



# Central Pennsylvania User Group Protecting Big Data

Howie Hirsch –  
Senior IT Specialist  
IBM Corporation  
Valley Forge, PA June 9, 2015



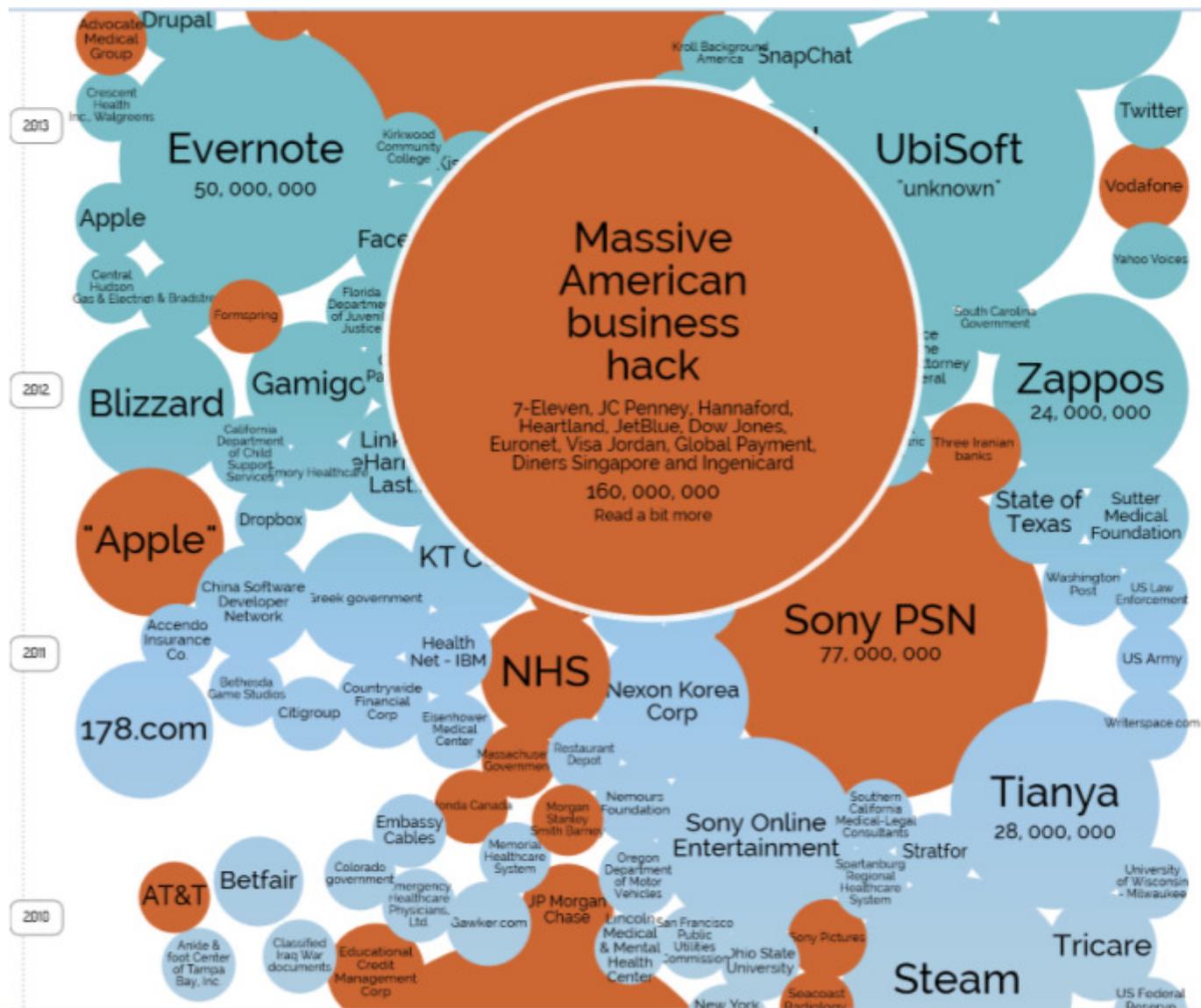
# Agenda

- **Big Data opportunities and threats**
- **Proactive and preventative information protection**
- **Summary and Call to Action**



# The who's who of the world's biggest data breaches....

<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/#>



## Why is it happening?

**Cloud**



private	public	SaaS
---------	--------	------

Data is...

- ✓ Leaving the Data Center
- ✓ Stored on shared drives
- ✓ Hosted by 3<sup>rd</sup> party
- ✓ Managed by 3<sup>rd</sup> party

**Consumerization of IT**

**Mobile**



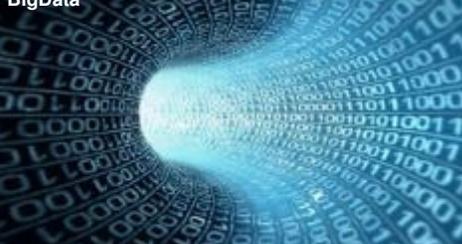
BYOD	Apps	Social
------	------	--------

Data is...

- ✓ Generated 24x7
- ✓ Used Everywhere
- ✓ Always Accessible
- ✓ On private devices

**Everything is Everywhere**

**BigData**



Hadoop	No-SQL	Files
--------	--------	-------

Data is...

- ✓ Produced in high volumes
- ✓ Stored unstructured
- ✓ Analyzed faster/cheaper
- ✓ Monetized

**Data Explosion**

- ✓ There is more data
- ✓ Data is leaving the data center
- ✓ Data is consumed everywhere
- ✓ Data is worth more than ever before

## Data Security is frequently in the news



President Obama declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation.”



Former NSA director tells the Financial Times that a cyber attack could cripple the nation's banking system, power grid, and other essential infrastructure.



U.S. Defense Secretary Chuck Hagel said that intelligence leaks by National Security Agency (NSA) contractor Edward Snowden were a serious breach that damaged national security



Hackers had broken into its in-store payments systems, in what could be the largest known breach of a retail company's computer network. Estimated 60 million credit card details stolen.



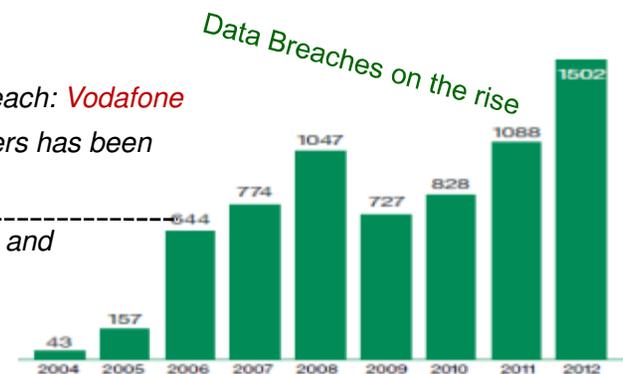
Hackers orchestrated multiple breaches of **Sony's** PlayStation Network knocking it offline for 24 days and costing the company an estimated \$171 million, and significantly damaged brand reputation



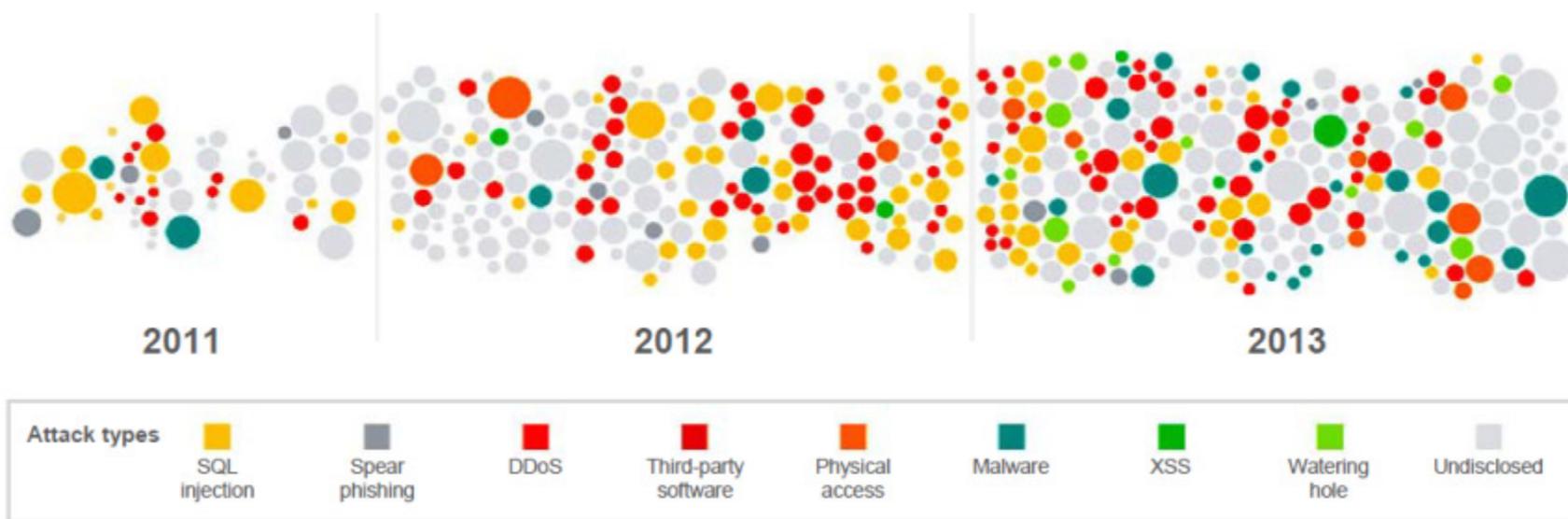
One of the world's largest corporations has been hit with a widespread data breach: **Vodafone Germany**, personal information on more than two million mobile phone customers has been stolen, extracted from an internal databases by an insider



In an act of industrial espionage, the Chinese government launched a massive and unprecedented attack on Google, Yahoo, and dozens of other Silicon Valley companies.... Google admitted that some of its intellectual property had been stolen



## Data breaches are on the rise...



Source: [IBM X-Force Threat Intelligence Quarterly – 1Q 2014](#)

Note: Size of circle estimates relative impact of incident in terms of cost to business.

