IBM IT Risk Management Seminar

Overcoming Data Demons: Protecting data privacy and ensuring data security

John Christopher Isaac

Senior IT Specialist

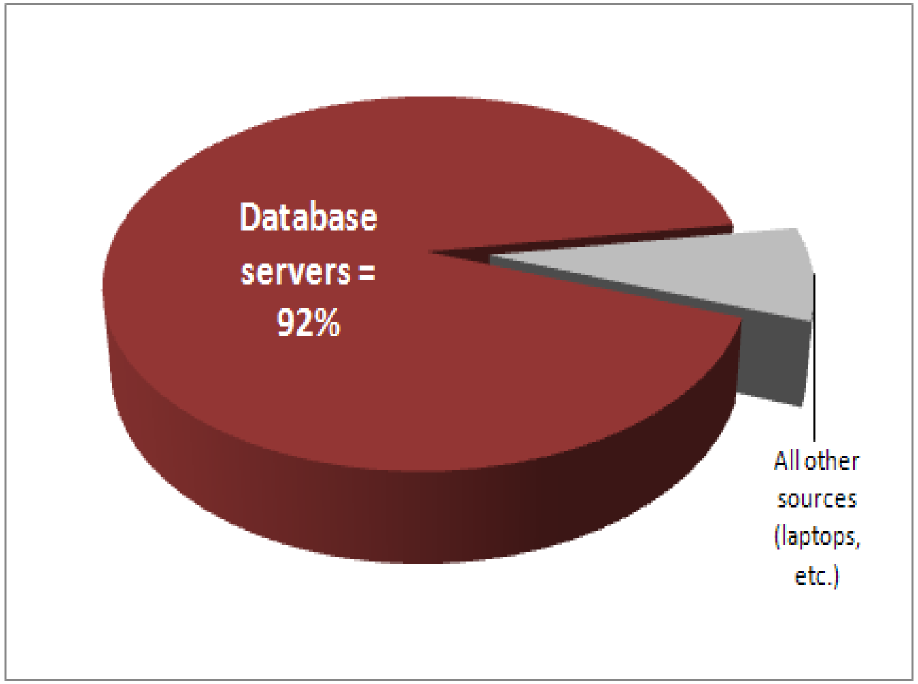
Information Management

Software Group

IBM ASEAN

Database Servers Are The Primary Source of Breached Data

Source of Breached Records



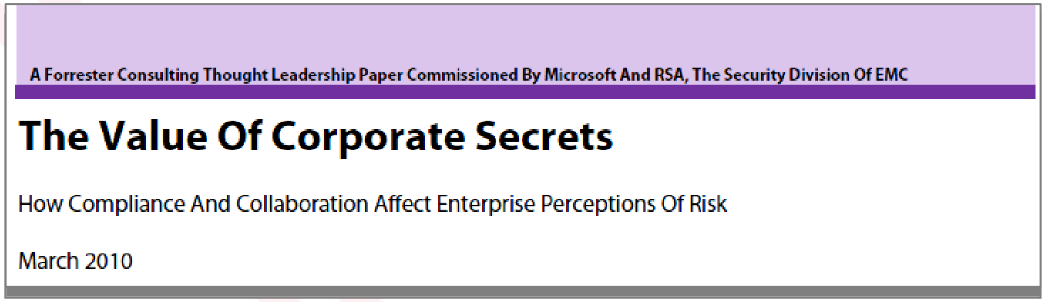
2010 Data Breach Report from Verizon Business RISK Team

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

… up from 75% in 2009 Report

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

Cost of a Data Breach



A Forrester Consulting Thought Leadership Paper Commissioned By Microsoft And RSA, The Security Division Of EMC

The Value Of Corporate Secrets

How Compliance And Collaboration Affect Enterprise Perceptions Of Risk

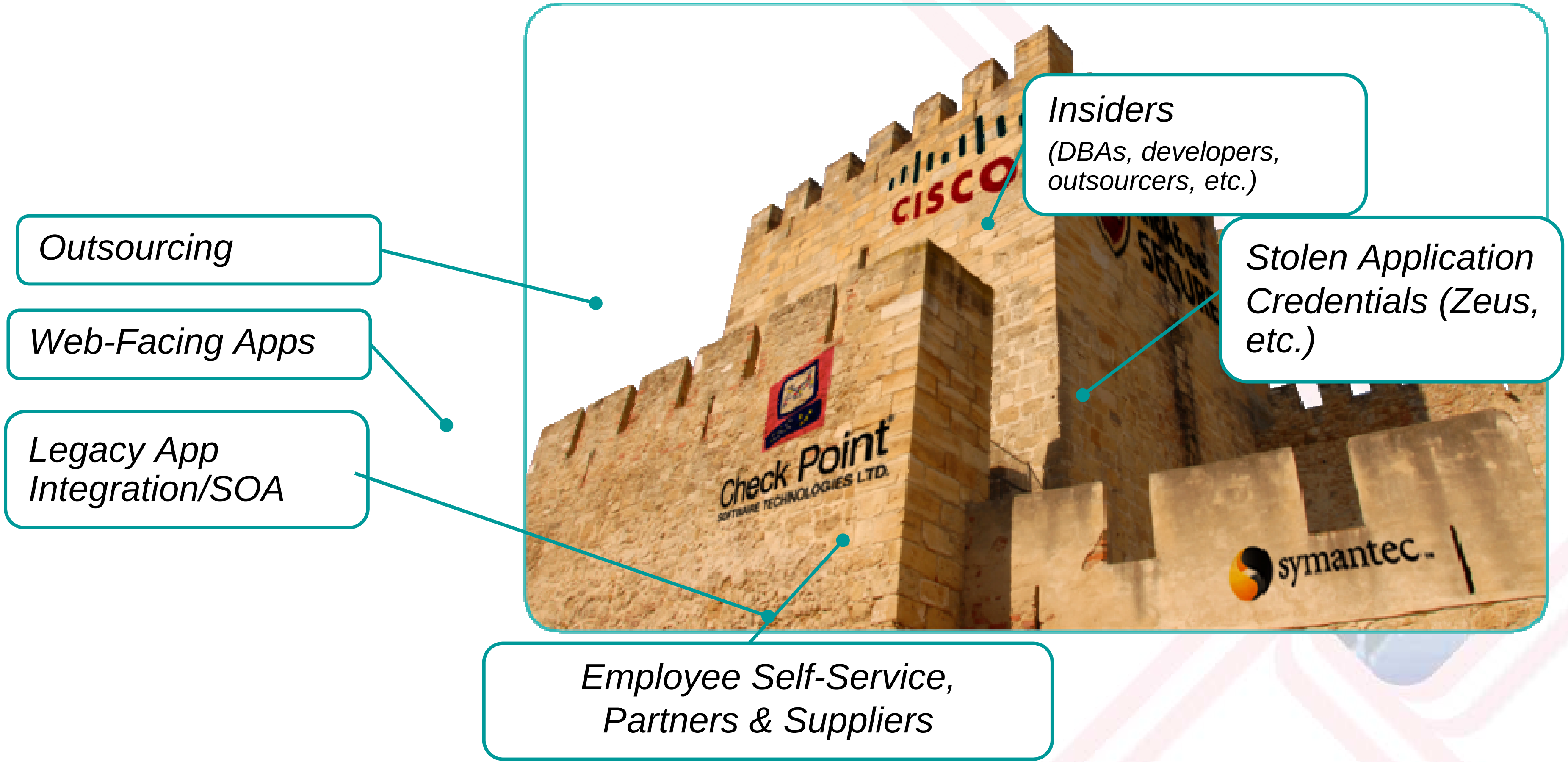
March 2010

- Forrester survey of 305 IT decision makers
- Secrets (e.g., strategic plans) are twice as valuable as custodial data (personal information, credit card data, etc.)
  - 2/3 of value in corporate information portfolio from non-regulated data (secrets)
- Companies focus mainly on preventing accidents (email, etc.)
  - But deliberate theft of information by employees is much more costly
  - Damage caused by rogue IT administrator = $482K (average)
  - Average cost of accidental leakage = $12K
- Most CISOs don't really know if their controls really work
- Note: Survey does not address other costs such as fines
  - Australian bank was fined $500K by VISA
  - Heartland breach cost = $140M

Perimeter Defenses 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



Outsourcing

Web-Facing Apps

Legacy App Integration/SOA

Insiders

(DBAs, developers, outsourcers, etc.)

Stolen Application Credentials (Zeus, etc.)

Employee Self-Service, Partners & Suppliers

Newly Discovered World Cup Database Breach Exposed 250,000 Attendees' Details

- Employee of the firm in charge of World Cup 2010 ticketing found peddling birth dates, passport, other data of 2006 World Cup customers
- Initially reported by Norwegian newspaper Dagbladet, the breach came to light when an employee of the firm in charge of World Cup 2010 ticketing circulated an e-mail peddling more than 250,000 2006 World Cup customer details, including such personal information as birth dates and passport information.
- "At the end of the '06 World Cup, a data destruction process should have been performed, and it clearly didn't occur to anyone [with FIFA or its IT firm]," Rachwald says. "[A good strategy should] identify what you have, attach risk and design a protection and destruction program."
- www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=227400151 (Dark Reading, September 10th, 2010)

Key Business Drivers for Database Activity Monitoring (DAM)

Continuously Monitor All Access to Sensitive Data:

1. **Prevent data breaches**
   - Cybercriminals & rogue insiders
   - Protect customer data & corporate secrets (IP)

2. **Assure data governance**
   - Prevent unauthorized changes to sensitive data by privileged users

3. **Reduce audit costs**
   - Automated, continuous controls
   - Simplified processes

Key Question

“Can you *prove* that *privileged users* have not jeopardized the integrity and/or privacy of your *sensitive data*?”

