Daniel Ling,

Senior Brand Specialist,

Information Management, IBM HK

Managing Data Privacy and the Entire Compliance Lifecycle

Information Management

Who Must Comply with PCI DSS?

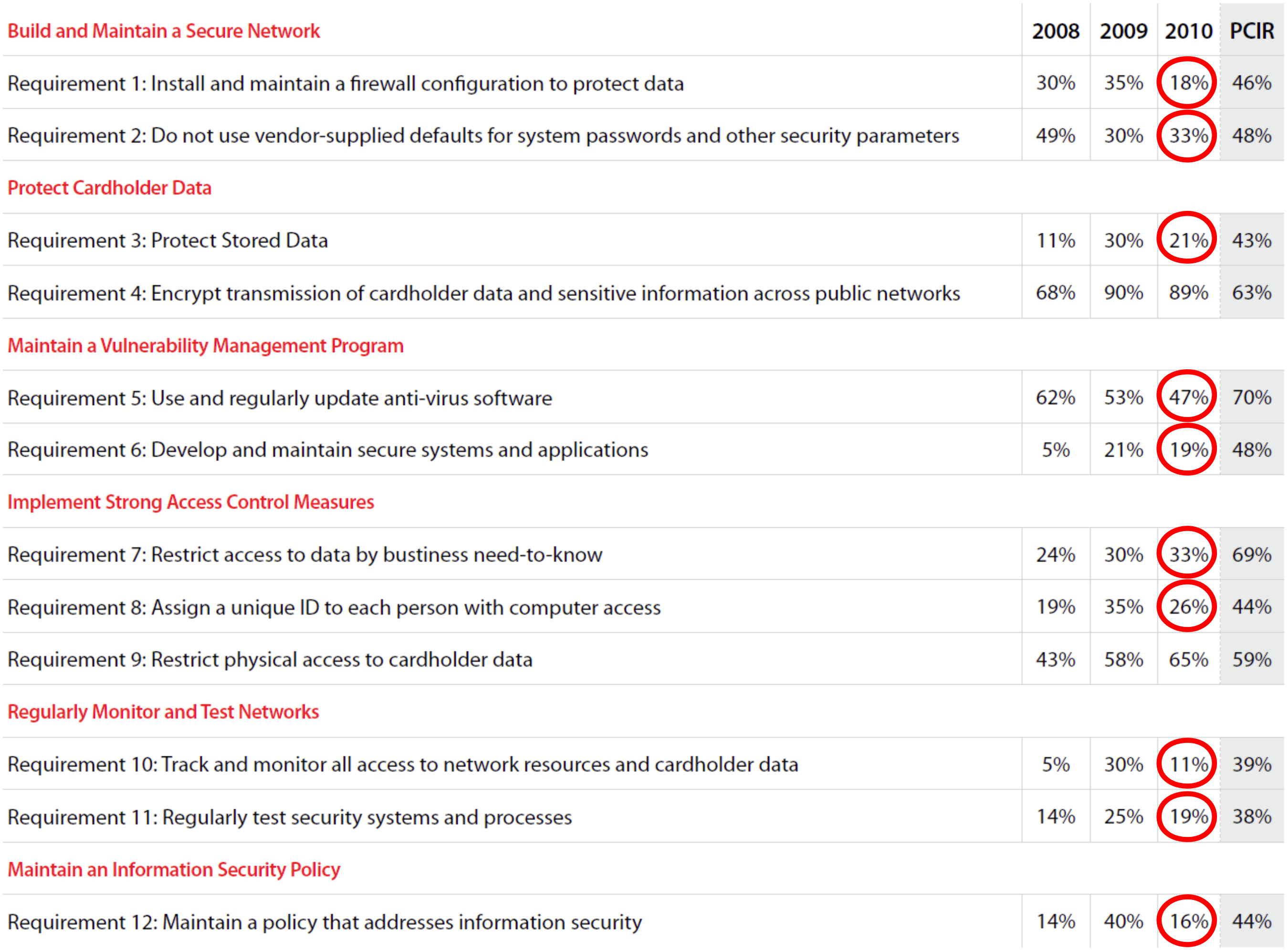
- All retailers who “**Process, Store or Transmit**” card data
- All Channels
  - Retail (physical) and traditional merchants
  - Point-of-Sale (POS)
  - Mail order / telephone order / catalogue
  - E-commerce
- Merchants are grouped into compliance risk levels, based on annual transaction volumes (per brand) processed:
  - Level 1 (over 6 million, channel independent)
  - Level 2 (150,000 to 6 million, channel independent)
  - Level 3 (20,000 to 150,000 e-commerce)
  - Level 4 (all others)

PCI DSS 12 Compliance Requirements - but over 200 sub categories

1	Install and maintain a firewall configuration to protect cardholder data	7	Restrict access to cardholder data by business need-to-know
2	Do not use vendor-supplied defaults for system passwords and other security parameters	8	Assign a unique ID to each person with computer access
3	Protect stored cardholder data	9	Restrict physical access to cardholder data
4	Encrypt transmission of cardholder data across open, public networks	10	Track and monitor all access to network resources and cardholder data
5	Use and regularly update anti-virus software or programs	11	Regularly test security systems and processes
6	Develop and maintain secure systems and applications	12	Maintain a policy that addresses information security for all personnel

PCI DSS Compliance is Not Easy – Recent Trends

Table 16. Percent of relevant organizations in compliance with PCI DSS requirements based on post-breach reviews conducted by Verizon IR team



Build and Maintain a Secure Network	2008	2009	2010	PCIR
Requirement 1: Install and maintain a firewall configuration to protect data	30%	35%	18%	46%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	49%	30%	33%	48%
Protect Cardholder Data				
Requirement 3: Protect Stored Data	11%	30%	21%	43%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	90%	89%	63%
Maintain a Vulnerability Management Program				
Requirement 5: Use and regularly update anti-virus software	62%	53%	47%	70%
Requirement 6: Develop and maintain secure systems and applications	5%	21%	19%	48%
Implement Strong Access Control Measures				
Requirement 7: Restrict access to data by bustiness need-to-know	24%	30%	33%	69%
Requirement 8: Assign a unique ID to each person with computer access	19%	35%	26%	44%
Requirement 9: Restrict physical access to cardholder data	43%	58%	65%	59%
Regularly Monitor and Test Networks				
Requirement 10: Track and monitor all access to network resources and cardholder data	5%	30%	11%	39%
Requirement 11: Regularly test security systems and processes	14%	25%	19%	38%
Maintain an Information Security Policy				
Requirement 12: Maintain a policy that addresses information security	14%	40%	16%	44%

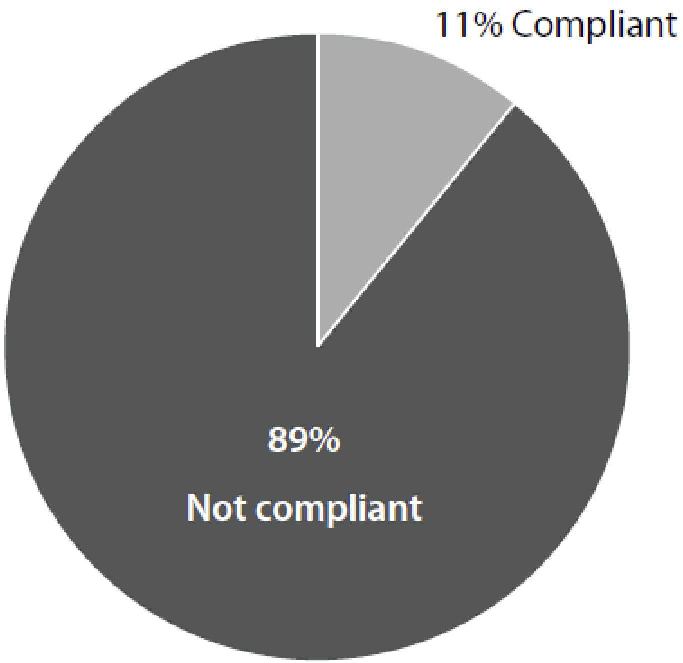
2011 Data Breach Report from Verizon Business RISK Team

www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

PCI DSS Compliance is Key to Breach Mitigation

PCI DSS Compliance Status

Figure 42. PCI DSS compliance status based on last official audit (or self-assessment)*



* Verizon caseload only

2011 Data Breach Report from Verizon Business RISK Team

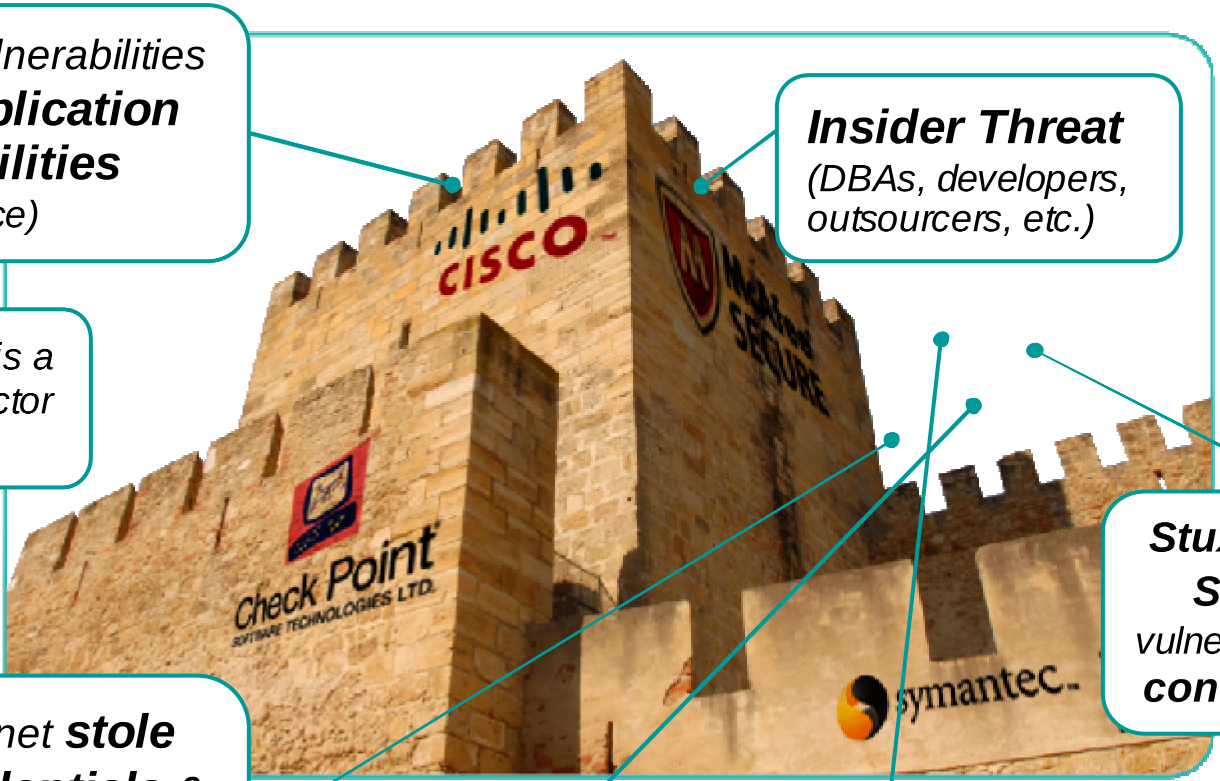
www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

