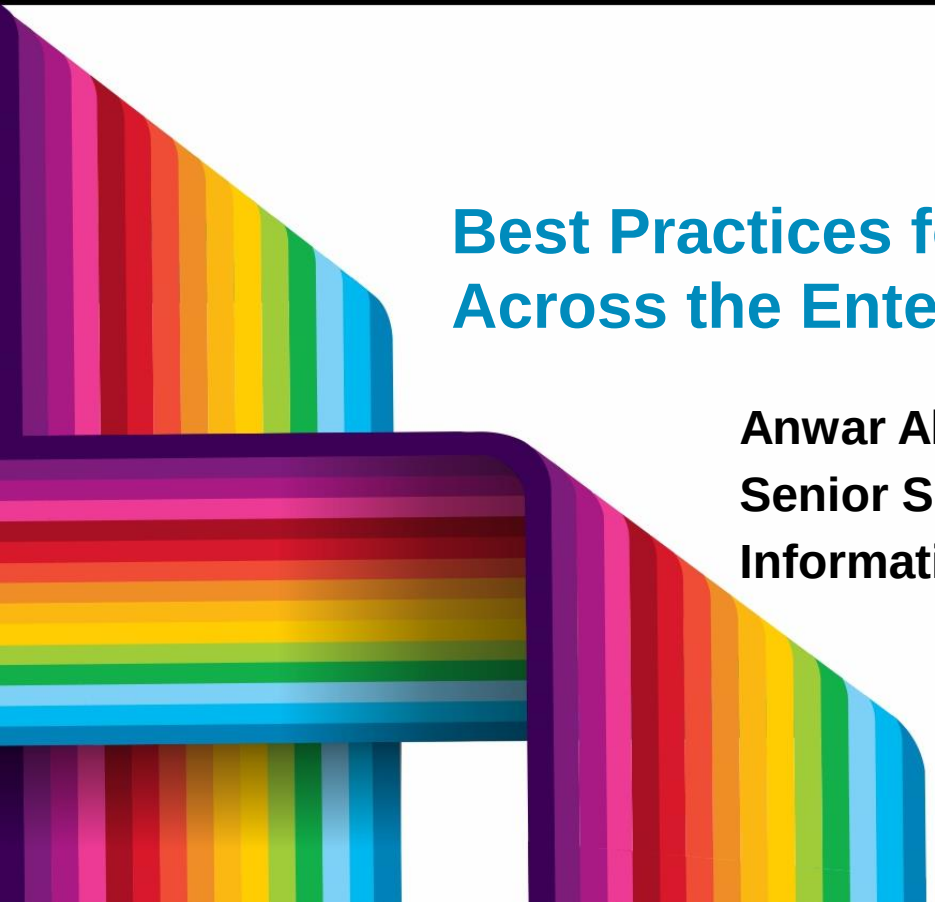
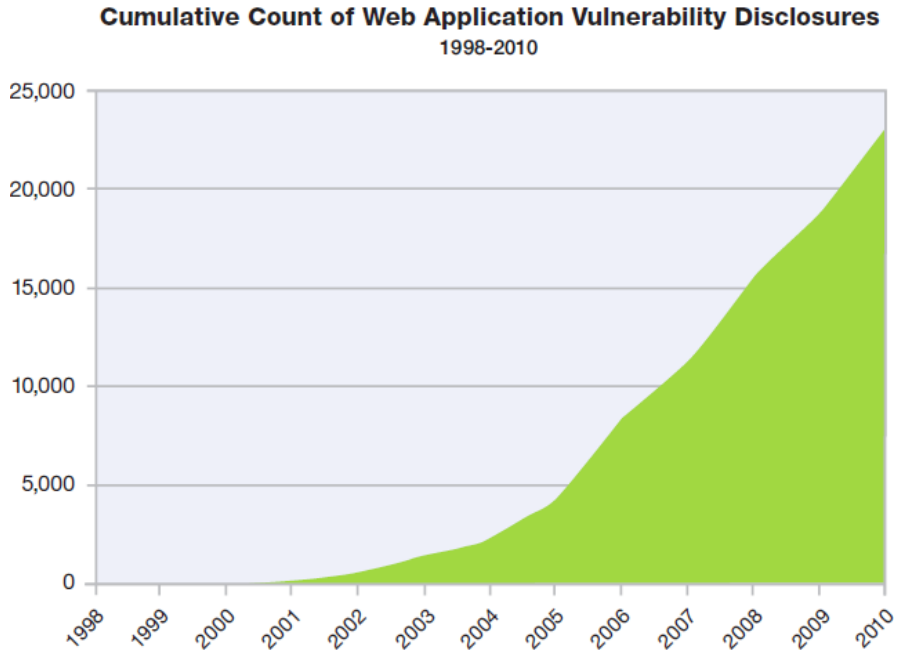
Business Connect
IBM Software Universe 2013
Meet Possible
19th March, Colombo

