IBM INFORMATION INTEGRATION
& GOVERNANCE SYMPOSIUM 2012

Delivering Trusted Information for Smarter Business Decisions

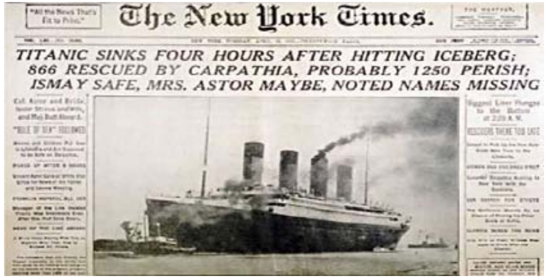
Jump Start PCI Compliance With InfoSphere Data Security

Steve Gibson

Senior Consultant, Data Security & Compliance

1st May 2012

Are You On The Crew Of Titanic, Ltd?



"All the News That's Fit to Print."

The New York Times.

TITANIC SINKS FOUR HOURS AFTER HITTING ICEBERG; 866 RESCUED BY CARPATHIA, PROBABLY 1250 PERISH; ISMAY SAFE, MRS. ASTOR MAYBE, NOTED NAMES MISSING

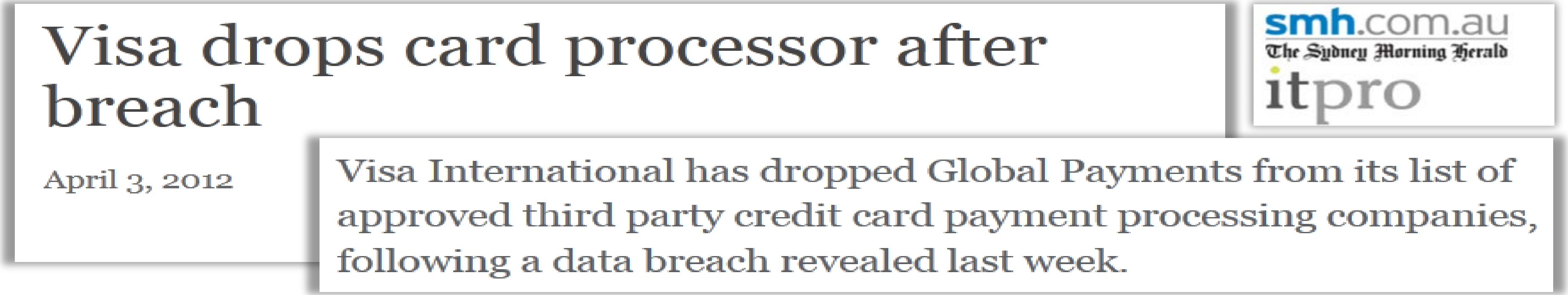
- **2223** People on the Titanic
- **48** Lifeboats in the design
- **20** Lifeboats actually carried
- **1517** Lost at sea

Titanic had enough lifeboats to be in compliance with the law!

- **??** Volume of Sensitive Data In Your Databases?
- **??** Your Data Security and Compliance Plan?
- **??** How Much of Your Plan is Implemented?
- **??** Volume of Data Lost in a Breach?

Is being legal enough to protect your data?

Why Should You Care About Data Security?

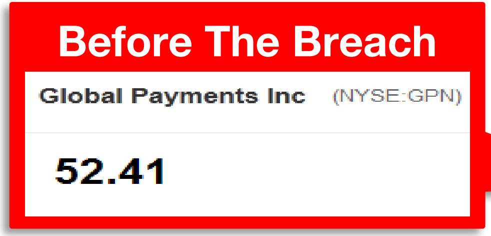


Visa drops card processor after breach

April 3, 2012

Visa International has dropped Global Payments from its list of approved third party credit card payment processing companies, following a data breach revealed last week.

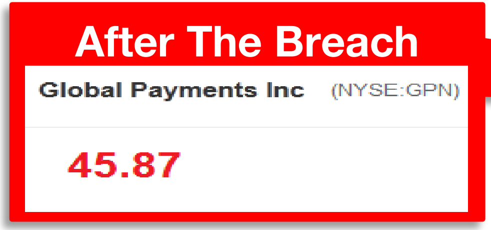
smh.com.au
The Sydney Morning Herald
itpro



Before The Breach

Global Payments Inc (NYSE:GPN)

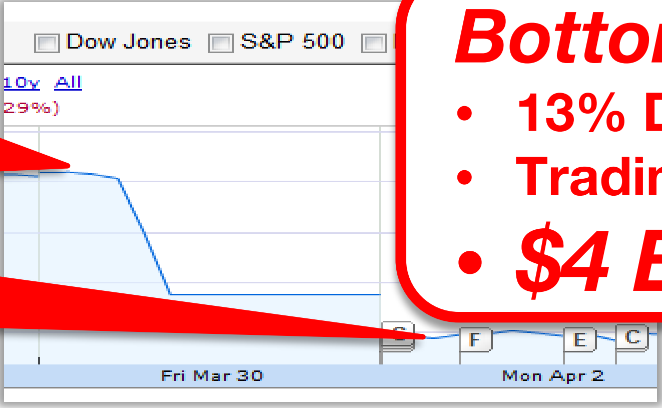
52.41



After The Breach

Global Payments Inc (NYSE:GPN)

45.87



Bottom Line?

- **13% Drop in Price**
- **Trading Halted**
- ***$4 Billion Wiped***

What Does PCI DSS Require?

