Payment Card Data
  - HIPAA: Privacy of Health Data
  - Sarbanes Oxley: Accuracy of Financial Data
  - EU Data Protection Directive: Protection of Personal Data
  - Data Protection Act (UK): Protection of Personal Data
- Requirements
  - Continuous Monitoring (Users, Schema, Backups, etc)
  - Data Protection (Encryption, Privilege Management, etc.)
  - Data Retention (Backups, User Activity, etc.)
  - Data Auditing (User activity, etc.)

PCI Security Standards Council™

HIPAA
Health Insurance Portability and Accountability Act

Sarbanes-Oxley
Financial and Accounting Disclosure Information

European Commission
Justice

Data Protection Act 1998

PCI DSS

PCI DSS v3.0
November 2013

3.5 Store cryptographic keys in a secure form (3.5.2), in the fewest possible locations (3.5.3) and with access restricted to the fewest possible custodians (3.5.1)

3.6 Verify that key-management procedures are implemented for periodic key changes (3.6.4)

And more!

MySQL Enterprise Edition

- New! MySQL Enterprise TDE
  - Data-at-Rest Encryption
  - Key Management/Security
- MySQL Enterprise Authentication
  - External Authentication Modules
    - Microsoft AD, Linux PAMs
- MySQL Enterprise Encryption
  - Public/Private Key Cryptography
  - Asymmetric Encryption
  - Digital Signatures, Data Validation
  - User Activity Auditing, Regulatory Compliance
- MySQL Enterprise Firewall
  - Block SQL Injection Attacks
  - Intrusion Detection
- MySQL Enterprise Audit
  - User Activity Auditing, Regulatory Compliance
- MySQL Enterprise Monitor
  - Changes in Database Configurations, Users Permissions, Database Schema, Passwords
- MySQL Enterprise Backup
  - Securing Backups, AES 256 encryption

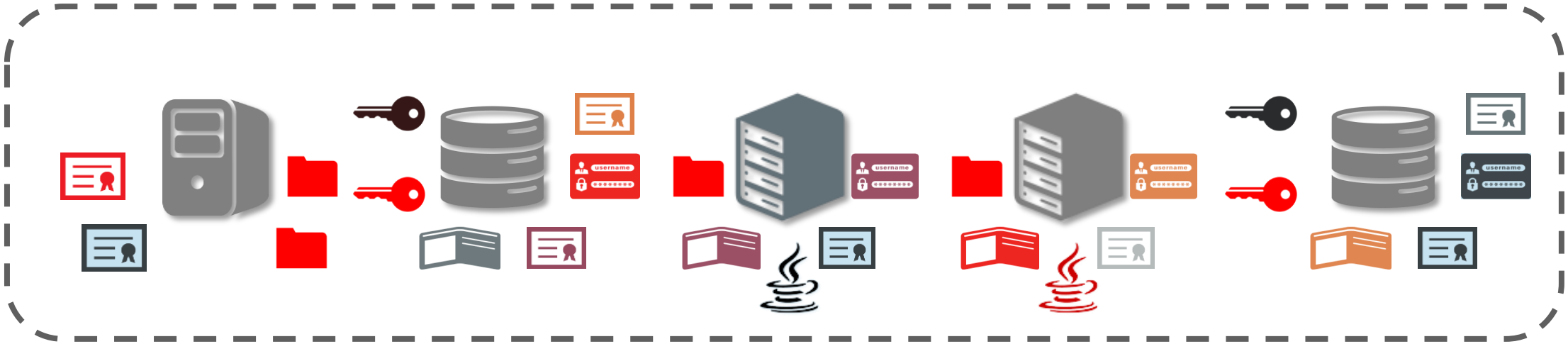
ORACLE

What is Transparent Data Encryption?