Top Data Protection Challenges

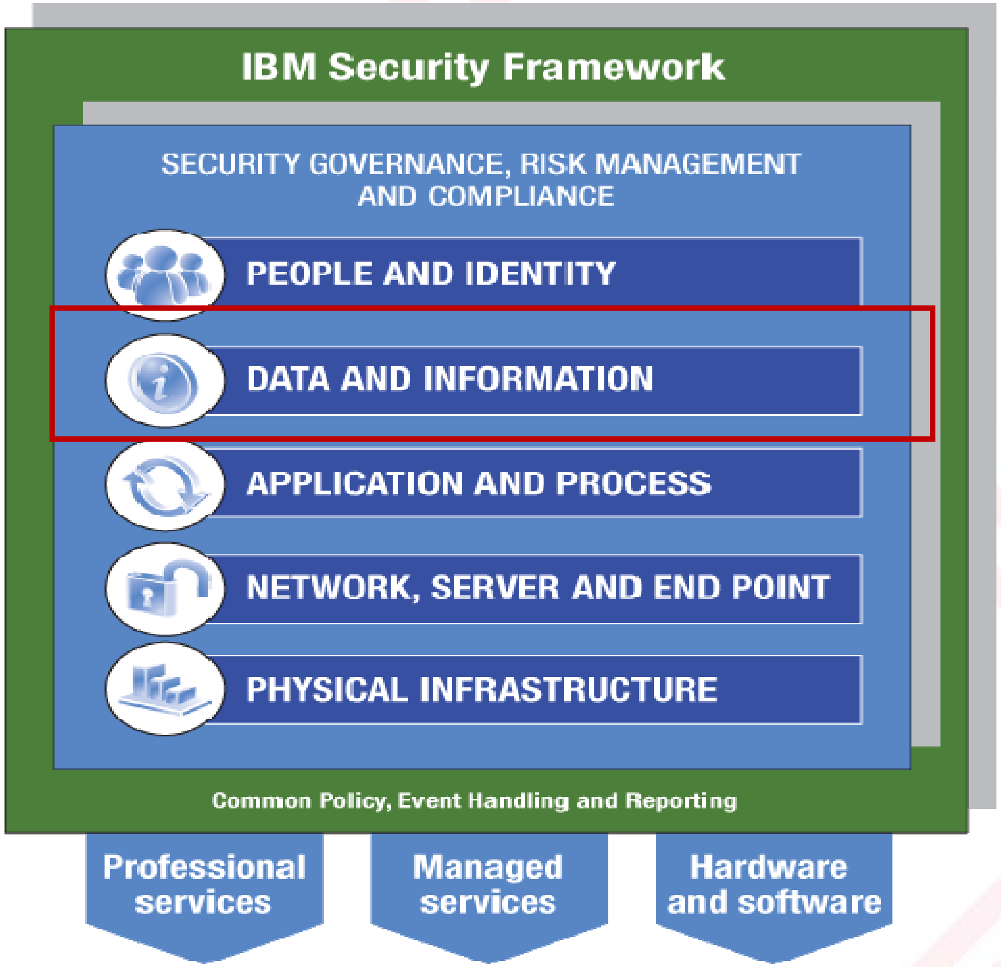
Where is my sensitive data located and who is using it?

How can I enforce access & change control policies for critical databases?

How do check for vulnerabilities and lock down database configurations?

How do I simplify & automate compliance?

Part of IBM Security Framework



IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

Top Regulations Impacting Databases

Data Governance

1. Sarbanes Oxley
2. Basel II
3. OFAC
4. Turnbull Report

Protect and control the ***process***

Data Privacy

1. Protection of Personal Information Act (SA)
2. Payment Card Industry (PCI)
3. EU DPD
4. Personal Information Protection & Electronic Documents Act (Canada)
5. AU/NZ NPP, etc.

Protect the ***data***

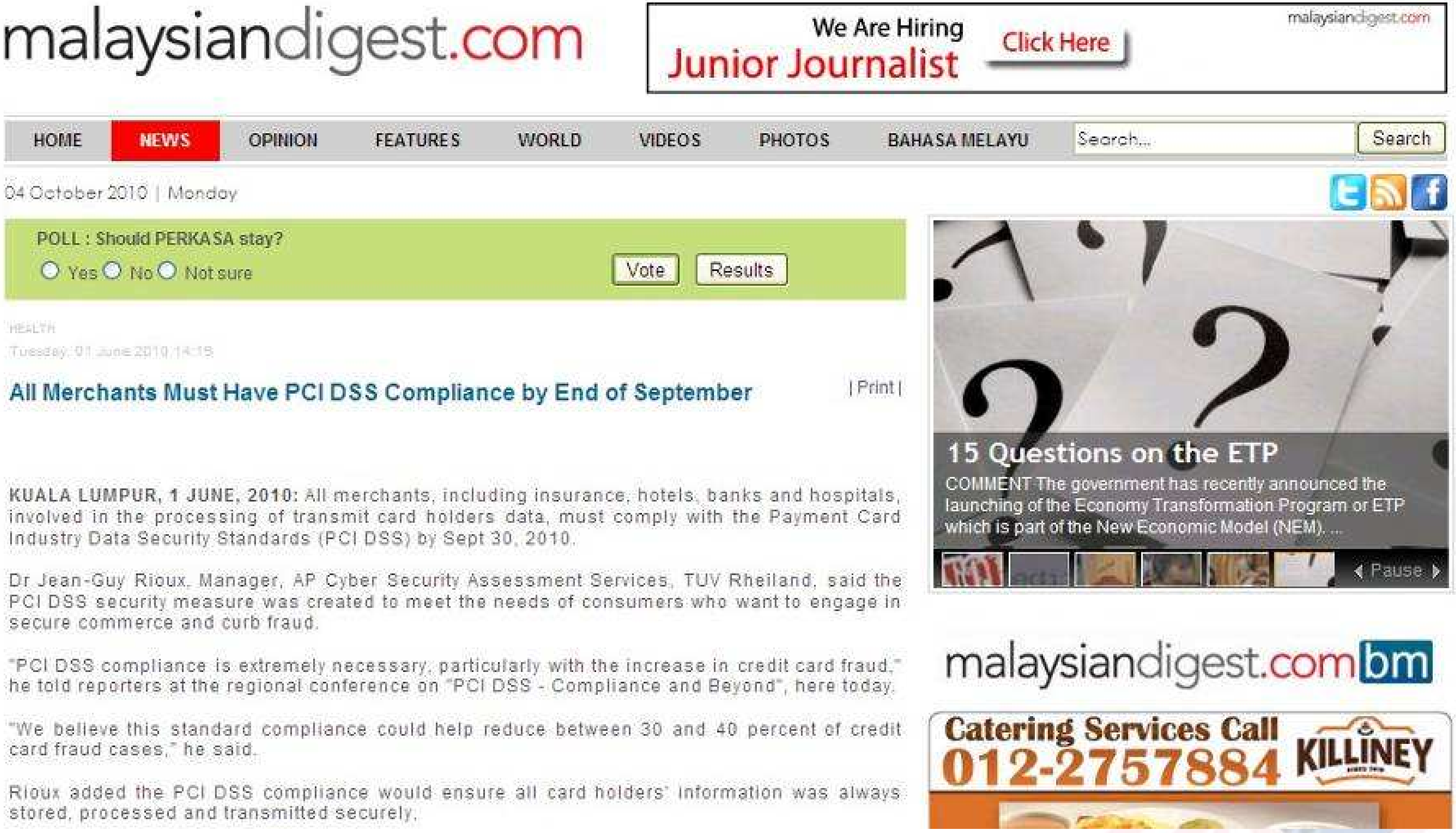
Courtesy: Gartner

Compliance Cheat Sheet

	SOX-like	PCI	Data Privacy
Key focus	Preventing unauthorized changes that could affect accuracy of financial reporting	Preventing theft of credit card or ATM data	Preventing identity theft
Primary groups or objects being monitored	Privileged users (DBAs, developers, outsourcers, etc.)	Privileged users (DBAs, developers, outsourcers, etc.); plus anyone who accesses sensitive cardholder data	Privileged users (DBAs, developers, outsourcers, etc.); plus anyone who accesses sensitive cardholder data
Primary SQL focus	DDL, DML	SELECTs	SELECTs
Typical Applications	ERP systems plus industry-specific	CRM systems plus industry-specific	HR systems plus industry-specific

Note: All compliance mandates are also concerned with monitoring security exceptions (such as failed logins & SQL errors) and changes in roles/permissions (GRANT, REVOKE).

PCI DSS Compliance in Malaysia



COMMENT The government has recently announced the launching of the Economy Transformation Program or ETP which is part of the New Economic Model (NEM). ...

HEALTH

Tuesday, 01 June 2010 14:15

All Merchants Must Have PCI DSS Compliance by End of September

| Print |

KUALA LUMPUR, 1 JUNE, 2010: All merchants, including insurance, hotels, banks and hospitals, involved in the processing of transmit card holders data, must comply with the Payment Card Industry Data Security Standards (PCI DSS) by Sept 30, 2010.

Dr Jean-Guy Rioux, Manager, AP Cyber Security Assessment Services, TUV Rheiland, said the PCI DSS security measure was created to meet the needs of consumers who want to engage in secure commerce and curb fraud.