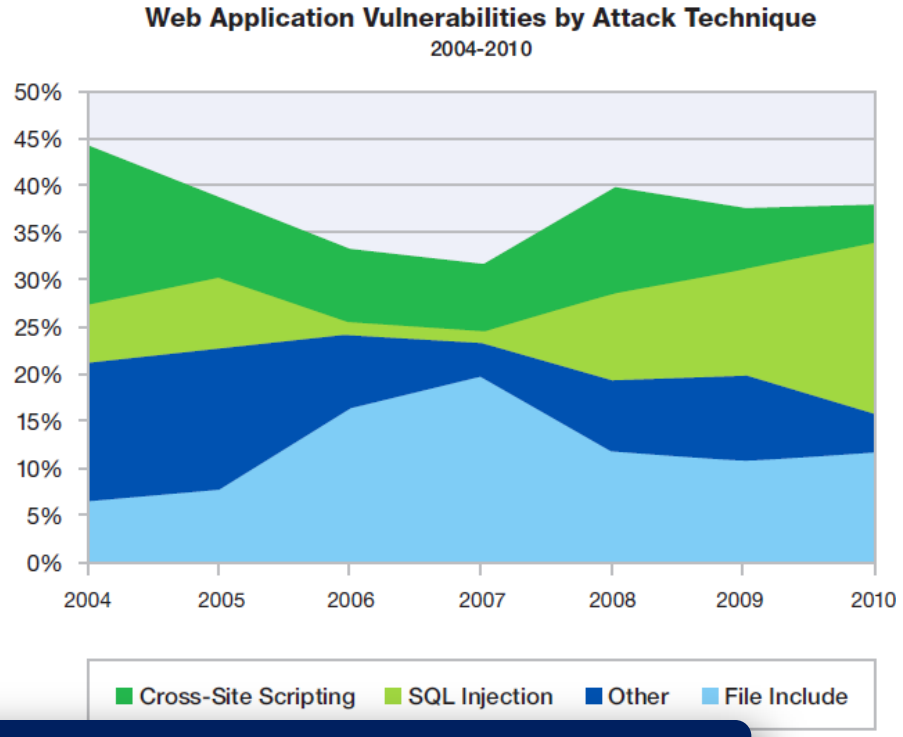


Best Practices for Protecting Information Across the Enterprise

Anwar Ali
Senior Solution Consultant
Information Management

Web Application Vulnerabilities Continue to Rise





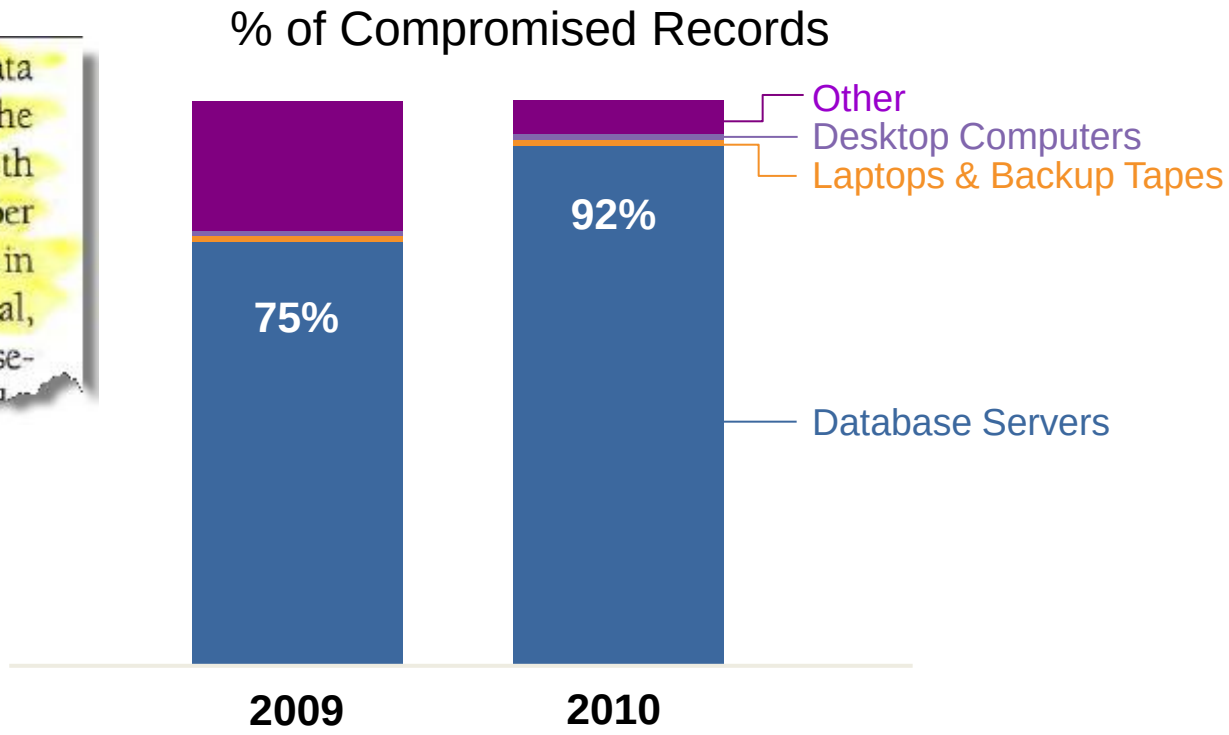
"The majority of web applications are custom … **the total number of web application vulnerabilities is likely much larger than the quantity of public reports** … Web application vulnerabilities may vastly exceed the quantity of other kinds of security issues on the Internet.

Source: IBM Security Solutions X-Force® Trend and Risk Report
www.ibm.com/security/xforce

Database Servers are the Primary Source of Breached Data

For example, the 2010 Verizon data breach report places databases as the top type of compromised asset by both the number of breaches and the number of records stolen. Yet our investments in protecting database systems is minimal, at best. When it comes to database se-

