

Best Practices for implementing Database Security

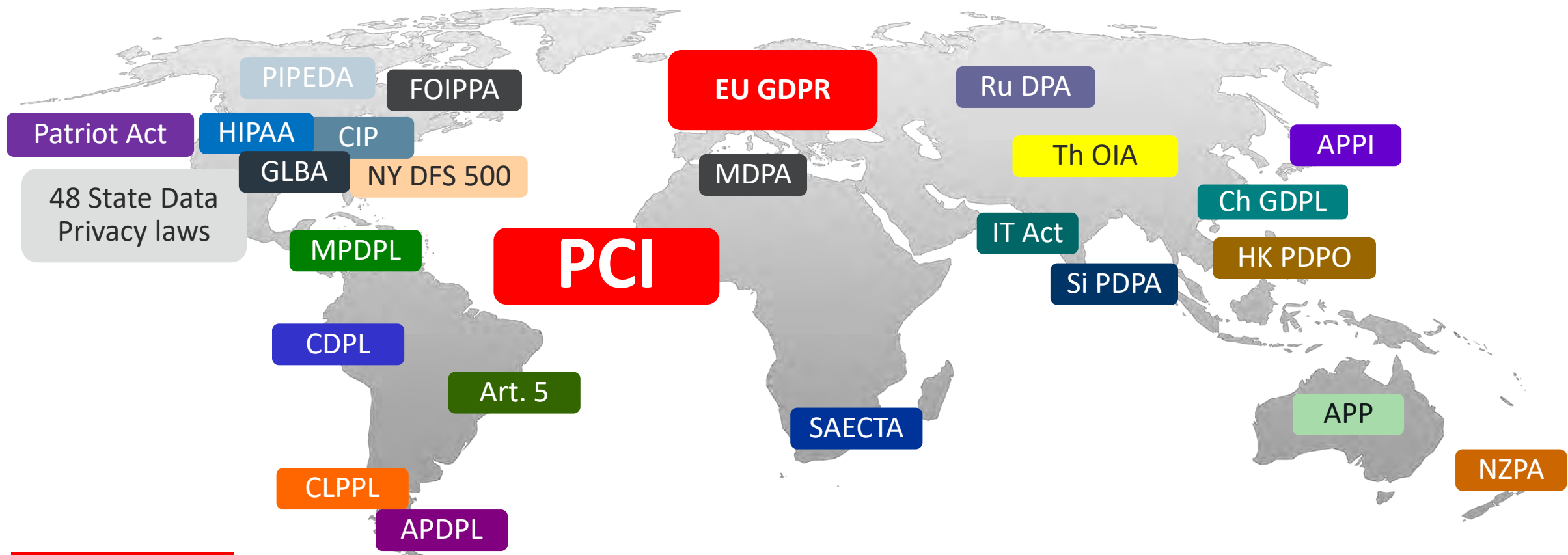
Comprehensive Database Security

Saikat Saha
Product Director
Database Security, Oracle
October 02, 2017

Safe Harbor Statement

The following 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.

Privacy & Security Regulations **Increasing** World-Wide



Data is Today's **Capital**

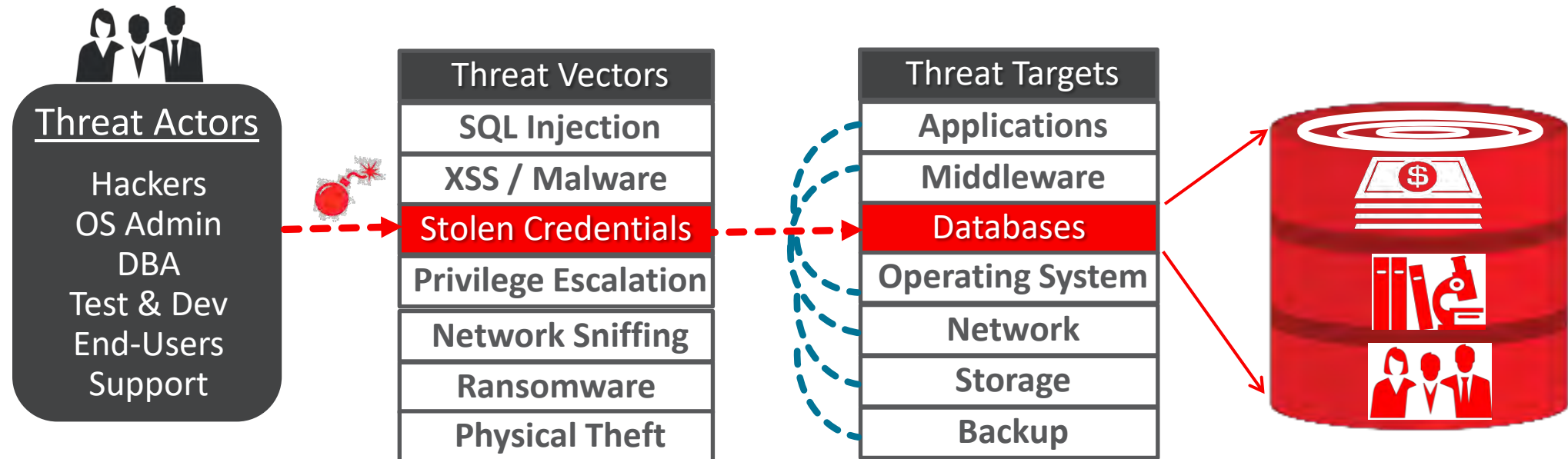
But in the Wrong Hands, Data Becomes the **New Liability**

- Data breaches are **exploding** world-wide
 - **Databases** continue to be the **prime target**
- **Fast Evolving, Stringent** Regulatory Landscape
 - Across industries and regions
 - Laws that aim to protect **data and citizen privacy**
- Data Security **Strategy**
 - Protect against multiple threat actors and multiple vectors
 - With **built-in, comprehensive** security controls
 - For **on-premise** and **cloud** databases