Table 10. Compromised assets by percent of breaches and percent of records\*

Type	Category	All Orgs		Larger Orgs	
Database server	Servers	6%	96%	33%	98%

*2012 Data Breach Report from Verizon Business RISK Team*

[http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xq.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xq.pdf)

# Data Governance and Security are changing rapidly

Data Explosion

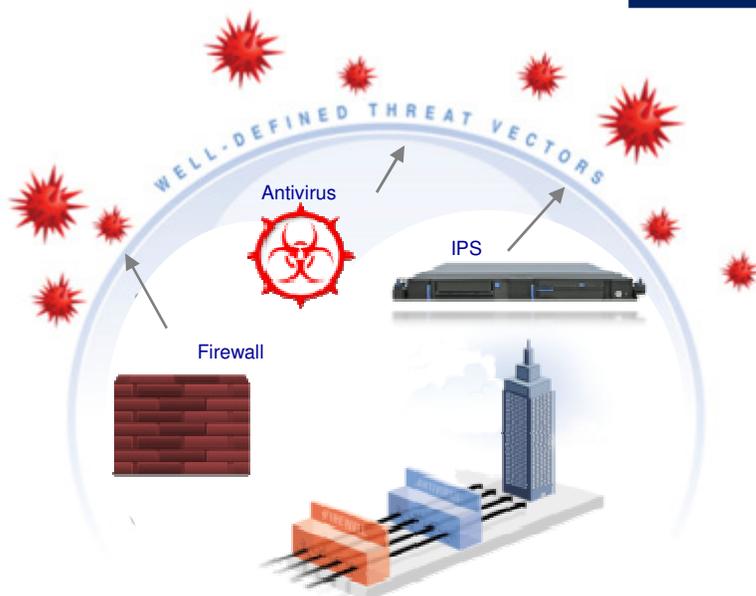
Consumerization of IT

Everything is Everywhere

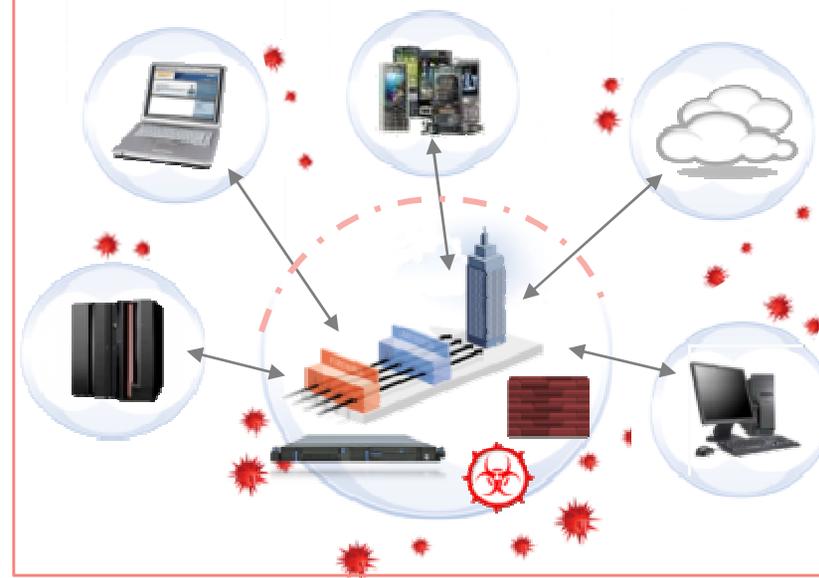
Attack Sophistication

Extending the perimeter; focus shifts to protecting the DATA

*Moving from traditional perimeter-based security...*



*...to logical "perimeter" approach to security—focusing on the data and where it resides*

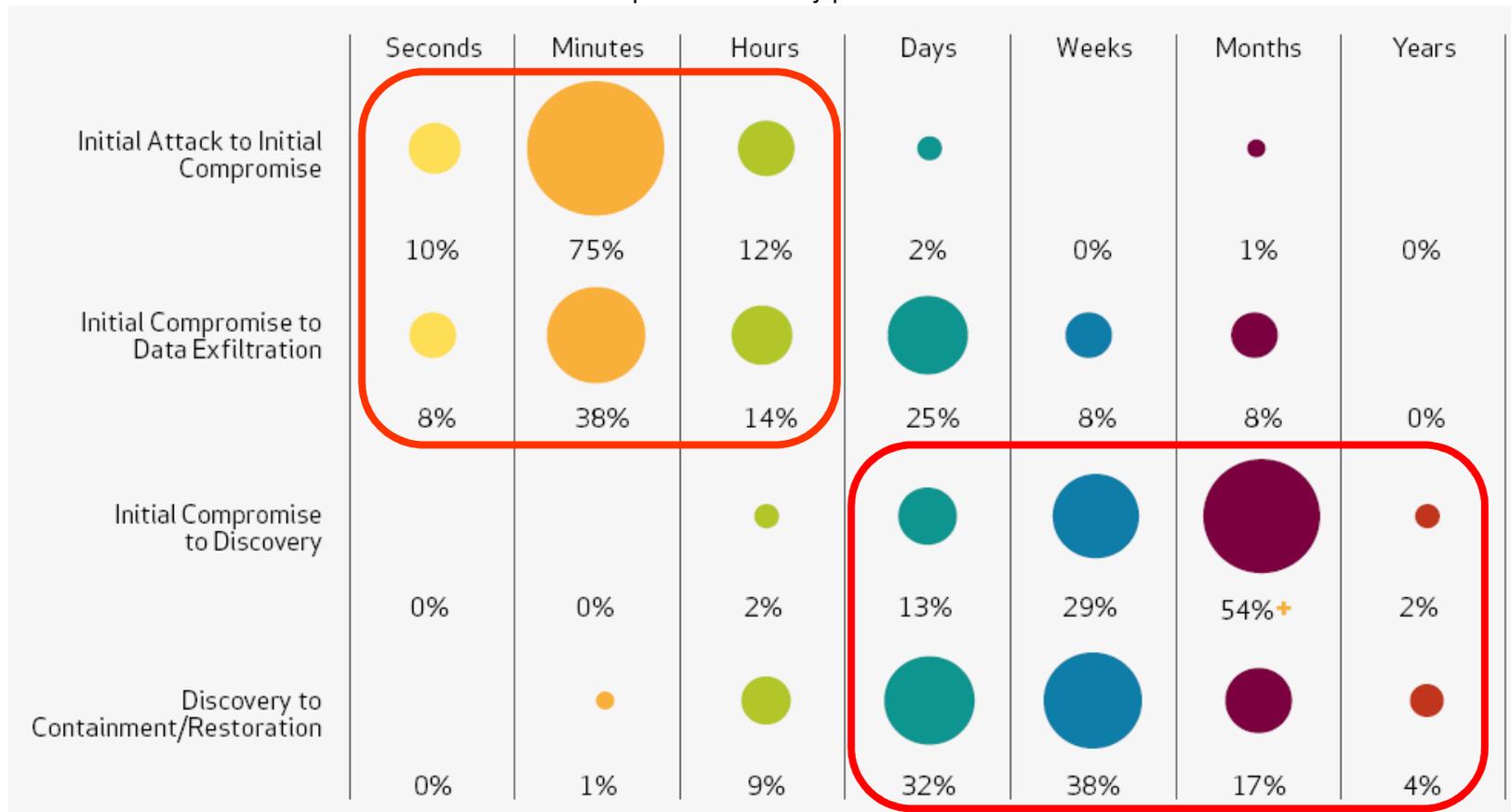


- Cloud, Mobile and Data momentum is breaking down the traditional perimeter and forcing us to look at security differently
- Focus needs to shift from the perimeter to the data that needs to be protected

## Real time monitoring and alerting is key

- Attacks occur in minutes yet not discovered for months without real-time monitoring
- Customers will say they have their own solution – but they never monitor in real time
- They can't act as fast as the bad guys with home grown solutions.

Time span of events by percent of breaches



# z Systems and Big Data

## A significant data source for today's business critical analytics

- **Data that originates and/or resides on zEnterprise**
  - 2/3 of business transactions for U.S. retail banks
  - 80% of world's corporate data
- **Businesses that run on zEnterprise**
  - 66 of the top 66 worldwide banks
  - 24 of the top 25 U.S. retailers
  - 10 of the top 10 global life/health insurance providers
- **The downtime of an application running on zEnterprise = approx 5 minutes per yr**
- **1,300+ ISVs run zEnterprise today**
  - More than 275 of these selling over 800 applications on Linux



“Breaches in data security have been increasing steadily over the last few years... These kind of incidents can seriously damage brand image and customer confidence... and impact share price and bottom line performance” — *Information Governance: Audit and Protection on the IBM System z platform (A report paid for by IBM in December 2011 by Mike Ferguson, independent analyst)*

## The potential costs of doing nothing

**\$5.5M<sup>(1)</sup>**  
**USD**  
 average cost  
 of a data breach

**\$194<sup>(1)</sup>**  
**USD**  
 Average cost per  
 Compromised  
 record

**28,349<sup>(1)</sup>**  
 average number of  
 breached records  
 per incident

**96%<sup>(2)</sup>**  
 of records  
 compromised  
 involving database  
 servers

## Using home grown approaches can be risky



**Manual approaches can**  
 leave you open to higher risk  
 and inefficiencies



**New sources of threats:**  
 outsourcing, webfacing  
 applications, mobile access,  
 stolen credentials and insiders



Requirements for privacy and  
 security by role can add  
**complexity**

(1) 2011 Cost of Data Breach Study United States Benchmark Research Conducted by Ponemon Institute LLC Report: March 2012, Sponsored by Symantec.

(2) "2012 Data Breach Investigations Report. A study conducted by the Verizon RISK Team with cooperation from the United States Secret Service, the Dutch National High Tech Crime Unit, the Australian Federal Police, the Irish Reporting & Information Security Service and the Police Central e-Crime Unit of the London Metropolitan Police."