- Data at Rest Encryption
  - Tablespaces, Disks, Storage, OS File system
- Transparent to applications and users
  - No application code, schema or data type changes
- Transparent to DBAs
  - Keys are hidden from DBAs, no configuration changes
- Requires Key Management
  - Protection, rotation, storage, recovery

ORACLE

Biggest Challenge: Encryption Key Management



Management

- Proliferation of encryption wallets and keys
- Authorized sharing of keys
- Key availability, retention, and recovery
- Custody of keys and key storage files

Regulations

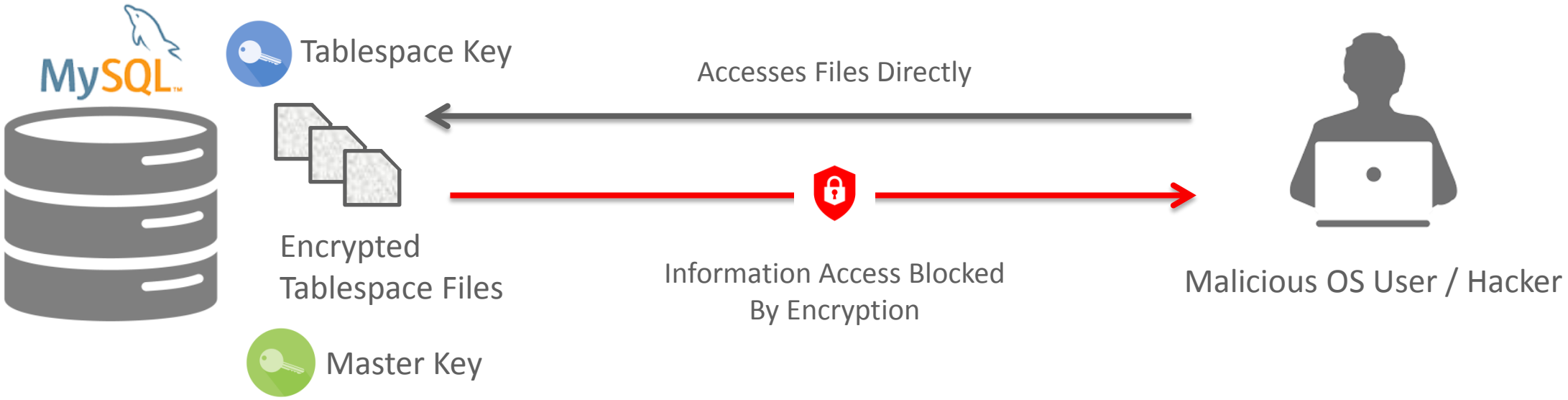
- Physical separation of keys from encrypted data
- Periodic key rotations
- Monitoring and auditing of keys
- Long-term retention of keys and encrypted data

MySQL Enterprise TDE: Goals

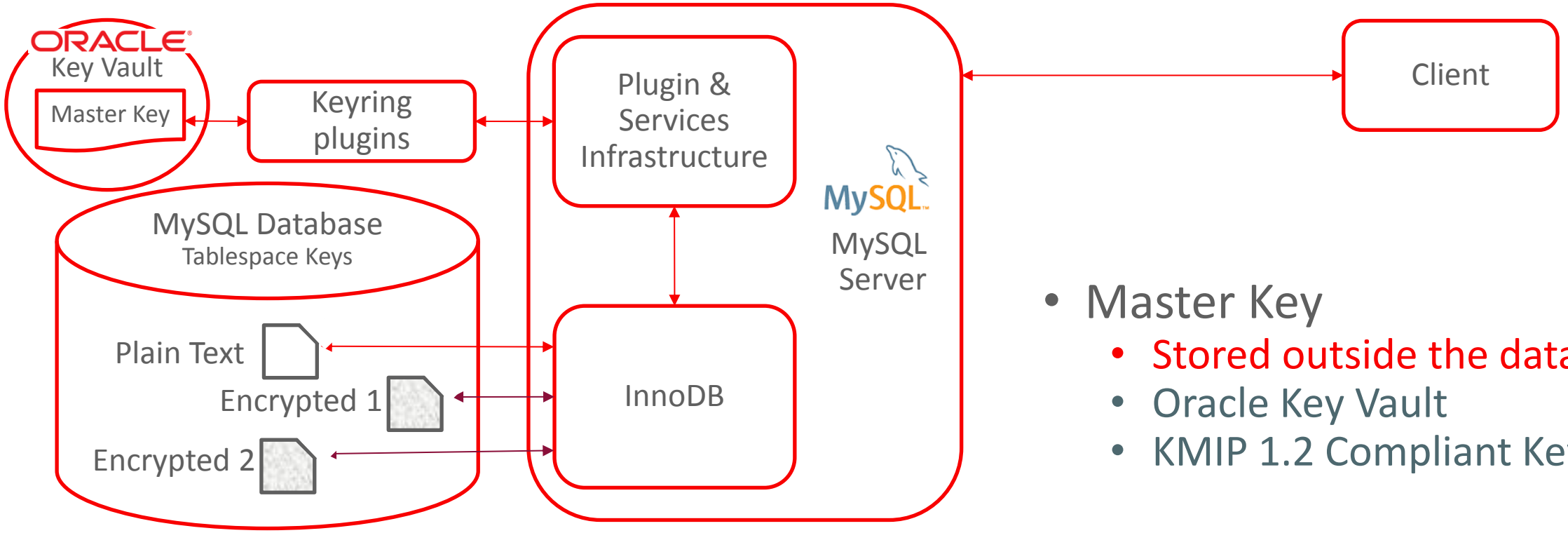
- Data at Rest Encryption
  - Tablespace Encryption
- Key Protection
  - Most Important and Difficult
- Strong Encryption
  - AES 256
- Simple to Manage
  - One master key for whole MySQL instance
- High Performance & Low Overhead
  - Simple Key Rotation without massive decrypt/encryption costs
- High Quality Infrastructure
  - Expand and support more security capabilities - encryption, keys, certs, …