Changing Threat Landscape

Databases remain the Target



Comprehensive Database Security Controls

Evaluate



Prevent



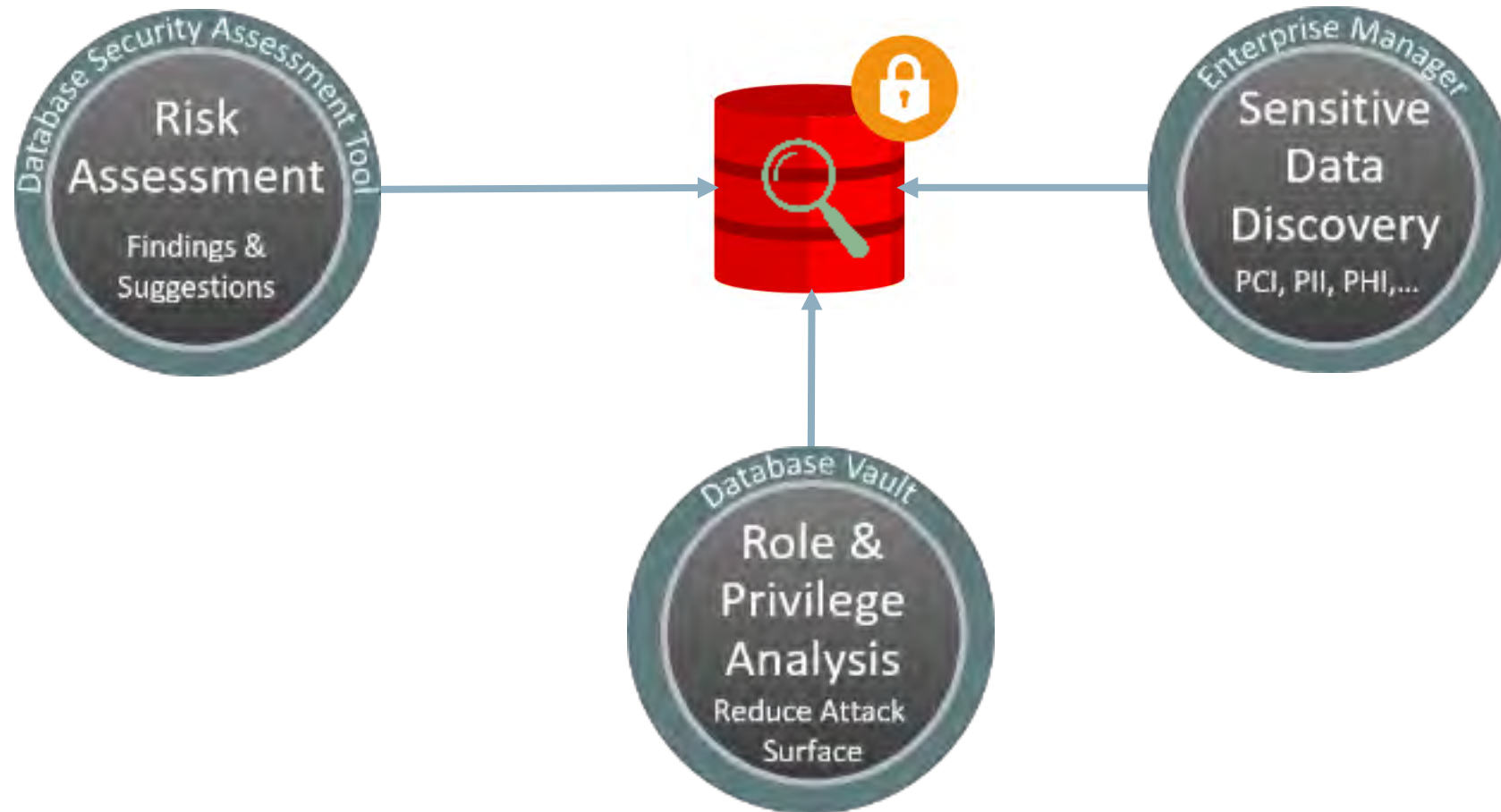
Detect



Data
Driven
Security



Evaluate Security Risks



Evaluative Controls – Customer Use Cases

US Insurance Provider

Situation: Dozens of production databases with no model of where sensitive data resides making it difficult to apply suitable security policies and controls

Solution: Sensitive Data Discovery with Oracle DB Security

Result: 400+ columns of SSN & other sensitive data identified

Benefit: Ability to apply appropriate security controls on data

Global Oil Field Services Provider

Situation: Hundreds of databases distributed around the globe, scattered across dozens of acquired companies; no unified configuration standard

Solution: Oracle Database Security Assessment (DBSAT)

Result: Significant misconfigurations identified, leading to a single configuration standard being applied everywhere

Benefit: Reduced risk of breach and easier security audits against a well-defined standard

Global Auto Manufacturer

Situation: Migrating SAP installation to a new infrastructure; desire to harden deployment at the same time

Solution: Oracle Database Security Assessment (DBSAT)

Result: Discovered many security issues including use of default SAP application account configured for password-less login

Benefit: Potential production vulnerability avoided

Very Large Semiconductor Manufacturer

Situation: Thousands of Oracle Databases managed by silos of administrators; no comprehensive picture of databases' security posture

Solution: Continuous compliance monitoring with Oracle Enterprise Manager Database Lifecycle Management Pack

Result: Near-real time alerts when any database configuration drift introduces security risk