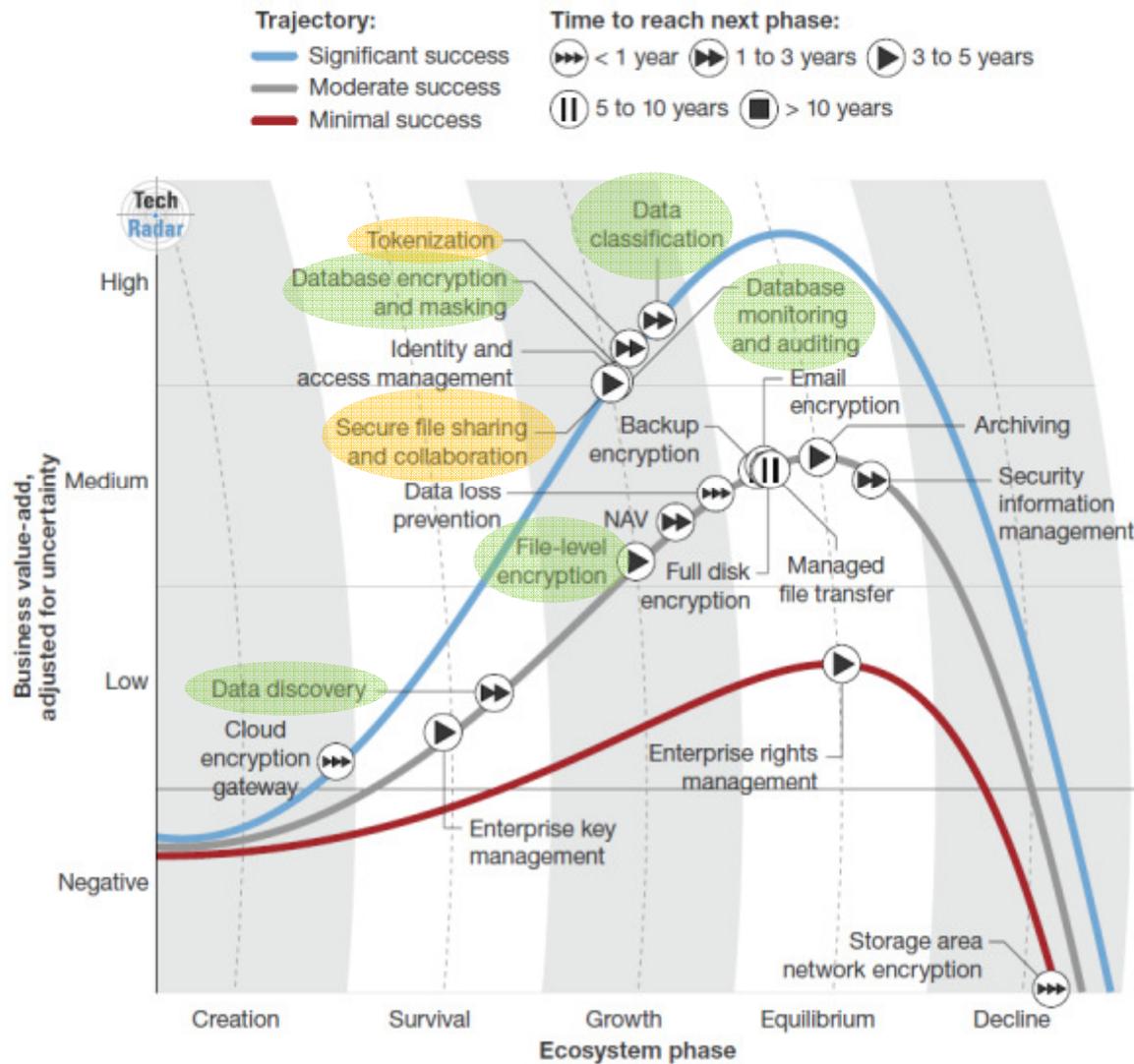
## IBM InfoSphere Information Governance solutions.



# Agenda

- **Big Data opportunities and threats**
- **Proactive and preventative information protection**
- **Summary and Call to Action**

# Focus moving to Data Centric Security



**FORRESTER**

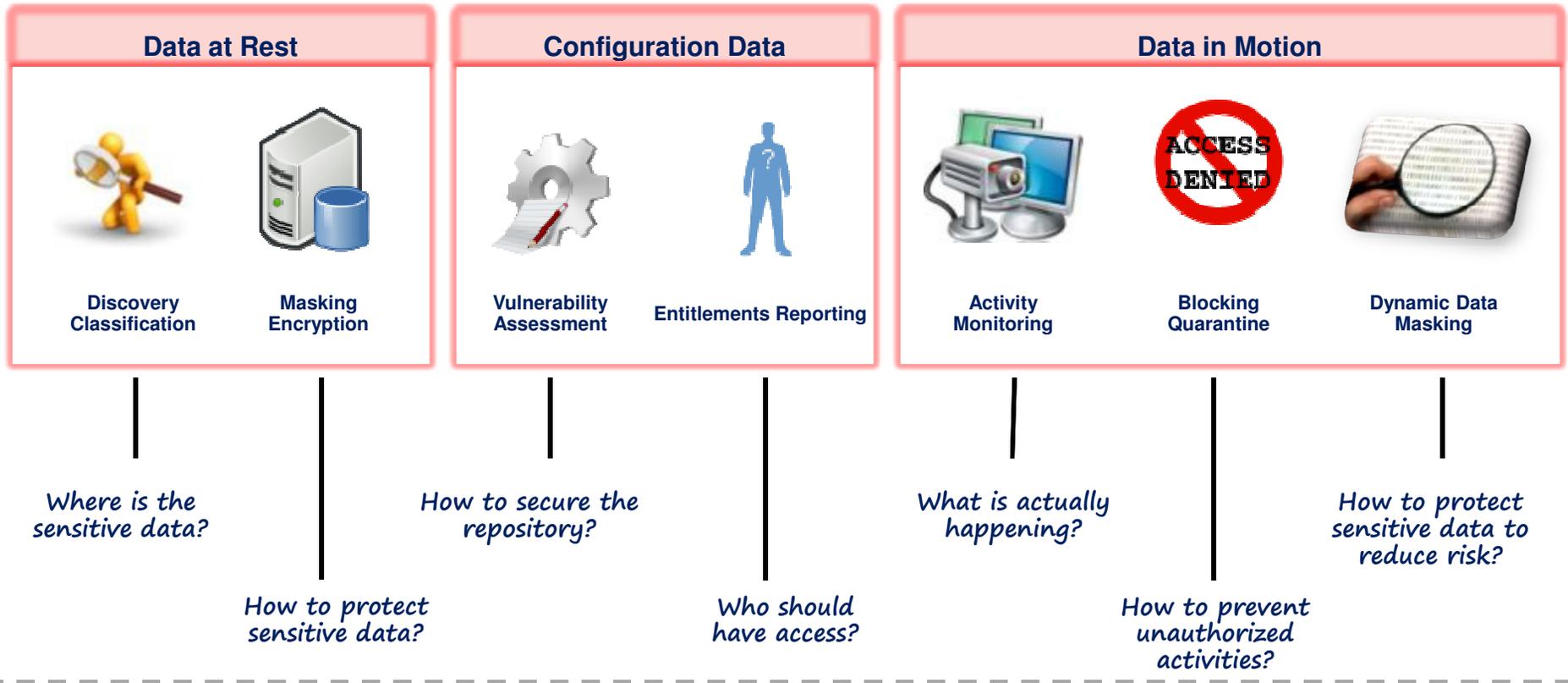
*"The shift to data-centric security is finally happening"*

TechRadar™: Data Security, Q2 2014  
by Stephanie Balaouras, John Kindervag, and Heidi Shey, April 22, 2014

Market leader

Within a year

# How we do it?



Security Policies

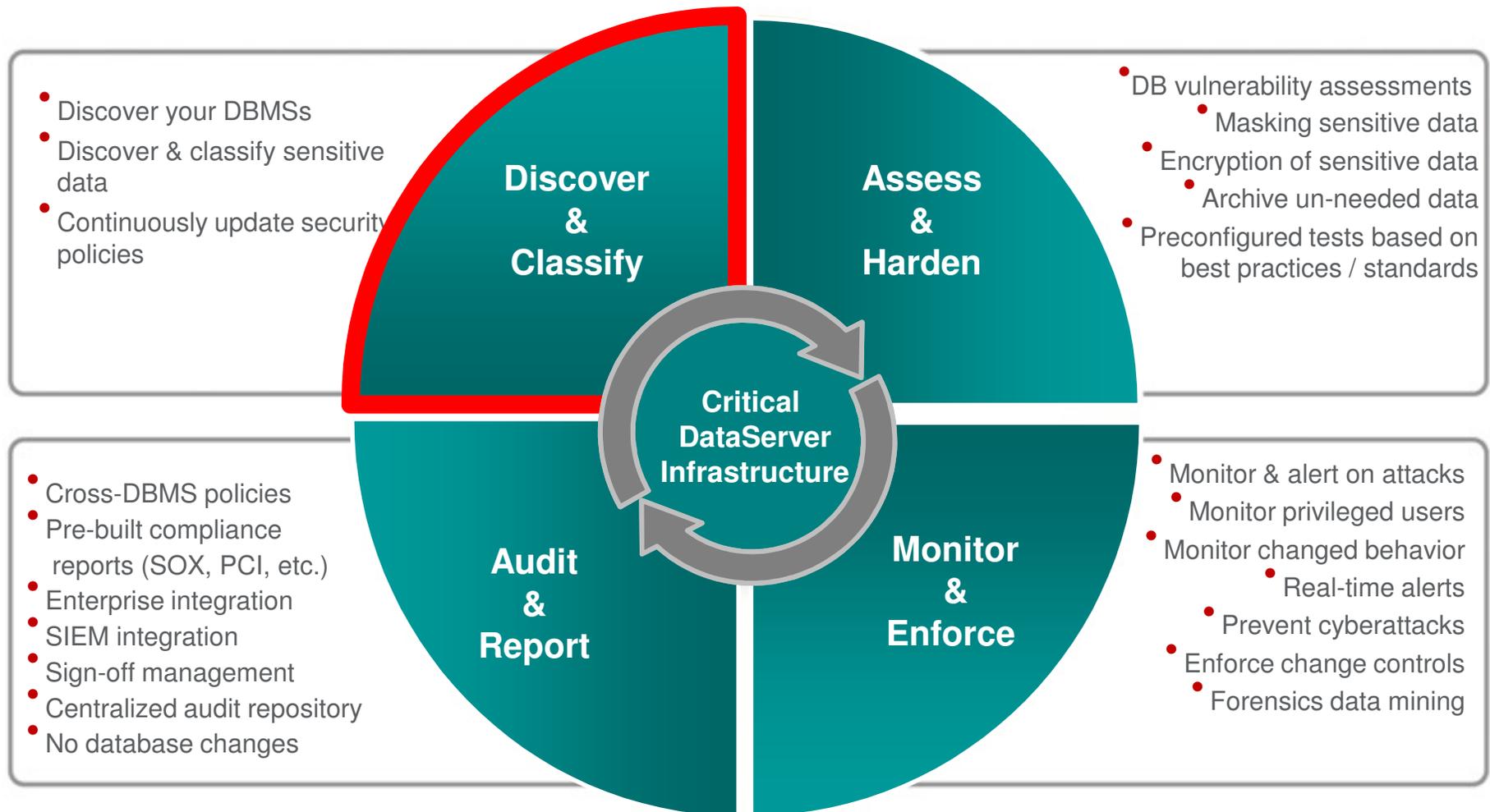
Dormant Data

Security Alerts / Enforcement

Dormant Entitlements

Compliance Reporting

# Address the Full Data Protection Lifecycle



## Find your Data Servers

- Scan the network to develop an inventory of databases
- Schedule regular scans to discover new instances
- Policy-based actions
  - Alerts
  - Add to group for monitoring