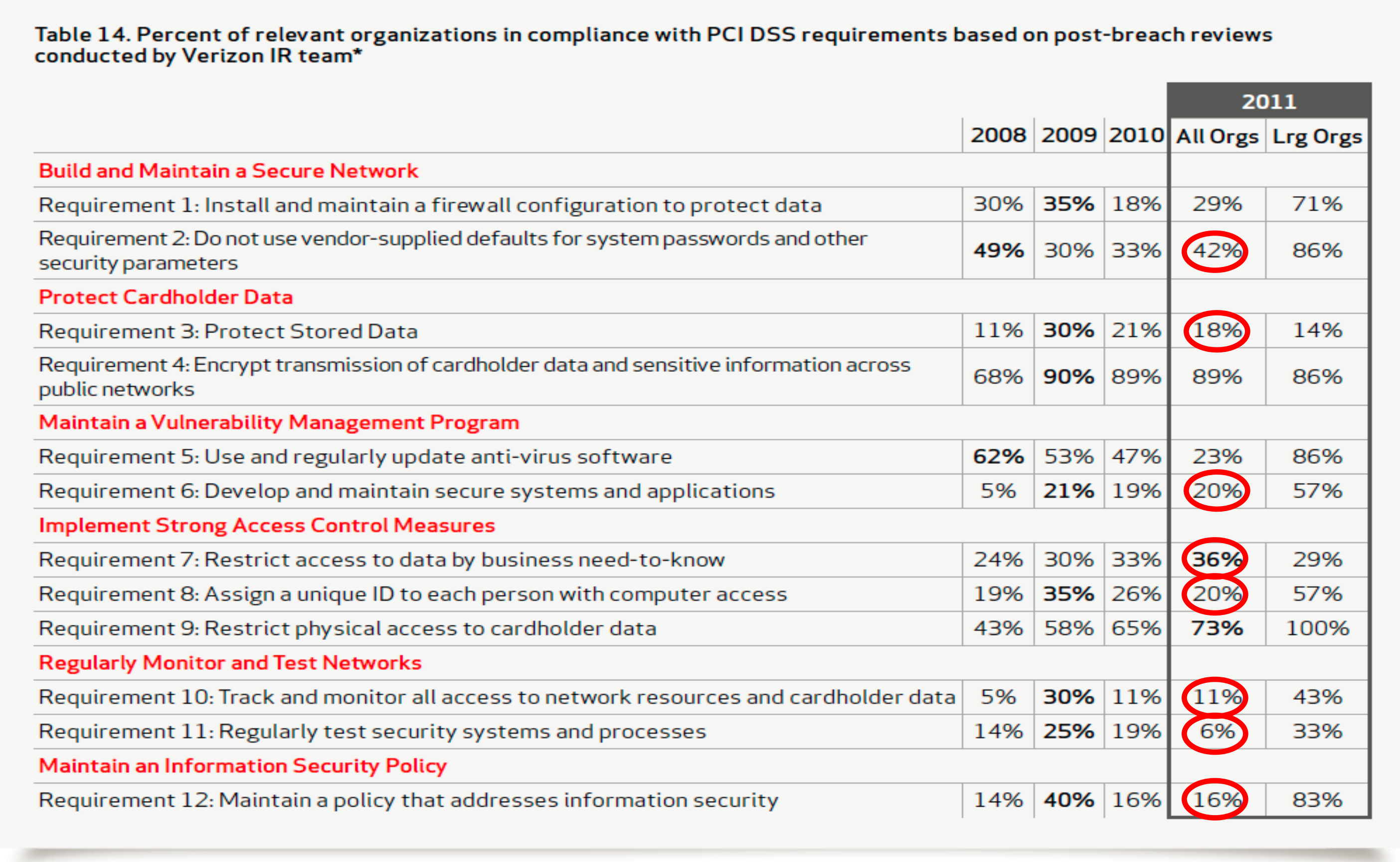


Table 14. Percent of relevant organizations in compliance with PCI DSS requirements based on post-breach reviews conducted by Verizon IR team*

				2011	
	2008	2009	2010	All Orgs	Lrg Orgs
Build and Maintain a Secure Network					
Requirement 1: Install and maintain a firewall configuration to protect data	30%	**35%**	18%	29%	71%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	**49%**	30%	33%	42%	86%
Protect Cardholder Data					
Requirement 3: Protect Stored Data	11%	**30%**	21%	18%	14%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	**90%**	89%	89%	86%
Maintain a Vulnerability Management Program					
Requirement 5: Use and regularly update anti-virus software	**62%**	53%	47%	23%	86%
Requirement 6: Develop and maintain secure systems and applications	5%	**21%**	19%	20%	57%
Implement Strong Access Control Measures					
Requirement 7: Restrict access to data by business need-to-know	24%	30%	33%	**36%**	29%
Requirement 8: Assign a unique ID to each person with computer access	19%	**35%**	26%	20%	57%
Requirement 9: Restrict physical access to cardholder data	43%	58%	65%	**73%**	100%
Regularly Monitor and Test Networks					
Requirement 10: Track and monitor all access to network resources and cardholder data	5%	**30%**	11%	11%	43%
Requirement 11: Regularly test security systems and processes	14%	**25%**	19%	6%	33%
Maintain an Information Security Policy					
Requirement 12: Maintain a policy that addresses information security	14%	**40%**	16%	16%	83%