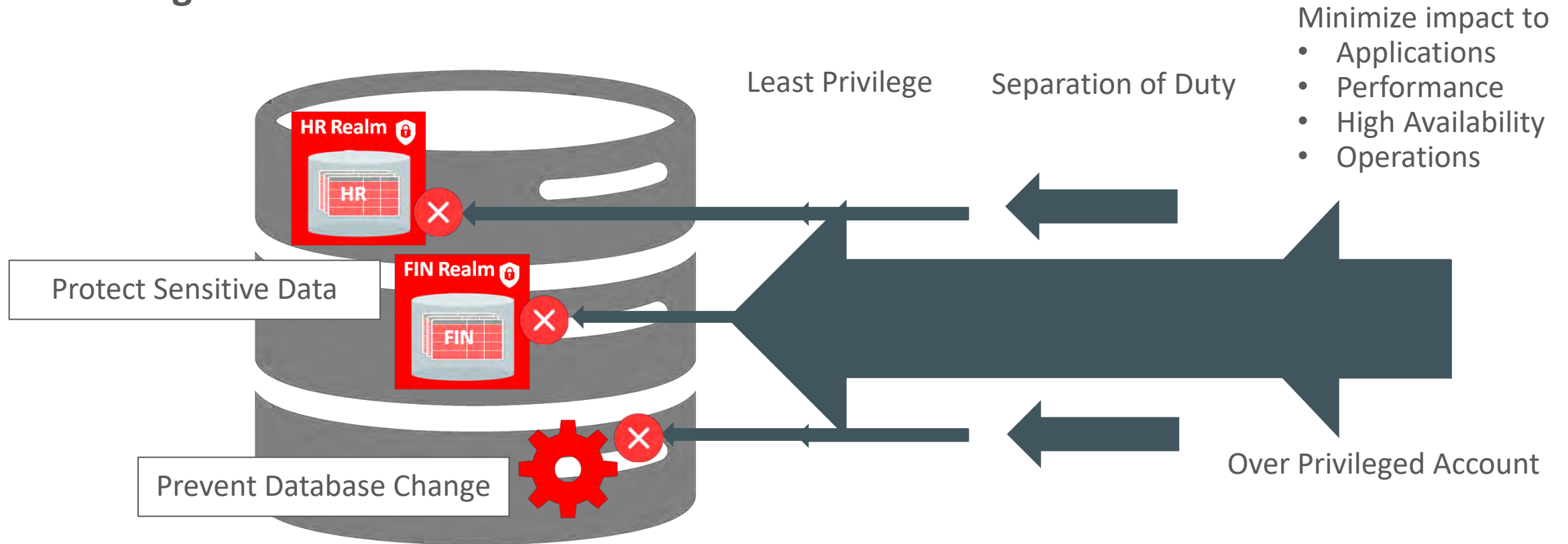
Benefit: Reduced audit costs, improved security