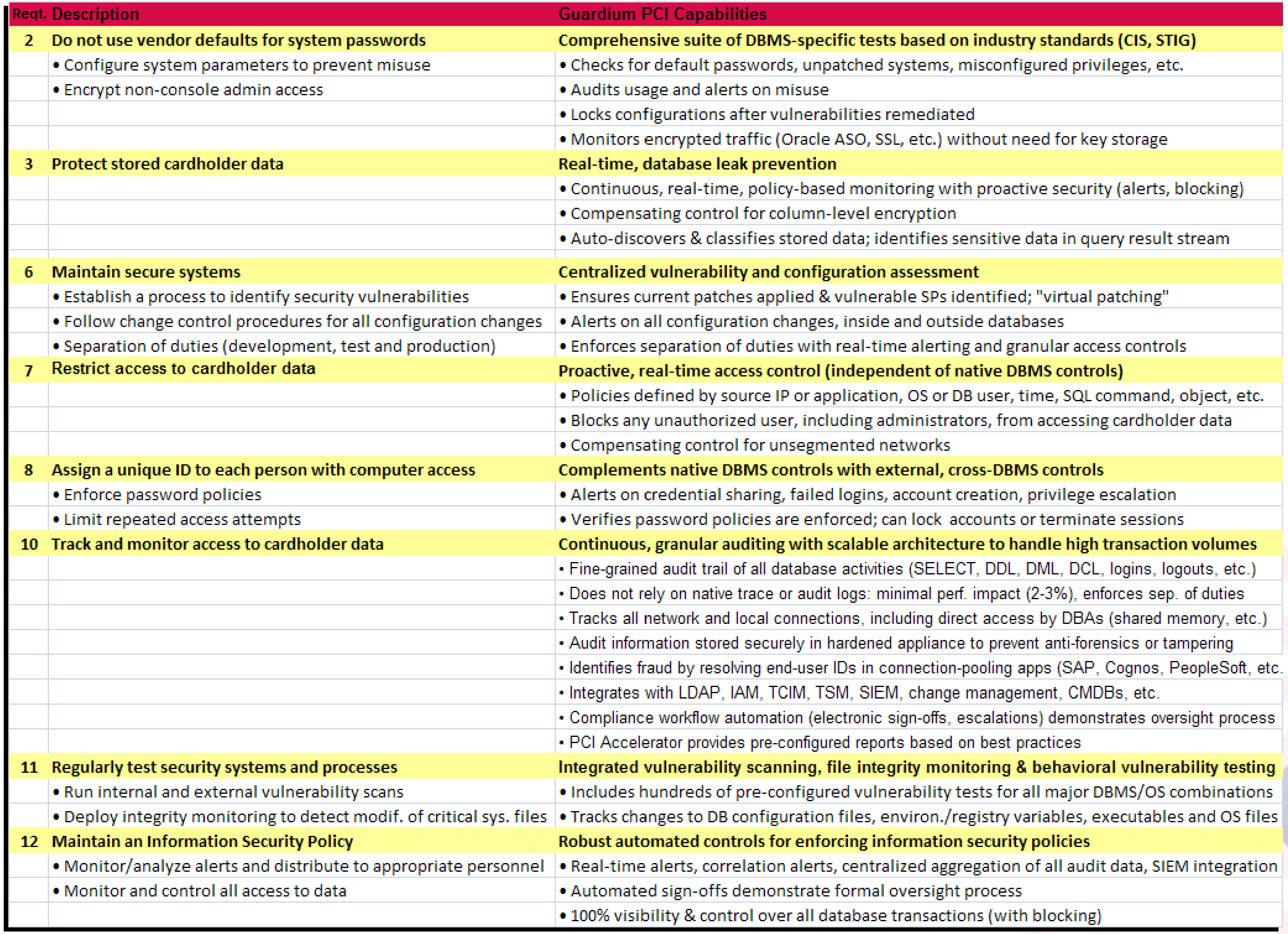
"PCI DSS compliance is extremely necessary, particularly with the increase in credit card fraud," he told reporters at the regional conference on "PCI DSS - Compliance and Beyond", here today.

"We believe this standard compliance could help reduce between 30 and 40 percent of credit card fraud cases," he said.

Rioux added the PCI DSS compliance would ensure all card holders' information was always stored, processed and transmitted securely.

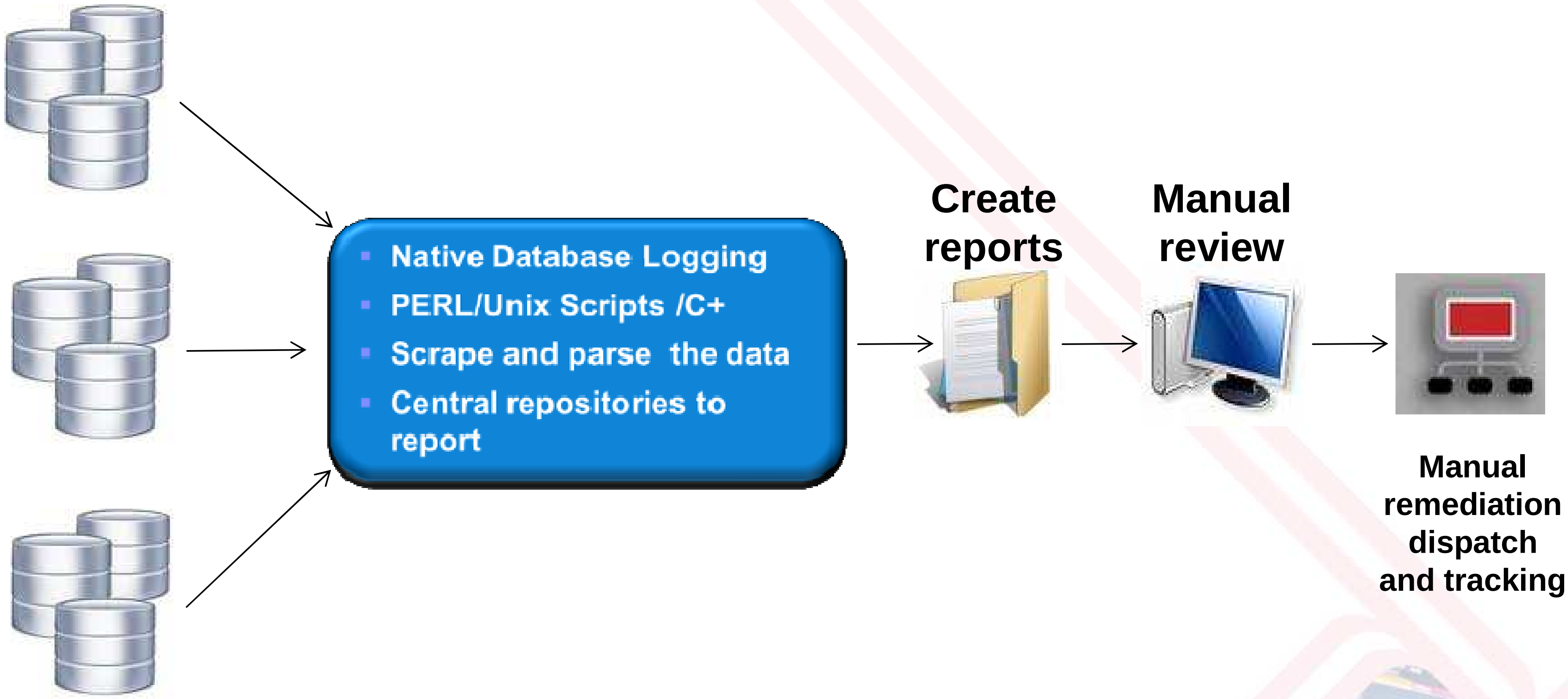
http://www.malaysiandigest.com/news/38-health/4203-all-merchants-must-have-pci-dss-compliance-by-end-of-september.html

How Guardium Addresses PCI-DSS



Reqt.	Description	Guardium PCI Capabilities
2	**Do not use vendor defaults for system passwords**	**Comprehensive suite of DBMS-specific tests based on industry standards (CIS, STIG)**
	• Configure system parameters to prevent misuse	• Checks for default passwords, unpatched systems, misconfigured privileges, etc.
	• Encrypt non-console admin access	• 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 stored data; identifies sensitive data in query result stream
6	**Maintain secure systems**	**Centralized vulnerability and configuration assessment**
	• Establish a process to identify security vulnerabilities	• Ensures current patches applied & vulnerable SPs identified; "virtual patching"
	• Follow change control procedures for all configuration changes	• Alerts on all configuration changes, inside and outside databases
	• Separation of duties (development, test and production)	• 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	• Alerts on credential sharing, failed logins, account creation, privilege escalation
	• Limit repeated access attempts	• 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, DDL, 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 processes**	**Integrated vulnerability scanning, file integrity monitoring & behavioral vulnerability testing**
	• Run internal and external vulnerability scans	• Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations
	• Deploy integrity monitoring to detect modif. of critical sys. files	• Tracks changes to DB configuration files, environ./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	• Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration
	• Monitor and control all access to data	• Automated sign-offs demonstrate formal oversight process
		• 100% visibility & control over all database transactions (with blocking)

What Database Audit Tools are Enterprises Using Today?



- Native Database Logging
- PERL/Unix Scripts /C+
- Scrape and parse the data
- Central repositories to report

Create reports

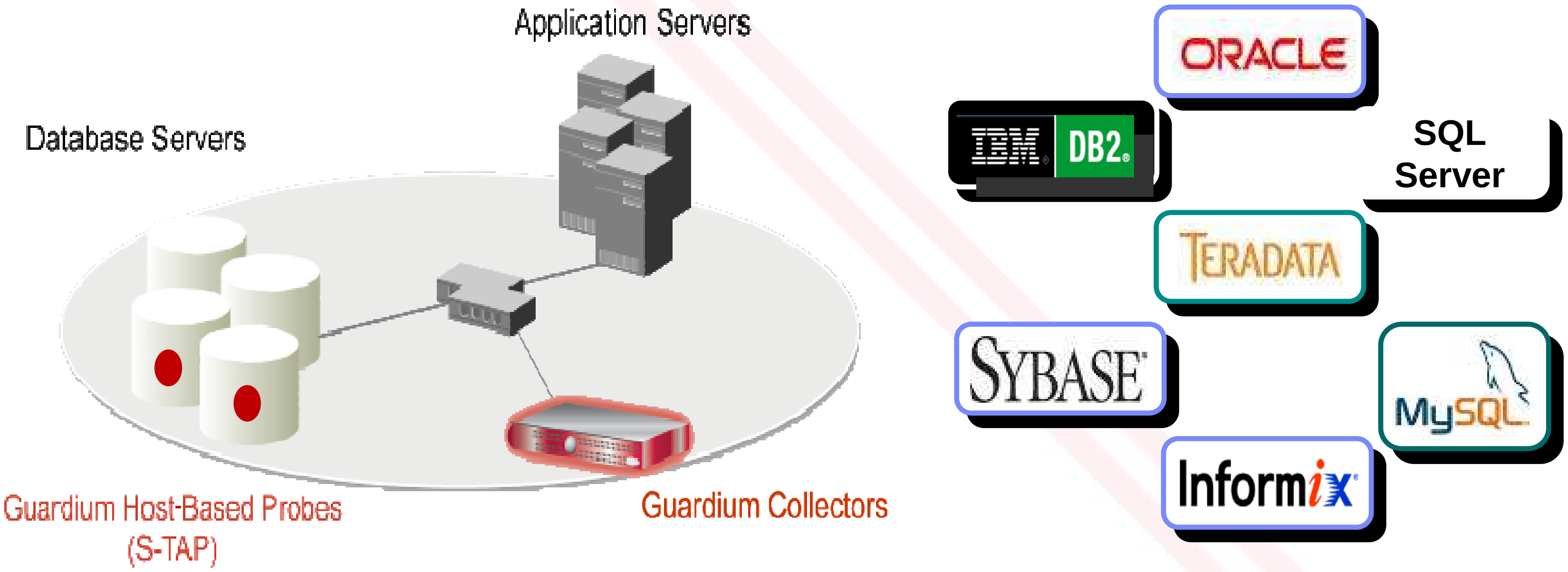
Manual review

Manual remediation dispatch and tracking

What Are the Challenges?