2012 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

twitter: *Follow* ***@ANZ_IM*** *or mention* ***#IIGS***

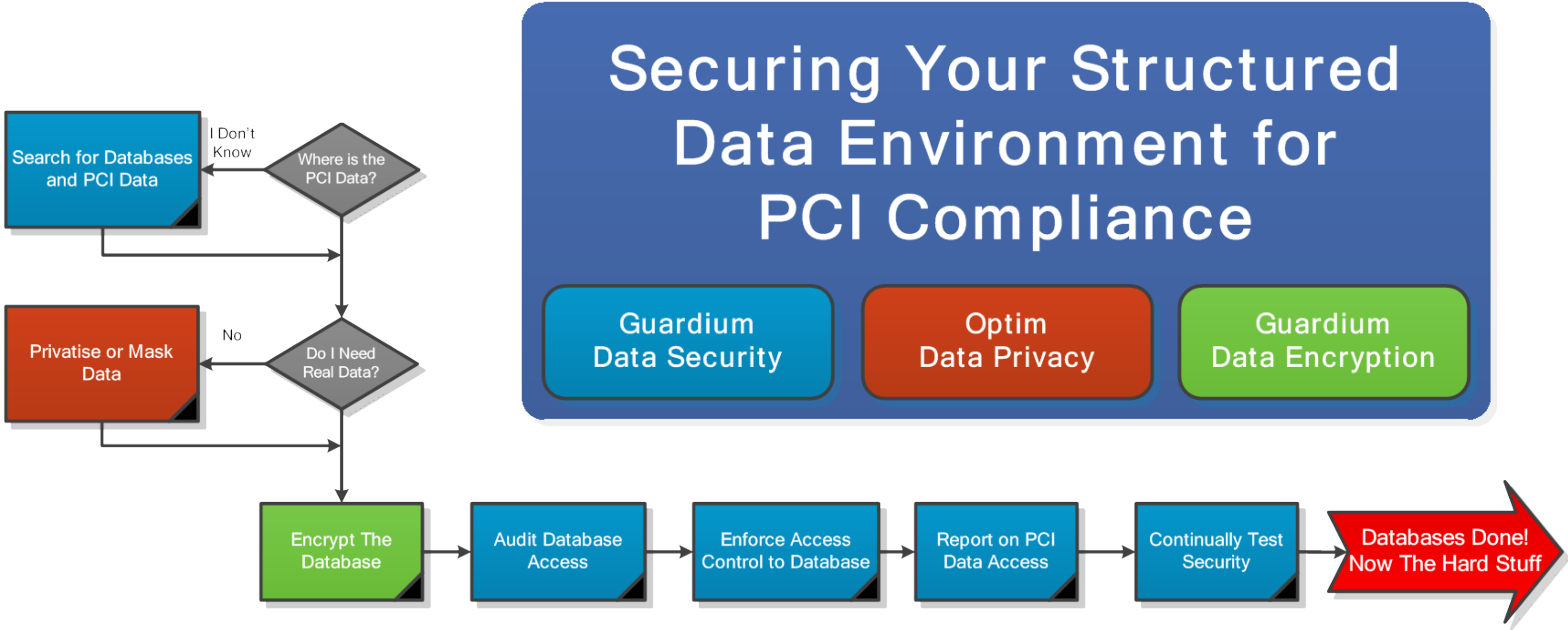
InfoSphere To The Rescue!

- Optim Data Privacy
- Guardium Data Encryption
- Guardium Data Security

"...the most powerful compliance regulations tools that the Test Center has ever seen."

CRN

Jump Start PCI Compliance

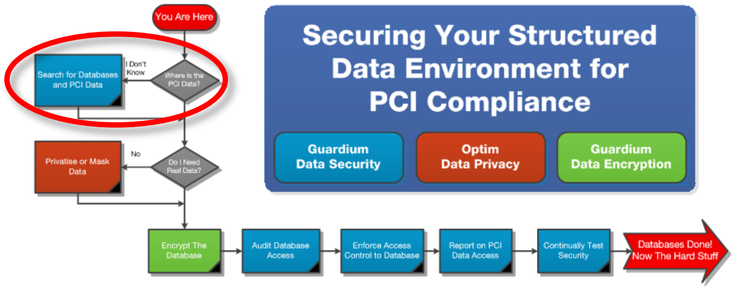


Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff

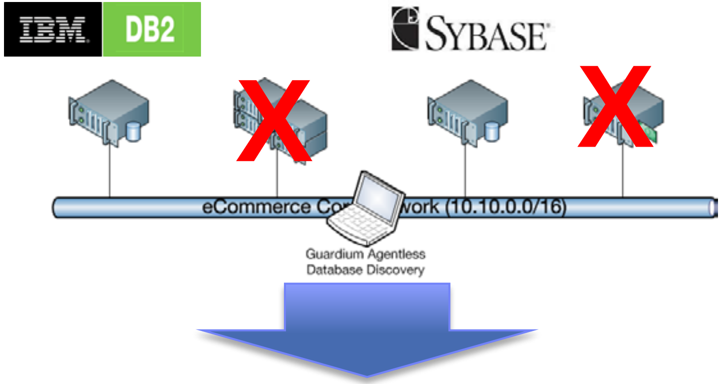
InfoSphere Data Governance

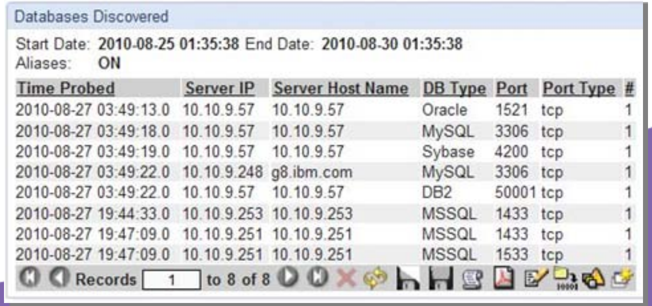
twitter: *Follow* ***@ANZ_IM*** *or mention* ***#IIGS***

Step 1 – Find Your Databases


You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff

- **Guardium Database Finder**
- Simple, Agentless Configuration
- Scan Hosts on the Network
- Identify All Database Servers
  - – IBM DB2 & Informix
  - – Oracle & MySQL
  - – MS SQLServer & Sybase
  - – Netezza & Teradata
  - – …and a host of others…
- Record and Report on all Found


IBM DB2
SYBASE
X
X
eCommerce Co... ...work (10.10.0.0/16)
Guardium Agentless Database Discovery



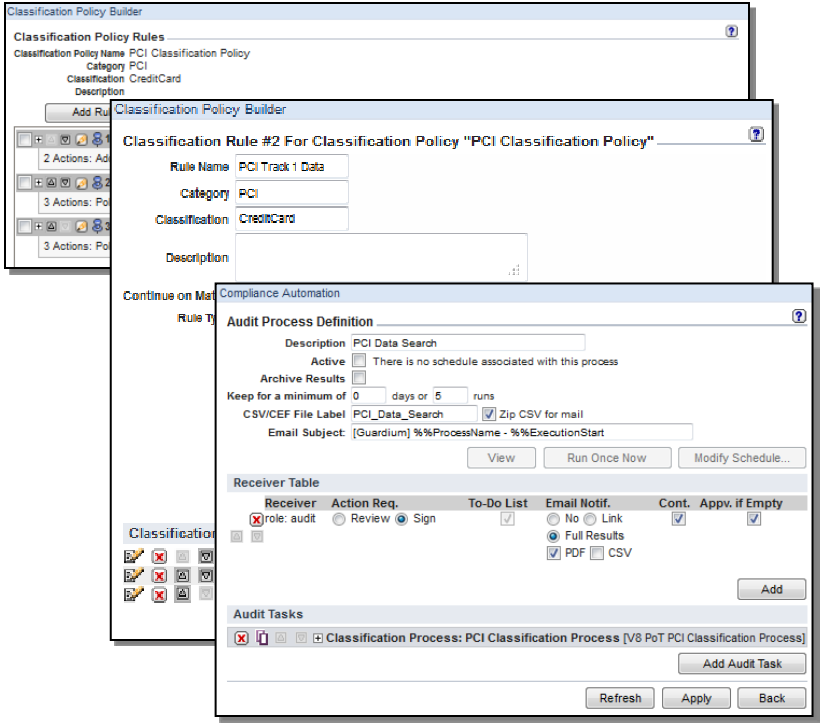
Databases Discovered

Start Date: **2010-08-25 01:35:38** End Date: **2010-08-30 01:35:38**
Aliases: **ON**