Prevent Data Compromise

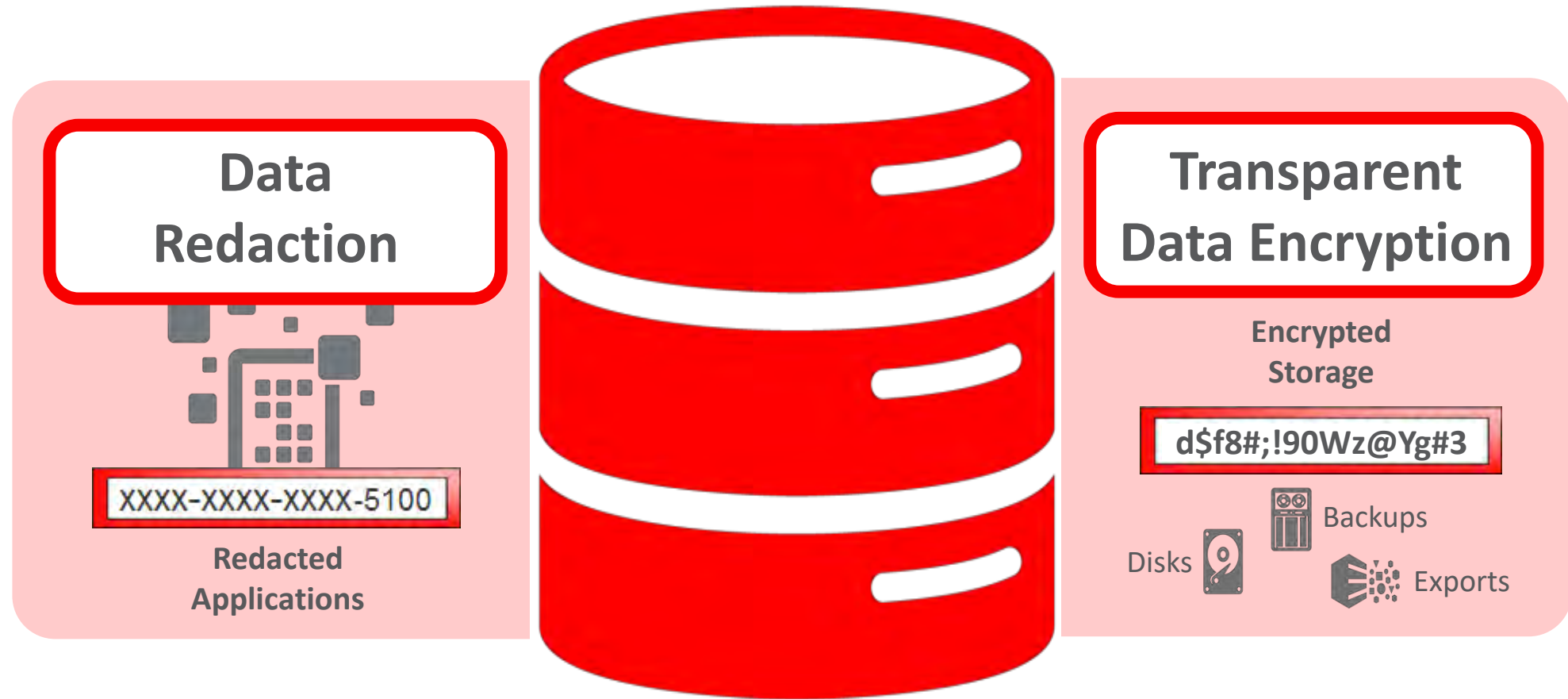


Oracle Database Vault

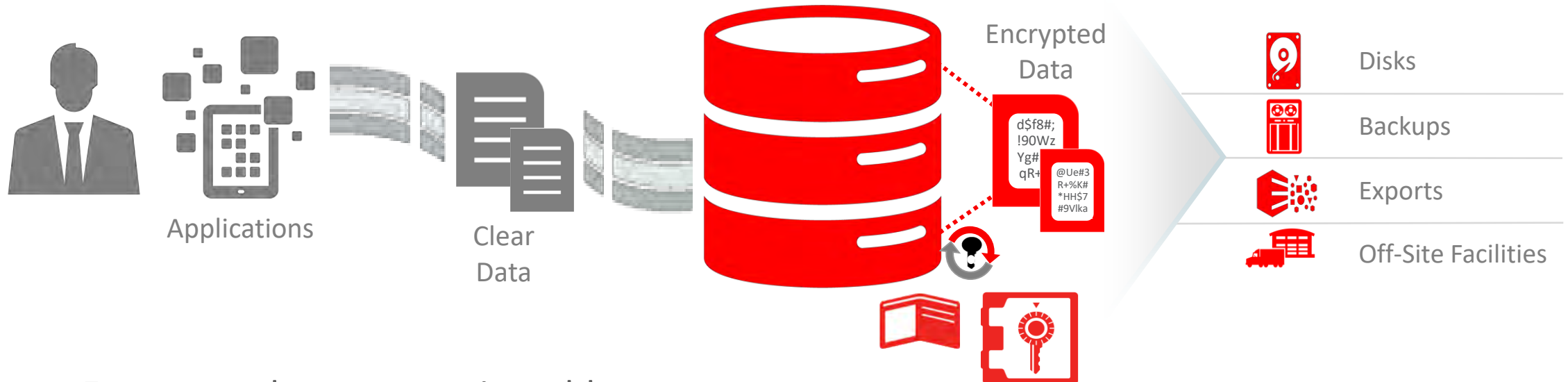
Reducing the Risk from Malicious Users



Oracle Advanced Security











Oracle Advanced Security Transparent Data Encryption (TDE)



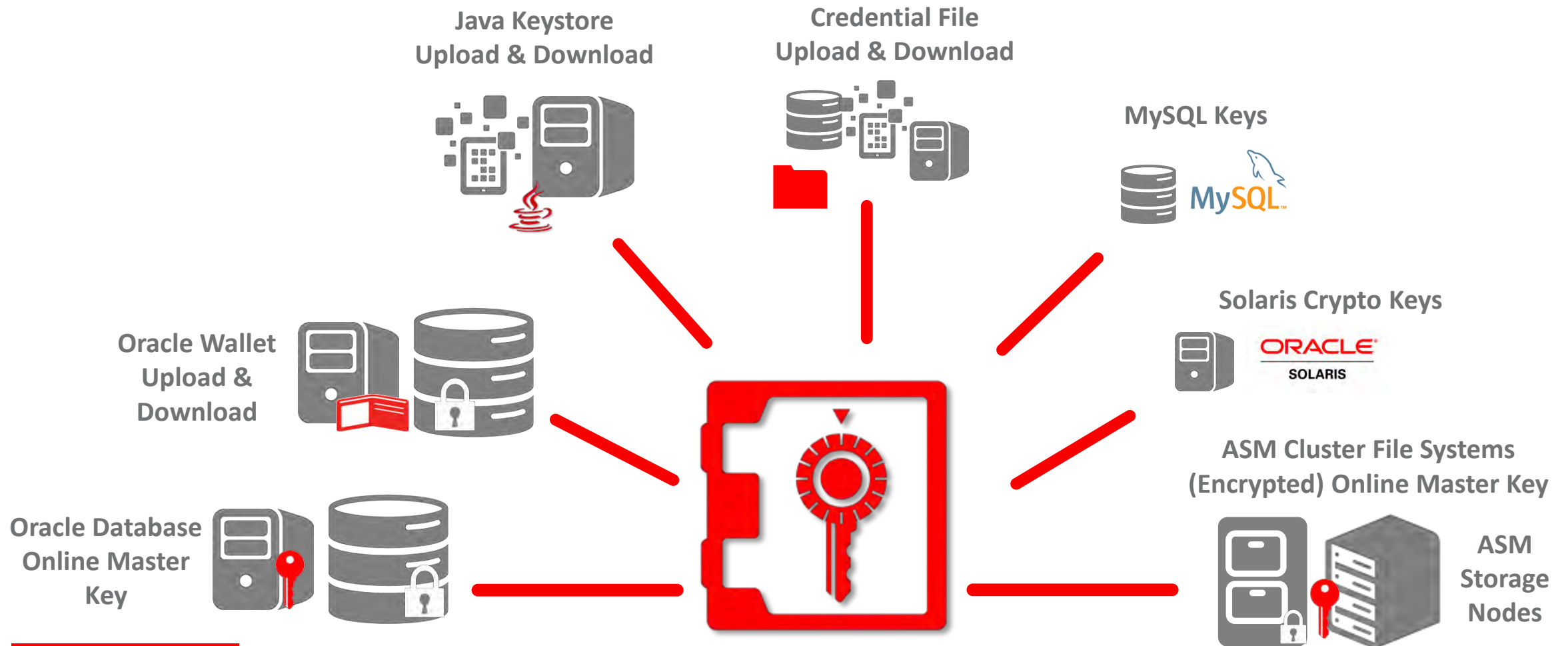
- Encrypts columns or entire tablespaces
- Protects the database files on disk and on backups
- High-speed performance
- Transparent to applications, no changes required
- Integrated with Oracle DB technologies