InformationWeek
"Epic Fail"
10/11/2010

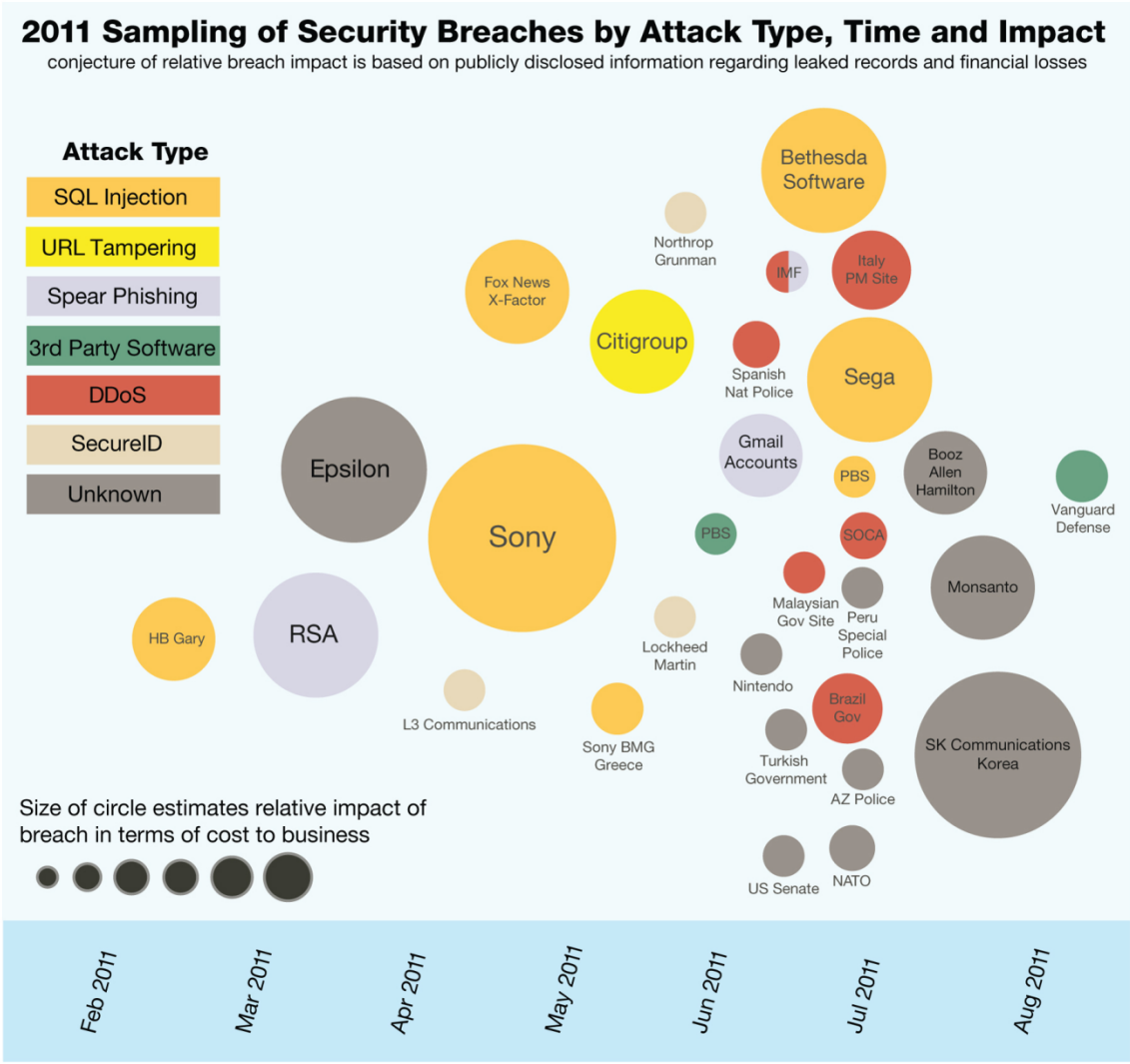


Sources: Verizon Business Data Breach Investigations Report 2009, 2010
www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Although much angst and security funding is given to ***offline data, mobile devices, and end-user systems,*** *these assets* ***are simply not a major point of compromise****."*

Data Breach in News

- Litany of significant data breaches
- Frequency is UP
- Security competence of many of the victims is … DOWN
- Attacks are getting more and more sophisticated.



Source: IBM X-Force® Research and Development

InfoSphere provides a complete data protection approach

Monitor database activity & assess vulnerabilities

Deploy centralized controls for real-time database monitoring

- ✓ *Policy-based controls to detect unauthorized activity*
- ✓ *Vulnerability assessment & change auditing*

InfoSphere Guardium DAM & VA Solution

Encrypt structured and unstructured data

Encrypt data with negligible performance impact

- ✓ *Encrypt files and structured data*
- ✓ *Unify policy and key management for central administration*

InfoSphere Guardium Data Encryption

Mask structured data

De-indentify sensitive data

- ✓ *Mask with pre-build functions or customize*
- ✓ *Mask consistently across systems*

InfoSphere Optim Data Masking

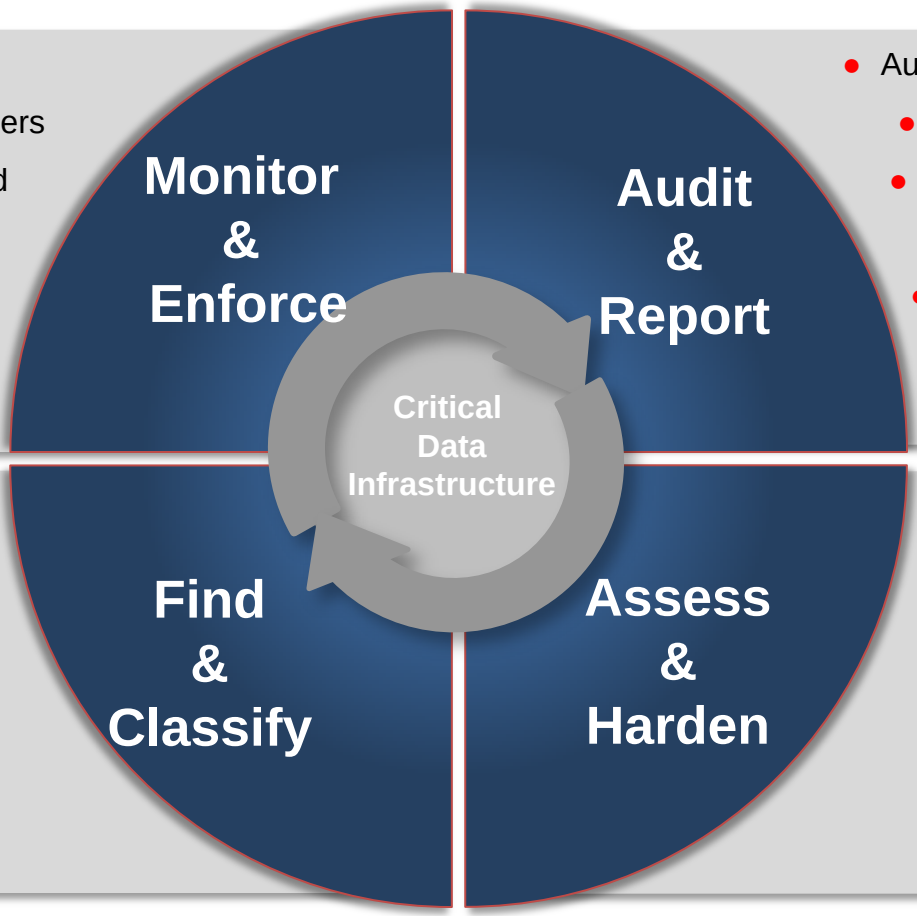
Satisfy compliance and regulatory mandates

Database Activity Monitoring & Vulnerability Assessment

Addressing the Full Lifecycle of Database Security & Compliance

Real-Time Database Security & Monitoring

- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration



- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)

The Compliance Mandate – What do you need to monitor?