- No separation of duties; DBA run the process
- Performance impact of native logging on the DBMS
- Limited scope of logging data
- Not real-time
- Significant labor cost to review data and maintain process
- Another data store to secure and manage
- Manual remediation is error prone and costly
- Poor audit trail
- Inconsistent policies across systems and business units
- Lack of DBMS expertise

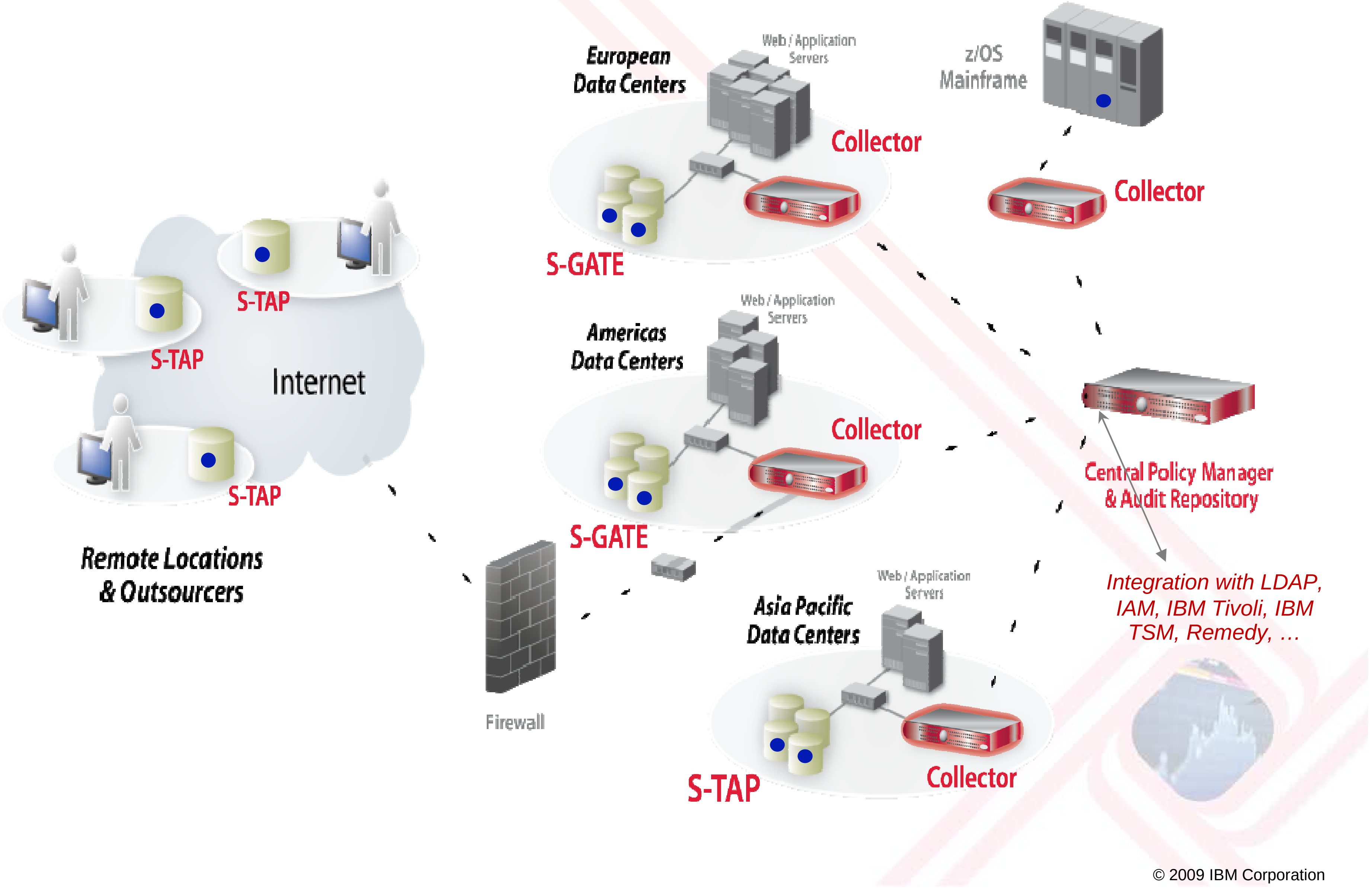
Real-Time Database Security and Monitoring



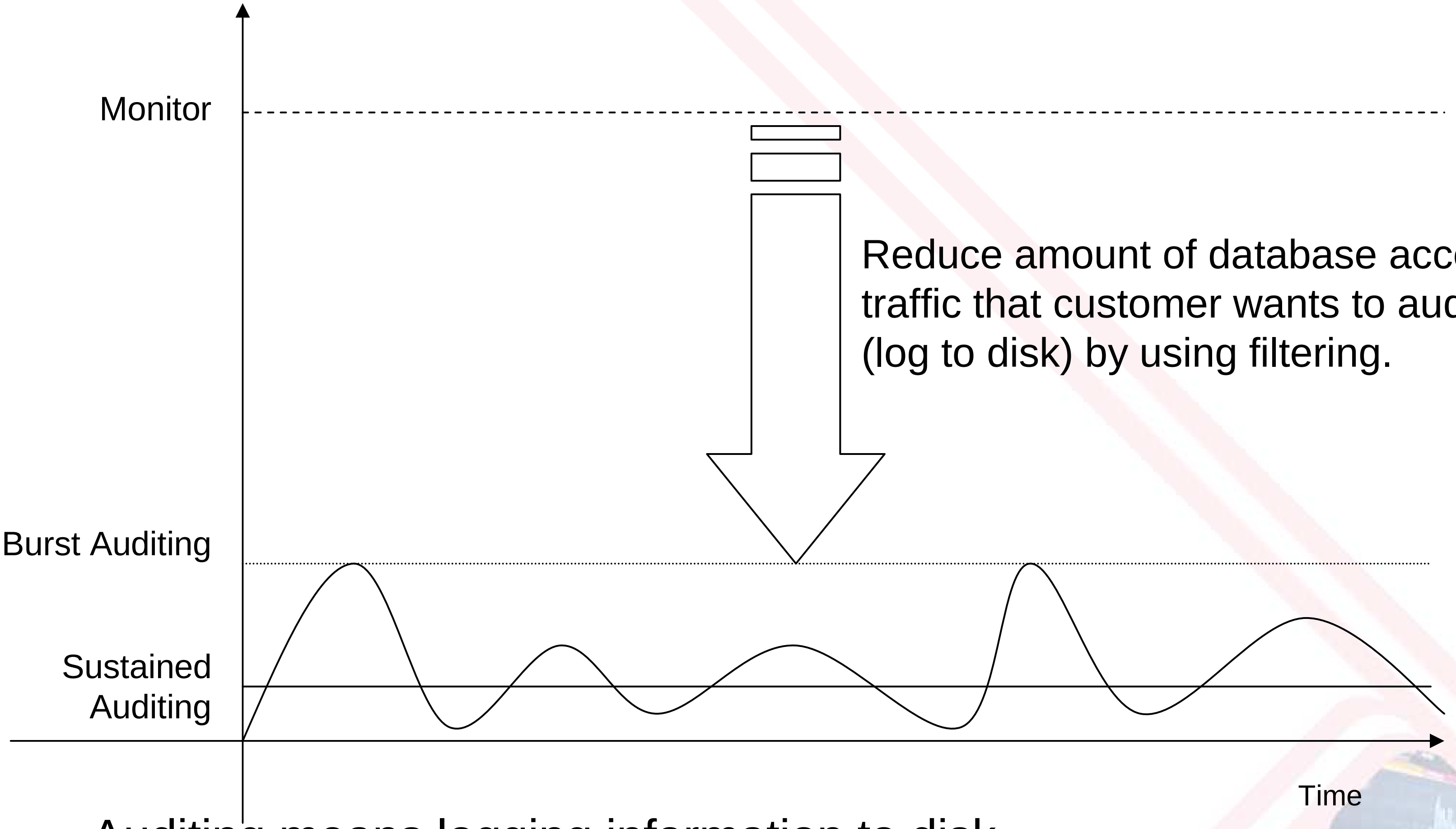
- Non-invasive architecture
  - Outside databases
  - Minimal performance impact
  - No DBMS or application changes
- Cross-DBMS solution
- 100% visibility including local DBA access

- Enforces separation of duties
- Does not rely on DBMS-resident logs that can easily be erased by attackers or rogue insiders
- Granular real-time, policies and auditing
  - Who, what, when, how
- Automated compliance reporting, sign-offs and escalations (SOX, PCI, NIST, etc.)