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#
2010-08-27 03:49:13.0	10.10.9.57	10.10.9.57	Oracle	1521	tcp	1
2010-08-27 03:49:18.0	10.10.9.57	10.10.9.57	MySQL	3306	tcp	1
2010-08-27 03:49:19.0	10.10.9.57	10.10.9.57	Sybase	4200	tcp	1
2010-08-27 03:49:22.0	10.10.9.248	g8.ibm.com	MySQL	3306	tcp	1
2010-08-27 03:49:22.0	10.10.9.57	10.10.9.57	DB2	50001	tcp	1
2010-08-27 19:44:33.0	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1
2010-08-27 19:47:09.0	10.10.9.251	10.10.9.251	MSSQL	1433	tcp	1
2010-08-27 19:47:09.0	10.10.9.251	10.10.9.251	MSSQL	1533	tcp	1

Result: PCI Candidates Identified

Step 1 – Find Your PCI Data



Classification Policy Builder

Classification Policy Rules

Classification Policy Name PCI Classification Policy
Category PCI
Classification CreditCard
Description

Add Ru

2 Actions: Ad
3 Actions: Po
3 Actions: Po

Classification Policy Builder

Classification Rule #2 For Classification Policy "PCI Classification Policy"

Rule Name: PCI Track 1 Data
Category: PCI
Classification: CreditCard
Description:

Continue on Mat
Rule Ty

Classificatio

Compliance Automation

Audit Process Definition

Description: PCI Data Search
Active ☐ There is no schedule associated with this process
Archive Results ☐
Keep for a minimum of 0 days or 5 runs
CSV/CEF File Label: PCI_Data_Search ☑ Zip CSV for mail
Email Subject: [Guardium] %%ProcessName - %%ExecutionStart

View | Run Once Now | Modify Schedule...

Receiver Table

Receiver	Action Req.	To-Do List	Email Notif.	Cont.	Appv. if Empty
☒ role: audit	○ Review ● Sign	☑	○ No ○ Link ● Full Results ☑ PDF ☐ CSV	☑	☑

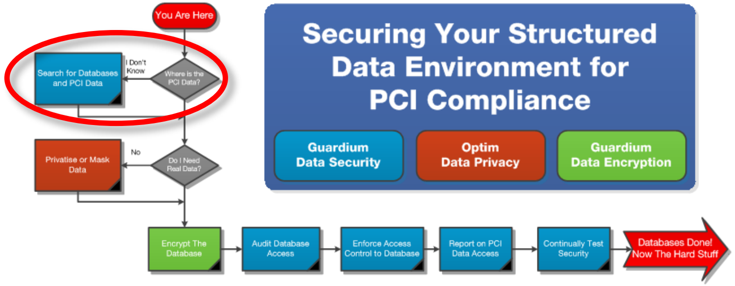
Add

Audit Tasks

☒ ⊞ **Classification Process: PCI Classification Process** [V8 PoT PCI Classification Process]

Add Audit Task

Refresh | Apply | Back



You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff

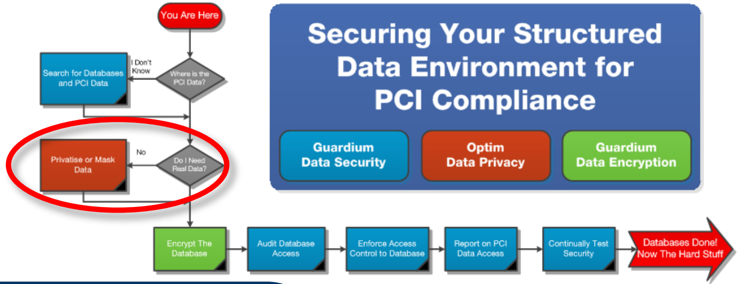
Securing Your Structured Data Environment for PCI Compliance

Guardium Data Security | **Optim Data Privacy** | **Guardium Data Encryption**

- **Guardium Sensitive Data Finder**
- Simple, Agentless Configuration
- Search Databases for PCI Data
  - Object/Column Name
  - Field Content
- Configurable Actions on Find
  - Add Object to Policy Group
  - Flag Policy Violation or Alert
- Production Ready
  - Immediate or Scheduled
  - Low Overhead

Result: PCI Scope Identified

Step 2 – De-Identify What You Can

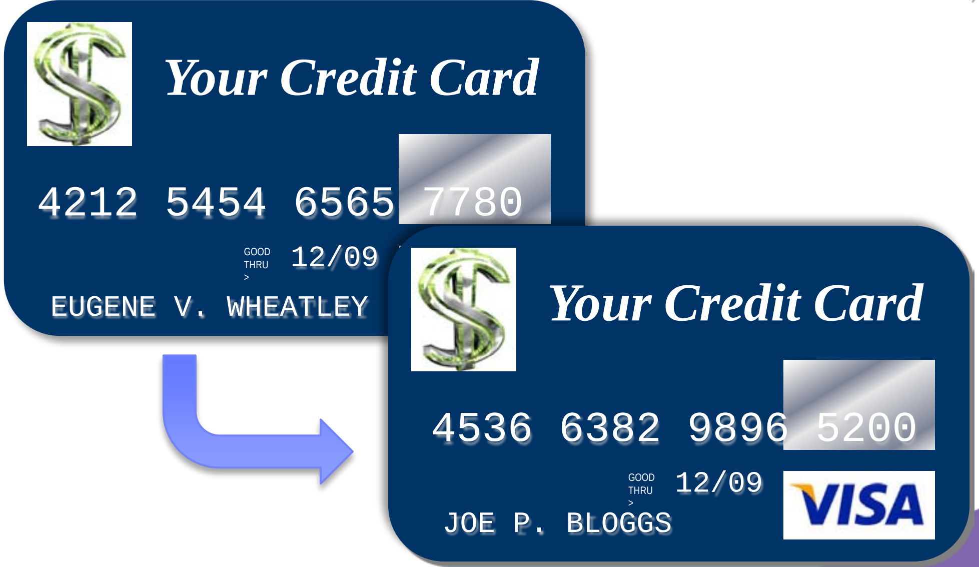

You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff
Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption