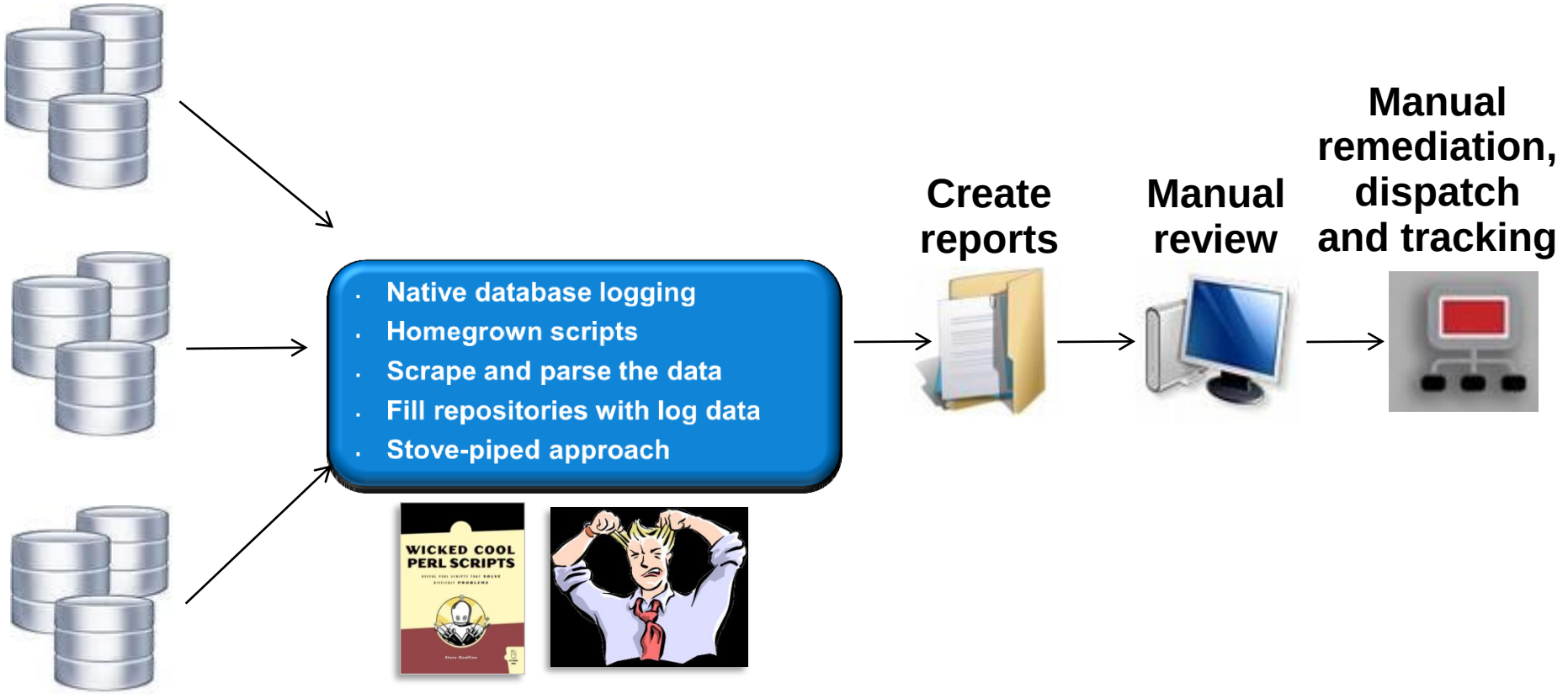
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