TDE Integration with Oracle Database

Database Technologies	Example Points of Integration	TDE Support
High-Availability Clusters	Oracle Real Application Clusters (RAC), Data Guard, Active Data Guard	
Backup and Restore	Oracle Recovery Manager (RMAN), Oracle Secure Backup	
Export and Import	Oracle Data Pump Export and Import	
Database Replication	Oracle Golden Gate	
Pluggable Databases	Oracle Multitenant Option	
Engineered Systems	Oracle Exadata Smart Scans	
Storage Management	Oracle Automatic Storage Management (ASM)	
Data Compression	Oracle Standard, Advanced , and Hybrid Columnar Compression	

Oracle Key Vault – Centralized Key Management



Preventive Controls – Customer Use Cases

Top Global Bank

Situation: 1,000s of databases; recent breach led to evaluation of security practices, and how they could be improved

Solution: Transparent Data Encryption and Oracle Database Vault

Result: Most databases encrypted within the first year. Database Vault security realms protect data from privileged accounts

Benefit: Confidentiality of data throughout the data lifecycle and protection from data loss from stolen privileged user credentials

Consumer Goods Manufacturer

Situation: Fourteen independent operating units consolidating different Oracle eBusiness Suite (EBS) instances; requirement to support migration and test

Solution: Data Masking with eBusiness Suite templates

Result: Substantial reduction in risk (and risk-mitigation costs) by removing sensitive data from non-production systems

Benefit: Initial consolidation of three business units was accomplished in the first year

Diversified Telecommunications Company

Situation: Board of Directors mandate to encrypt databases for critical applications by end of 2017

Solution: Transparent Data Encryption with Oracle Key Vault

Result: Encrypted 50 databases containing sensitive customer data

Benefit: Information protection throughout data lifecycle at scale with automated key management

European Government Ministry

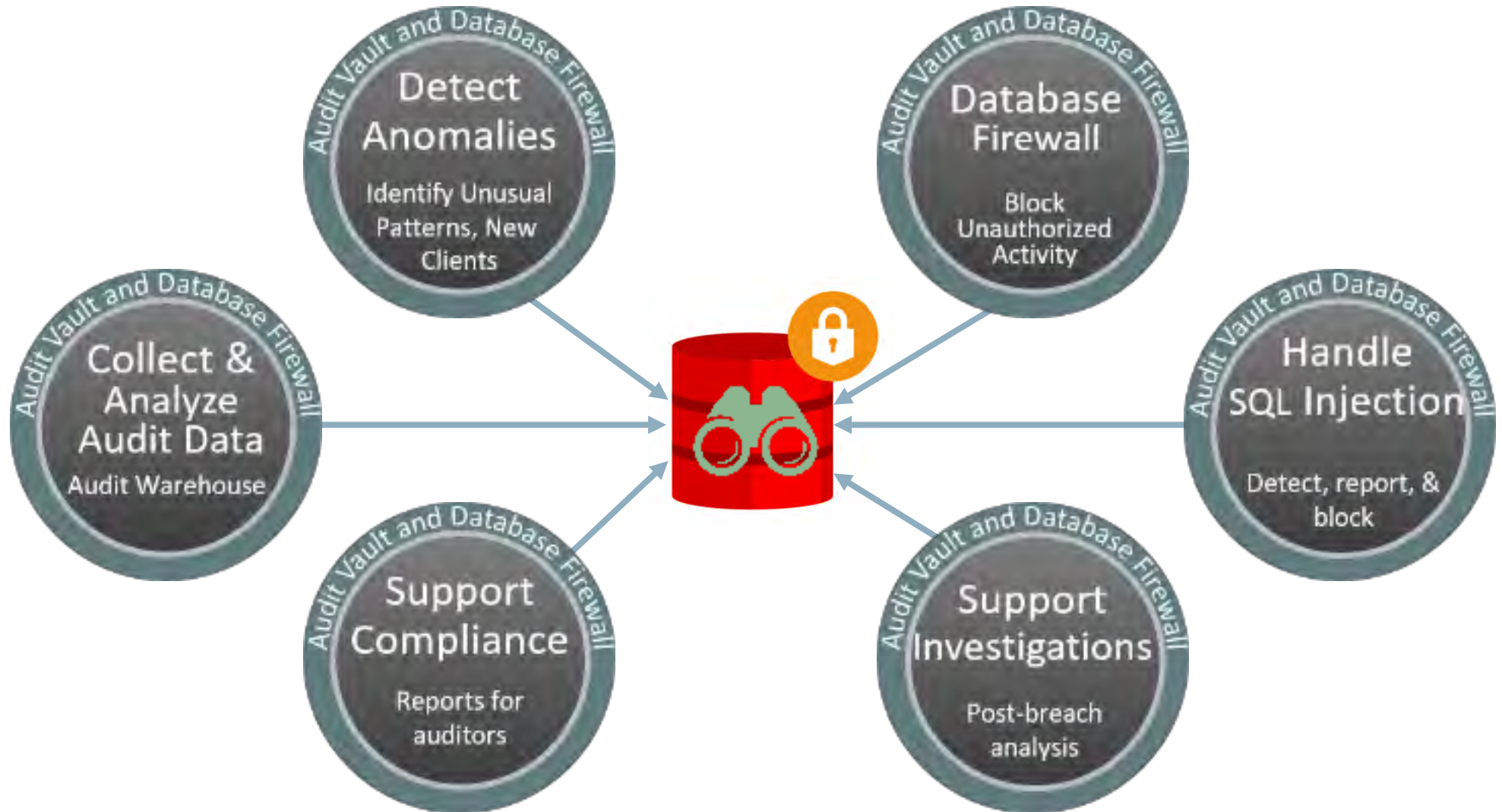
Situation: Hortonworks Hadoop with sensitive/classified information