> “One of the lingering questions from our discussions around PCI in this report is always that of relevancy. **It’s all well and good to validate compliance with the PCI DSS, but does it actually help reduce risk?** Insofar as that translates to a sincere security program—one that seeks to maintain validation on an ongoing basis—**the data strongly suggests the answer is “yes.”**

… 54% of breaches, 83% of records

Perimeter Defenses & Identity Management No Longer Sufficient

"A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls." *William J. Lynn III, U.S. Deputy Defense Secretary*



49% of new vulnerabilities are ***Web application vulnerabilities*** *(X-Force)*

SQL Injection *is a leading attack vector (X-Force)*

Insider Threat *(DBAs, developers, outsourcers, etc.)*

88% *of F500 companies have* ***employees infected with ZeuS*** *(RSA)*

Stuxnet *exploited* ***SQL Server*** *vulnerability to attack* ***control systems***

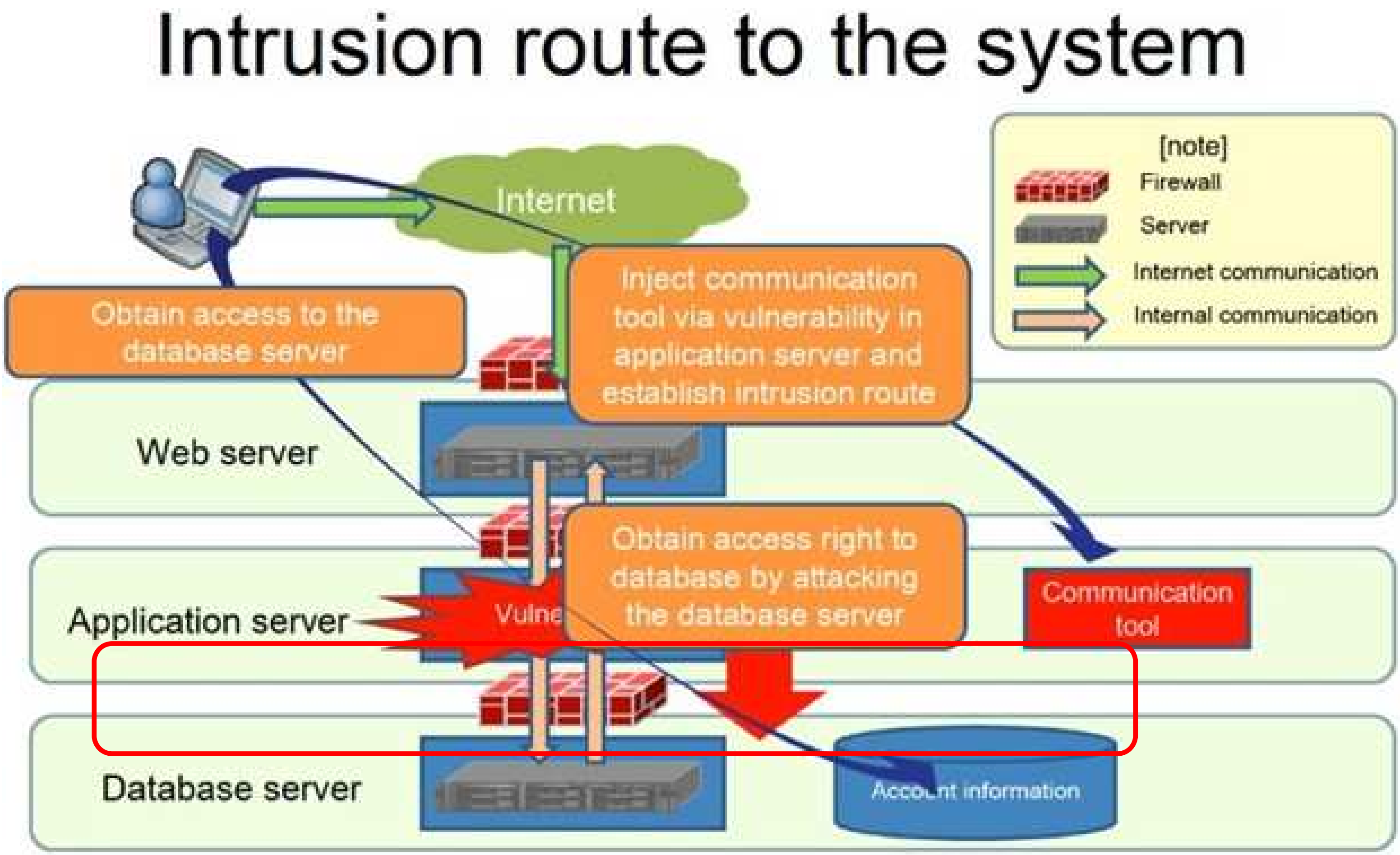
Kneber Botnet ***stole 68,000 credentials & 2,000 SSL certificates*** *over 4-week period (NetWitness)*

Epsilon ***data breach*** *affects* ***millions*** *(****outsourced*** *provider)*

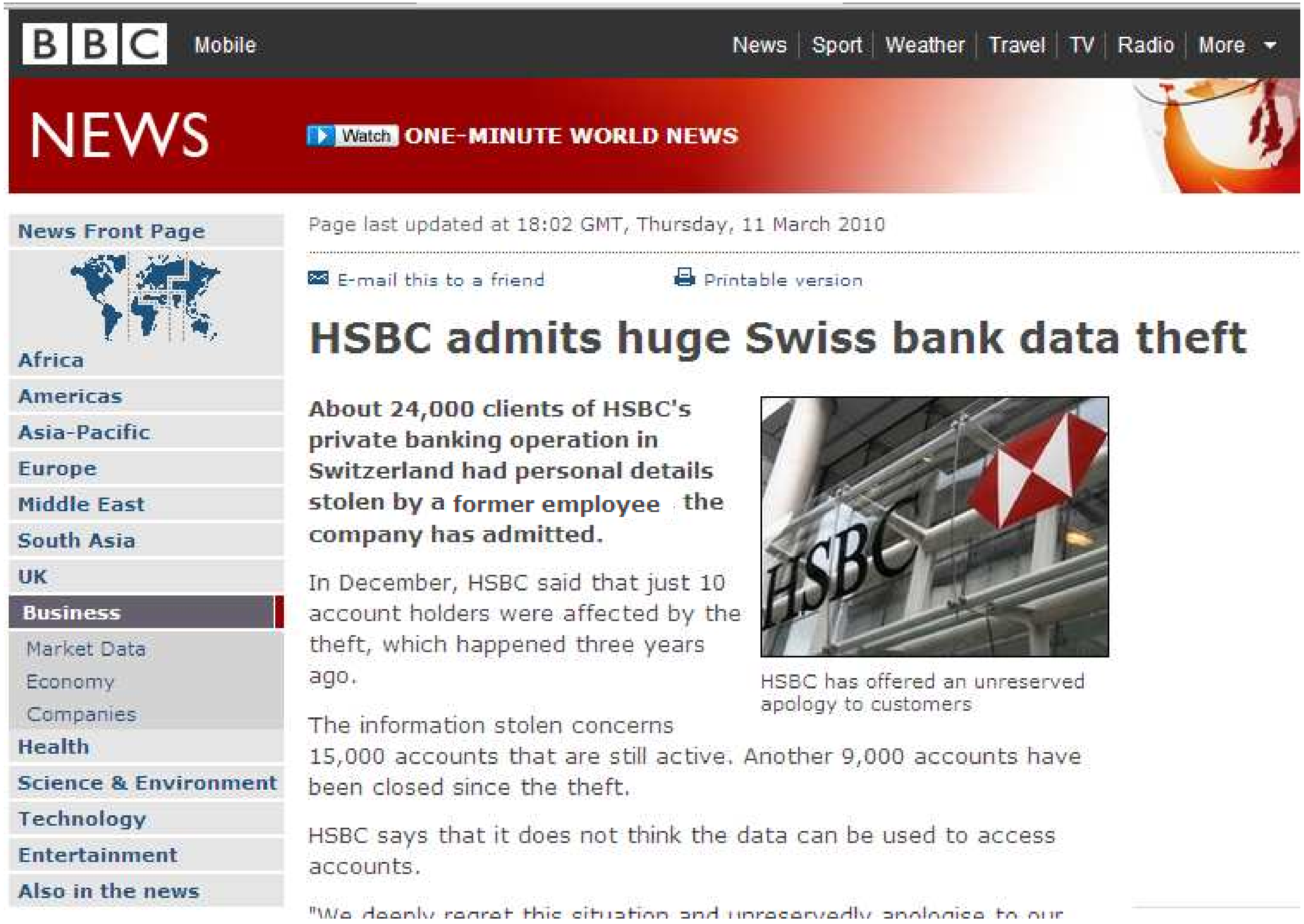
#1 VM vulnerability is ***VM guest hopping*** *(hypervisor escape) (X-Force)*

100+ Million Accounts Compromised in Database Breach

Japan


Intrusion route to the system
[note]
Firewall
Server
Internet communication
Internal communication
Internet
Obtain access to the database server
Inject communication tool via vulnerability in application server and establish intrusion route
Web server
Obtain access right to database by attacking the database server
Application server
Vulne
Communication tool
Database server
Account information

https://threatpost.com/en_us/blogs/what-sony-playstation-network-attack-can-teach-us-about-database-security-051211



Page last updated at 18:02 GMT, Thursday, 11 March 2010

HSBC admits huge Swiss bank data theft

About 24,000 clients of HSBC's private banking operation in Switzerland had personal details stolen by a former employee the company has admitted.

In December, HSBC said that just 10 account holders were affected by the theft, which happened three years ago.

HSBC has offered an unreserved apology to customers

The information stolen concerns 15,000 accounts that are still active. Another 9,000 accounts have been closed since the theft.

HSBC says that it does not think the data can be used to access accounts.