Administration Console   Access Management   Tools   Daily Monitor   SQL Guard Monitor   Tap Monitor   Incidents							
SQL Count							
Session Count							
Logged Threshold Alerts							
Logged R/T Alerts							
Exception Count							
Dropped Requests							
TCP Exceptions							
Admin User Logins							
Databases by Type							
<b>Databases Discovered</b>							
Retrospective Report Requests							
Values Changed							
Throughput							
<b>Databases Discovered</b>							
Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49							
<u>Time Probed</u>	<u>Server IP</u>	<u>Server Host Name</u>	<u>DB Type</u>	<u>Port</u>	<u>Port Type</u>	<u>#</u>	
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp	1	
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1	
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp	1	
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp	1	
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1	
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp	1	

# Sensitive Data Discovery

**The Problem:** Finding Sensitive Data can be difficult:

- Sensitive data can't be found just by a simple data scan.
- “Corporate memory” is poor
- Hundreds of tables and millions of rows:
- Data quality problems make discovery more difficult

## The Solution:

- Common PII data element discovery
  - Pre-Defined Scanning
- Custom sensitive data discovery
  - Supply Discovery with “descriptions/examples”
  - Discovery will scan for matching columns
- Hidden sensitive data discovery
  - Sensitive data embedded in free text columns
    - Scan by “floating” patterns
  - Sensitive data that is partial or hidden

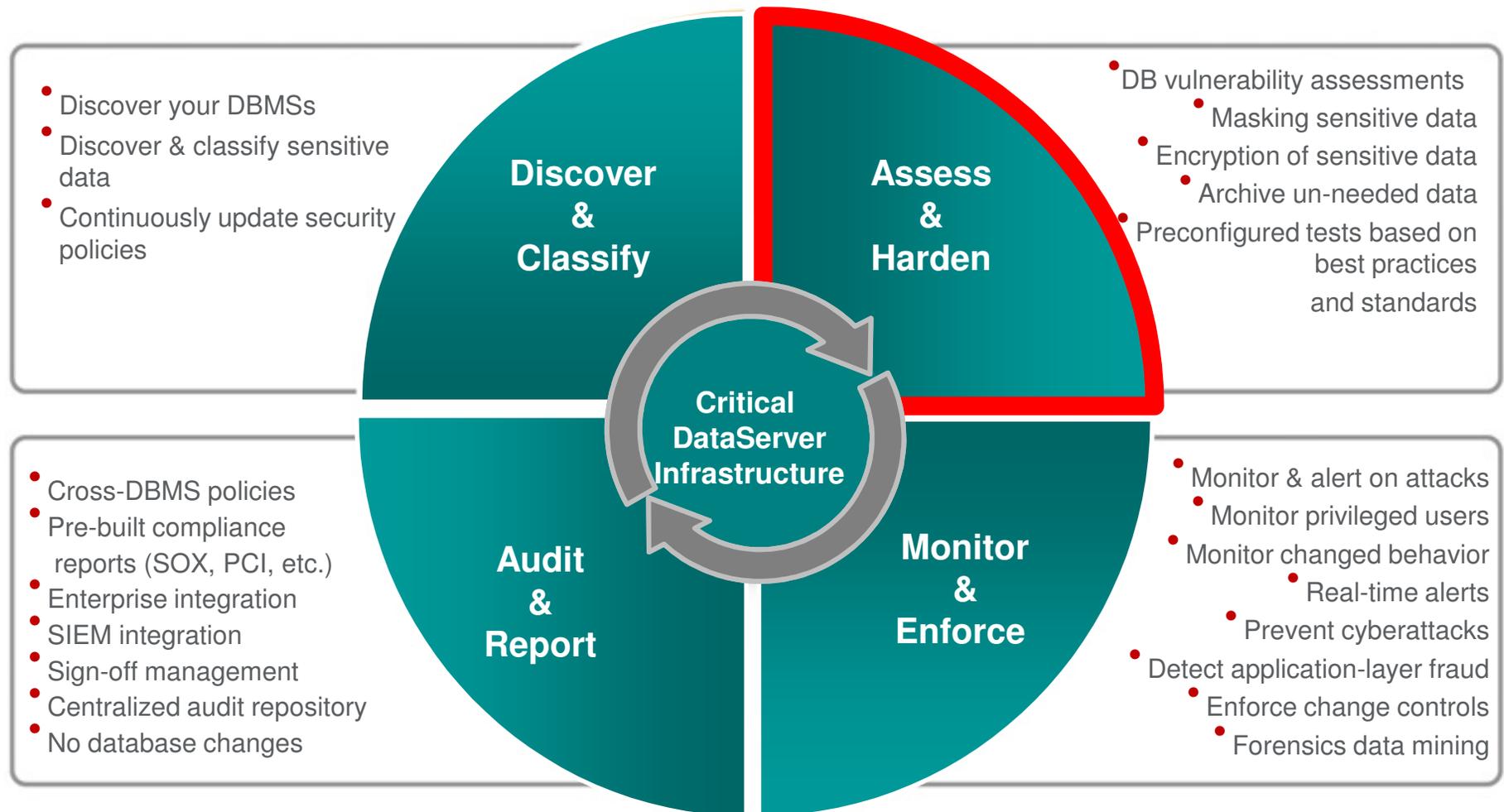
## Sensitive Relationship Discovery

System A Table 1		System A Table 15		
Number	Name	Patient	Result	Test
3544600986	AlexFulltheim	3802468	N	53
5728150928	BarneySolo	4182715	N	53
3786736304	BillAlexander	4600986	N	32
6783802468	BobSmith	5061085	N	53
4035567193	EileenKratchman	5567193	N	72
8037409934	FredSimpson	6123913	Y	47
4306123913	George Brett	6736304	N	34
9525061085	JamieSlattery	7409934	N	34
4594182715	JimJohnson	8150928	N	47
1288966020	MartinAston	8966020	N	34

System Z Table 25	
Test	Name
53	Streptococcus pyogenes
72	Pregnancy
32	Alzheimer Disease
47	Hemorrhoids
34	Dermatamycoses

# Address the Full Data Protection Lifecycle



## Vulnerability Assessment

Based on best practices

- Cost effectively improve the security of data servers by conducting automated database vulnerability assessment tests
  - Packaged tests to detect vulnerabilities including inappropriate privileges, grants, default accounts and passwords, security exposures, patches, etc.
  - Capabilities enabling the development of custom tests
- Based on industry standards such as STIG and CIS
- Management of VA testing from central InfoSphere Guardium console for enterprise-wide control
- Integrated with other InfoSphere Guardium elements for improved process efficiency, including Compliance Workflow Automation and audit repository
- Based on DISA STIG and CIS security standards
  - Server defaults
  - Patch levels
  - OS and DBMS Vulnerability Assessment

# Identify Unpatched and Misconfigured Systems

Current Test Results

**IBM InfoSphere® Guardium®**  
 Results for Security Assessment: **SQL Server Assessment**  
 Assessment executed: 2010-08-27 13:20:06.0  
 From: 2010-08-07 13:20:06.0  
 To: 2010-08-27 13:20:06.0  
 Client IP or IP subnet: Any  
 Sensor IP or IP subnet: Any

- Select a result -  
Download PDF

Tests passing **57%**  
\*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practices. Refer to the recommendations of the individual tests to learn how you can achieve best-practice status. You should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View logs](#)  
[Jump to Data source host](#)

**Assessment Result History**

**Result Summary** Showing 95 of 95 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	1p	2f	15p	8f	--
Authentication	--	2f	3p	1f	--
Configuration	1p	--	13p	14f	14e
Version	--	--	1p	1f	--
Other	1p	--	4p	2f	1e

Current filtering applied:

- Test Severities: - Show All -
- Data source Severities: - Show All -
- Scores: - Show All -
- Types: - Show All -

[Reset Filtering](#)  [Filter / Sort Controls](#)

**Assessment Test Results**  Compare with other results Showing 95 of 95 results (0 filtered)

Test / Data source	Result
<b>No Individual User Access To syscomments And sp_helptext</b>	<b>Fail</b> Code visibility vulnerability found
<b>No Select Privileges On System Tables/Views in Application Databases</b>	<b>Fail</b> Some application databases have SELECT privileges granted to system tables.