Solution: BigData SQL, Oracle Data Redaction and Virtual Private Database (VPD) across Oracle DB and Hadoop

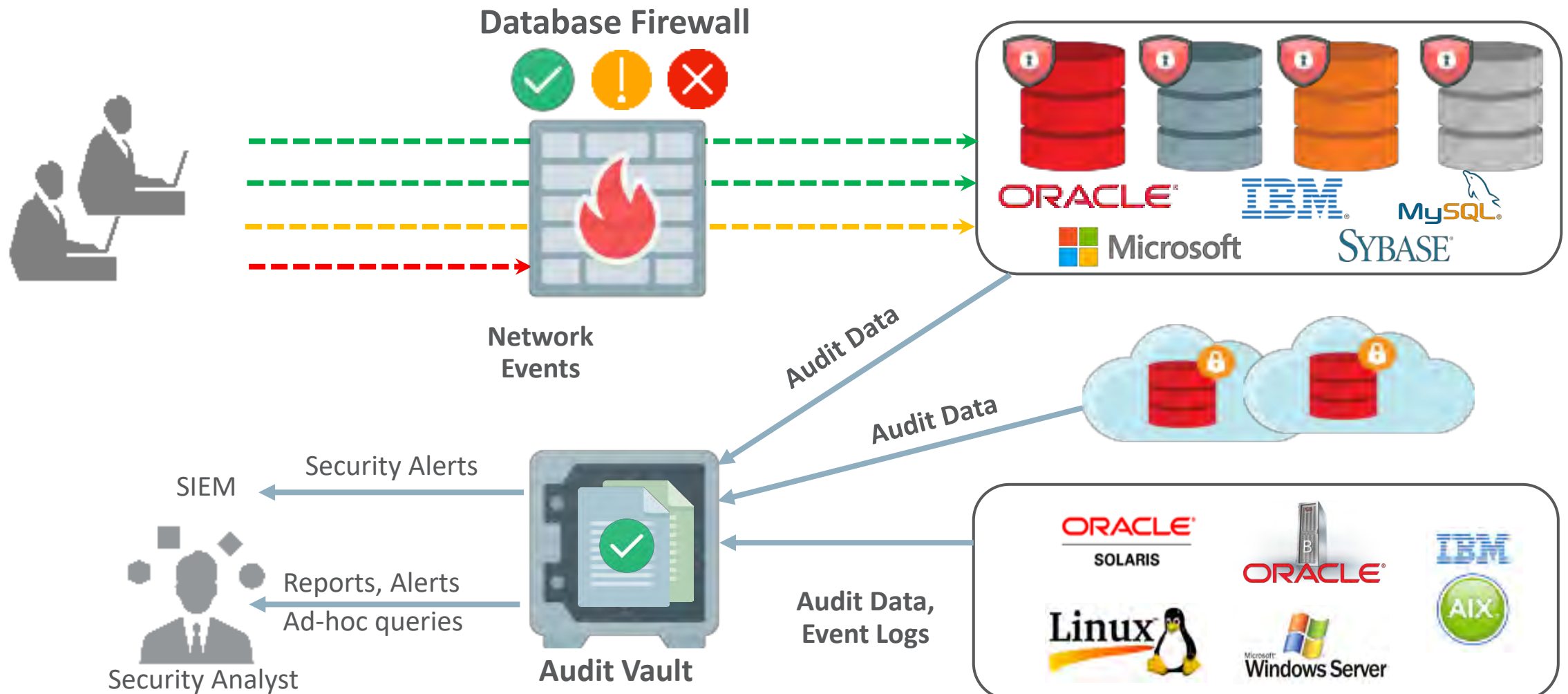
Result: Ability to restrict user access to sensitive data in data lake

Benefit: Data from a single big data repository can be shared among agencies while maintaining adherence to data classification policies

Detect Anomalies, Support Investigations



Monitor and Audit Enterprise Databases



Detective Controls – Customer Use Cases

North American Retailer

Situation: Heterogeneous DB environment supporting over 700 stores in US, Canada, Japan, Australia and Mexico; requirement to comply with complex world-wide privacy regulations

Solution: Oracle Audit Vault and Database Firewall

Result: Monitor over 400 databases (Oracle, IBM DB2, Microsoft SQL Server) with daily activity reporting from audit logs

Benefit: Improved security and streamlined compliance reporting

Multinational Semiconductor Company

Situation: 100s of production databases containing sensitive IP; need to monitor for potential attacks and support compliance audits

Solution: Oracle Audit Vault and Database Firewall

Result: 200+ databases monitored within 3 months with regular reporting of audit information

Benefit: Improved visibility and reporting for regulatory audits

National Health Ministry

Situation: Public health record system; requirement for bank-strength security features

Solution: Oracle Database Firewall

Result: Monitoring access to health records in multivendor systems (Oracle MySQL, Sybase, IBM, MS SQL Server) to detect suspicious or inappropriate behavior