- **Optim Data Privacy**

- Intelligent, Referentially Intact Masking
  - Fictional, Valid Credit Card Numbers
  - De-Identify Names & Addresses
  - Random or Algorithm Based
  - Cross Application Referential Integrity

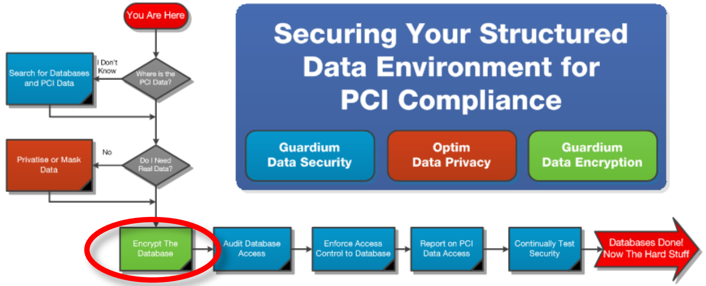
- Fully Integrated with Test Data Management Solutions

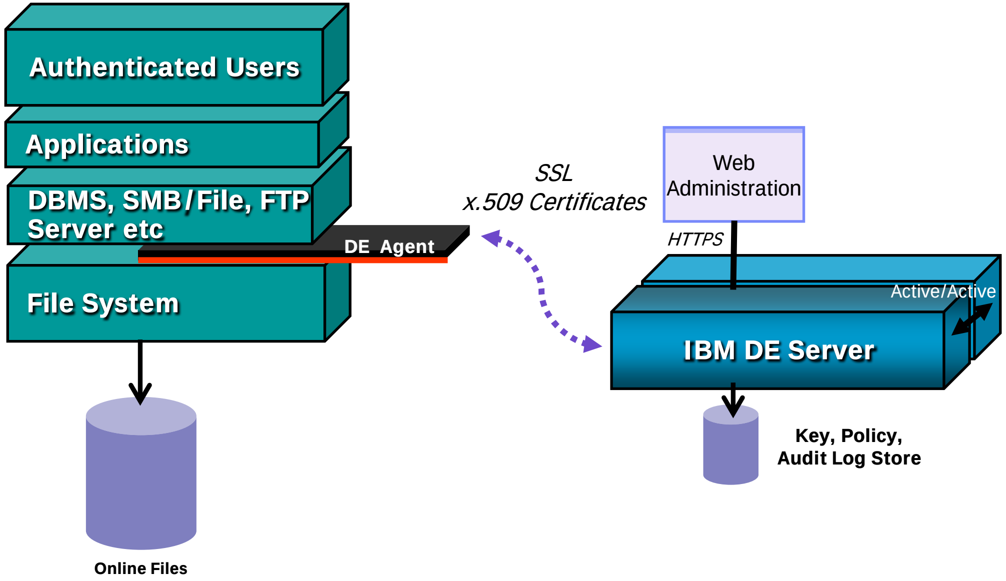
- ***Want More? Be Back Here at 2:30***



Result: PCI Scope Minimised

Step 3 – Encrypt Databases


You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff
Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption

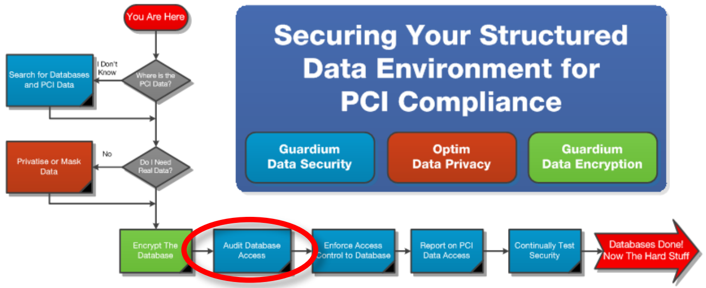


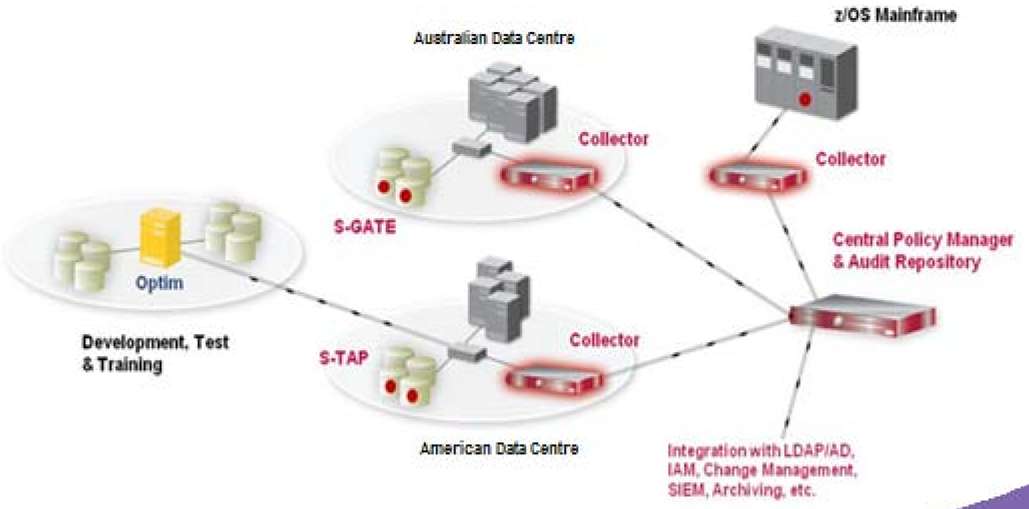
- **Guardium Data Encryption**
- File System Encryption & Auditing
- Totally Transparent
  - No Application Changes
  - No Database Changes
- Cross Platform
  - Mainframe (DB2 & IMS)
  - Unix, Linux
  - Windows
- Strong Key Management