Result History

Prioritized Breakdown

Filters and Sort Controls

Detailed Test Results

Detailed Remediation Suggestions

## Eliminate inappropriate privileges

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Priv.	<a href="#">Access To The UTL_FILE Package is restricted</a>	ORACLE: Oracle EE - Joe	Fail	Major	Found Exec UTL_FILE privilege granted to public  <i>Recommendation: Permissions to execute the UTL_FILE package have been granted to users other than DBAs. UTL_FILE allows users to access operating system files from Oracle, which may result in a security breach.</i>
Conf.	<a href="#">LOG_ARCHIVE_DUPLEX_DEST Set</a>	ORACLE: Oracle EE - Joe	Fail	Major	Parameter: 'LOG_ARCHIVE_DUPLEX_DEST' is not set.  <i>Recommendation: LOG_ARCHIVE_DUPLEX_DEST is not set. We recommend to set this parameter to a valid directory owned by Oracle set with owner and group read/write permissions only.</i>
Conf.	<a href="#">MAX_ENABLED_ROLES is not greater than 30</a>	ORACLE: Oracle EE - Joe	Fail	Major	Parameter: 'MAX_ENABLED_ROLES' with a value of '150' has been obsoleted for version 10.2.  <i>Recommendation: Max_enabled_roles is set to a value higher than 30. This parameter should be limited as much as possible (Typically SYS gets 20 roles by default)</i>
Priv.	<a href="#">No 'Catalog' Role Assignments</a>	ORACLE: Oracle EE - Joe	Fail	Major	Some users or roles other than predefined dba or roles have been granted default roles: SH, OLAPSYS, PERFSTAT, IX.  <i>Recommendation: Access to Data Dictionary and Catalog roles, 'SELECT_CATALOG_ROLE', 'OLAP_DBA', 'EXECUTE_CATALOG_ROLE', 'DELETE_CATALOG_ROLE', 'RECOVERY_CATALOG_OWNER' is granted to some users. We recommend restricting access to the Data Dictionary. Access to the Data Dictionary should be done using the V\$ views. 'SELECT_CATALOG_ROLE' may be granted to 'SYS', 'DBA', 'OEM_MONITOR', 'EXP_FULL_DATABASE', 'IMP_FULL_DATABASE', 'OLAP_DBA', 'OLAP_USER'. 'OLAP_DBA' may be granted to 'SYS', 'DBA', 'OLAPSYS'. 'EXECUTE_CATALOG_ROLE' may be granted to 'SYS', 'DBA', 'EXP_FULL_DATABASE', 'IMP_FULL_DATABASE'. 'DELETE_CATALOG_ROLE' may be granted to 'SYS', 'DBA'. 'RECOVERY_CATALOG_OWNER' may be granted to 'SYS'.</i>
Priv.	<a href="#">No Authority To Create Libraries</a>	ORACLE: Oracle EE - Joe	Fail	Major	Some users or roles without DBA or IMP_FULL_DATABASE authority have CREATE LIBRARY privileges: MDSYS, DMSYS, EXFSYS, ORDSYS, ORDPLUGINS, XDB.  <i>Recommendation: The CREATE LIBRARY (or CREATE ANY LIBRARY) privilege has been granted to some users. We recommend revoking this privilege unless it is absolutely necessary for a very minimal number of users to have the privilege. These privileges can be used to access the operating system, and they allow a user to load an operating system binary file and make calls to that binary's functions.</i>
Priv.	<a href="#">No Roles With The Admin Option</a>	ORACLE: Oracle EE - Joe	Fail	Major	Found roles granted WITH ADMIN option  <i>Recommendation: Roles have been granted with the admin option to roles or users other than DBA, SYS, and SYSTEM. When a role is grantable, a user can grant that role to other users. Since granting roles should be restricted, we recommend that you not grant roles with the GRANT option</i>



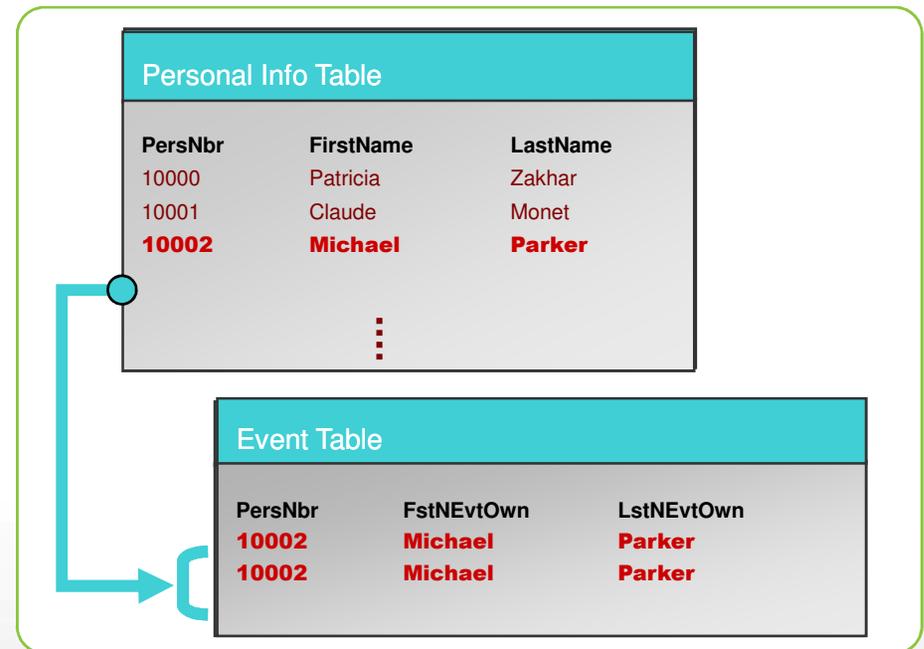
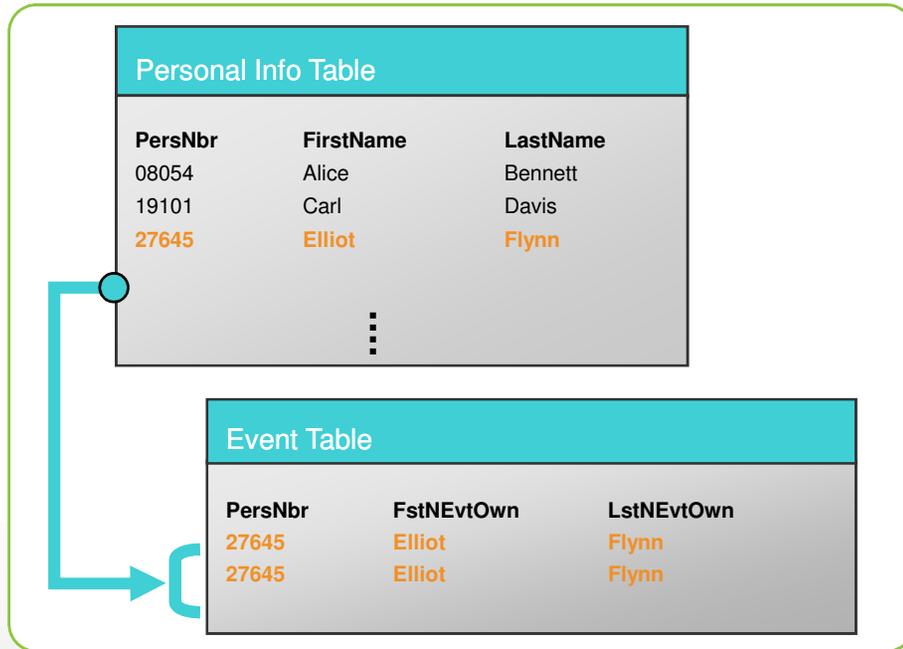
# Sensitive Data Masking

Masked or transformed data must be appropriate to the context:

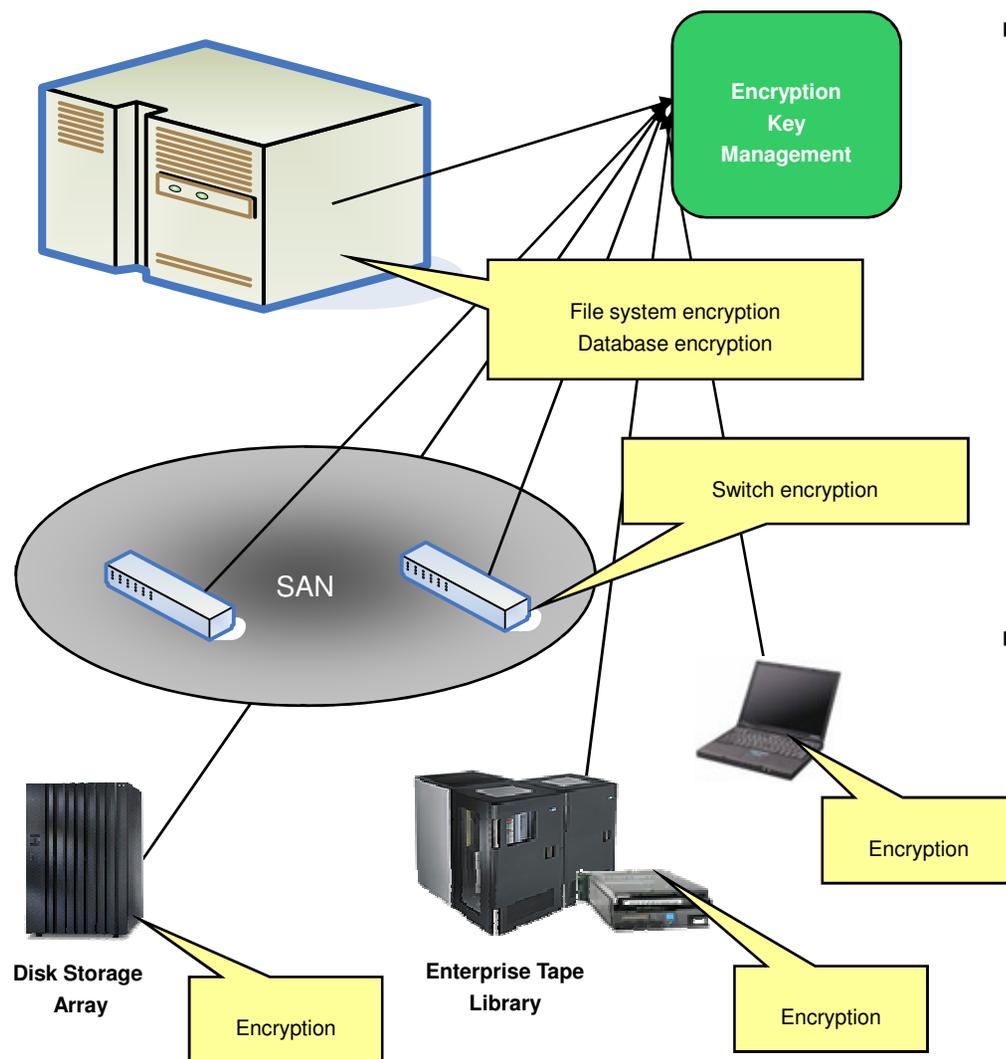
- Consistent formatting (alpha to alpha)
- Context and application aware
- Within permissible range of values
- Maintain referential integrity

A comprehensive set of data masking techniques to transform or de-identify data, including:

- String literal values
- Arithmetic expressions
- Lookup values
- Character substrings
- Concatenated expressions
- Trans Col
- Random or sequential numbers
- Date aging