"We deeply regret this situation and unreservedly apologise to our

Source : http://news.bbc.co.uk/2/hi/business/8562381.stm

Type of compromised assets for breach

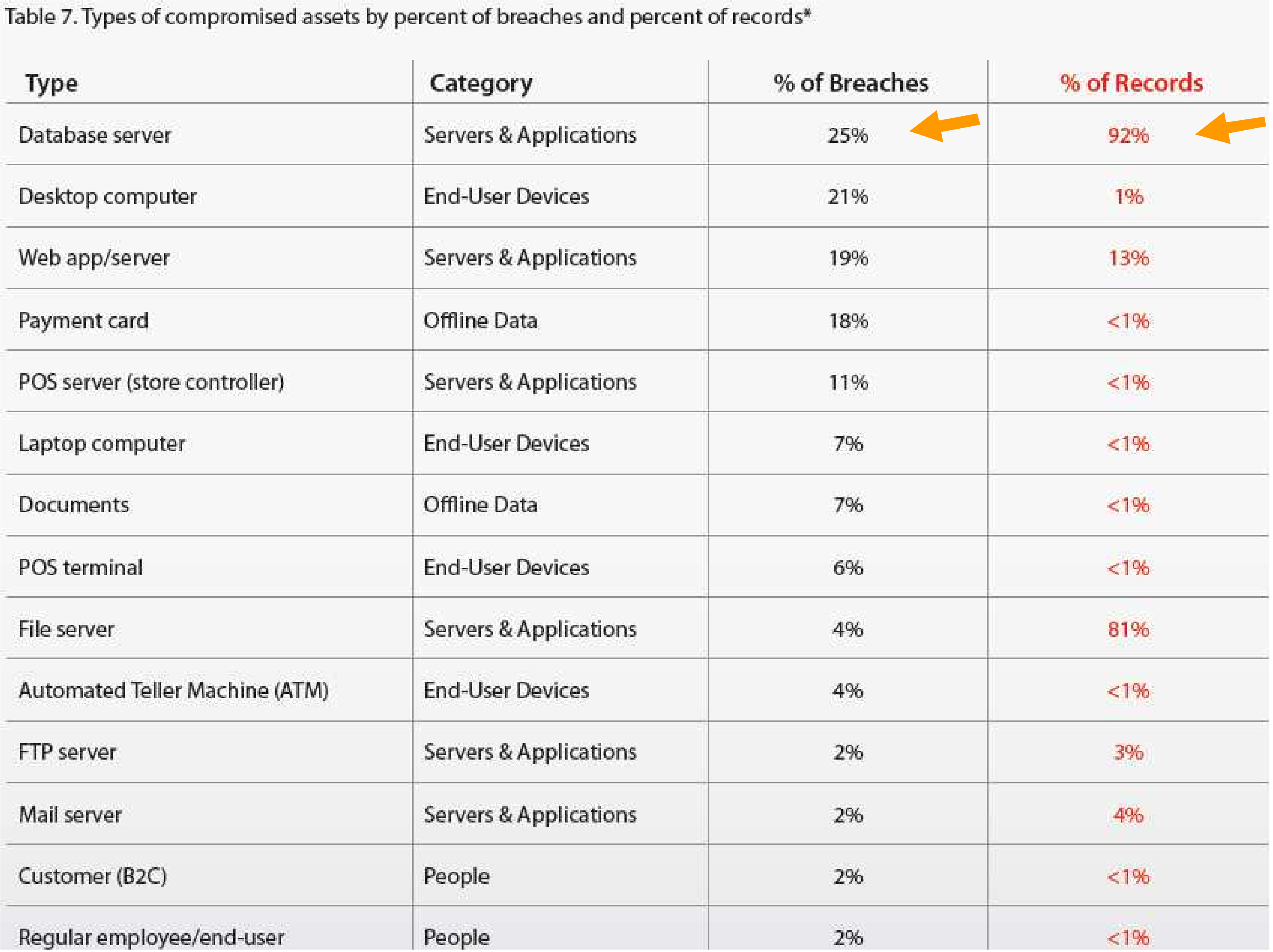


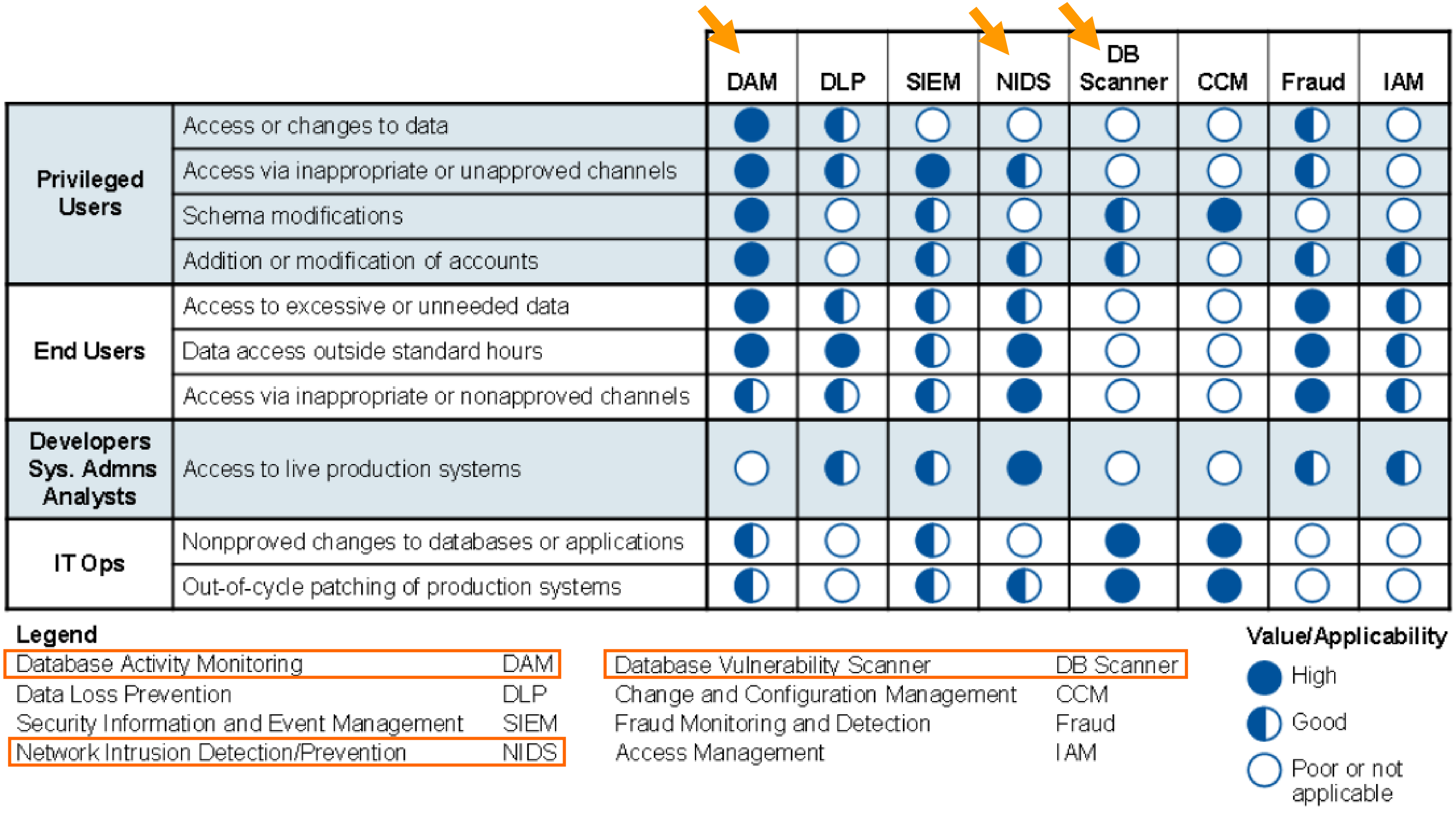
Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%
Customer (B2C)	People	2%	<1%
Regular employee/end-user	People	2%	<1%

Source : http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Gartner 2010 - Ten Database Activities Enterprises Need to Monitor

Figure 1. Applicable Use Cases for Use in the Evaluation and Selection Process



		DAM	DLP	SIEM	NIDS	DB Scanner	CCM	Fraud	IAM
Privileged Users	Access or changes to data	●	◐	○	○	○	○	◐	○
	Access via inappropriate or unapproved channels	●	◐	●	◐	○	○	◐	○
	Schema modifications	●	○	◐	○	◐	●	○	○
	Addition or modification of accounts	●	○	◐	◐	◐	○	◐	◐
End Users	Access to excessive or unneeded data	●	◐	◐	◐	○	○	●	◐
	Data access outside standard hours	●	●	◐	●	○	○	●	◐
	Access via inappropriate or nonapproved channels	◐	◐	◐	●	○	○	●	◐
Developers Sys. Admns Analysts	Access to live production systems	○	◐	◐	●	○	○	◐	◐
IT Ops	Nonpproved changes to databases or applications	◐	○	◐	○	●	●	○	○
	Out-of-cycle patching of production systems	◐	○	◐	◐	●	●	○	○

Legend

Database Activity Monitoring	DAM
Data Loss Prevention	DLP
Security Information and Event Management	SIEM
Network Intrusion Detection/Prevention	NIDS
Database Vulnerability Scanner	DB Scanner
Change and Configuration Management	CCM
Fraud Monitoring and Detection	Fraud
Access Management	IAM

Value/Applicability

- ● High
- ◐ Good
- ○ Poor or not applicable

Source: Gartner (April 2010)

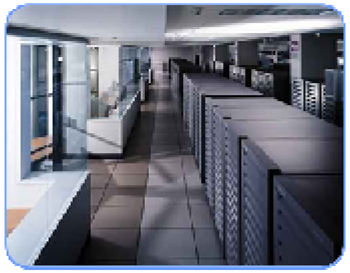
Key Business Drivers for IBM Guardium Database Security Solution

1. Prevent data breaches

- Mitigate external & internal threats
- Secure customer & credit card data, ACH data, strategic plans & IP

2. Assure data governance

- Prevent unauthorized changes to financial and ERP data

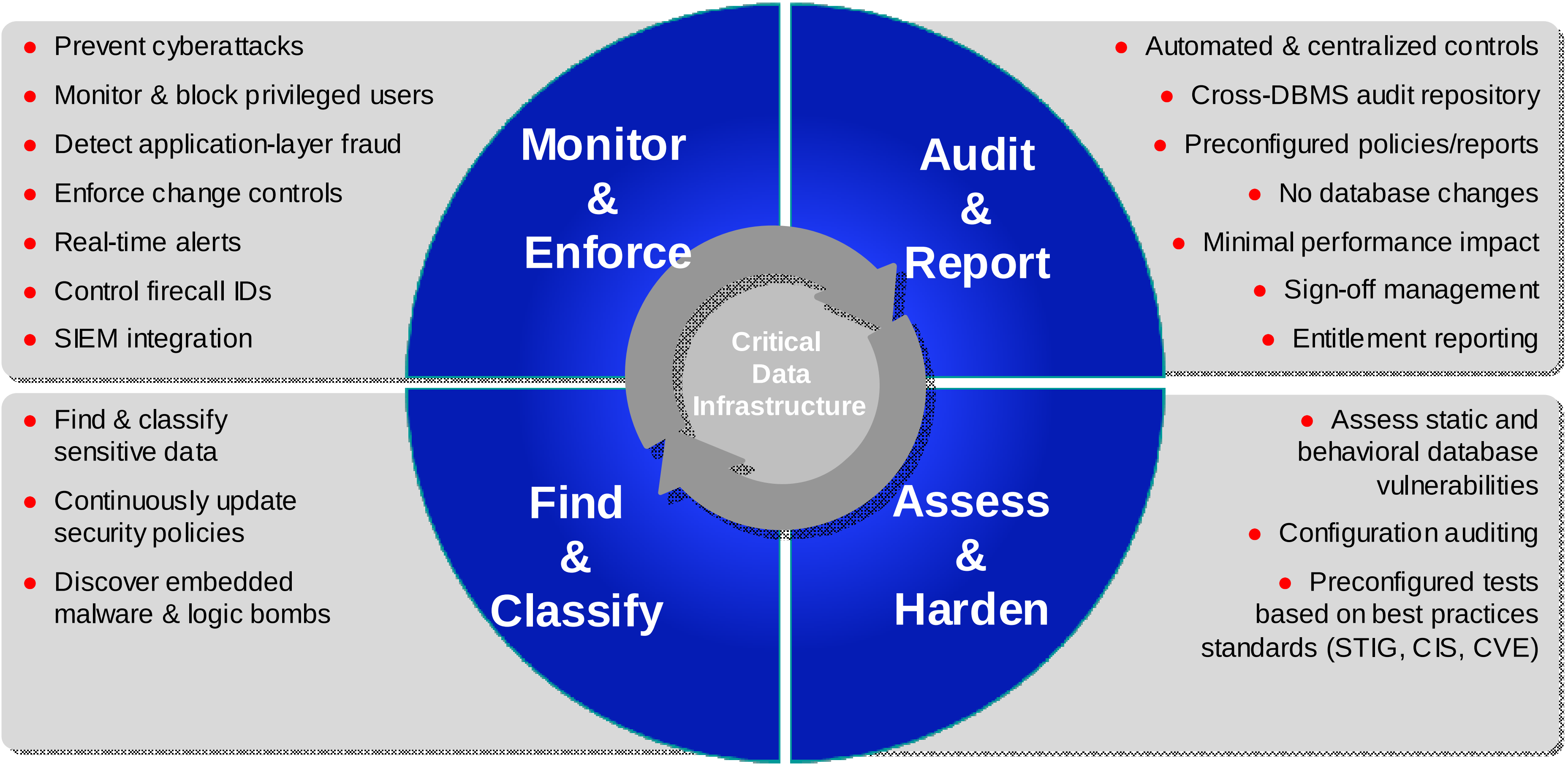


3. Reduce cost of compliance

- Automated, continuous controls
- Simplified audits
- Minimal performance impact
- No changes to databases or applications