Benefit: Improved posture for this patient “opt-in” service

Consumer Credit Reporting Company

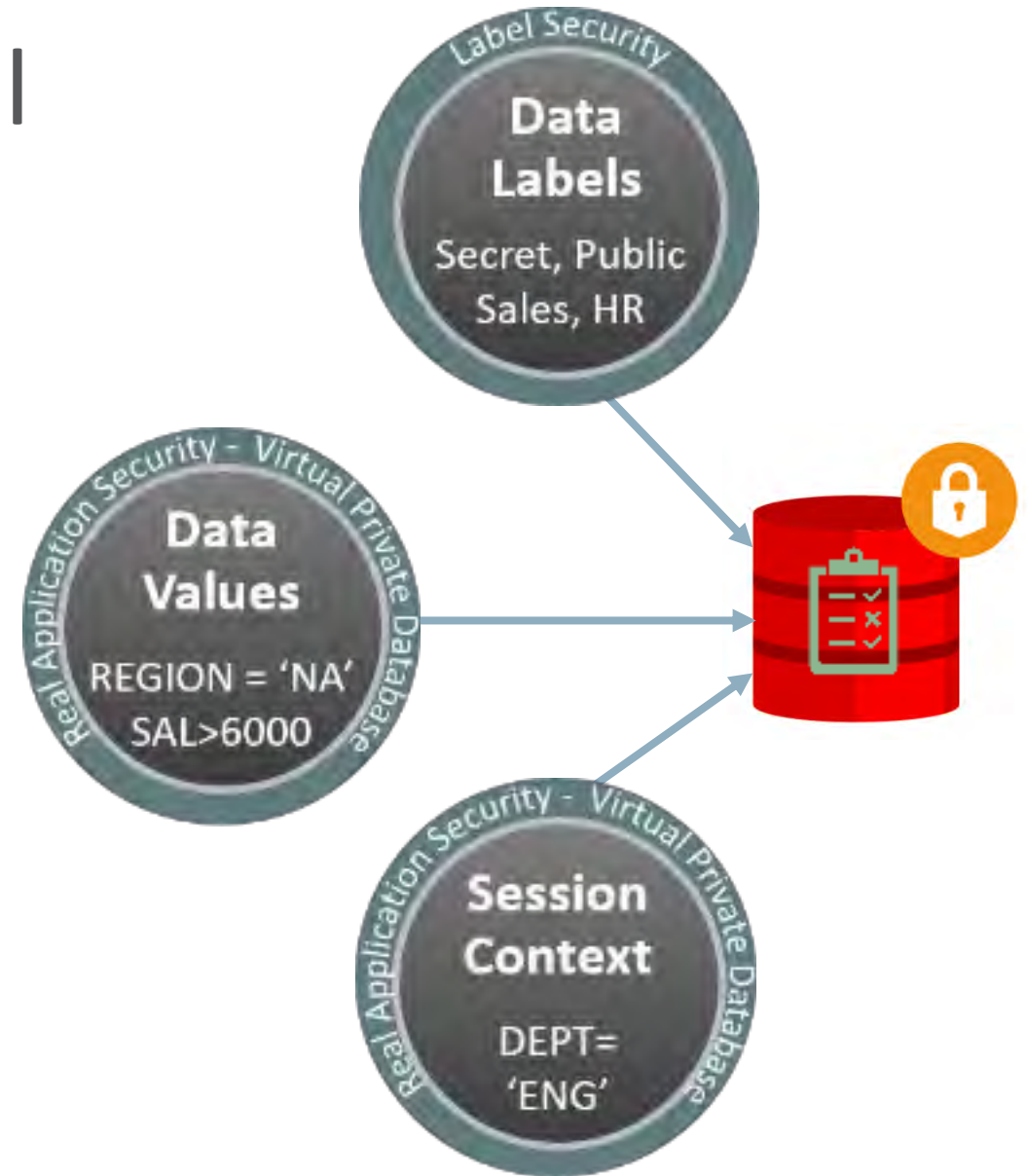
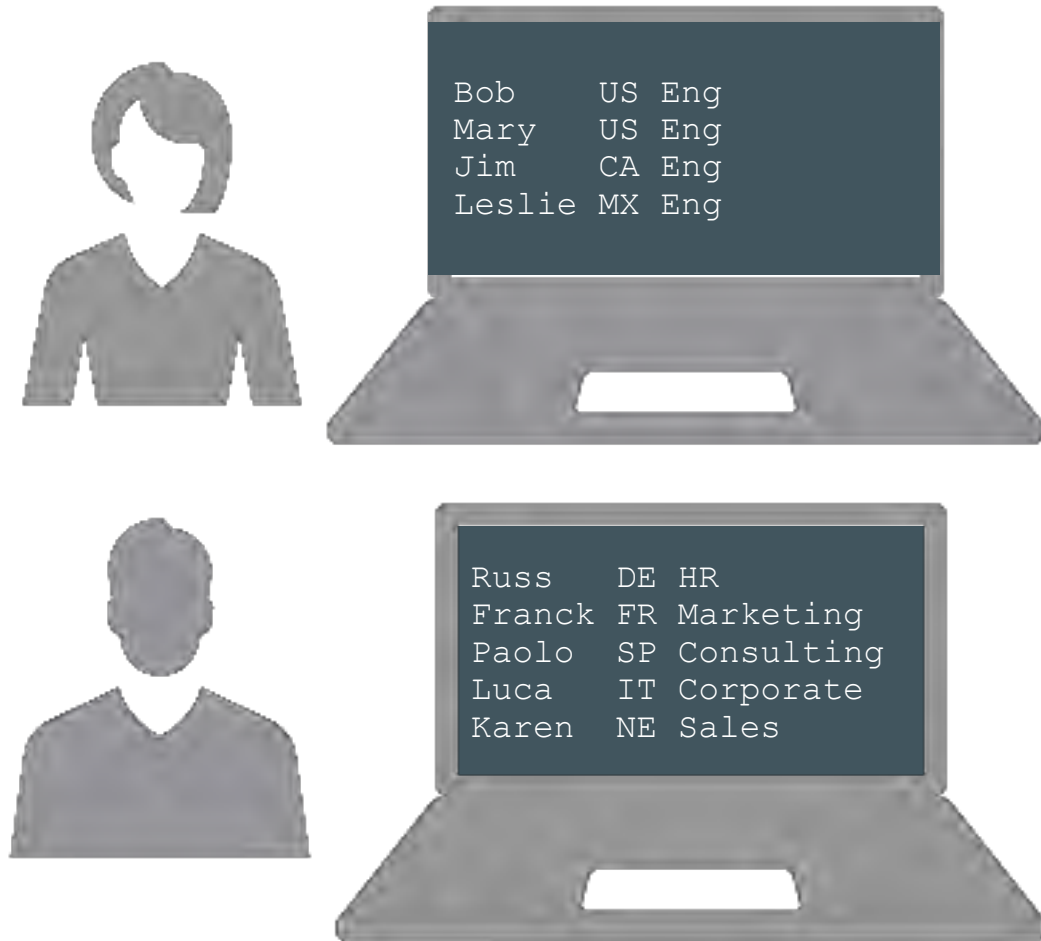
Situation: Need to comply with PCI DSS, SOX and GLBA