ORACLE

MySQL Transparent Data Encryption



MySQL Transparent Data Encryption: 2 Tier Architecture



- Master Key
  - Stored outside the database
  - Oracle Key Vault
  - KMIP 1.2 Compliant Key Vault
- Tablesapce Key
  - Protected by master key

MySQL Key Ring

Key Vault
or KMIP v1.2 Compliant Key Vault

Get/Put MySQL Keys
On MySQL Keyring

- Keys are only accessible to internal components
  - Internal Code or Internal plugins
- Key Rings are not persistent
  - In memory and protected in memory
- ACLs for who key is for
  - i.e. InnoDB Tablespaces

Using MySQL Transparent Data Encryption

SQL

- New option in CREATE TABLE ENCRYPTION="Y"
- New SQL : ALTER INSTANCE ROTATE INNODB MASTER KEY

Plugin Infrastructure

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

Keyring plugin

- Used to retrieve keys

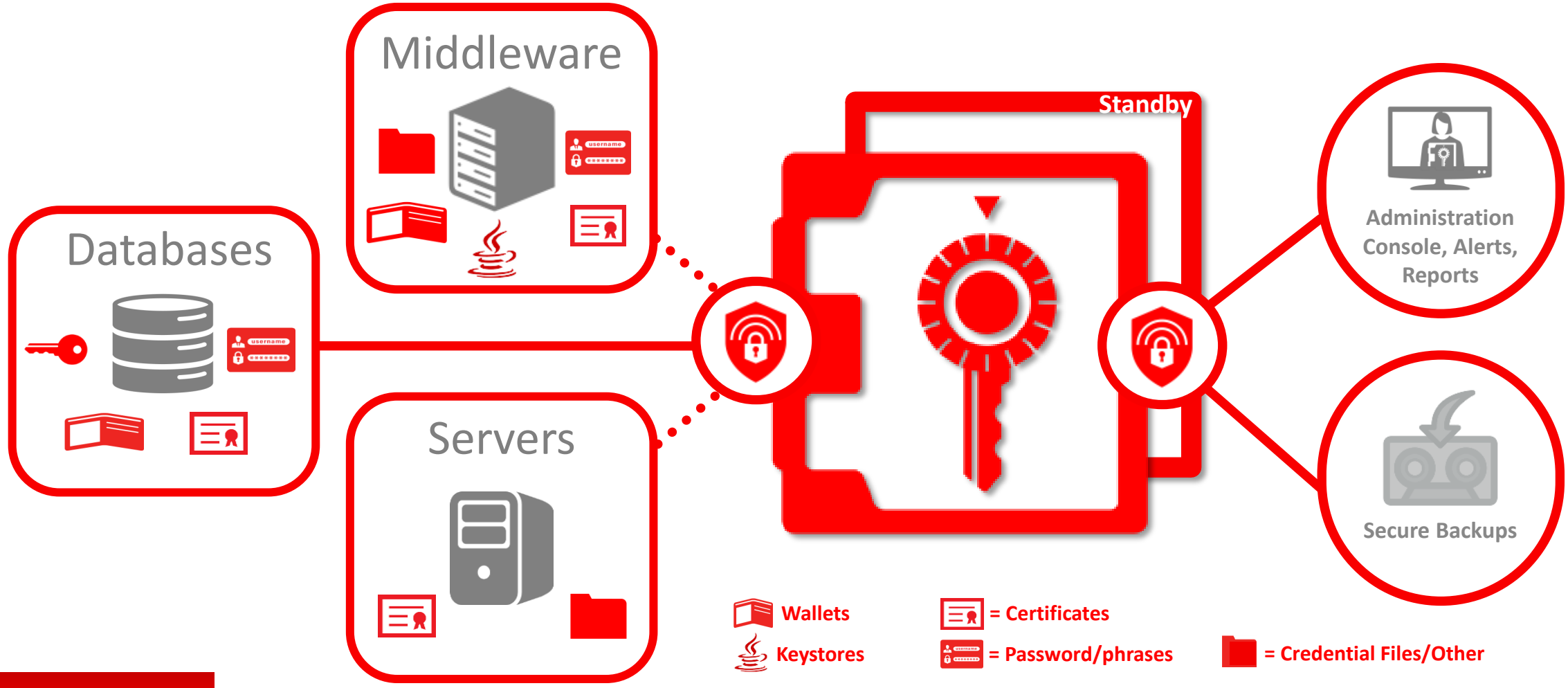