IBM Guardium address 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

Monitor & Enforce

Audit & Report

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

Critical Data Infrastructure

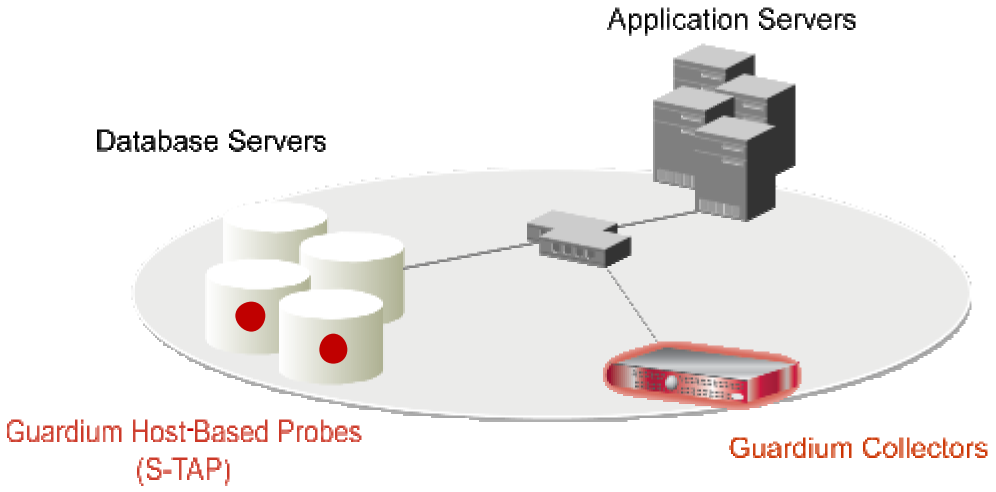
- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

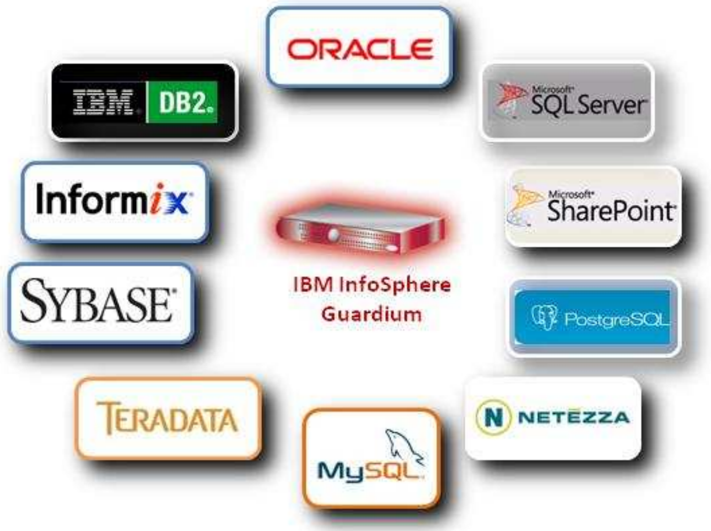
Find & Classify

Assess & Harden

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

Non-Invasive, Real-Time Database Security & Monitoring

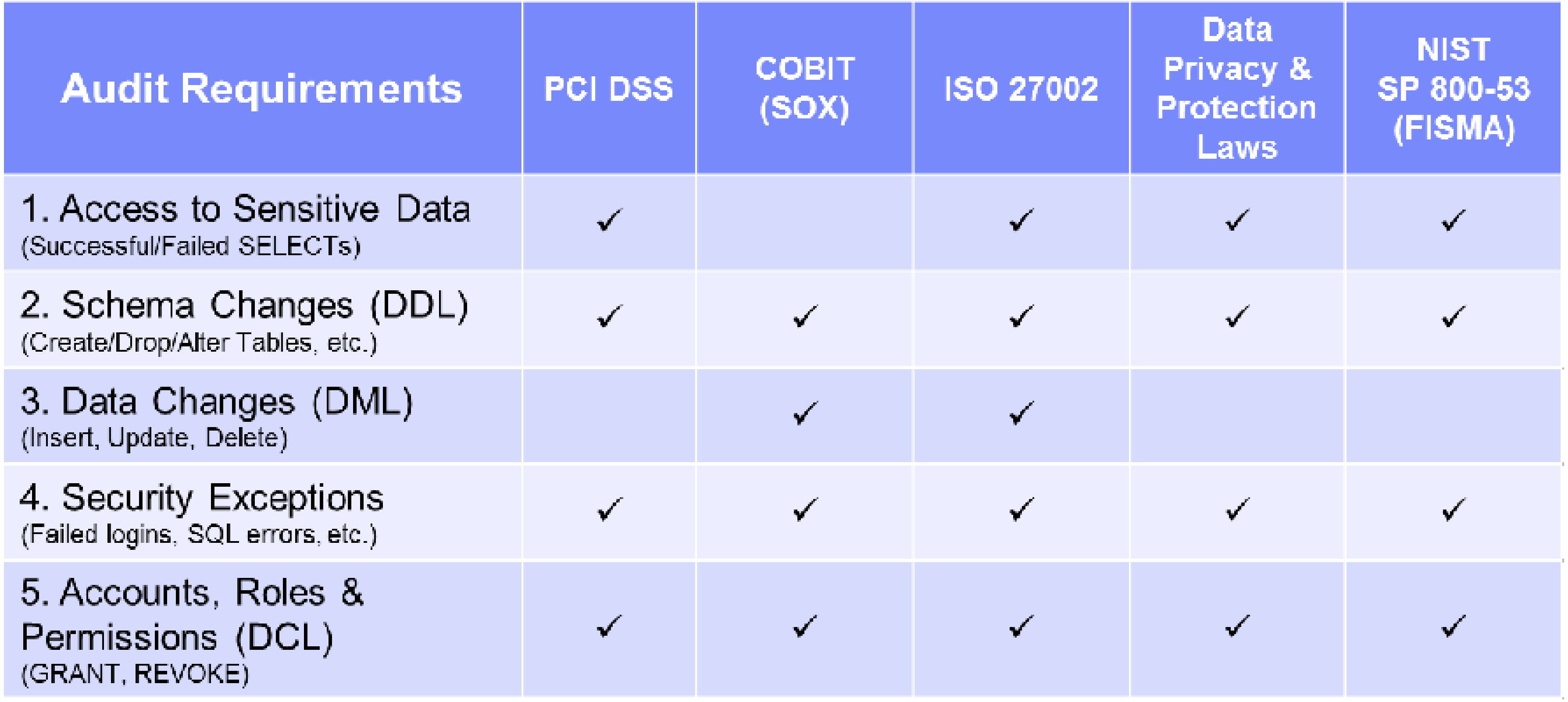




- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes

- 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***

The Compliance Mandate – What do you need to monitor?

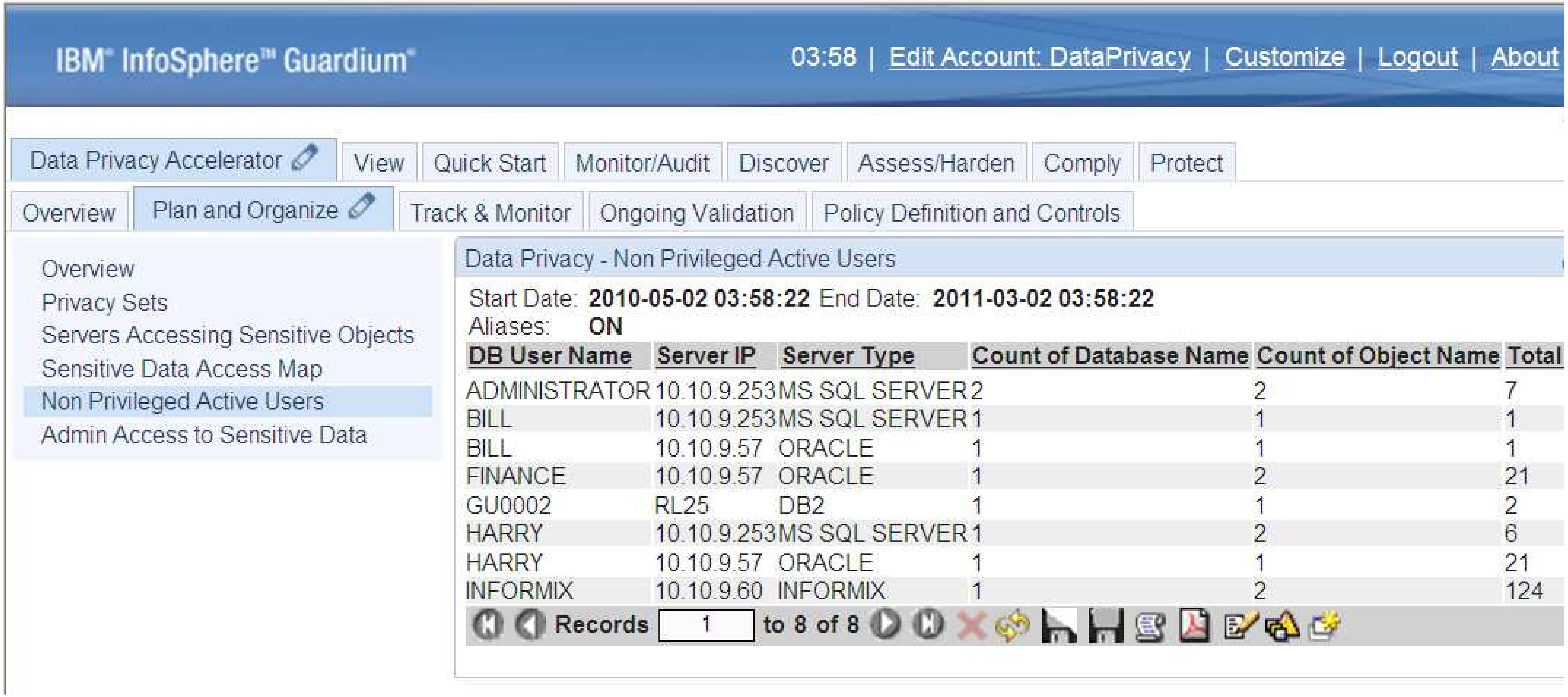


Audit Requirements	PCI DSS	COBIT (SOX)	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)	✓		✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)		✓	✓		
4. Security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