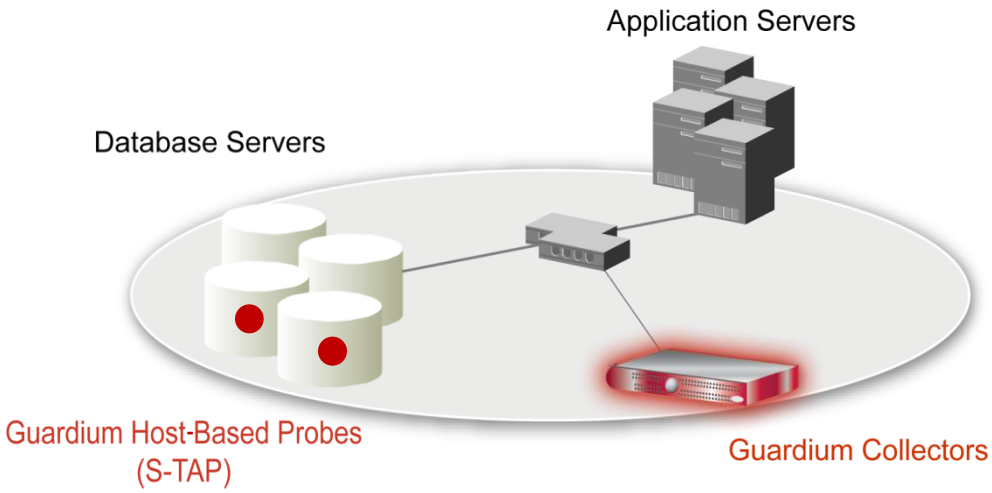
How Guardium Addresses PCI-DSS

Req	Description	InfoSphere Guardium Capability
2	**Do not use vendor defaults for system passwords**	**Comprehensive suite of DBMS-specific tests based upon industry standards (CIS, STIG)**
	• Configure system parameters to prevent misuse • Encrypt non-console admin access	✓ Checks for default passwords, unpatched systems, misconfigured privileges, etc. ✓ Audits usage and alerts on misuse ✓ Locks configurations after vulnerabilities remediated ✓ Monitors encrypted traffic (Oracle, ASO, SSL, etc.) without need for key storage
3	**Protect stored cardholder data**	**Real-time database leak prevention**
		✓ Continuous, real-time, policy-based monitoring with proactive security (alerts, blocking) ✓ Compensating control for column-level encryption ✓ Auto-discovers & classifies data; Identifies sensitive data in query result stream
6	**Maintain secure systems**	**Centralized vulnerability and configuration assessment**
	• Establish a process to identify security vulnerabilities • Follow change control procedures for all configuration changes • Separation of duties (development, test, and production)	✓ Ensures current patches applied and vulnerable SPs identified; “Virtual Patching” ✓ Alerts on all configuration changes, inside and outside databases ✓ Enforces separation of duties with real-time alerting and granular access controls
7	**Restrict access to cardholder data**	**Proactive, real-time access control (independent of native DBMS controls)**
		✓ Policies defined by source IP or application, OS or DB user, time, SQL command, object, etc. ✓ Blocks any unauthorized user, including administrators, from accessing cardholder data ✓ Compensating control for unsegmented networks.
8	**Assign a unique ID to each person with computer access**	**Complements native DBMS controls with external, cross-DBMS controls**
	• Enforce password policies • Limit repeated access attempts	✓ Alerts on credential sharing, failed logins, account creation, privilege escalation ✓ Verifies password policies are enforced; can lock accounts or terminate sessions
10	**Track and monitor access to cardholder data**	**Continuous, granular auditing with scalable architecture to handle high transaction volumes**
		✓ Fine-grained audit trail of all database activities (SELECT, DDS, DML, DCL, logins, logouts, etc.) ✓ Does not rely on native trace or audit logs: minimal perf. Impact (2-3%), enforces sep. of duties. ✓ Tracks all network and local connections, including direct access by DBAs (shared memory, etc.) ✓ Audit information stored securely in hardened appliance to prevent anti-forensics or tampering ✓ Identifies fraud by resolving end-user IDs in connection-pooling apps (SAP, Cognos, PeopleSoft, etc.) ✓ Integrates with LDAP, IAM, TCIM, TSM, SIEM, change management, CMDBs, etc.) ✓ Compliance workflow automation (electronic sign-offs, escalations) demonstrates oversight process ✓ PCI Accelerator provides pre-configured reports based on best practices
11	**Regularly test security systems and process**	**Integrated vulnerability scanning, file integrity monitoring & behavioral vulnerability testing**
	• Run internal and external vulnerability scans • Deploy integrity monitoring to detect mods of critical system files	✓ Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations ✓ Tracks changes to DB configuration files, environment/registry variables, executables and OS files
12	**Maintain an Information Security Policy**	**Robust automated controls for enforcing information security policies**
	• Monitor/Analyze alerts and distribute to appropriate personnel • Monitor and control all access to data	✓ Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration ✓ Automated sign-offs demonstrate formal oversight process ✓ 100% visibility & control over all database transactions (with blocking)

What Database Audit Tools are Enterprises Using Today?



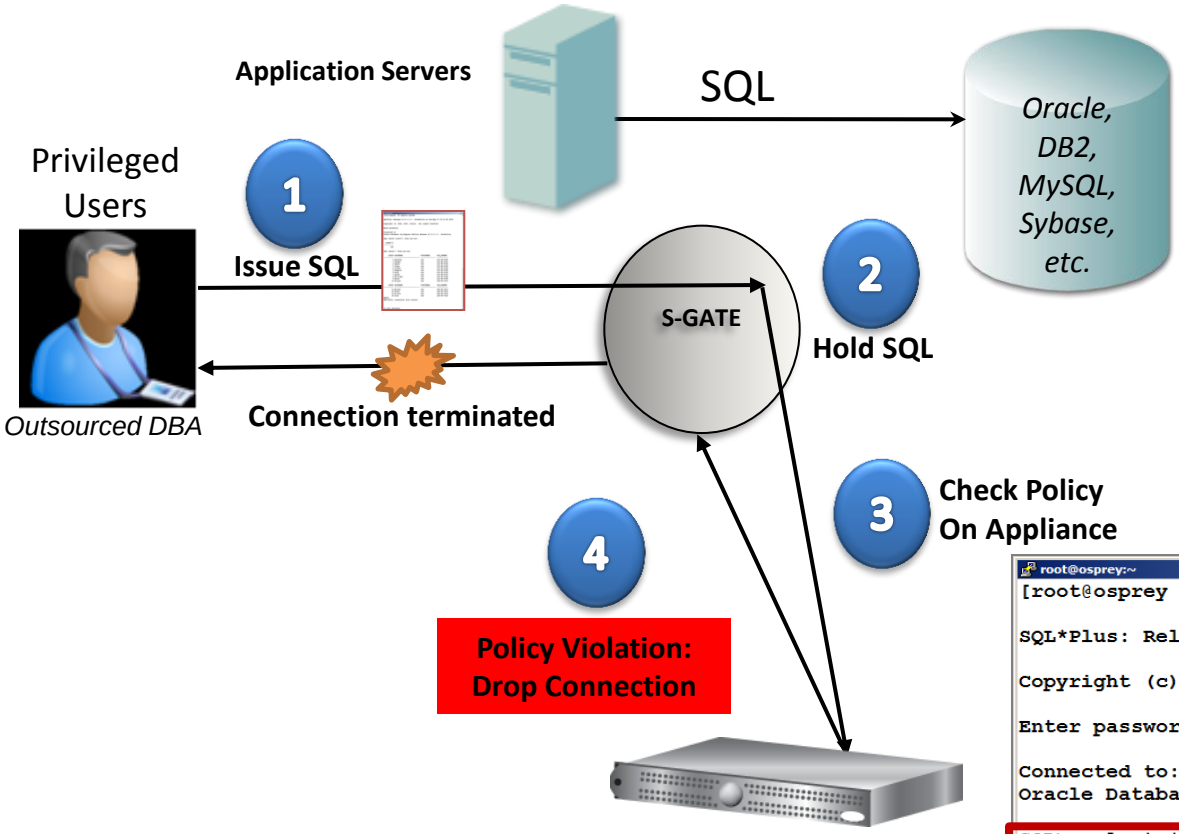
Non-Invasive, Real-Time Database Security & Monitoring



- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes

- Supports Separation of Duties
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

Cross-DBMS, Data-Level Access Control (S-GATE)

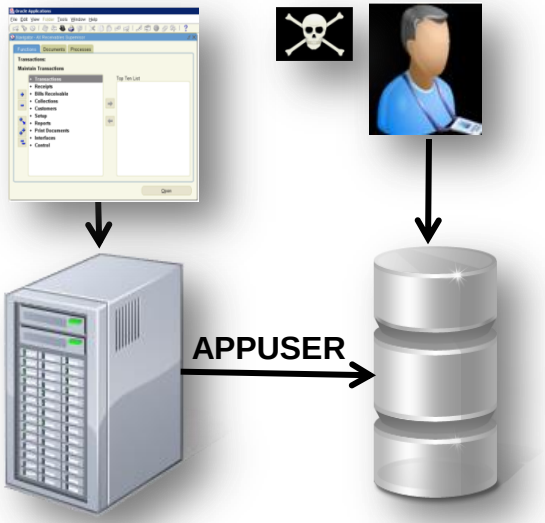


- ✓ Cross-DBMS policies
- ✓ Block privileged user actions
- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic

```
root@osprey:~
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel


SQL>
```