Federated System Design

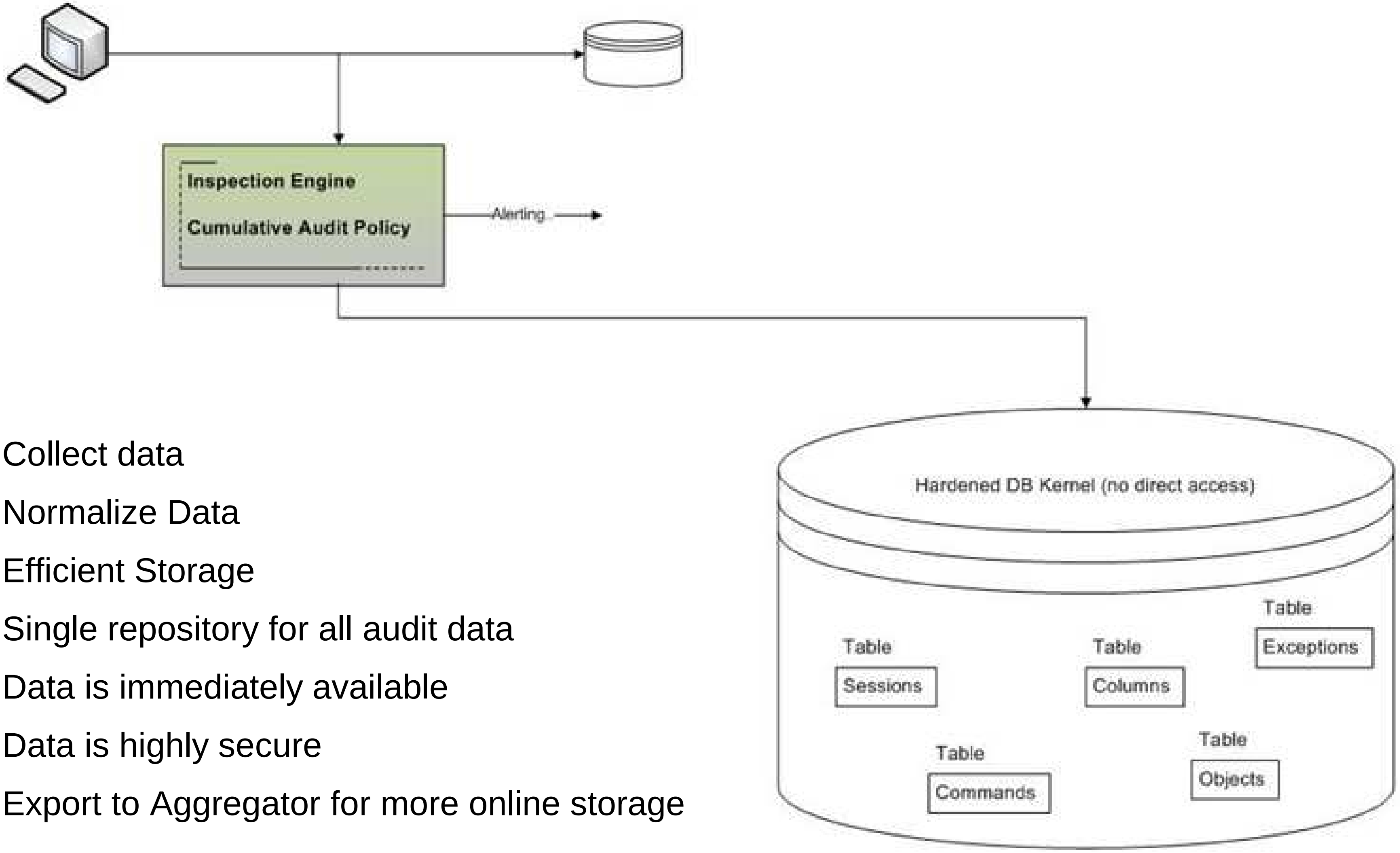


Monitoring vs Auditing



Auditing means logging information to disk
Monitor means watching all traffic (alerts, report DB errors, etc)

Guardium Collection Process

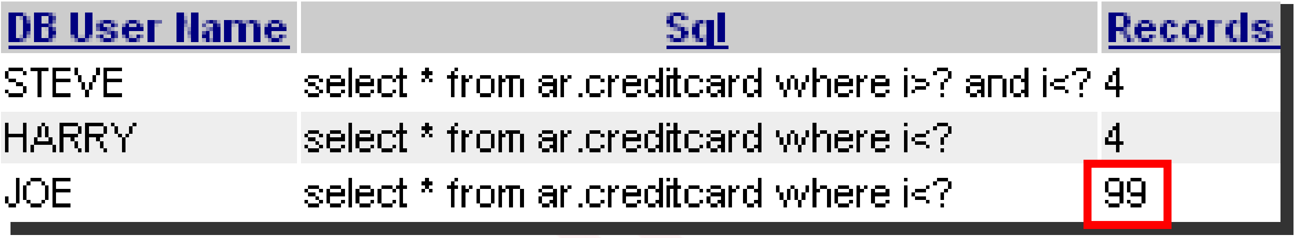


- Collect data
- Normalize Data
- Efficient Storage
- Single repository for all audit data
- Data is immediately available
- Data is highly secure
- Export to Aggregator for more online storage

Controlling Data Leakage Through Authorized Users

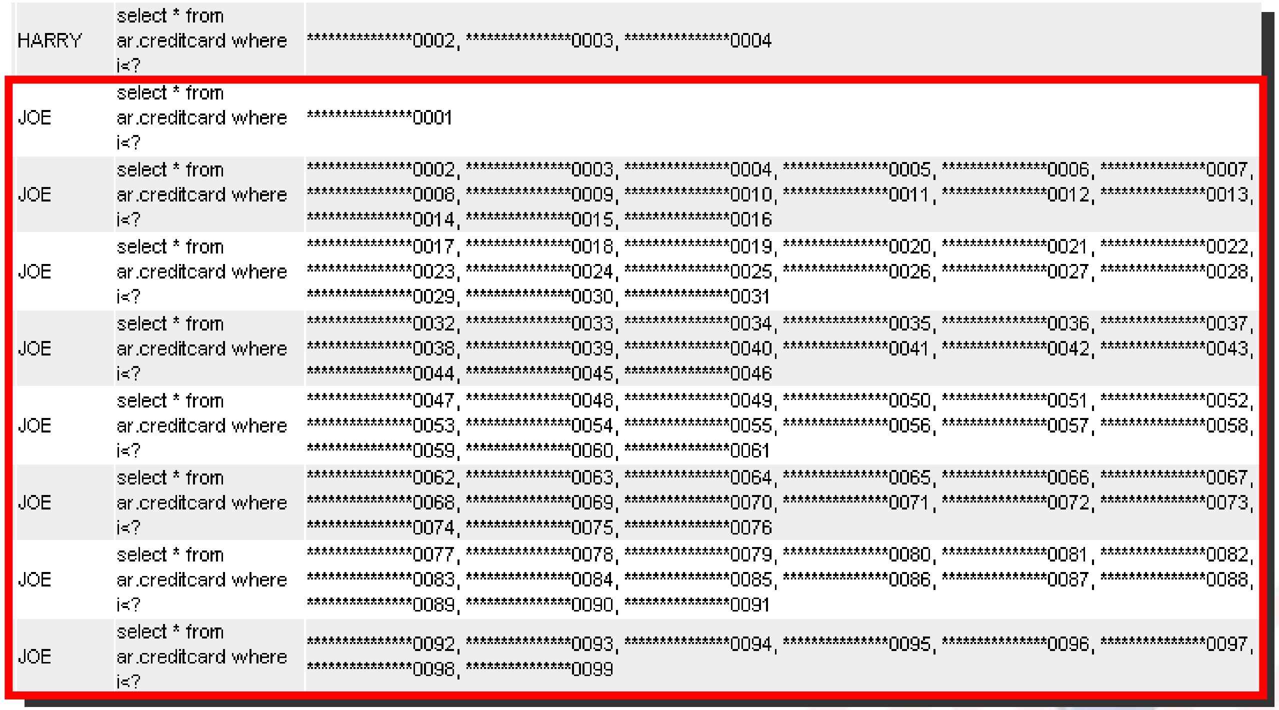
Should my CSR view 99 records in an hour?

Is this normal?



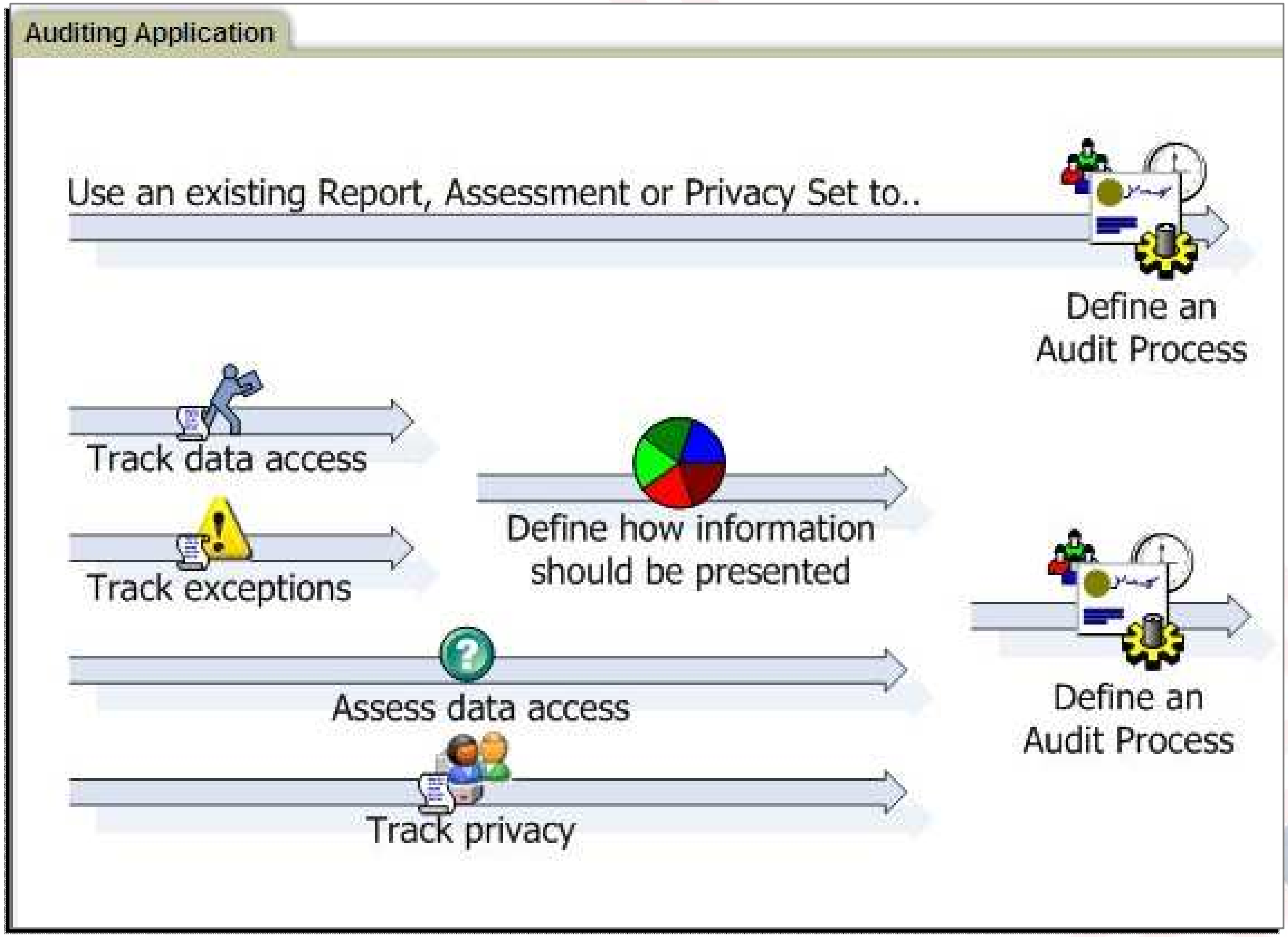
DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

What exactly did Joe see?