Result: Compliant - PCI Req 3.4, 3.5, 11.5

Step 4 – Audit all Data Access

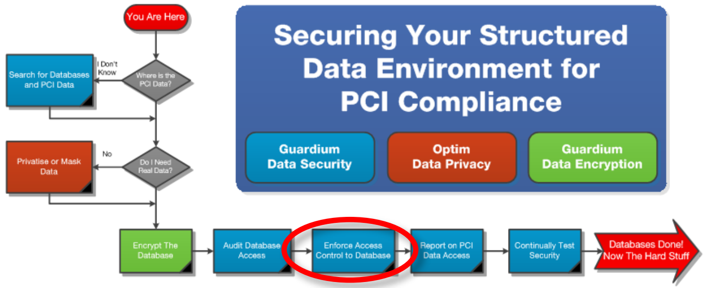
- **Guardium Database Activity Monitoring**
- Cross Platform Database Monitoring
- Out of Box PCI Monitoring Policy
- Configurable Audit Detail Level
- Identify Application User
- Secure, Tamper Proof Audit Trail
- Real Time Anomaly Detection & Alerting
- Complete Audit Retention Control

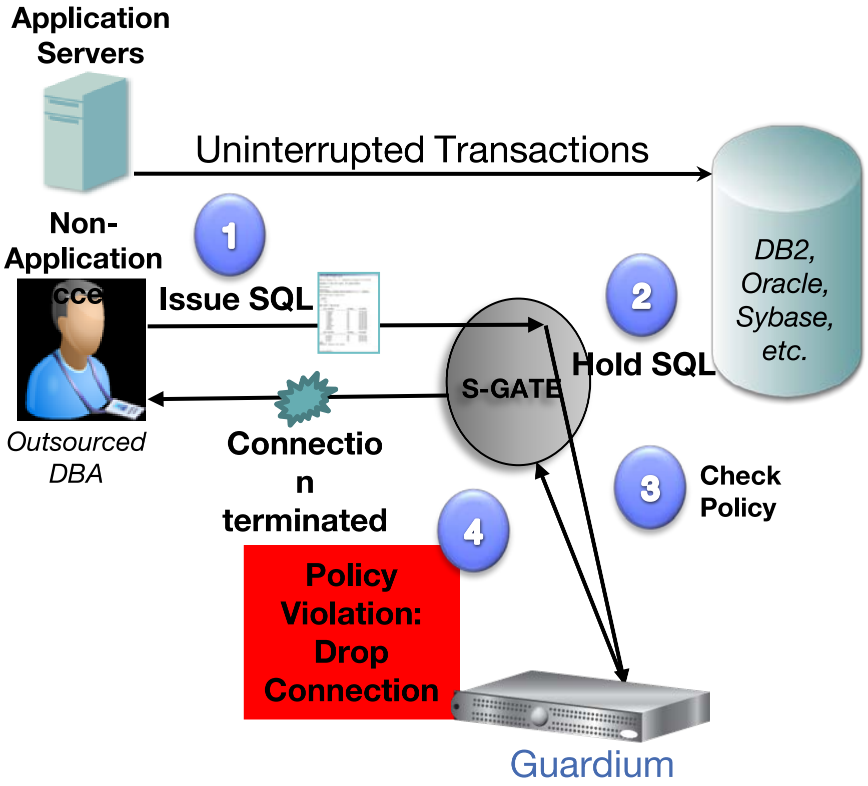

You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff
Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption


z/OS Mainframe
Australian Data Centre
Collector
Collector
S-GATE
Central Policy Manager & Audit Repository
Optim
Development, Test & Training
S-TAP
Collector
American Data Centre
Integration with LDAP/AD, IAM, Change Management, SIEM, Archiving, etc.

Result: Compliant - PCI Req 10

Step 5 – Enforce Access Control to PCI Data

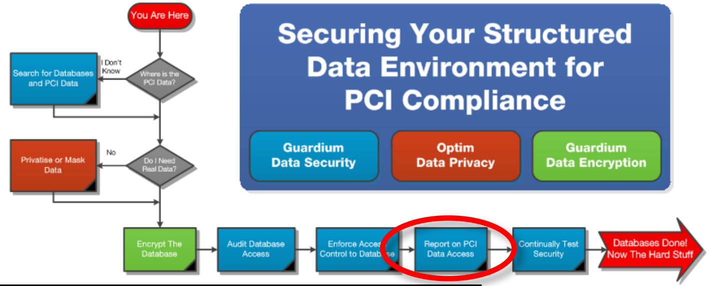

You Are Here
Search for Databases and PCI Data
I Don't Know
Where is the PCI Data?
Privatise or Mask Data
No
Do I Need Real Data?
Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff



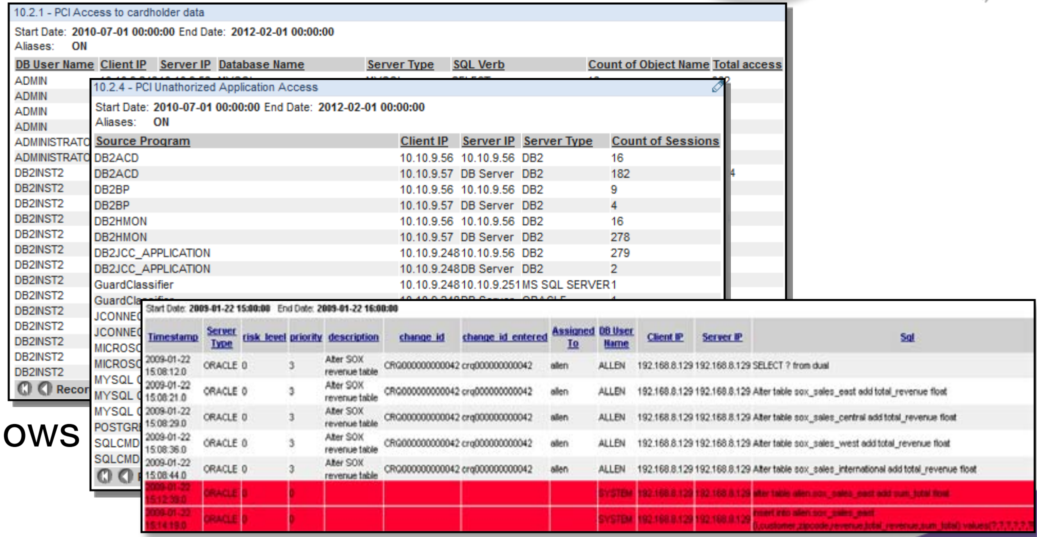
- **Guardium Data Level Access Control**
- No Impact on Application Access
- Control Privileged Credentials
- Network or Local Access
- Fine Grained, Cross Platform Policy
- Alert, Terminate & Quarantine
- Mask Card Numbers in Results
- Enforce Change Control

Result: Compliant
PCI Req 3.3, 6.4, 7.1, 7.2

Step 6 – Report on all PCI Data Access


You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Securing Your Structured Data Environment for PCI Compliance
Guardium Data Security
Optim Data Privacy
Guardium Data Encryption
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff

- **Guardium Database Activity Monitoring**
- Out Of Box 300+ Reports
- Includes PCI Compliance Reports
- Fully Configurable Report Creation
- Enrich Reports with External Data
  - Change Control Reconciliation
- Automated & Audited Compliance Workflows
  - Report Creation & Distribution
  - Review, Escalation & Signoff Management
  - Custom Workflow Processes



10.2.1 - PCI Access to cardholder data

Start Date: **2010-07-01 00:00:00** End Date: **2012-02-01 00:00:00**
Aliases: **ON**

DB User Name	Client IP	Server IP	Database Name	Server Type	SQL Verb	Count of Object Name	Total access
ADMIN							
ADMIN							
ADMIN							
ADMIN							
ADMINISTRATO							
ADMINISTRATO							
DB2INST2							
DB2INST2							4
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							
DB2INST2							

Recor

10.2.4 - PCI Unathorized Application Access

Start Date: **2010-07-01 00:00:00** End Date: **2012-02-01 00:00:00**
Aliases: **ON**

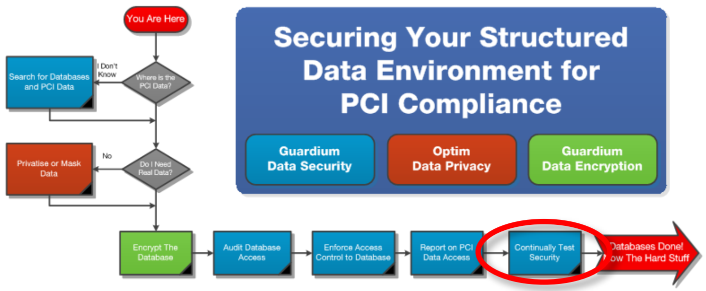
Source Program	Client IP	Server IP	Server Type	Count of Sessions
DB2ACD	10.10.9.56	10.10.9.56	DB2	16
DB2ACD	10.10.9.57	DB Server	DB2	182
DB2BP	10.10.9.56	10.10.9.56	DB2	9
DB2BP	10.10.9.57	DB Server	DB2	4
DB2HMON	10.10.9.56	10.10.9.56	DB2	16
DB2HMON	10.10.9.57	DB Server	DB2	278
DB2JCC_APPLICATION	10.10.9.248	10.10.9.56	DB2	279
DB2JCC_APPLICATION	10.10.9.248	DB Server	DB2	2
GuardClassifier	10.10.9.248	10.10.9.251	MS SQL SERVER	1
GuardCla				
JCONNEC				
JCONNEC				
MICROSO				
MICROSO				
MYSQL C				
MYSQL C				
MYSQL C				
POSTGRE				
SQLCMD				
SQLCMD				

Start Date: **2009-01-22 15:00:00** End Date: **2009-01-22 16:00:00**

Timestamp	Server Type	risk_level	priority	description	change_id	change_id_entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:08:12.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	SELECT ? from dual
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (),customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?