InnoDB

- Support for encrypted tables
- IMPORT/EXPORT of encrypted tables
- Support for master key rotation

Encryption Key Management

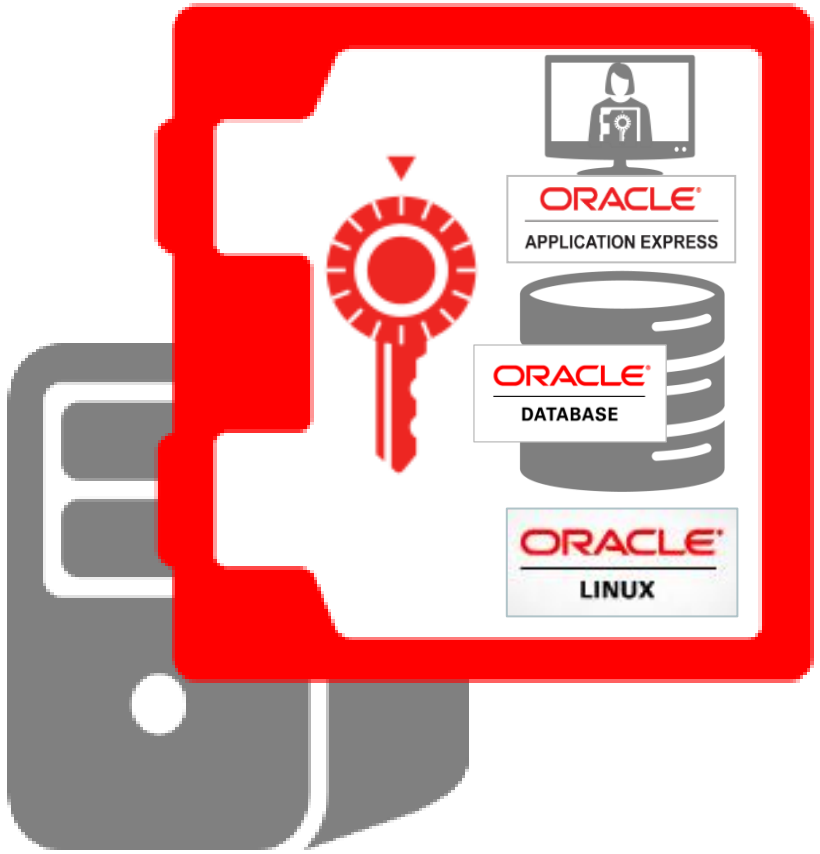
Key Vaults and Key Stores

Key Vaults and Key Stores: General Purpose



Oracle Key Vault

- Turnkey solution based on hardened stack
- Includes Oracle Database and security options
- Open x86-64 hardware to choose from
- Easy to install, configure, deploy, and patch
- Separation of duties for administrative users
- Full auditing, preconfigured reports, and alerts



MySQL Enterprise TDE: Oracle Key Vault KMIP Compliant

- Uses Oracle KMIP Client Library
- DBA never knows the Master Key
- Only a Oracle Key Vault Admin(s) have Master Key access
- Keys are protected and secure
- Oracle Key Vault has built-in redundancy, backup
- Enables customers to meet regulatory requirements