IBM Guardium Data Privacy Accelerator module :

- Security Overview : Non Privileged Active Users


IBM® InfoSphere™ Guardium®
03:58 | Edit Account: DataPrivacy | Customize | Logout | About
Data Privacy Accelerator
View
Quick Start
Monitor/Audit
Discover
Assess/Harden
Comply
Protect
Overview
Plan and Organize
Track & Monitor
Ongoing Validation
Policy Definition and Controls
Overview
Privacy Sets
Servers Accessing Sensitive Objects
Sensitive Data Access Map
Non Privileged Active Users
Admin Access to Sensitive Data
Records 1 to 8 of 8

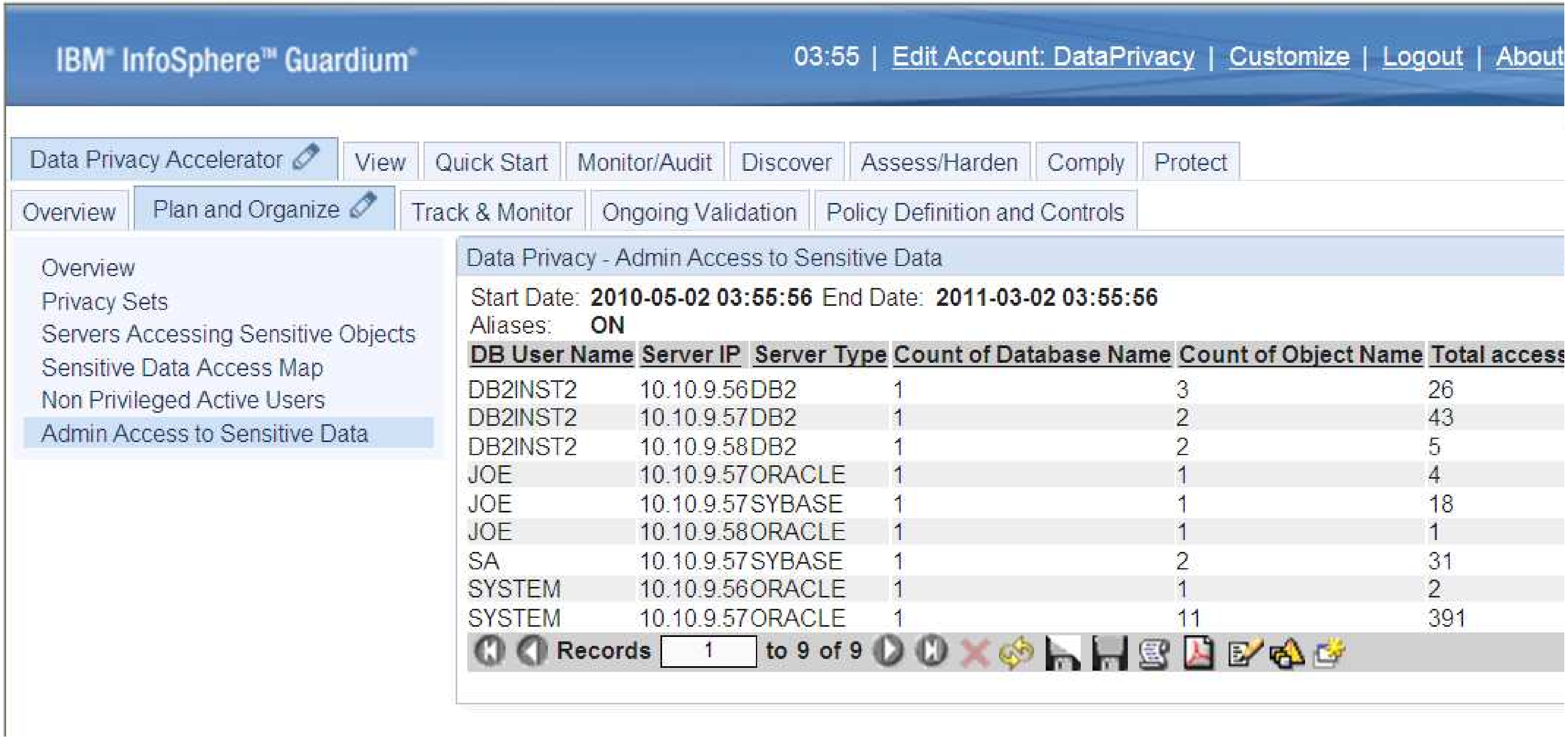
Data Privacy - Non Privileged Active Users

Start Date: **2010-05-02 03:58:22** End Date: **2011-03-02 03:58:22**
Aliases: **ON**

DB User Name	Server IP	Server Type	Count of Database Name	Count of Object Name	Total
ADMINISTRATOR	10.10.9.253	MS SQL SERVER	2	2	7
BILL	10.10.9.253	MS SQL SERVER	1	1	1
BILL	10.10.9.57	ORACLE	1	1	1
FINANCE	10.10.9.57	ORACLE	1	2	21
GU0002	RL25	DB2	1	1	2
HARRY	10.10.9.253	MS SQL SERVER	1	2	6
HARRY	10.10.9.57	ORACLE	1	1	21
INFORMIX	10.10.9.60	INFORMIX	1	2	124

IBM Guardium Data Privacy Accelerator module :

- Security Overview : Admin Access to Sensitive Data


IBM® InfoSphere™ Guardium®
03:55 | Edit Account: DataPrivacy | Customize | Logout | About
Data Privacy Accelerator
View
Quick Start
Monitor/Audit
Discover
Assess/Harden
Comply
Protect
Overview
Plan and Organize
Track & Monitor
Ongoing Validation
Policy Definition and Controls
Overview
Privacy Sets
Servers Accessing Sensitive Objects
Sensitive Data Access Map
Non Privileged Active Users
Admin Access to Sensitive Data
Records 1 to 9 of 9

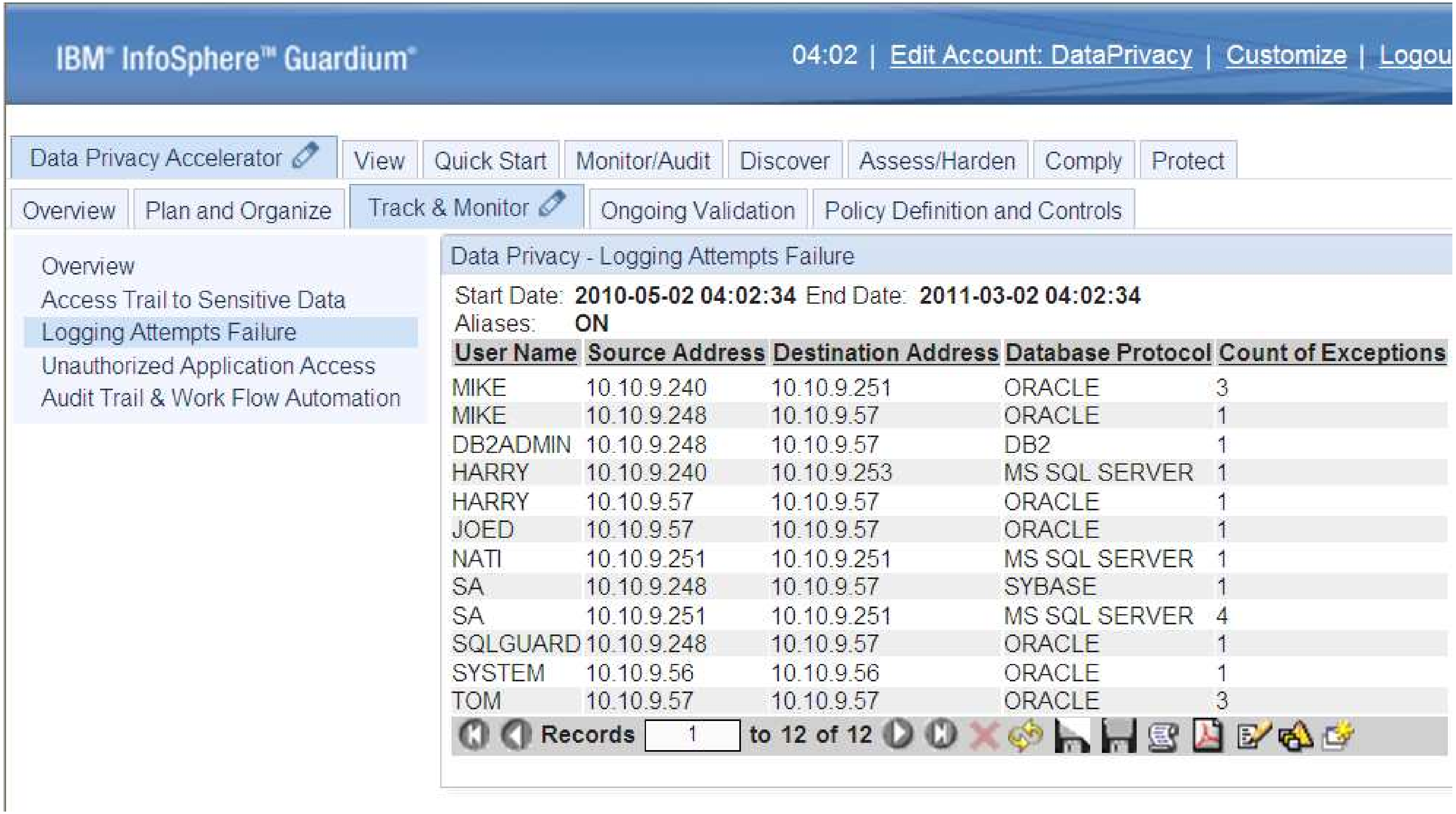
Data Privacy - Admin Access to Sensitive Data

Start Date: **2010-05-02 03:55:56** End Date: **2011-03-02 03:55:56**
Aliases: **ON**

DB User Name	Server IP	Server Type	Count of Database Name	Count of Object Name	Total access
DB2INST2	10.10.9.56	DB2	1	3	26
DB2INST2	10.10.9.57	DB2	1	2	43
DB2INST2	10.10.9.58	DB2	1	2	5
JOE	10.10.9.57	ORACLE	1	1	4
JOE	10.10.9.57	SYBASE	1	1	18
JOE	10.10.9.58	ORACLE	1	1	1
SA	10.10.9.57	SYBASE	1	2	31
SYSTEM	10.10.9.56	ORACLE	1	1	2
SYSTEM	10.10.9.57	ORACLE	1	11	391

IBM Guardium Data Privacy Accelerator module :

- Track & Monitor : Logging Attempts Failure



IBM® InfoSphere™ Guardium®
04:02 | Edit Account: DataPrivacy | Customize | Logou
Data Privacy Accelerator
View
Quick Start
Monitor/Audit
Discover
Assess/Harden
Comply
Protect
Overview
Plan and Organize
Track & Monitor
Ongoing Validation
Policy Definition and Controls
Overview
Access Trail to Sensitive Data
Logging Attempts Failure
Unauthorized Application Access
Audit Trail & Work Flow Automation
Records
to 12 of 12