HARRY	select * from ar.creditcard where i<?	***************0002, ***************0003, ***************0004
JOE	select * from ar.creditcard where i<?	***************0001
JOE	select * from ar.creditcard where i<?	***************0002, ***************0003, ***************0004, ***************0005, ***************0006, ***************0007, ***************0008, ***************0009, ***************0010, ***************0011, ***************0012, ***************0013, ***************0014, ***************0015, ***************0016
JOE	select * from ar.creditcard where i<?	***************0017, ***************0018, ***************0019, ***************0020, ***************0021, ***************0022, ***************0023, ***************0024, ***************0025, ***************0026, ***************0027, ***************0028, ***************0029, ***************0030, ***************0031
JOE	select * from ar.creditcard where i<?	***************0032, ***************0033, ***************0034, ***************0035, ***************0036, ***************0037, ***************0038, ***************0039, ***************0040, ***************0041, ***************0042, ***************0043, ***************0044, ***************0045, ***************0046
JOE	select * from ar.creditcard where i<?	***************0047, ***************0048, ***************0049, ***************0050, ***************0051, ***************0052, ***************0053, ***************0054, ***************0055, ***************0056, ***************0057, ***************0058, ***************0059, ***************0060, ***************0061
JOE	select * from ar.creditcard where i<?	***************0062, ***************0063, ***************0064, ***************0065, ***************0066, ***************0067, ***************0068, ***************0069, ***************0070, ***************0071, ***************0072, ***************0073, ***************0074, ***************0075, ***************0076
JOE	select * from ar.creditcard where i<?	***************0077, ***************0078, ***************0079, ***************0080, ***************0081, ***************0082, ***************0083, ***************0084, ***************0085, ***************0086, ***************0087, ***************0088, ***************0089, ***************0090, ***************0091
JOE	select * from ar.creditcard where i<?	***************0092, ***************0093, ***************0094, ***************0095, ***************0096, ***************0097, ***************0098, ***************0099

Document and Define a Process



Auditing Application

Use an existing Report, Assessment or Privacy Set to..

Define an Audit Process

Track data access

Track exceptions

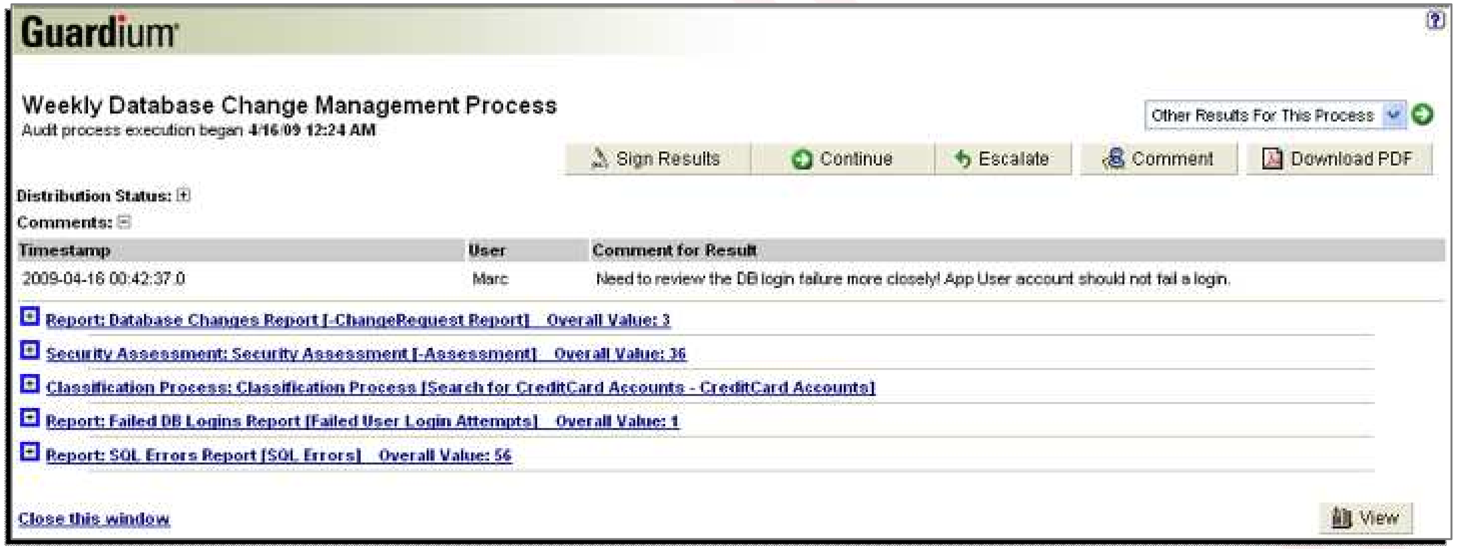
Define how information should be presented

Assess data access

Track privacy

Define an Audit Process

Automating Sign-offs & Escalations



Weekly Database Change Management Process

Audit process execution began **4/16/09 12:24 AM**

Distribution Status: ⊞

Comments: ⊟

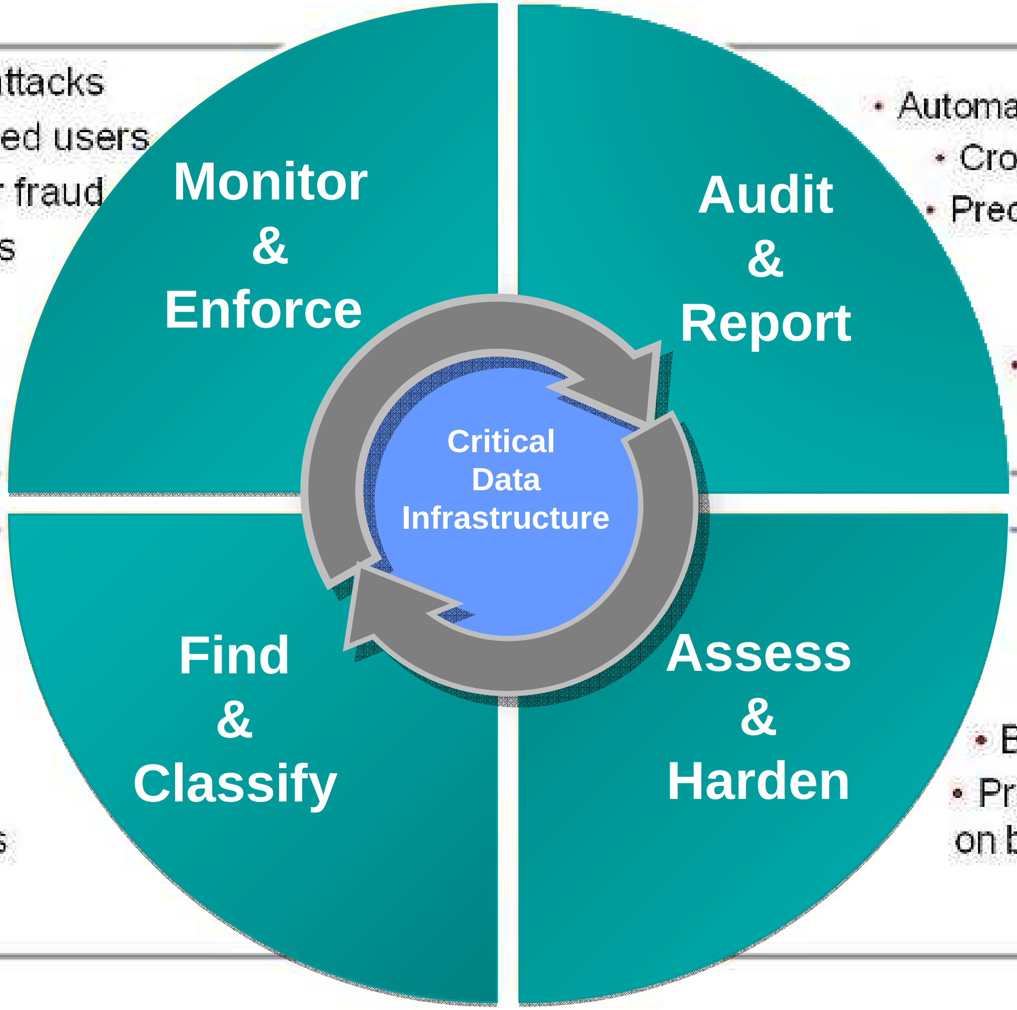
Timestamp	User	Comment for Result
2009-04-16 00:42:37.0	Marc	Need to review the DB login failure more closely! App User account should not fail a login.