Session Terminated

Granular Policies with Detective & Preventive Controls



Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

Not ☐ Server IP / and/or Group: Production Servers

Not ☑ Client IP / and/or Group: Authorized Client IPs

Not ☐ Client MAC | Net. Protocol | and/or Group

Not ☐ DB Name

Not ☐ DB User: APPUSER

Field Name

Object: INVENTORY

Command: DROP TABLE

Min. Ct. 0 | Reset Interval (minutes) 0

Continue to next Rule ☐ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

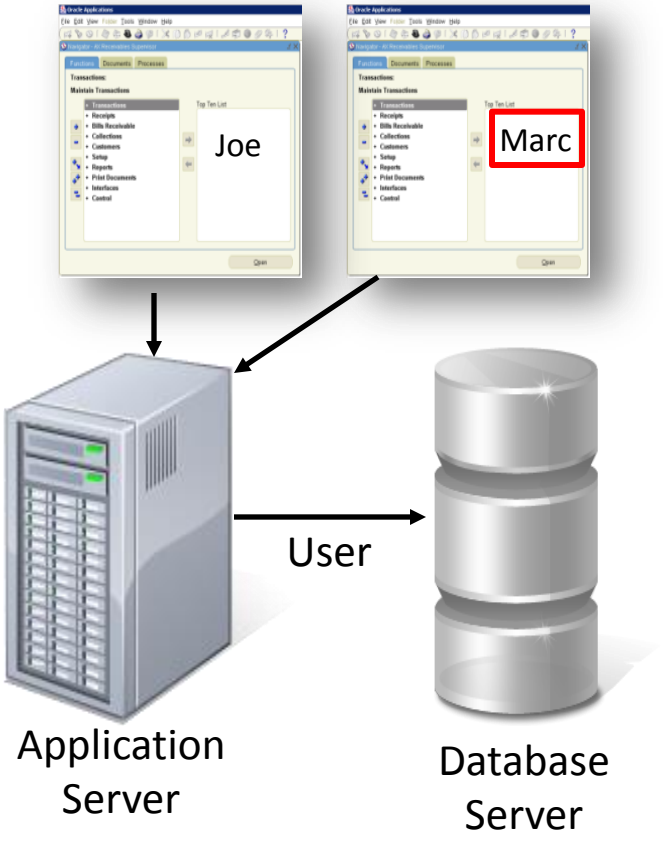
☒ Notification Type MAIL Mail User marc_gamache@guardium.com

ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

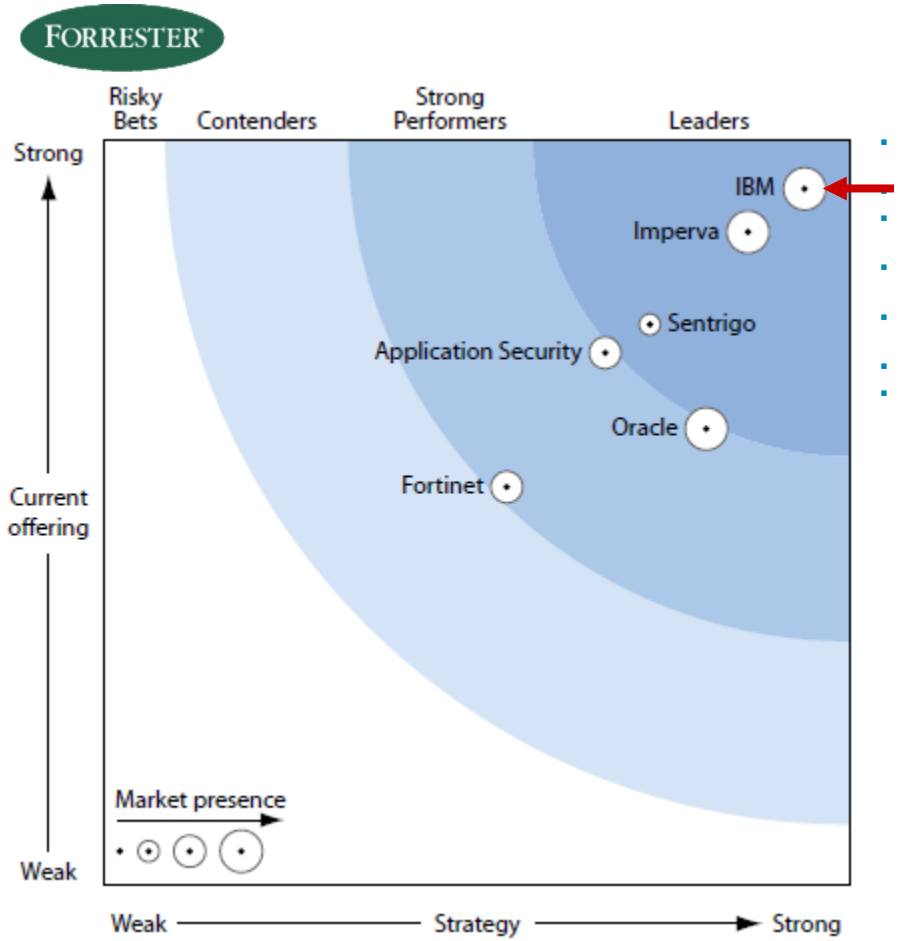
Identifying Fraud at the Application Layer



DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***Issue***: Application server uses generic service account to access DB
  - ***Doesn't identify who*** initiated transaction (connection pooling)
- ***Solution***: Guardium tracks access to application ***user associated with specific SQL commands***
  - Out-of-the-box support for all major enterprise applications (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) and custom applications (WebSphere, WebLogic, ….)
  - Deterministic vs. time-based "best guess"
  - No changes to applications

Highest Overall Score for Current Offering, Strategy, & Market Presence



- *"Guardium continues to demonstrate its leadership in supporting very large heterogeneous environments, delivering high performance and scalability, simplifying administration, and performing real-time database protection."*
- *"IBM continues to focus on innovation and extending the Guardium product to integrate with other IBM products."*
- *#1 score in all 3 Top Categories and all 17 subcategories along with perfect scores for Audit Policies; Auditing Repository; Corporate Strategy; Installed Base; Services; and International Presence.*
- *"Guardium offers support for almost any of the features that one might find in an auditing and real-time protection solution."*
- *"Guardium offers strong support for database-access auditing, application auditing, policy management, auditing repository, and real-time protection."*
- *"Guardium has been deployed across many large enterprises and hundreds of mission-critical databases."*
- *"IBM offers comprehensive professional services to help customers with complex environments as well as those who need assistance implementing database security across their enterprise."*