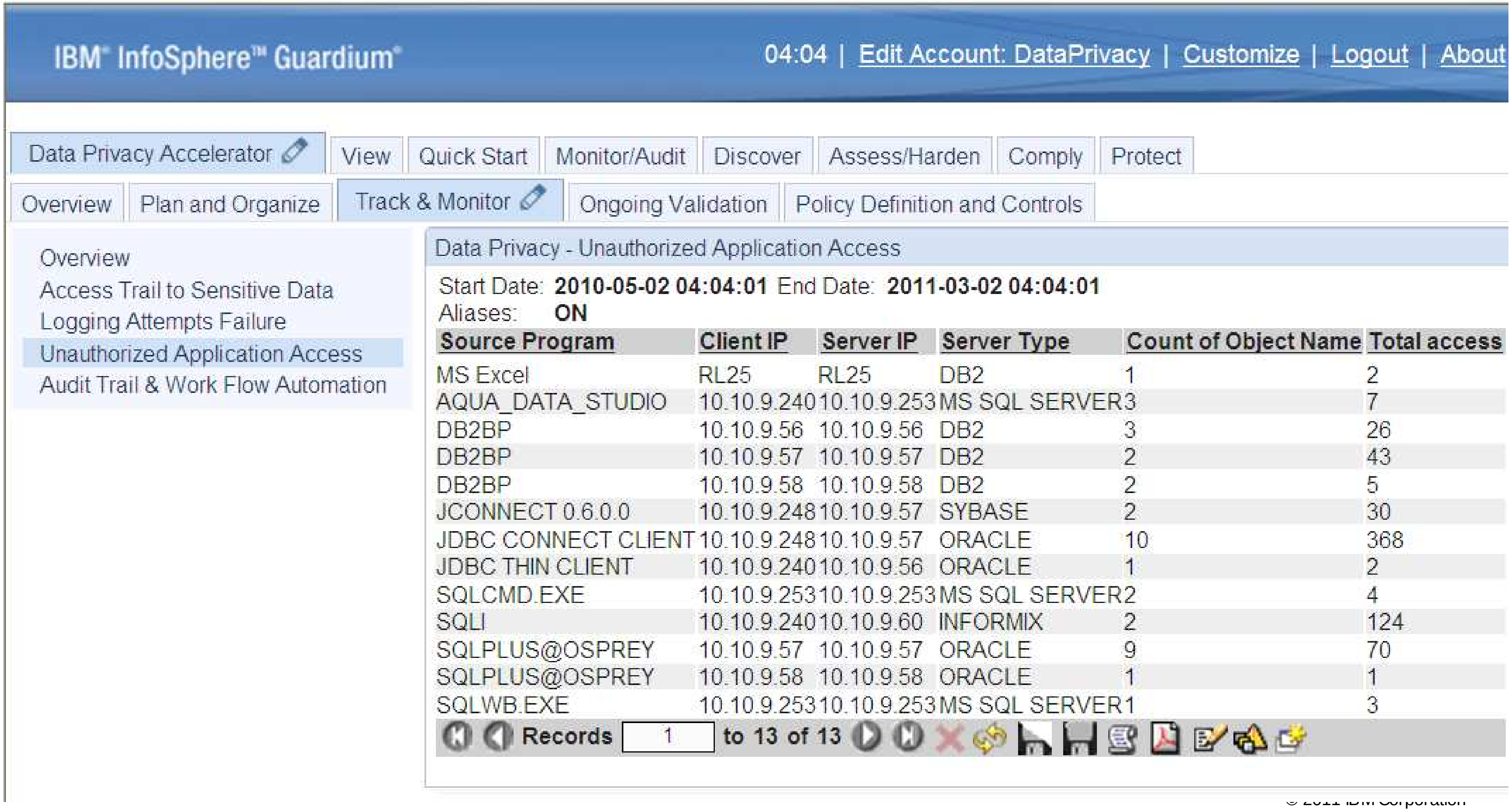
Data Privacy - Logging Attempts Failure

Start Date: **2010-05-02 04:02:34** End Date: **2011-03-02 04:02:34**
Aliases: **ON**

User Name	Source Address	Destination Address	Database Protocol	Count of Exceptions
MIKE	10.10.9.240	10.10.9.251	ORACLE	3
MIKE	10.10.9.248	10.10.9.57	ORACLE	1
DB2ADMIN	10.10.9.248	10.10.9.57	DB2	1
HARRY	10.10.9.240	10.10.9.253	MS SQL SERVER	1
HARRY	10.10.9.57	10.10.9.57	ORACLE	1
JOED	10.10.9.57	10.10.9.57	ORACLE	1
NATI	10.10.9.251	10.10.9.251	MS SQL SERVER	1
SA	10.10.9.248	10.10.9.57	SYBASE	1
SA	10.10.9.251	10.10.9.251	MS SQL SERVER	4
SQLGUARD	10.10.9.248	10.10.9.57	ORACLE	1
SYSTEM	10.10.9.56	10.10.9.56	ORACLE	1
TOM	10.10.9.57	10.10.9.57	ORACLE	3

IBM Guardium Data Privacy Accelerator module :

- Track & Monitor : Unauthorized Application Access



IBM® InfoSphere™ Guardium®
04:04 | Edit Account: DataPrivacy | Customize | Logout | About
Data Privacy Accelerator
View
Quick Start
Monitor/Audit
Discover
Assess/Harden
Comply
Protect
Overview
Plan and Organize
Track & Monitor
Ongoing Validation
Policy Definition and Controls
Overview
Access Trail to Sensitive Data
Logging Attempts Failure
Unauthorized Application Access
Audit Trail & Work Flow Automation

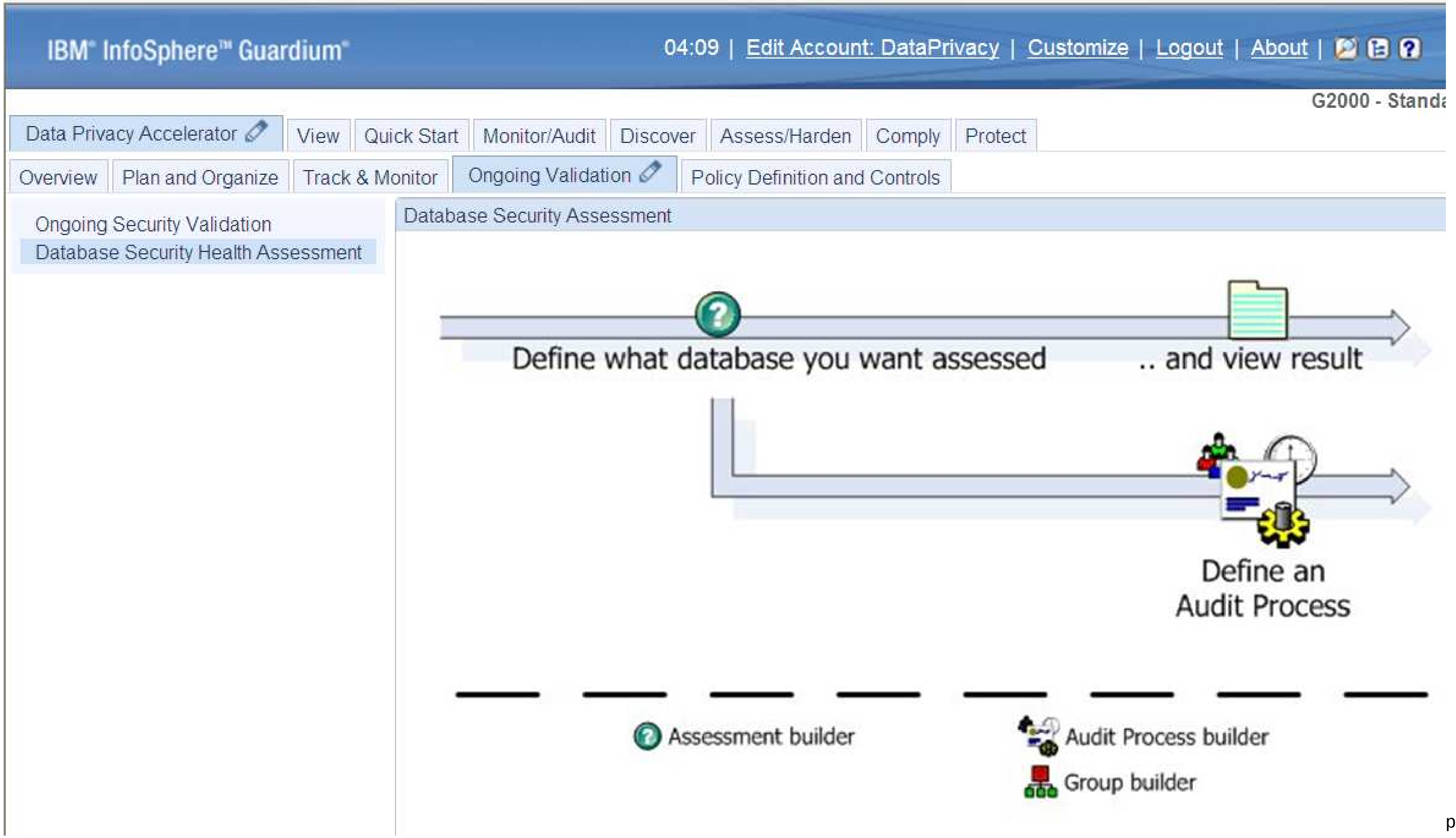
Data Privacy - Unauthorized Application Access

Start Date: **2010-05-02 04:04:01** End Date: **2011-03-02 04:04:01**
Aliases: **ON**