- ⊟ Report: Database Changes Report [-ChangeRequest Report] Overall Value: 3
- ⊟ Security Assessment: Security Assessment [-Assessment] Overall Value: 36
- ⊟ Classification Process: Classification Process [Search for CreditCard Accounts - CreditCard Accounts]
- ⊟ Report: Failed DB Logins Report [Failed User Login Attempts] Overall Value: 1
- ⊟ Report: SQL Errors Report [SQL Errors] Overall Value: 56

Close this window

- Automate entire compliance workflow
  - Report distribution to oversight team
  - Electronic sign-offs
  - Escalations, comments & exception handling
- Provide visibility and tracking of status
- Addresses need to document oversight and resolution processes
- Results of audit process stored with audit data in secure audit repository
- Streamlines and simplifies compliance processes

Functional Modules



- Prevent SQL injection attacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Forensics data mining
- SIEM integration

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- Sign-off management
- Long-term retention
- No database changes or performance impact

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

- Assess database vulnerabilities
- Configuration auditing
- Behavioral vulnerabilities
- Preconfigured tests based on best practices standards (STIG, CIS)

Securing SAP & Siebel: 239% ROI and <6 Months Payback

Forrester Consulting

The Total Economic Impact™ Of Guardium Database Monitoring, Security and Auditing

For A Global Consumer Products Company

Commissioned Forrester Consulting Case Study

- **Who:** F500 consumer food manufacturer ($15B revenue)
- **Need:** Secure SAP & Siebel data for SOX
  - Enforce change controls & implement consistent auditing across platforms
- **Environment**
  - SAP, Siebel, Manugistics, IT2 + 21 other Key Financial Systems (KFS)
  - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results: 239% ROI & 5.9 months payback, plus:**
  - **Proactive security:** Real-time alert when changes made to critical tables
  - **Simplified compliance**: Passed 4 audits (internal & external)
    - *"The ability to associate changes with a ticket number makes our job a lot easier … which is something the auditors ask about."* [Lead Security Analyst]
  - **Strategic focus on data security**
    - *"There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers."*

Simplifying Enterprise Security for Dell

CASE STUDY: SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

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.

Published case study in Dell Power Solutions

- **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: Deployed 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.”

PCI Compliance for McAfee.com

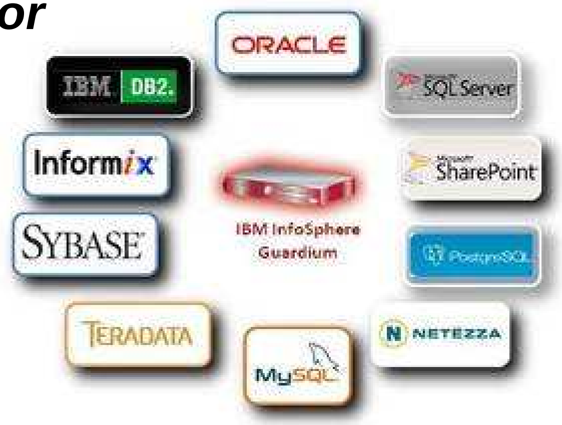
- **Who:** Global security company
- **Need:** Safeguard millions of PCI transactions
  - Maintain strict SLAs with ISP customers (Comcast, COX, etc.)
  - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
  - Multiple data centers; clustered databases
  - Integrated with ArcSight SIEM
  - Expanding coverage to SAP systems for SOX
- **Previous Solution:** Central database audit repository with native DBMS logs
  - Massive data volumes; performance & reliability issues
  - Separation of Duties (SOD) issues
- **Results**
  - *“McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with PCI-DSS – but given our significant transaction volumes, performance and reliability considerations were crucial.”*

Top 5 Global Bank with Multiple Business Units

- **Who:** Major global bank with multiple business units via mergers & acquisitions
  - Retail & corporate banking
  - Investment banking
  - Mortgage banking
- **Need:** Ensure privacy & integrity of all critical enterprise data
  - Financial & HR data; ERP data; credit card data; PII; strategic & intellectual property
  - Address PCI (Reqts. 3, 6 & 10); SOX; international data privacy laws; internal standards
- **Environment**
  - Oracle, SQL Server, Sybase, DB2 UDB; DB2 on z & iSeries; Informix; MySQL; Teradata
  - Solaris, HP-UX, AIX, Windows, Linux
  - Now monitoring ~2,000 database instances
- **Alternatives considered**
  - Native logging/auditing from Oracle
  - Symantec/ESM plus products from smaller vendors
- **Results**
  - Saving $1.5M per year in storage costs alone (for native audit trails)
  - Guardium now a standard part of bank infrastructure
  - Culture change – awareness of data security
  - New processes to investigate insider threats

Introducing InfoSphere Guardium 8

The Industry’s Broadest Platform Support for Database Security & Compliance

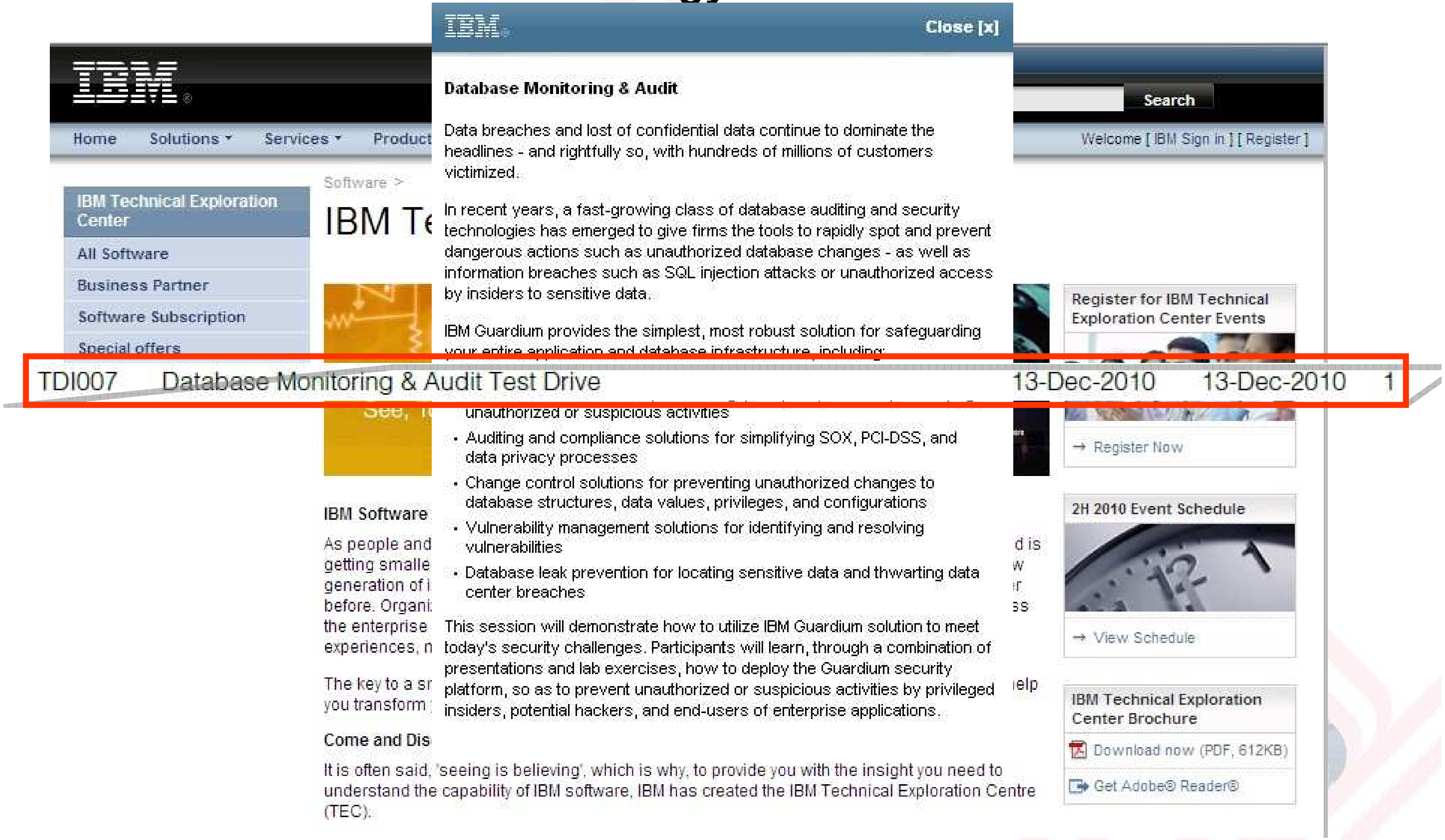


- Robust risk mitigation & data security
  - Beyond real-time monitoring to granular, proactive, access controls
  - Enhanced blocking: Cross-DBMS policies for Fire-ID management & User Quarantine
  - Without risky changes or root access to DBMS
- Enhanced SAP monitoring for fraud
  - More detailed information that goes beyond SAP logs => which SAP objects touched
  - No changes to SAP or databases
- First solution to monitor SharePoint repositories for sensitive data access
  - Customer information, corporate financials, strategic plans, new product designs, …
- New capabilities for DB2 for z (mainframe)
  - New vulnerability assessment (VA) module to identify weak permissions
  - New event capture technology based on robust, IBM-developed mainframe agent currently deployed at hundreds of mainframe sites
    - Replaces previous agent developed by a third-party
  - *Use case: Mainframe DBA or SYSADMIN accesses sensitive customer HR data*

InfoSphere Guardium 8 – Cont'd

- Entitlement reporting: Unified solution for all DBMS platforms
- Advanced compliance oversight & workflow automation
  - Now supports customized distribution to specific teams on line item basis (e.g., exceptions, escalations, sign-offs, etc.)
- Vulnerability assessment enhancements
  - 500 new tests; many with added tags for CVE standard
  - Tests based on industry-standard CIS Benchmark & DoD STIG
- Integration with Tivoli SIEM
  - Combines database monitoring information with log information from other sources (Windows, Unix, firewalls, IDS, etc.) for enterprise-wide security dashboard
  - Complements previous integration with other popular SIEM platforms
- New DBMS platforms
  - Netezza & PostreSQL, in addition to previous support for Oracle, SQL Server, IBM DB2 & Informix, Sybase ASE & IQ, MySQL, Teradata
- Numerous scalability & usability enhancements based on feedback from the world's largest & most diverse installations:
  - Automated on-boarding of new DBMS instances; new GUI; enhanced agent management; new Configuration Auditing templates; expanded API; …

Guardium - Proof Of Technology



Database Monitoring & Audit

Data breaches and lost of confidential data continue to dominate the headlines - and rightfully so, with hundreds of millions of customers victimized.