ORACLE

Example Commands

- Installation
  - Set configuration for MySQL to talk to Oracle Key Vault
  - Connect to MySQL
    - install plugin okv_kmip_keyring_file soname ‘okv_kmip_keyring.dll';
- Encrypt a table
  - CREATE TABLE `<table>` (`ID` int(11) NOT NULL AUTO_INCREMENT, `Name` char(35) NOT NULL DEFAULT '', …) ENGINE=InnoDB … ENCRYPTION="Y"
- Rotate Master Key
  - ALTER INSTANCE ROTATE INNODB MASTER KEY;

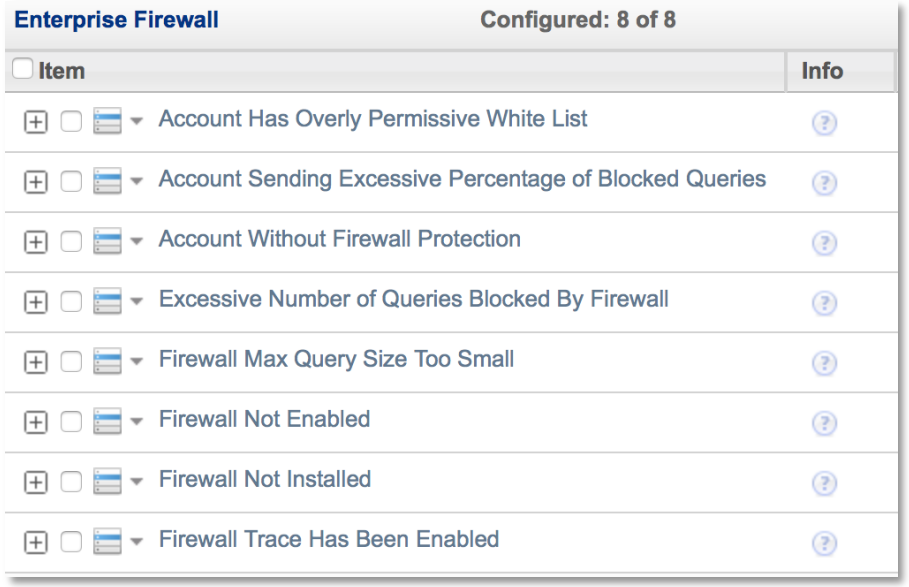
Notes about configuration

- --early-plugin-load
  - Usage : same as –plugin-load : “<plugin>=<library>”
  - Loading keyring plugin from Oracle Key Vault into the instance before InnoDB starts:
  - Enables recovery of encrypted tablespaces

ORACLE

MySQL Enterprise Firewall

- Real Time Protection
  - Queries analyzed and matched against White List
- Blocks SQL Injection Attacks
  - Block Out of Policy Transactions
- Intrusion Detection
  - Detect and Alert on Out of Policy Transactions
- Learns White List
  - Automated creation of approved list of SQL command patterns on a per user basis
- Transparent
  - No changes to application required



MySQL Enterprise Firewall monitoring

MySQL Enterprise Authentication

Integrates MySQL with existing security infrastructures

- Integrate with Centralized Authentication Infrastructure
  - Centralized Account Management
  - Password Policy Management
  - Groups & Roles
- PAM (Pluggable Authentication Modules)
  - Standard interface (Unix, LDAP, Kerberos, others)
  - Windows
    - Access native Windows service - Use to Authenticate users using Windows Active Directory or to a native host

MySQL Enterprise Encryption

- MySQL encryption functions
  - Symmetric encryption AES256 (All Editions)
  - Public-key / asymmetric cryptography – RSA
- Key management functions
  - Generate public and private keys
  - Key exchange methods: DH
- Sign and verify data functions
  - Cryptographic hashing for digital signing, verification, & validation – RSA,DSA

MySQL Enterprise Audit

- Out-of-the-box logging of connections, logins, and query
- User defined policies for filtering, and log rotation
- Dynamically enabled, disabled: no server restart
- XML-based audit stream per Oracle Audit Vault spec

Adds regulatory compliance to MySQL applications (HIPAA, Sarbanes-Oxley, PCI, etc.)

ORACLE

Program Agenda

1. Introduction to Transparent Data Encryption in MySQL
2. Demo
3. Notes about configuration
4. Questions

ORACLE®