Source: "The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011" (May 2011)

Chosen by Leading Organizations Worldwide

- 8 of the top 10 global banks
- 5 of the top 6 global insurers
- 4 of the top 4 health care providers
- 8 of the top 10 telecoms
- 3 of the top 4 auto makers
- 3 of the world’s favorite beverage brands
- 2 of the top 3 global retailers

- Top government agencies
- Top global cardholder brand
- Top energy suppliers
- The most recognized name in PCs
- #1 dedicated security company
- Media & entertainment brands
- International airline brands

Validated by Industry Experts

"Dominance in this space"
#1 Scores for Current Offering, Architecture & Product Strategy

"Most Powerful Compliance Regulations Tools ... Ever"

"5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based security."

"Guardium is ahead of the pack and gaining speed."

"Top of DBEP Class"
"Practically every feature you'll need to lock down sensitive data."

2007 Editor's Choice Award in "Auditing and Compliance"

"Enterprise-class data security product that should be on every organization's radar."

Data Encryption

The Data Threats – Data at Rest & Data in Transit

- Online – internal threats
  - Attackers breaking through perimeter security
  - Privileged user abuse
  - Data replicates to many locations
- Offline – theft and loss
  - Backups typically written to portable media
  - Often stored offsite for long periods

- Onwire – internal and external threats
  - Hackers and sniffers picking data off the network

Encryption Technologies

- Inline Encryptors – Block device encryptors
  - Application/Database Transparency
  - Limited threat capabilities (theft of storage device)
  - Limited key management and auditing
- Column Encryption
  - OS Transparency
  - Affects application development, database design, SQL Plans, and performance
  - Limited to database data only data
- Application Encryptors
  - Feature Rich
  - Application Intrusive (application code changes required)
  - Affects application development, database design, SQL Plans, and performance
  - Purchased Applications will not work
- File & Tablespace & Backup Encryption
  - Application Transparency
  - Feature Rich
  - OS Dependent
  - No DBMS security independent

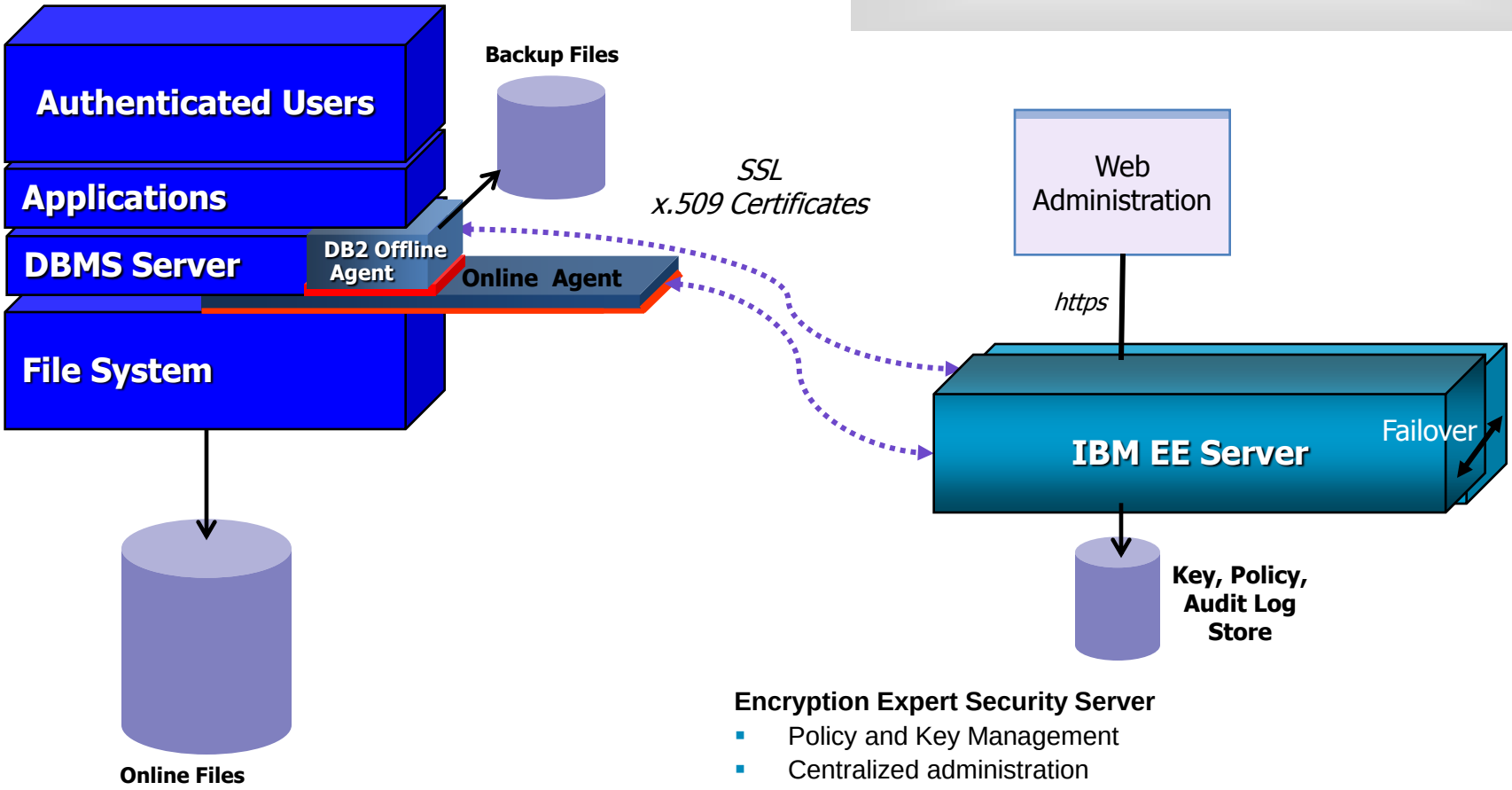
What is IBM Database Encryption Expert?