In recent years, a fast-growing class of database auditing and security technologies has emerged to give firms the tools to rapidly spot and prevent dangerous actions such as unauthorized database changes - as well as information breaches such as SQL injection attacks or unauthorized access by insiders to sensitive data.

IBM Guardium provides the simplest, most robust solution for safeguarding your entire application and database infrastructure, including:

- unauthorized or suspicious activities
- Auditing and compliance solutions for simplifying SOX, PCI-DSS, and data privacy processes
- Change control solutions for preventing unauthorized changes to database structures, data values, privileges, and configurations
- Vulnerability management solutions for identifying and resolving vulnerabilities
- Database leak prevention for locating sensitive data and thwarting data center breaches

This session will demonstrate how to utilize IBM Guardium solution to meet today's security challenges. Participants will learn, through a combination of presentations and lab exercises, how to deploy the Guardium security platform, so as to prevent unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise applications.

TDI007	Database Monitoring & Audit Test Drive	13-Dec-2010	13-Dec-2010	1

Register for IBM Technical Exploration Center Events
→ Register Now
2H 2010 Event Schedule
→ View Schedule
IBM Technical Exploration Center Brochure
Download now (PDF, 612KB)
Get Adobe® Reader®

IBM Software

As people and ... getting smalle... generation of i... before. Organi... the enterprise ... experiences, n...

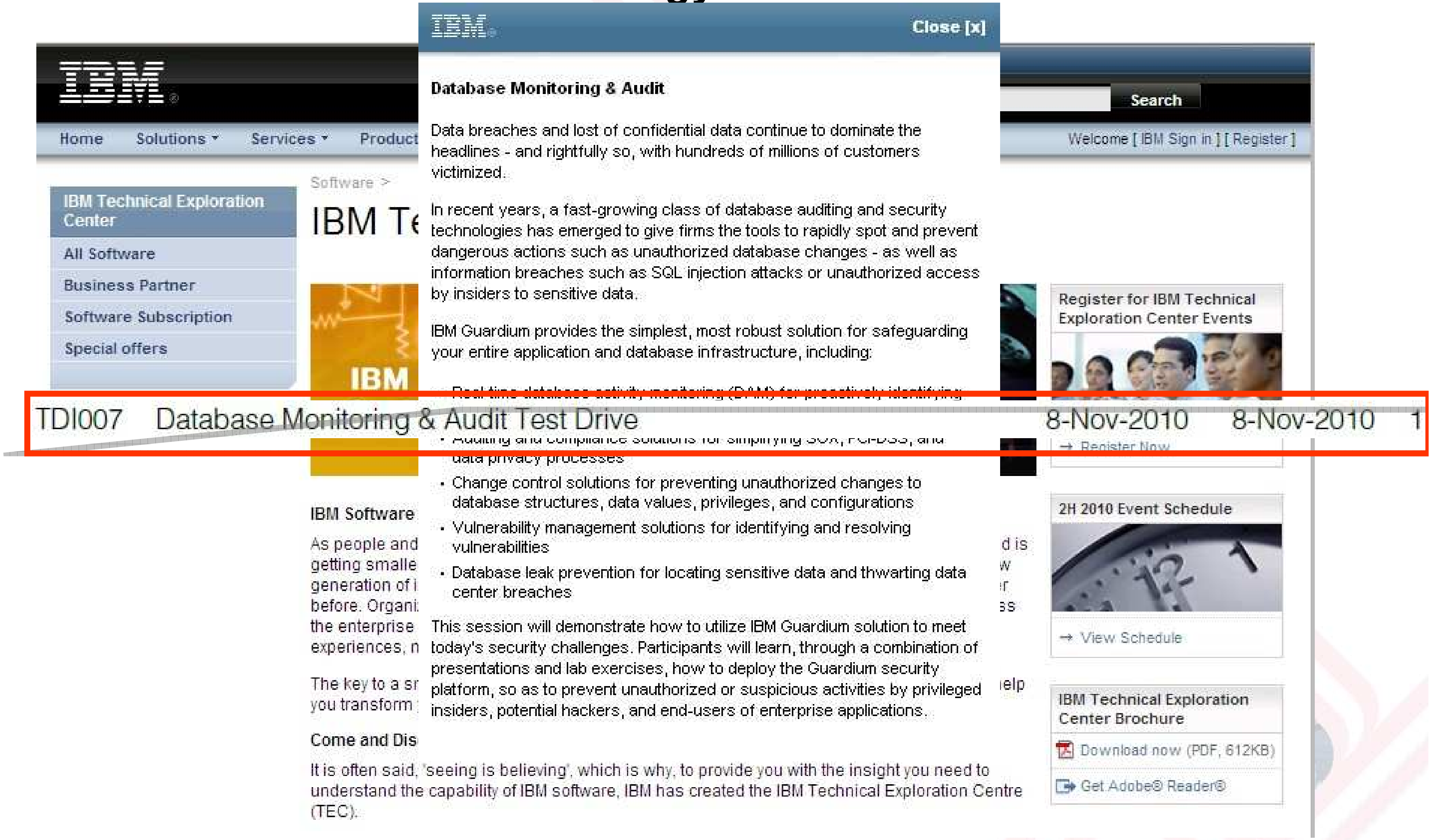
The key to a sr... you transform ...

Come and Dis

It is often said, 'seeing is believing', which is why, to provide you with the insight you need to understand the capability of IBM software, IBM has created the IBM Technical Exploration Centre (TEC).

Register at: http://www-01.ibm.com/software/my/TEC/

Guardium - Proof Of Technology



Database Monitoring & Audit

Data breaches and lost of confidential data continue to dominate the headlines - and rightfully so, with hundreds of millions of customers victimized.

In recent years, a fast-growing class of database auditing and security technologies has emerged to give firms the tools to rapidly spot and prevent dangerous actions such as unauthorized database changes - as well as information breaches such as SQL injection attacks or unauthorized access by insiders to sensitive data.

IBM Guardium provides the simplest, most robust solution for safeguarding your entire application and database infrastructure, including:

- Real-time database activity monitoring (DAM) for proactively identifying
- Auditing and compliance solutions for simplifying SOX, PCI-DSS, and data privacy processes
- Change control solutions for preventing unauthorized changes to database structures, data values, privileges, and configurations
- Vulnerability management solutions for identifying and resolving vulnerabilities
- Database leak prevention for locating sensitive data and thwarting data center breaches

This session will demonstrate how to utilize IBM Guardium solution to meet today's security challenges. Participants will learn, through a combination of presentations and lab exercises, how to deploy the Guardium security platform, so as to prevent unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise applications.

TDI007	Database Monitoring & Audit Test Drive	8-Nov-2010	8-Nov-2010	1

IBM Te

IBM Software

As people and ... d is getting smalle ... w generation of i ... r before. Organi: ... ss the enterprise experiences, n

The key to a sr ... ielp you transform

Come and Dis

It is often said, 'seeing is believing', which is why, to provide you with the insight you need to understand the capability of IBM software, IBM has created the IBM Technical Exploration Centre (TEC).

Register for IBM Technical Exploration Center Events

→ Register Now

2H 2010 Event Schedule

→ View Schedule

IBM Technical Exploration Center Brochure

Download now (PDF, 612KB)

Get Adobe® Reader®

Register at: http://www-01.ibm.com/software/sg/TEC/

Chosen by Leading Organizations Worldwide

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 4 of the top 6 global insurers
- 2 of the world’s favorite beverage brands
- The most recognized name in PCs
- 25 of the world’s leading telcos

- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

The Choice of Financial Services Leaders

citi	Bank of America	HSBC	RBS The Royal Bank of Scotland Group	Santander
MasterCard	SOCIETE GENERALE	ING	Itaú	CHASE
PRUDENTIAL	Aetna	BARCLAYS	AVIVA	NEW YORK LIFE
Allianz	Yorkshire BUILDING SOCIETY	POLCARD	threadneedle.	PING AN 平安
البنك السعودي الفرنسي Banque Saudi Fransi	MetLife	Daiwa House	Bank of Tokyo-Mitsubishi UFJ MUFG	GE Money WORLDWIDE
Putnam INVESTMENTS	clearstream DEUTSCHE BÖRSE GROUP	FEDERAL TRADE COMMISSION PROTECTING AMERICA'S CONSUMERS	sogei	AIG Bank

gracias
merci
obrigado
graciñas
obrigada
hvala
dank
thank
grâces
gràcies
rahmat
wel
mauruuru
terima
takk
kasih
kié
asante
murakoze
tesekkur
gratias
basque
pers
mamnun
grazie
mèsi
aabhar
much
salamat
plural
tänan
tapadh
ni
je
kop
khun
ko
po
pa
cám
asko
formal
singular
sah
agimus
grandmercé
diolch
diky
olun
muchas
nizzik
manana
kiitos
maita
mersi
mercé
dankon
akpé
faleminderit
dhanyavad
diakuiu
dakujem
sana
deu
nanni
bedankt
milesker
beacôp
Allahu
khob
leat
chnorakaloutioun
dziękuję
go
ederim
edirem
krap
najis
leibh
shukriya
mochchakkeram
faafetai
didi
kyay
enkosi
nirringrazzjak
arigatô
grazzi
bayarlalaa
blagodaram
dhanyavaad
dhanyabaad
sagolun
grassie
respectful
gracie
sheun
dhanyavadalu
blagodaria
madloba
mahalo
aahe
informal
saha
maith
Barak
dhanyavadagalu
aabhari
dankewol
ngiyabonga
dziakuju
dankie
danke
kha
sag
ago
hamnida
sobodi
akun
chai
misaotra
meharbani
gratzias
familiar
ju
aguyjé
ačiū
fyri
nandri
agat
raibh
kam
lava
paldies
köszönöm
chokrane
děkuji
dieuf
marahaba
efharisto
barkal
northern
djiere
eskerrik
fiik
motashakkeram
danki
côps
mulțumesc