Result: Compliant - PCI Req 10

Step 7 – Continually Test Security

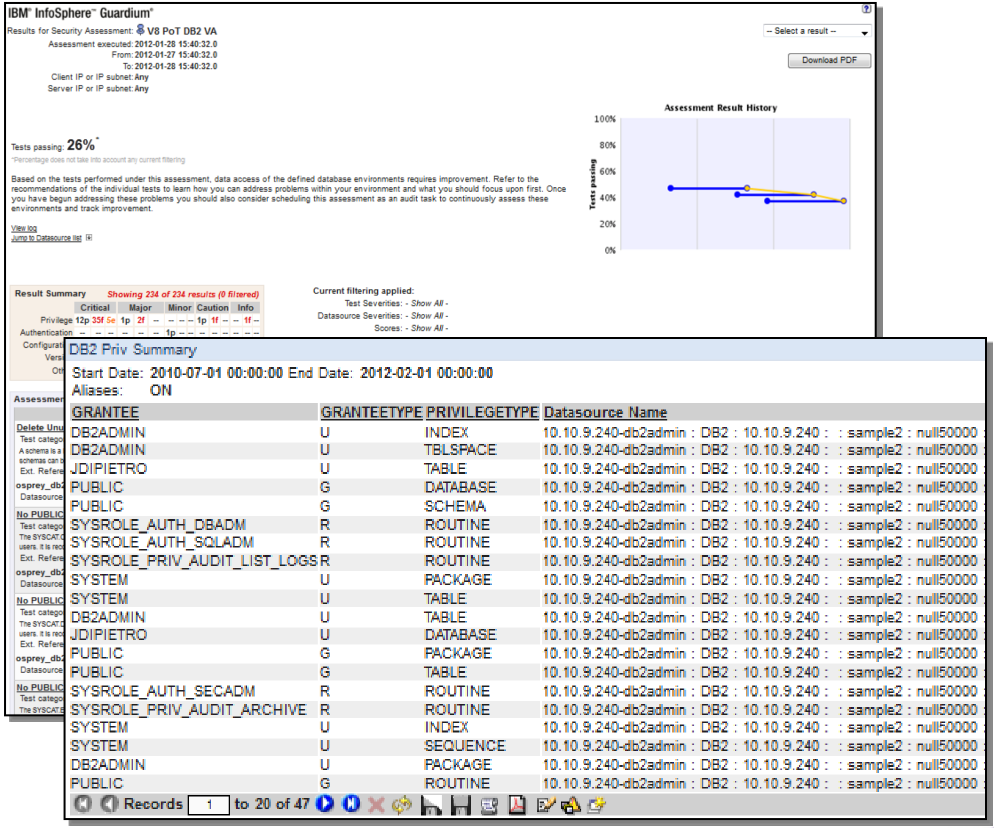

You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff

Securing Your Structured Data Environment for PCI Compliance

Guardium Data Security

Optim Data Privacy

Guardium Data Encryption



IBM® InfoSphere™ Guardium®

Results for Security Assessment: V8 PoT DB2 VA

Assessment executed: 2012-01-28 15:40:32.0
From: 2012-01-27 15:40:32.0
To: 2012-01-28 15:40:32.0
Client IP or IP subnet: Any
Server IP or IP subnet: Any

Tests passing: 26%*

*Percentage does not take into account any current filtering

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 234 of 234 results (0 filtered)*

	Critical			Major			Minor			Caution			Info		
Privilege	12p	35f	5e	1p	2f	--	--	--	--	1p	1f	--	--	1f	--
Authentication	--	--	--	--	--	--	1p	--	--	--	--	--	--	--	--
Configurati															
Versi															
Oth															

Current filtering applied:
Test Severities: - *Show All* -
Datasource Severities: - *Show All* -
Scores: - *Show All* -

Assessmen

Delete Unu
Test catego
A schema is a
schemas can b
Ext. Refere
osprey_db2
Datasource

No PUBLIC
Test catego
The SYSCAT.C
users. It is rec
Ext. Refere
osprey_db2
Datasource

No PUBLIC
Test catego
The SYSCAT.D
users. It is rec
Ext. Refere
osprey_db2
Datasource

No PUBLIC
Test catego
The SYSCAT.E

DB2 Priv Summary

Start Date: 2010-07-01 00:00:00 End Date: 2012-02-01 00:00:00
Aliases: ON

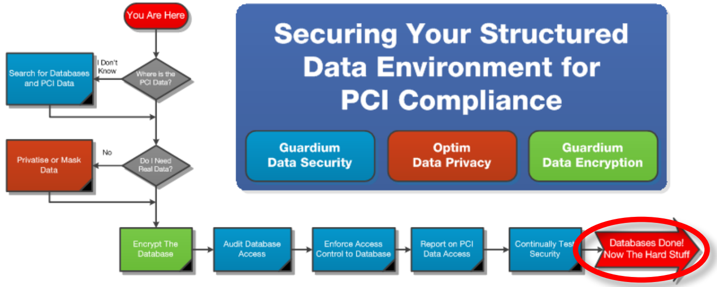
GRANTEE	GRANTEETYPE	PRIVILEGETYPE	Datasource Name
DB2ADMIN	U	INDEX	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
DB2ADMIN	U	TBLSPACE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
JDIPIETRO	U	TABLE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
PUBLIC	G	DATABASE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
PUBLIC	G	SCHEMA	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSROLE_AUTH_DBADM	R	ROUTINE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSROLE_AUTH_SQLADM	R	ROUTINE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSROLE_PRIV_AUDIT_LIST_LOGS	R	ROUTINE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSTEM	U	PACKAGE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSTEM	U	TABLE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
DB2ADMIN	U	TABLE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
JDIPIETRO	U	DATABASE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
PUBLIC	G	PACKAGE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
PUBLIC	G	TABLE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSROLE_AUTH_SECADM	R	ROUTINE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSROLE_PRIV_AUDIT_ARCHIVE	R	ROUTINE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSTEM	U	INDEX	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
SYSTEM	U	SEQUENCE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
DB2ADMIN	U	PACKAGE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000
PUBLIC	G	ROUTINE	10.10.9.240-db2admin : DB2 : 10.10.9.240 : : sample2 : null50000

Records 1 to 20 of 47

- **Guardium Vulnerability Assessment**
- Automated Security Testing of Databases
- Database Patch Levels
- Known Vulnerabilities – XForce, CIS & STIG
- Prioritised Identification & Remediation
- Entitlement Reporting
  - Who Has What Privilege?

Result: Compliant - PCI Req 6.1, 6.2, 6.3, 6.6, 11.2

…And The Rest…



Securing Your Structured Data Environment for PCI Compliance

Guardium Data Security

Optim Data Privacy

Guardium Data Encryption

You Are Here
Where is the PCI Data?
I Don't Know
Search for Databases and PCI Data
Do I Need Real Data?
No
Privatise or Mask Data
Encrypt The Database
Audit Database Access
Enforce Access Control to Database
Report on PCI Data Access
Continually Test Security
Databases Done! Now The Hard Stuff

- Requirement 1 – Use Network Firewalls
- Requirement 4 – Encrypt Network Transactions
- Requirement 5 – Anti Virus
- Requirement 8 – Uniquely Identify Users
- Requirement 9 – Restrict Physical Access
- Requirement 12 – Implement Security Policy

IBM® Security

Security Intelligence.
Think Integrated.

Case Study : PCI 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."*

Introducing McAfee Online Backup

Easily and safely protect all of your digital files and memories

Questions

twitter: *Follow* ***@ANZ_IM*** *or mention* ***#IIGS***

IBM Data Security & Compliance Globally Used By…

- 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
- 2 of the top 3 Global retailers
- 3 of the world’s favorite beverage brands
- The World #1 Global Credit Card Brand
- The Worlds Best Recognised Supplier of PCs
- The World #1 Dedicated Security Company