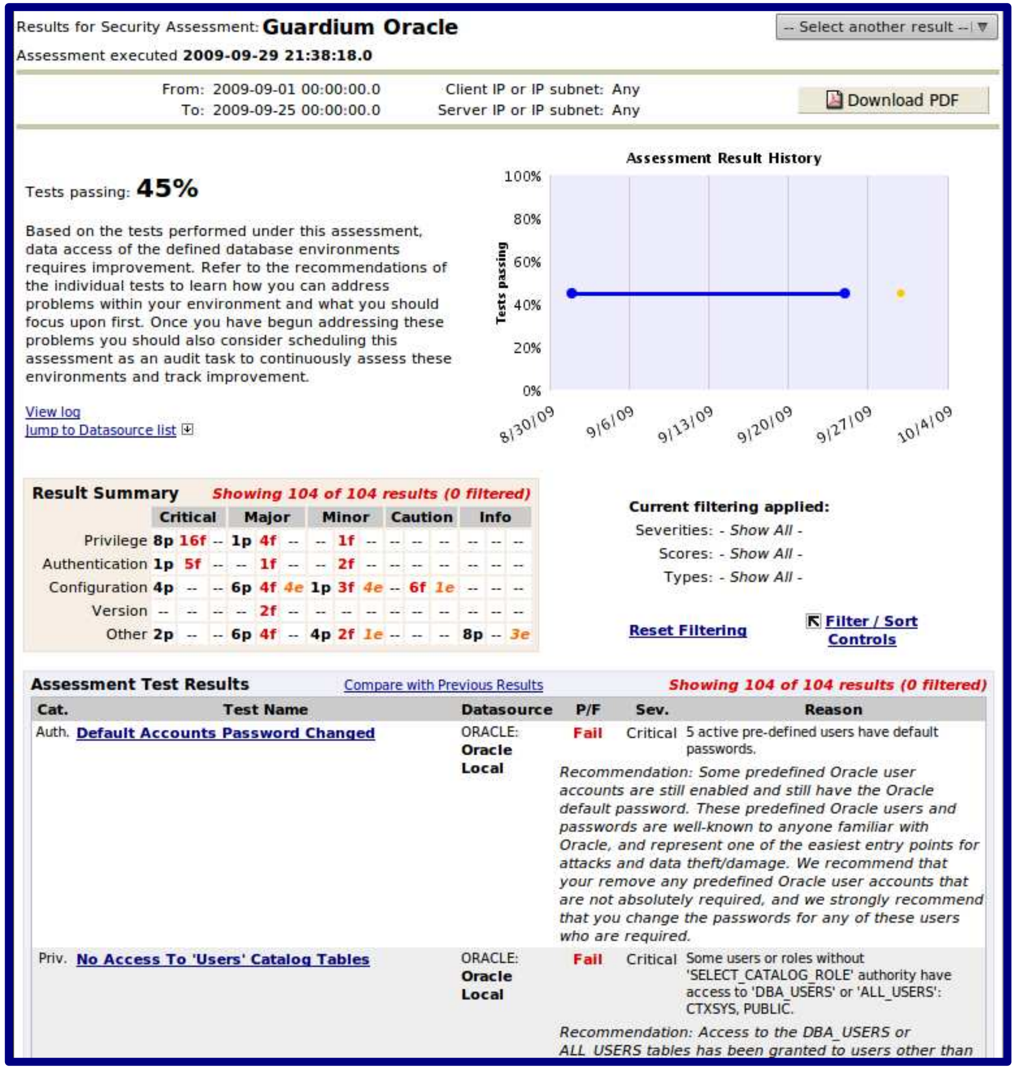
Source Program	Client IP	Server IP	Server Type	Count of Object Name	Total access
MS Excel	RL25	RL25	DB2	1	2
AQUA_DATA_STUDIO	10.10.9.240	10.10.9.253	MS SQL SERVER	3	7
DB2BP	10.10.9.56	10.10.9.56	DB2	3	26
DB2BP	10.10.9.57	10.10.9.57	DB2	2	43
DB2BP	10.10.9.58	10.10.9.58	DB2	2	5
JCONNECT 0.6.0.0	10.10.9.248	10.10.9.57	SYBASE	2	30
JDBC CONNECT CLIENT	10.10.9.248	10.10.9.57	ORACLE	10	368
JDBC THIN CLIENT	10.10.9.240	10.10.9.56	ORACLE	1	2
SQLCMD.EXE	10.10.9.253	10.10.9.253	MS SQL SERVER	2	4
SQLI	10.10.9.240	10.10.9.60	INFORMIX	2	124
SQLPLUS@OSPREY	10.10.9.57	10.10.9.57	ORACLE	9	70
SQLPLUS@OSPREY	10.10.9.58	10.10.9.58	ORACLE	1	1
SQLWB.EXE	10.10.9.253	10.10.9.253	MS SQL SERVER	1	3

IBM Guardium Data Privacy Accelerator module :

- Ongoing Validation : Database Security Assessment



Vulnerability Assessments Report Sample



Results for Security Assessment: **Guardium Oracle**

Assessment executed **2009-09-29 21:38:18.0**

From:	2009-09-01 00:00:00.0	Client IP or IP subnet:	Any
To:	2009-09-25 00:00:00.0	Server IP or IP subnet:	Any

Tests passing: **45%**

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

View log

Jump to Datasource list

Result Summary *Showing 104 of 104 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	8p	16f	--	1p	4f	--	--	1f	--	--	--	--	--	--	--
Authentication	1p	5f	--	--	1f	--	--	2f	--	--	--	--	--	--	--
Configuration	4p	--	--	6p	4f	4e	1p	3f	4e	--	6f	1e	--	--	--
Version	--	--	--	--	2f	--	--	--	--	--	--	--	--	--	--
Other	2p	--	--	6p	4f	--	4p	2f	1e	--	--	--	8p	--	3e

Current filtering applied:

Severities: *- Show All -*

Scores: *- Show All -*

Types: *- Show All -*

Reset Filtering

Filter / Sort Controls

Assessment Test Results Compare with Previous Results *Showing 104 of 104 results (0 filtered)*

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Auth.	**Default Accounts Password Changed**	ORACLE: **Oracle Local**	Fail	Critical	5 active pre-defined users have default passwords. *Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that your remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.*
Priv.	**No Access To 'Users' Catalog Tables**	ORACLE: **Oracle Local**	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. *Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than*

Result History

Summary Outlining Results

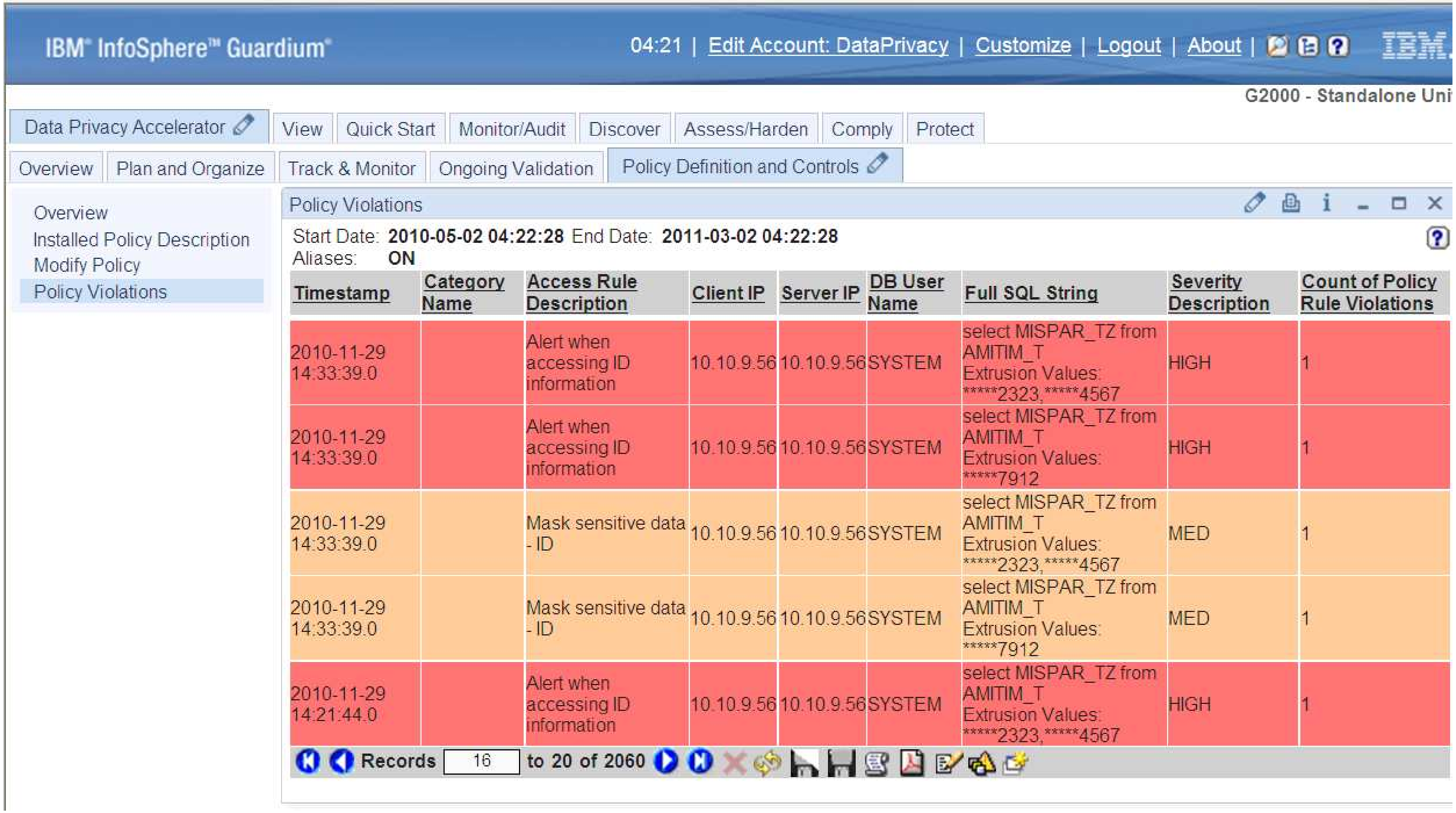
Filters and Sort Controls

Detailed Test Results

Detailed Descriptions of Fixes

IBM Guardium Data Privacy Accelerator module :

- Policy Controls : Policy Violations



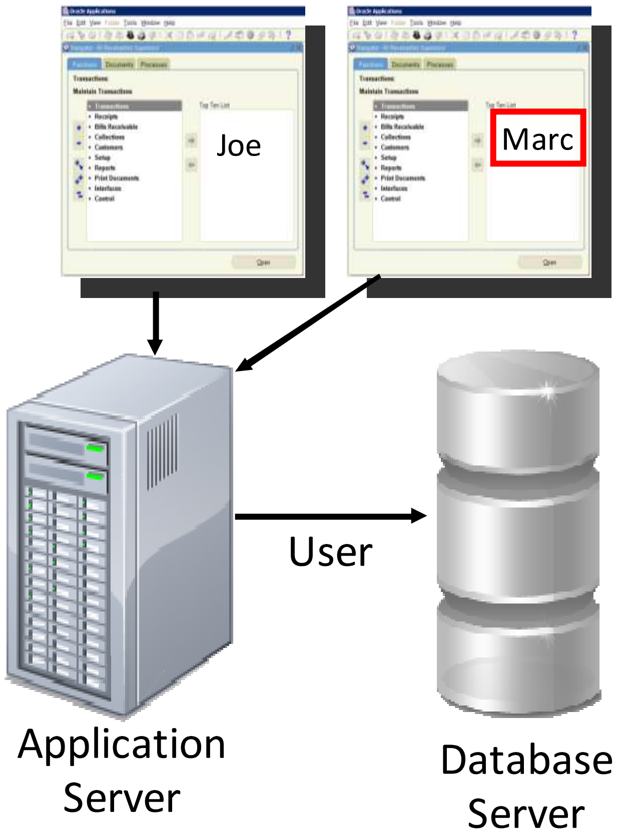
Policy Violations

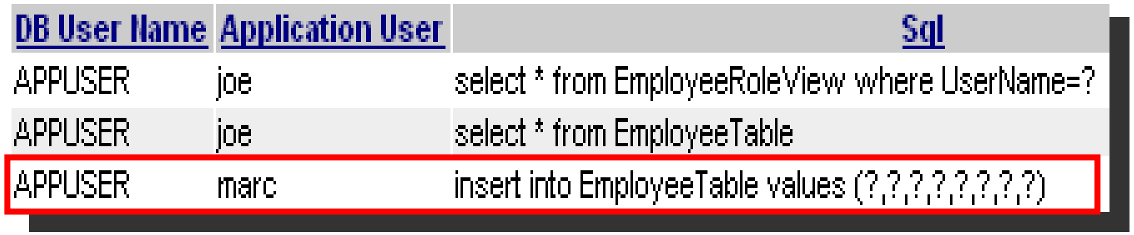
Start Date: **2010-05-02 04:22:28** End Date: **2011-03-02 04:22:28**
Aliases: **ON**