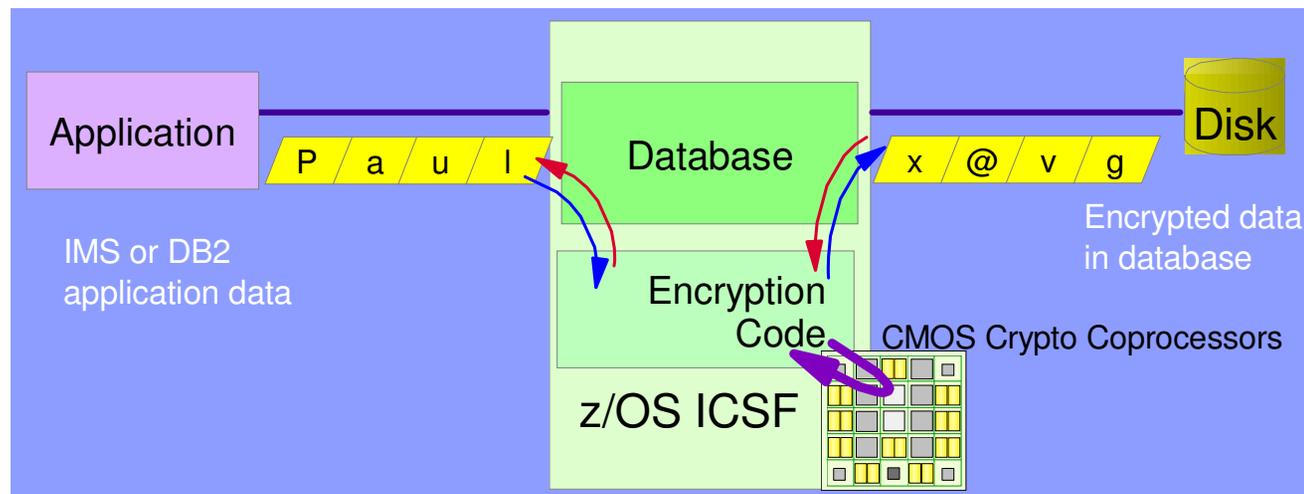


## Encryption is everywhere – but where and how makes a difference



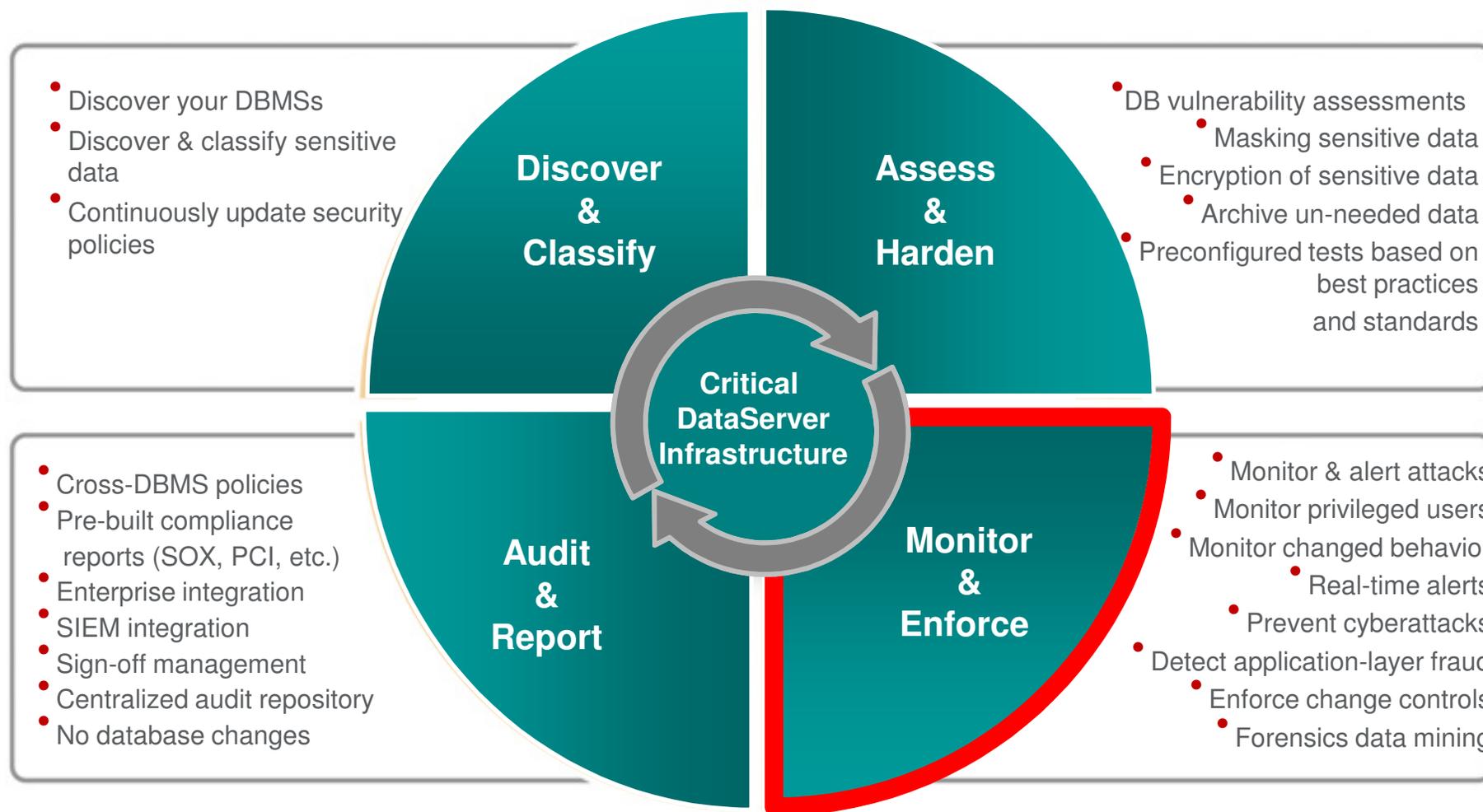
- **Encryption choices – why should encryption be built into storage**
  - Performance – cryptography can be computationally intensive
  - Efficiency - encrypted data is not able to be compressed or de-duplicated
  - Security - Data in transit should use temporary keys, data at rest should have long term retention and robust management
  - Scalability – best to distribute cryptography across many devices
- **Key Management Interoperability Protocol Standard makes this viable**
  - Four years now have demonstrated interoperability at the RSA conference with 8+ vendors
  - TKLM includes a c source reference implementation

## Data Encryption for DB2 and IMS



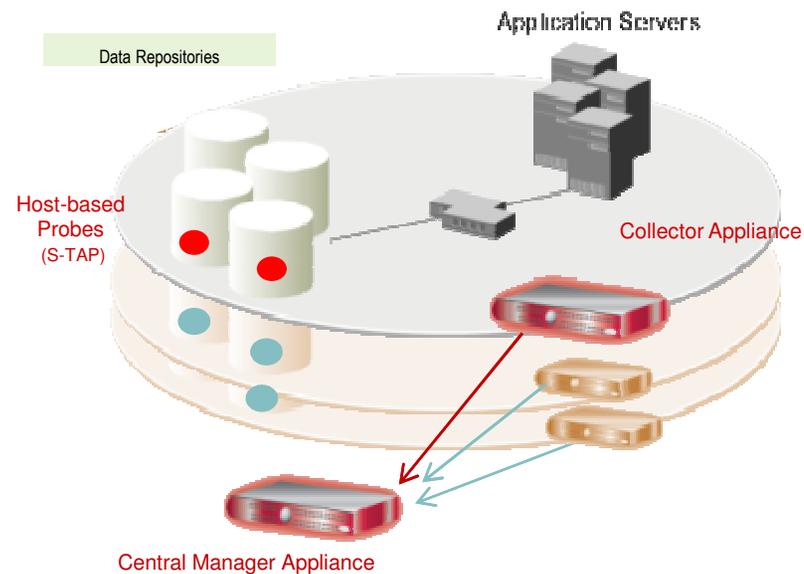
- Supports all levels of DB2
- No application changes needed
- Applications need no awareness of keys
- Supports both secure key and clear key encryption
- Index access is unaffected by encryption
- Compatible with DB2 Load/Unload utilities and DB2 Tools
- EDITPROC, FIELDPROC, or UDF invocation
- Data encryption on disk
- Data on channel is encrypted (protects against channel/network sniffers)
- Existing authorization controls accessing this data are unaffected
- Assumption made that access is through the DBMS, or, direct access invokes the DBMS data exits

# Address the Full Data Protection Lifecycle



## Data Activity Monitoring

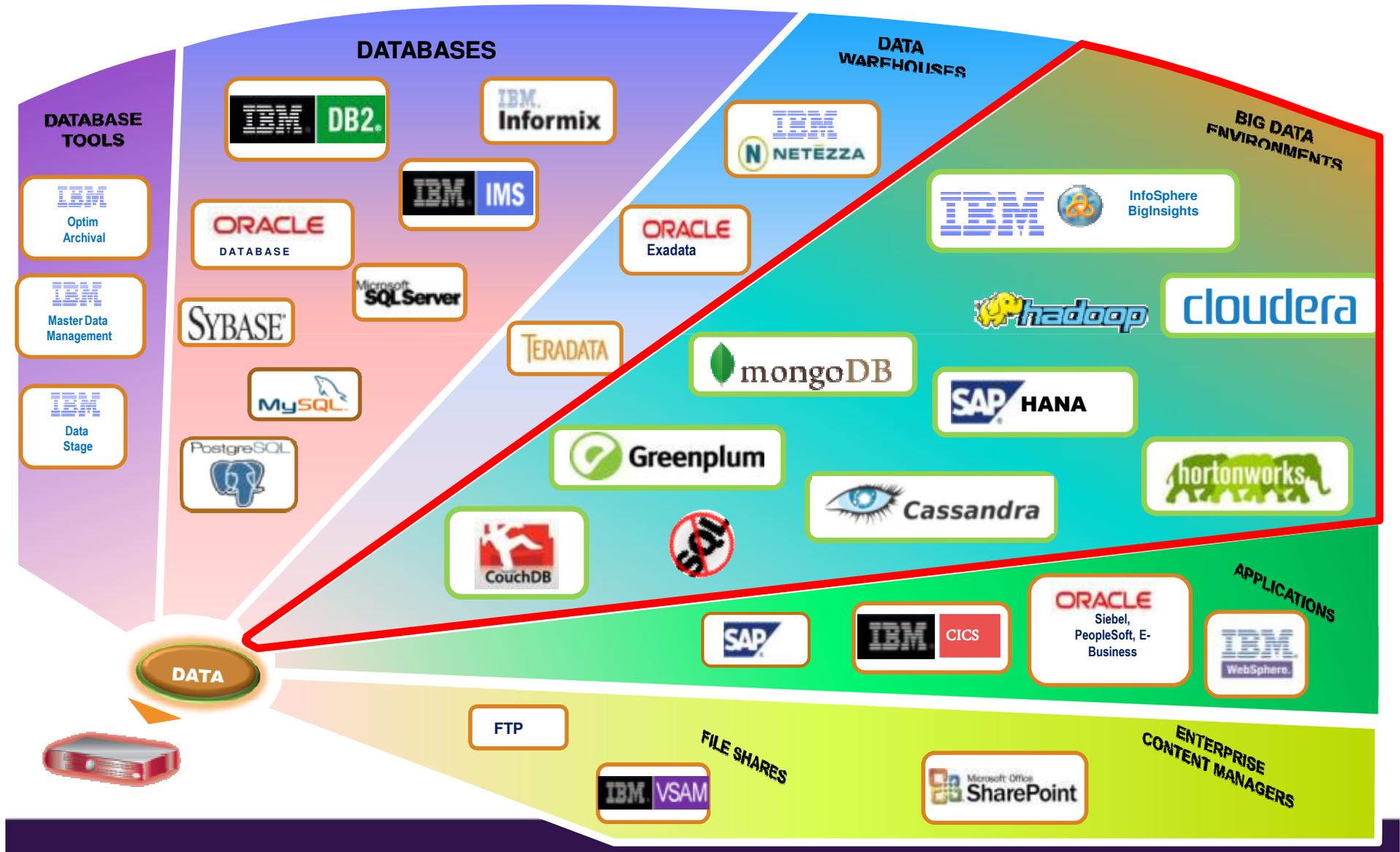
- ✓ **Activity Monitoring**  
Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users
- ✓ **Blocking & Masking**  
Data protection compliance automation
- ✓ **Vulnerability Assessment**  
Database infrastructure scanning for missing patches, mis-configured privileges and other vulnerabilities