- Data protection for your database environments
  - High performance encryption, access control and auditing
  - Data privacy for both online and backup environments
  - Unified policy and key management for centralized administration across multiple data servers
- Transparency to users, databases, applications, storage
  - No coding or changes to existing IT infrastructure
  - Protect data in any storage environment
  - User access to data same as before
- Centralized administration
  - Policy and Key management
  - Audit logs
  - High Availability

Encryption Expert Architecture

Components:

- EE Security Server
- EE Secure Offline Agent
- EE Secure File System Online Agent



Encryption Expert Security Server

- Policy and Key Management
- Centralized administration
- Separation of duties

Data Masking

Vulnerable non-production environments at risk

Most ignore security in non-production environments

70%

of organizations surveyed use live customer data in non-production environments (testing, Q/A, development)

Database Trends and Applications. *Ensuring Protection for Sensitive Test Data*

$194

per record
cost of a data breach

The Ponemon Institute. *2012 Cost of Data Beach Study*

50%

of organizations surveyed have no way of knowing if data used in test was compromised

The Ponemon Institute. *The Insecurity of Test Data: The Unseen Crisis*

52%

of surveyed organizations outsource development

The Ponemon Institute. *The Insecurity of Test Data: The Unseen Crisis*

What is data masking?

- **Definition**
  *Method for creating a **structurally similar but inauthentic** version of an organization's data. The **purpose is to protect the actual data** while having a functional substitute for occasions when the real data is not required.*

- **Requirement**
  *Effective data masking requires data to be altered in a way that the **actual values cannot be determined** or reengineered, **functional appearance is maintained**.*

- **Other Terms Used**
  Obfuscation, scrambling, data de-identification

- **Commonly masked data types**
  Name, address, telephone, SSN/national identity number, credit card number

- **Methods**
  - Static Masking: *Extracts rows from production databases, obfuscating data values that ultimately **get stored in the columns in the test databases***
  - Dynamic Masking: *Masks specific data elements **on the fly** without touching applications or physical production data store*

IBM InfoSphere Optim Data Masking Solution

De-identify sensitive information with realistic *but fictional* data

Personal identifiable information is masked with realistic but fictional data

Requirements

- Protect confidential data used in test, training & development systems
- Mask data on screen in applications
- Implement proven data masking techniques
- Support compliance with privacy regulations
- Solution supports custom & packaged ERP applications

Benefits

- Protect sensitive information from misuse and fraud
- Prevent data breaches and associated fines
- Achieve better information governance

Contextually accurate masked data facilitates business processes

Satisfy Privacy regulations

- String literal values
- Character substrings & concatenation
- Random or sequential numbers

Reduce risk of data breaches

- Arithmetic expressions
- Lookup values
- Business data types (CCN, NID)

Maintain value of test data

- Generic mask
- Dates
- User defined

Patient Information

Patient No.	123456	**SSN**	333-22-4444		
Name	Erica Schafer				
Address	12 Murray Court				
City	Austin	**State**	TX	**Zip**	78704

Data is masked with contextually correct data to preserve integrity of data

Personal Info Table

PersNbr	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	**Pablo**	**Picasso**

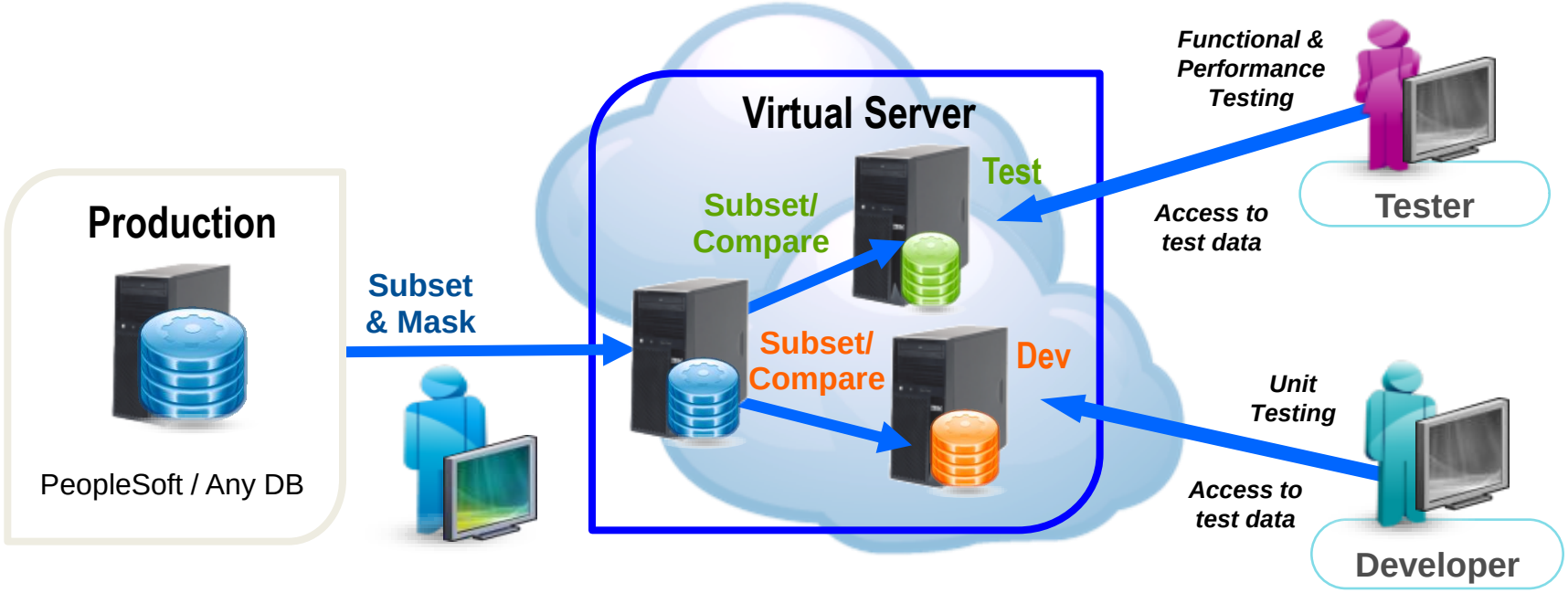
Referential integrity is maintained with key propagation

Event Table

PersNbr	FstNEvtOwn	LstNEvtOwn
10002	**Pablo**	**Picasso**
10002	**Pablo**	**Picasso**

InfoSphere Optim Test Data Management Solution

Automate creation of "right size" test data in private cloud



The Choice of the Fortune 500

Questions