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Count of Policy Rule Violations
2010-11-29 14:33:39.0		Alert when accessing ID information	10.10.9.56	10.10.9.56	SYSTEM	select MISPAR_TZ from AMITIM_T Extrusion Values: *****2323,*****4567	HIGH	1
2010-11-29 14:33:39.0		Alert when accessing ID information	10.10.9.56	10.10.9.56	SYSTEM	select MISPAR_TZ from AMITIM_T Extrusion Values: *****7912	HIGH	1
2010-11-29 14:33:39.0		Mask sensitive data - ID	10.10.9.56	10.10.9.56	SYSTEM	select MISPAR_TZ from AMITIM_T Extrusion Values: *****2323,*****4567	MED	1
2010-11-29 14:33:39.0		Mask sensitive data - ID	10.10.9.56	10.10.9.56	SYSTEM	select MISPAR_TZ from AMITIM_T Extrusion Values: *****7912	MED	1
2010-11-29 14:21:44.0		Alert when accessing ID information	10.10.9.56	10.10.9.56	SYSTEM	select MISPAR_TZ from AMITIM_T Extrusion Values: *****2323,*****4567	HIGH	1

Records 16 to 20 of 2060

Capable to identify the “Real End User” activities - rather than connection information only

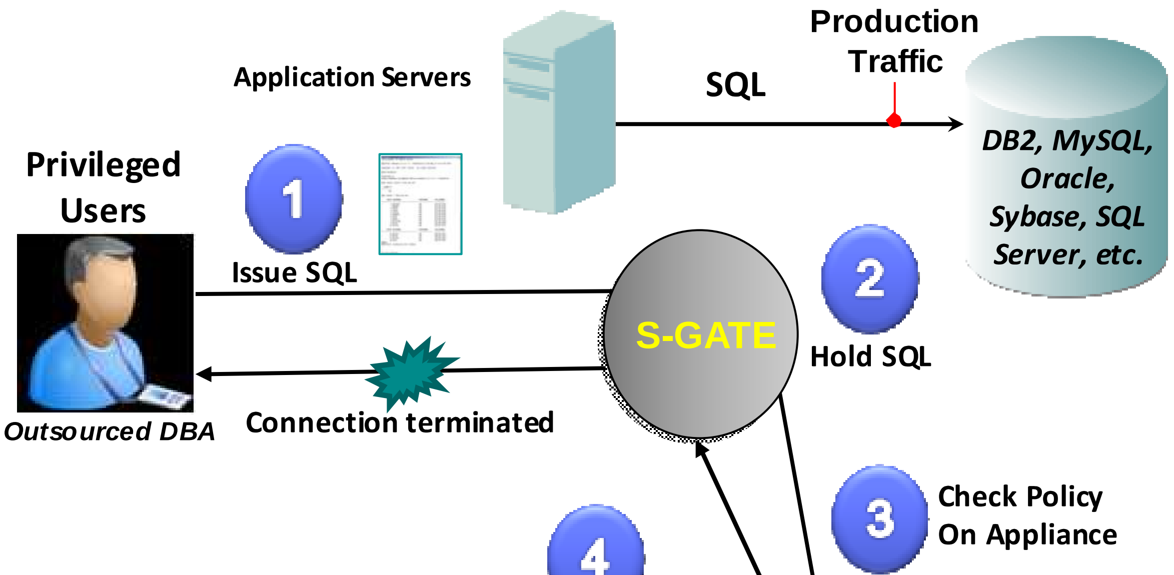




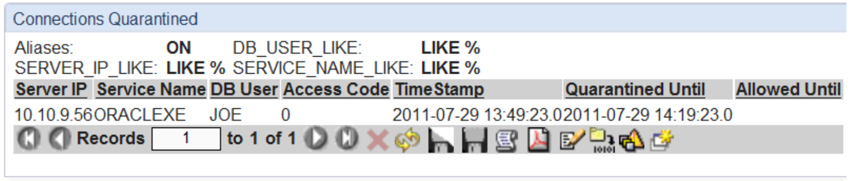
DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

- ***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

Restrict Access to Cardholder / Personal Data by Business Need-to-Know



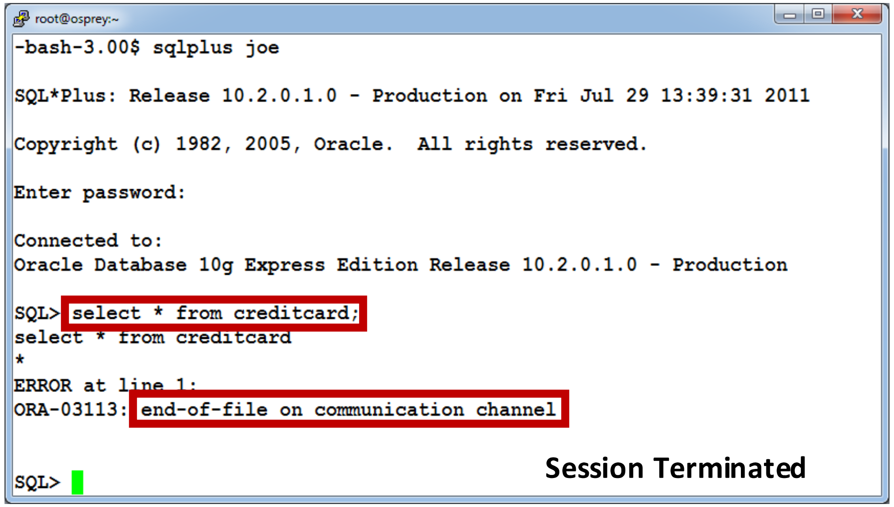
- ✓ No database or application changes
- ✓ Without risk of inline appliances that can interfere with critical application traffic
- ✓ Prevents external attacks as well as policy violations by privileged users (DBAs, developers, outsourced personnel)
- ✓ Part of unified database security solution with single set of policies for fine-grained auditing, VA, discovery, access control, …



Connections Quarantined

Aliases: ON DB_USER_LIKE: LIKE %
SERVER_IP_LIKE: LIKE % SERVICE_NAME_LIKE: LIKE %

Server IP	Service Name	DB User	Access Code	TimeStamp	Quarantined Until	Allowed Until
10.10.9.56	ORACLEXE	JOE	0	2011-07-29 13:49:23.0	2011-07-29 14:19:23.0	



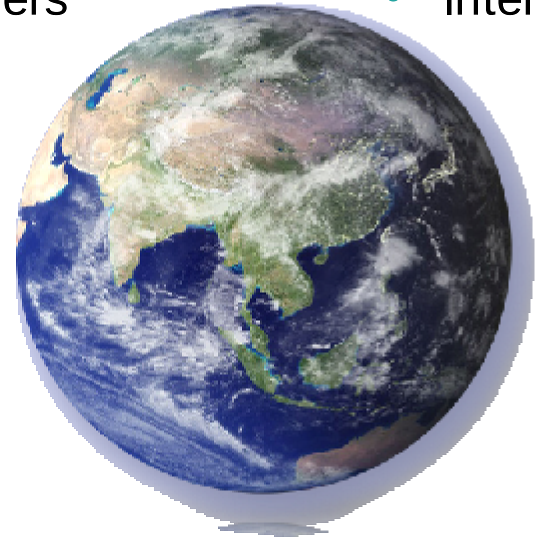
```
-bash-3.00$ sqlplus joe

SQL*Plus: Release 10.2.0.1.0 - Production on Fri Jul 29 13:39:31 2011

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

Chosen by Leading Organizations Worldwide

- 7 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 world’s favorite beverage brands
- 3 of the top 4 auto makers
- 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



Simplifying Enterprise Security for Dell

CASE STUDY:
SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

By Phil Neray
Addison Lawrence
David McMaster
Venugopal Nonavinakere

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

Securely maintaining sensitive financial and customer information in enterprise data cen-

desk—helps to ensure that a formal process is in place for tracking and addressing exceptions such as failed

Published case study in Dell Power Solutions

- **Who:** Connects with 5.4 billion+ customers every day
- **Need:**
  - Improve database security for SOX, PCI & SAS70
  - Simplify & automate compliance controls
- **Guardium Deployment:**
  - Phase 1: Deployed to 300 DB servers in 10 data centers (in 12 weeks)
  - Phase 2: Deploying to additional 725 database servers
- **Environment:**
  - Oracle & SQL Server on Windows, Linux; Oracle RAC, SQL Server clusters
  - Oracle EBS, JDE, Hyperion plus in-house applications
- **Previous Solution:** Native logging (MS) or auditing (Oracle) with in-house scripts
  - Supportability issues; DBA time required; massive data volumes; SOD issues.
- **Results:** Automated compliance reporting; real-time alerting; centralized cross-DBMS policies; closed-loop change control with Remedy integration
  - Guardium “successfully met Dell’s requirements without causing outages to any databases; produced a significant reduction in auditing overhead in databases.”

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.”

“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."

IBM Services, Software and Hardware for Total PCI Compliance

Meeting Requirements of the Digital Dozen

The products outlined in this chart highlight IBM capabilities. Please call your local IBM executive for a full listing of all products and services that map to PCI requirements

IBM PROFESSIONAL SERVICES

IBM SOFTWARE SOLUTIONS

1 FIREWALL TO PROTECT CARDHOLDER DATA

- IBM Proventia Server Intrusion Prevention System (IPS)
- IBM Proventia Network (IPS)
- IBM Global Services

2 NO DEFAULT PASSWORDS OR SECURITY PARAMETERS

- IBM Tivoli Access Manager
- IBM Proventia Network Multi-Function Security
- (MFS) –IBM Global Services

3 PROTECT STORED CARDHOLDER DATA

- IBM Storage Manager
- IBM Proventia Server IPS
- IBM PKI Services
- IBM Global Services
- IBM System z Encryption Solutions
- IBM IMS and DB2 Encryption Tool

4 ENCRYPT TRANSMISSION

- IBM Data Encryption of IMS and DB2
- IBM System z network encryption
- DataPower XML Security Gateway
- Proventia Network Intrusion Prevention System

5 USE & UPDATE ANTI-VIRUS SOFTWARE

- IBM Proventia Desktop Endpoint Security
- IBM Proventia Network Enterprise Scanner
- IBM Global Services

IBM HARDWARE

6 SECURE SYSTEMS & APPLICATIONS

- IBM Software Development Platform
- IBM Tivoli CCMBD
- IBM Global Services
- IBM Rational AppScan
- IBM Systems and Storage

7 RESTRICT ACCESS

- IBM Tivoli Access Manager
- IBM Tivoli zSecure Admin
- IBM Tivoli Compliance Insight Manager
- IBM Global Services

IBM MANAGED SERVICES

8 UNIQUE IDs

- IBM Tivoli Identity Manager
- IBM Tivoli Federated Identity Manager
- IBM Global Services

9 RESTRICT PHYSICAL ACCESS

- IBM Digital Video Surveillance
- IBM Biometric Access Control
- IBM Global Services

10 MONITOR ACCESS

- IBM Tivoli Compliance Insight Manager
- IBM Tivoli Security Operations Manager
- IBM Proventia Server IPS
- IBM Global Services

11 TEST SECURITY SYSTEMS AND PROCESS

- IBM ISS Products & Services
- Tivoli Security Compliance Manager
- IBM Proventia Network Anomaly Detection System (ADS)
- IBM Global Services
- IBM Rational AppScan

12 SECURITY POLICY FOR EMPLOYEES & CONTRACTORS

- IBM Global Services
- Tivoli Console Insight Manager

SECURE & PROTECT CARDHOLDER DATA

Thank You
Smarter software for a smarter planet
Information Management