Solution: Oracle Database Firewall

Result: Monitoring of peak loads of 10k transactions/sec while maintaining database performance

Benefit: Improved database traffic visibility

Data-Driven Access Control



Data-Driven Security Controls – Customer Use Cases

Defense/Commercial Manufacturer

Situation: Managing data for both commercial and government customers; US ITAR regulations

Solution: Oracle Label Security

Result: Ability to comply with ITAR requirements for data using existing information systems

Benefit: Reduced systems and management costs

US Healthcare Provider

Situation: Consolidated patient data; HIPAA/HITRUST requirement for patient consent prior to data sharing

Solution: Oracle Label Security

Result: Enforcement of data access based with labels indicating patient consent status

Benefit: Compliance with HITRUST requirements with minimal system modifications

Electric Utility Service Provider

Situation: Securing multiple departmental applications from accessing Billing/utility data from diverse sources

Solution: Real Application Security data realms/columns

Result: Applications leverage common data access policy enforcement at database

Benefit: Cost savings; no access controls per applications

Large Asset Management Company

Situation: Hundreds of business analysts needing access to raw data, but not access to certain sensitive data elements

Solution: Virtual Private Database

Result: Column-level access controlled by data values

Benefit: Analysts were able to access data objects without risk of proliferation of sensitive data

Comprehensive Database Security Controls

Evaluate



Prevent



Detect



Data
Driven
Security



Comprehensive Database Security Controls

Defense in depth Security

EVALUATE	PREVENT	DETECT	DATA DRIVEN SECURITY
Privilege Analysis	DBA & Operation Controls	Database Firewall	Label based Security
Security Configuration	Data Masking and Subsetting	Centralized Monitoring	Real Application Security
Security Assessment	Key Management	Alerting & Reporting	Row Level Security
Sensitive Data Discovery	Data Redaction	Database Auditing	Crypto Toolkit for Applications
	Data Encryption		

Oracle Database Security Strategy

ANTICIPATE THREATS & MITIGATE



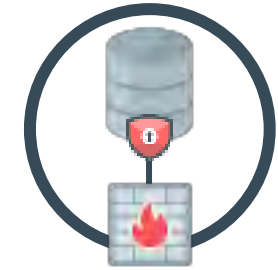
Transparent Data Encryption, DBA Control, Redaction, Masking, Privilege Analysis, DB Firewall, RAS, Cloud, ...

DEFENSE-IN-DEPTH SECURITY CONTROLS



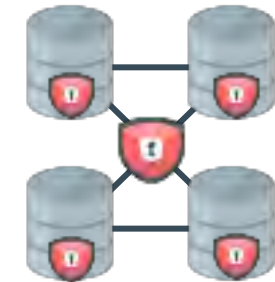
Overlapping controls: Encryption, masking, auditing, monitoring, access control, redaction, ...

SECURITY INSIDE-OUT



Security close to the data: Eliminates guesswork, maximizes performance, application transparency

ENTERPRISE DEPLOYMENTS



Across multiple systems: Operating systems, heterogeneous databases, applications, Cloud, ...

Passport to the Cloud

Analytics

Monday's Word Of The Day

Remember this word and return to the reception desk in the IT Infrastructure area in Moscone West left rear to have your Passport stamped.

Database Security at Oracle OpenWorld 2017

Session	Title	Speaker	Location	Date & Time
CON6571	Cybersecurity and Compliance in 2017: Database Security Is Business-Critical	Vipin Samar, SVP, Oracle	Moscone West - 3011	Mon., 1:15-2:00 PM
CON6574	NEW FEATURE! Centralized Database User Management Using Active Directory	Alan Williams, Oracle Keith Wilcox, Epsilon	Moscone West - 3011	Mon., 3:15-4:00 PM
CON6575	NEW! Database Security Assessment Tool Discovers Top Security Risks	Pedro Lopes, Oracle	Moscone West - 3011	Mon., 5:45-6:30 PM
CON6573	Data Management and Security in the GDPR Era	Russ Lowenthal, Oracle Franck Hourdin, Oracle Mike Turner, Capgemini	Moscone West - 3011	Tues., 3:45-4:30 PM
CON6580	Encrypt Your Crown Jewels and Manage Keys Efficiently with Oracle Key Vault	Saikat Saha, Oracle Hamid Habet, Allianz	Moscone West - 3011	Tues., 4:45-5:30 PM
CON6576	Accelerate Your Compliance Program with Oracle Audit Vault and Database Firewall	Ram Subramanian, Symantec Rohit Muttepawar, Symantec George Csaba, Oracle	Moscone West - 3011	Tues., 5:45-6:30 PM
CON6572	Inside the Head of a Database Hacker	Mark Fallon, Oracle	Moscone West - 3014	Wed., 11:00-11:45 AM
CON6618	Sneak Preview: Oracle Data Security Cloud Service	Vikram Pesati, Oracle Michael Mesaros, Oracle	Moscone West - 3011	Wed., 2:00-2:45 PM
CON6578	Top Five Tips for Building Secure Database Applications	Scott Rotondo, Oracle	Moscone West - 3011	Wed., 4:30-5:15 PM

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.

Integrated Cloud

Applications & Platform Services

ORACLE®