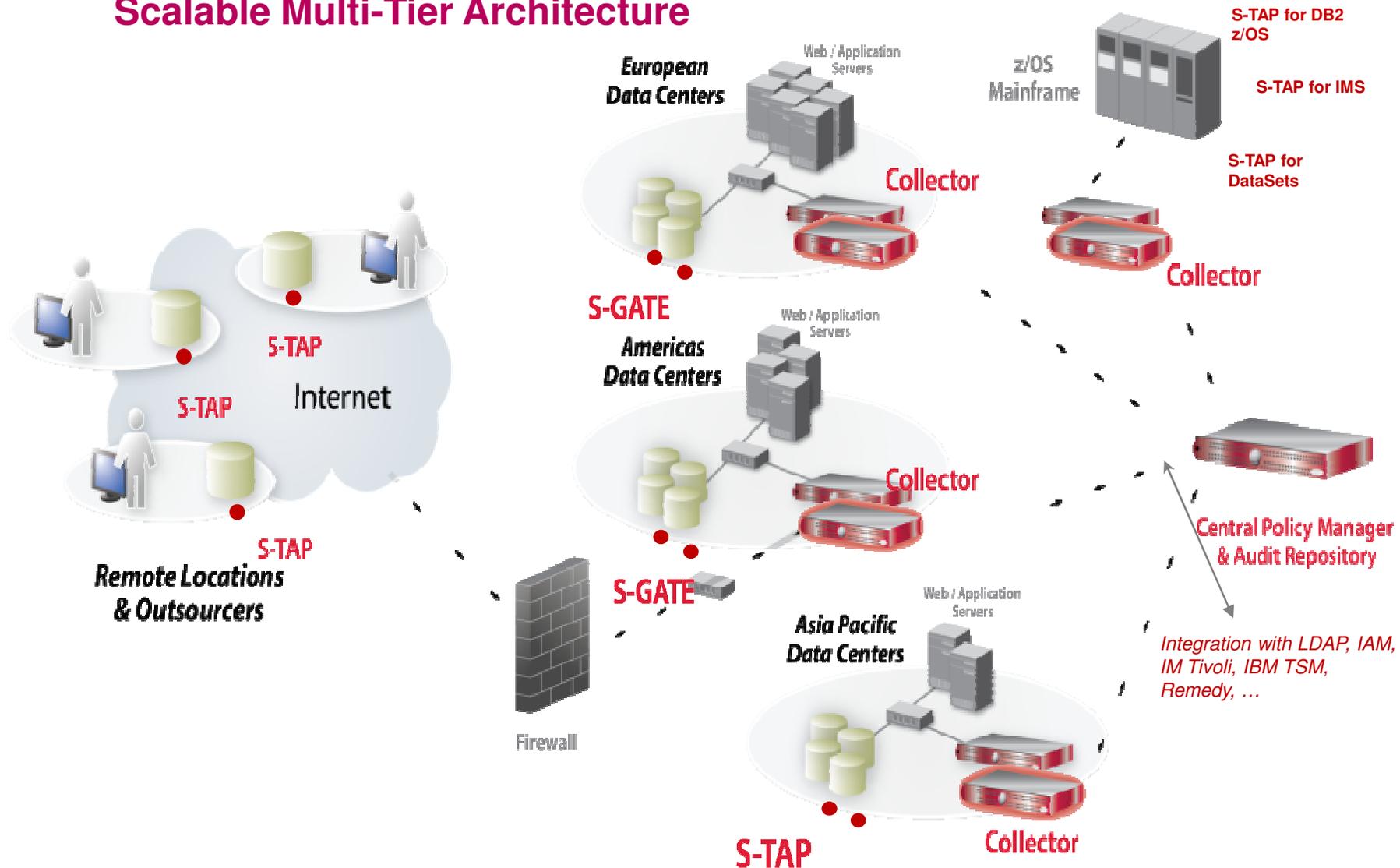
### Key Characteristics

- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized & suspicious activity
- Granular, real-time policies
  - *Who, what, when, how*
- 100% visibility including local DBA access
- Minimal performance impact
- Does not rely on resident logs that can easily be erased by attackers, rogue insiders
- No environment changes
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

## Extend Activity Monitoring to Big Data, Warehouses, File Shares



# Scalable Multi-Tier Architecture



## Cross-platform policies and auditing across enterprise

Unified cross-platform policies easily defined

Responsive actions defined within policies

Single audit repository enables enterprise-wide compliance reporting and analytics

**Access Rule Definition**

Rule #2 of policy v8

Description: Granular Cross Platform Policy Rule

Category: Security Classification: Operations Severity: HIGH

Criteria:

- Server IP / and/or Group: (Public) PCI Authorized Server IPs
- Client IP / and/or Group: (Public) PCI Authorized Client IPs
- Client MAC
- Net Prtcl. / and/or Group
- DB Type
- Svc. Name / or Group
- DB Name / or Group
- DB User / or Group
- Client IP/Srv / or Group
- App. User / or Group
- OS User / or Group
- Src App. / or Group
- Field / or Group
- Object / or Group: (Public) PCI Cardholder Sensitive objects
- Command / and/or Group
- Object/Cmd. Group

Object/Field Group

Patterns

XML Pattern

App Event Exists: Event Type / Event User Name

App Event Values: Text / and/or Group

Numeric / Date

Data Pattern

Time Period

Minimum Count / Reset Interval (0) minutes / Message Template: Default

Quarantine for (0) minutes / Records Affected Threshold (0) / Rec. Vals.  / Cont. to next rule

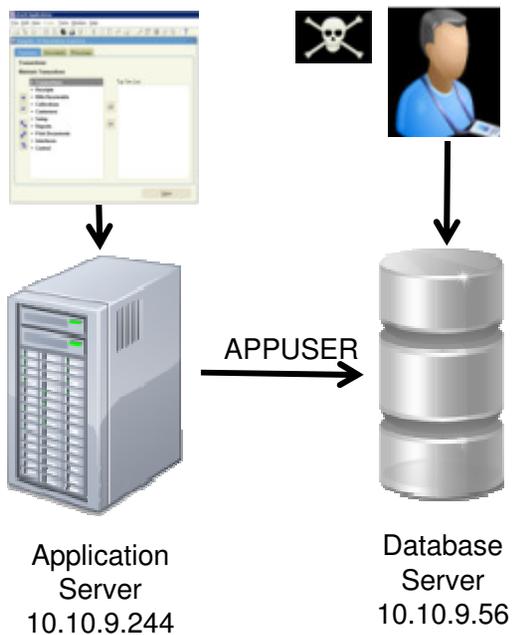
**Actions**

ALERT PER MATCH

Add Action

Back Save

## A simple policy example: *Application bypass*



Rule #1 Description	non-App Source AppUser Connection		
Category	Security	Classification	Breach
Severity	MED		
Hot	<input type="checkbox"/>	Server IP	/ / and/or Group Production Servers
Hot	<input checked="" type="checkbox"/>	Client IP	/ / and/or Group Authorized Client IPs
Hot	<input type="checkbox"/>	Client MAC	Net. Protocol / and/or Group
Hot	<input type="checkbox"/>	DB Name	
Hot	<input type="checkbox"/>	DB User	APPUSER
Field Name			
Object	EmployeeTable		
Command	Select		
Min. Ct.	0	Reset Interval (minutes)	0
Continue to next Rule	<input type="checkbox"/>	Rec. Vals.	<input checked="" type="checkbox"/>
Action	ALERT PER MATCH		
<b>Notification</b>			
<input checked="" type="checkbox"/>	Notification Type MAIL Mail User marc_gamache@guardium.com		

### Sample Alert

From: GuardiumAlert@guardium.com  
 To: Marc Gamache  
 Cc:  
 Subject: (c1) SQLGUARD ALERT

Sent: Wed 4/15/2009 8:00 AM

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: INS DB Protocol Version: 3.8 DB User: APPUSER  
 Application User Name  
 Source Program: IDBC THIN CLIENT Authorization Code: 1 Request Type: SQL\_LANG Last Error:  
 SQL: select \* from EmployeeTable

## Identify inappropriate use by authorized users

Should my customer service rep view 99 records in an hour when the average is 4?

<u>DB User Name</u>	<u>Sql</u>	<u>Records</u>
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

*Is this normal?*

*What did they 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

## Quick Search (db activities, exception, violations)

The screenshot shows the IBM InfoSphere Guardium interface. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar, there is a navigation menu with options like "System View", "Administration Console", "Tools", "Daily Monitor", "Guardium Monitor", "Tap Monitor", "Incident Management", and "Reports". The main content area displays a table of database activities. The table has columns for S-TAP Host, S-TAP Version, DB Server Type, Status, Last Response Received, Instance Name, Primary Host Name, KTAP, TEE, MSS Shm, Win DB2 Shm, Win Local TCP, Pipes, Encrypted?, Firewall Installed, DB Install Dir, DB Port Min, and DB Port Max. The table contains four rows of data, all with a status of "Active". To the right of the table, there is a "Request Rate" graph showing a line chart with a peak around 2:30 PM. Below the graph, there is a search bar with the text "Search create scott" and a magnifying glass icon.

S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Instance Name	Primary Host Name	KTAP	TEE	MSS Shm	Win DB2 Shm	Win Local TCP	Pipes	Encrypted?	Firewall Installed	DB Install Dir	DB Port Min	DB Port Max
9.70.144.50	9.0.0_r51367_v90_1-20130513_0008	DB2	Active	2013-05-22 15:23:04		9.70.148.79	Yes	No	No	N/A	N/A	No	Unencrypted	No	/home/db2inst1	50000	50000
9.70.144.50	9.0.0_r51367_v90_1-20130513_0008	INFORMIX	Active	2013-05-22 15:23:04		9.70.148.79	Yes	No	No	N/A	N/A	No	Unencrypted	No	/home/informix	1400	1400
9.70.144.50	9.0.0_r51367_v90_1-20130513_0008	MYSQL	Active	2013-05-22 15:23:04		9.70.148.79	Yes	No	No	N/A	N/A	No	Unencrypted	No	/home/mysql51	3351	3351
9.70.144.50	9.0.0_r51367_v90_1-20130513_0008	MYSQL	Active	2013-05-22 15:23:04		9.70.148.79	Yes	No	No	N/A	N/A	No	Unencrypted	No	/home/mysql50	3350	3350

For manually entered search terms, the following rules apply:

- For exact match, use double quotes. Example: "Connection Profiling List Alert"
- For results that have all specified terms (AND condition), enter terms separated by a space. Example: hadoop getlisting
- To get results that include any specified terms, use OR (or |) between the terms. Example: hadoop OR client
- To exclude a term, use NOT (or -). Example: NOT hadoop
- Use the wildcard character (\*) at beginning or end of a string. Example: \*.10.70.30



## Outliers – finding the needle in the security haystack

- Advanced *Machine Learning* algorithm
- Unsupervised model – models normal activity patterns and analyzes new activities as they accumulate.
- Intuitive interface that clearly summarizes normal activities (who/what/when/where) and pinpoints anomalies and suspicious activities
- Cluster-based analysis - predicts the appearance of data together, and flag anomalies when data appear out of “context” (i.e., if cluster is missing members)

# Outliers Analysis

The user opens 'Search/Browse' to see the all activity overview.

In the overview chart the user notices medium (Tuesday, 15:00 clock) and high (Wednesday, 02:00) marked outliers.

The user wants to get more information especially about the high classified outliers.

*Anomaly Hours are marked in Red or Yellow. Click on the bubble navigates to the Outlier View*

The screenshot shows the IBM InfoSphere Guardium Search/Browse interface. The top navigation bar includes 'View', 'QuickStart', 'Monitor/Audit', 'Discover', 'Assess/Harden', 'Comply', 'Protect', 'Capture/Replay', and 'Search/Browse'. Below the navigation bar is a search bar with the text 'Type search keywords here' and a '1 Day' filter. The main content area is divided into three sections: 'Where', 'What', and 'Who', each with a list of attributes and values. The 'Where' section includes Source Program (256), Server (94), Datasource Type (6), and Database Name (125). The 'What' section includes Object (2054) and Verb (25). The 'Who' section includes OS User (5023), Database User (5456), Client IP (4895), and Client Hostname (4895). Below these sections is a 'When' section with Date / Time (24) and an 'Exception' section with Error Type (12), Outlier Type (4), Violation (200), and Alerts (25). The central part of the interface is a line chart titled 'Activity' showing activity levels over time. The chart has a legend for 'Activity' (blue line), 'Outliers: High' (red circle), and 'Outliers: Medium' (yellow circle). The x-axis shows time from 12:00 on Tuesday, July 25th, to 12:00 on Wednesday, July 26th. The y-axis shows activity levels from 0 to 180. A yellow circle highlights a medium outlier at 15:00 on Tuesday, and a red circle highlights a high outlier at 02:00 on Wednesday. Below the chart is a tabbed interface with 'Activity' selected. Below the tabs is a 'Summary by Datasource' section with a dropdown menu. The main part of the interface is a table with the following columns: Server, Database, DB Type, Source Program, DB User, OS User, Client Hostname, Client IP, Verb, Object, and When. The table contains 12 rows of activity data.

Server	Database	DB Type	Source Program	DB User	OS User	Client Hostname	Client IP	Verb	Object	When
9.148.11.1	DBNAME1	DB2	PROG1	AABRAMS	AABRAMS	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.11.1	DBNAME2	DB2	APPABC	ABRAMS	ABRAMS	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm
9.148.11.2	DBNAME3	Oracle	APPNAME	ABRAMS	ABRAMS	Name1	9.234.22.9	SELECT	OBJECT1, OBJECT2	07/26/2013 02:55 am
9.148.11.2	DBNAME4	DB2	DFD234	SMITHJ	SMITHJ	Name1	9.234.22.9	INSERT	OBJECT3, OBJECT4	07/26/2013 02:55 pm
9.148.11.3	DBNAME5	Hadoop	PROG1	JSMITH	JSMITH	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.11.3	DBNAME5	DB2	APPABC	SMITH	SMITH	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm
9.148.12.1	DBNAME1	DB2	APPNAME	BONNER	BONNER	Name1	9.234.22.9	SELECT	OBJECT1, OBJECT2	07/26/2013 02:55 am
9.148.12.1	DBNAME2	DB2	DFD234	BONNER	BONNER	Name1	9.234.22.9	INSERT	OBJECT3, OBJECT4	07/26/2013 02:55 pm
9.148.13.1	DBNAME3	Oracle	PROG1	WARWU	WARWU	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.13.1	DBNAME4	DB2	APPABC	WU	WU	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm

# Outliers Details

The 'Outliers' tab contains more information about the selected timeframe with high classified outliers.

The 'Type' explains the reason. Examples: New/Unique, Rare, Exceptional Volume, Exceptional Errors

The user can then interactively investigate each finding by Filtering-In / Out data or by using the Context Menu to navigate to the "Related Activities", "Related Errors", History or any other related data.

**IBM InfoSphere Guardium** | Search/Browse

Search, browse, and filter information about monitored objects, systems, and users. [Learn More](#)

Filters: **Data/Time='7/26 2:00am'; Outlier Type='High'** | 1 Day | View

**Where**

- Source Program: 1
- Server: 1
- Datasource Type: 3
- Database Name: 4

**What**

- Object: 3
- Verb: 4

**Who**

- OS User: 1
- Database User: 2
- Client IP: 2
- Client Hostname: 2

**When**

Date / Time: 7/26 2:00 am

**Exception**

- Error Type: 3
- Outlier Type: 1
- Violation: 0
- Alerts: 0

**Activity** | **Outliers** | Errors | Alerts | Violations

Overview | Details by Datasource | Details by User

Score	Type	Datasource	Verb	Object	User	Count	Cluser
100	New	DBNAME1	CREATE VIEW	SURPISE	SNOWDEN	123	100
99	Volume	DBNAME1	SELECT	PAYROLL, SALARY	SI	123	94
97	Error	DBNAME3	INSERT	PAYROLL, SALARY	SI	123	89
89	Error	DBNAME145	SELECT	PRODUCT-X	M	75	23

Context Menu:

- Show Related Activity
- Show Related Exceptions
- Show Related Violations
- Add as Filter

## Monitoring on System z - Recent Enhancements

- Termination of suspicious DB2 activity
  - Terminate a DB2 thread that a Guardium policy has flagged as high risk
- Many new System z RACF vulnerability tests
  - directly or via zSecure Integration
- New Entitlement Reporting for z
  - DB2 Catalog and RACF via zSecure
- New monitoring of DataSet activity (sequential and partitioned)
- Centralized IMS management
- Expanded DB2 monitoring including DB2 start and stop
- Resiliency across network or server outages
  - Consistent across all platforms
- Appliance based policy administration
  - Consistent with Distributed policies on Guardium UI

## Automate oversight processes to ensure compliance and reduce operational costs

Easily create custom processes by specifying unique combination of workflow steps, actions and users

- Use case  
*Different oversight processes for financial servers than PCI servers*

Supports automated execution of oversight processes on a report line item basis, maximizing efficiency without sacrificing security

- Use case  
*Daily exception report contains 4 items I know about and have resolved, but one that needs detailed investigation. Send 3 on for sign-off; hold one*

**Event Type**

Existing Task Event Types

Event Type	First Status	Allowed Status
Task: Daily PCI DSS Incident Report	Open	Approved, Not Approved, Open, Review state

Description: Daily PCI DSS Incident Report

First Status: Open

Allowed Status:

Allowed Status	Allowed Status
Open	Approved (Final)
	Not Approved (Final)
	Open
	Review state

Predefined Event Actions:

Event Action Description	Prior Status	Next Status	Sign-off
Under review	Open	Review state	<input type="checkbox"/>
Approved	Review state	Approved	<input checked="" type="checkbox"/>
Not approved	Review state	Not Approved	<input checked="" type="checkbox"/>

Rules:

- Rules have been assigned to this event type with status: **Approved** [Rules]
- Rules have been assigned to this event type with status: **Open** [Rules]
- Rules have been assigned to this event type with status: **Not Approved** [Rules]
- No rules have been assigned to this event type with status: **Review state** [Rules]

Buttons: New Event Type, Event Status

**Compliance Automation**

**Audit Process Definition**

Description: Daily PCI DSS Incident Report

Active:  There is no schedule associated with this process

Archive Results:

Keep for a minimum of: 90 days or 3 years

CSARCER File Label: Daily\_PCI\_DSS\_Incident\_Report [2] Do CSV for mail

Email Subject: Daily PCI DSS Incidents for Remediation and Sign-off

Buttons: View, Run Once Now, Modify Schedule

Receiver Table:

Receiver	Action Req.	To-Do List	Email Notif.	Cont. Appro. if Empty
Payment Card (D) Admin (Ernst Proberfeld)	Review Sign	<input type="checkbox"/>	No Link Full Results	<input checked="" type="checkbox"/>
Global InfoSec (Max Dufresne)	Review Sign	<input type="checkbox"/>	No Link Full Results	<input checked="" type="checkbox"/>

Add Receiver: Receiver name [Search users]

Action Required:  Review  Sign

To-Do List:  Add

Email Notification:  None  Link Only  Full Results

Continuation:

Approve if Empty:  Yes

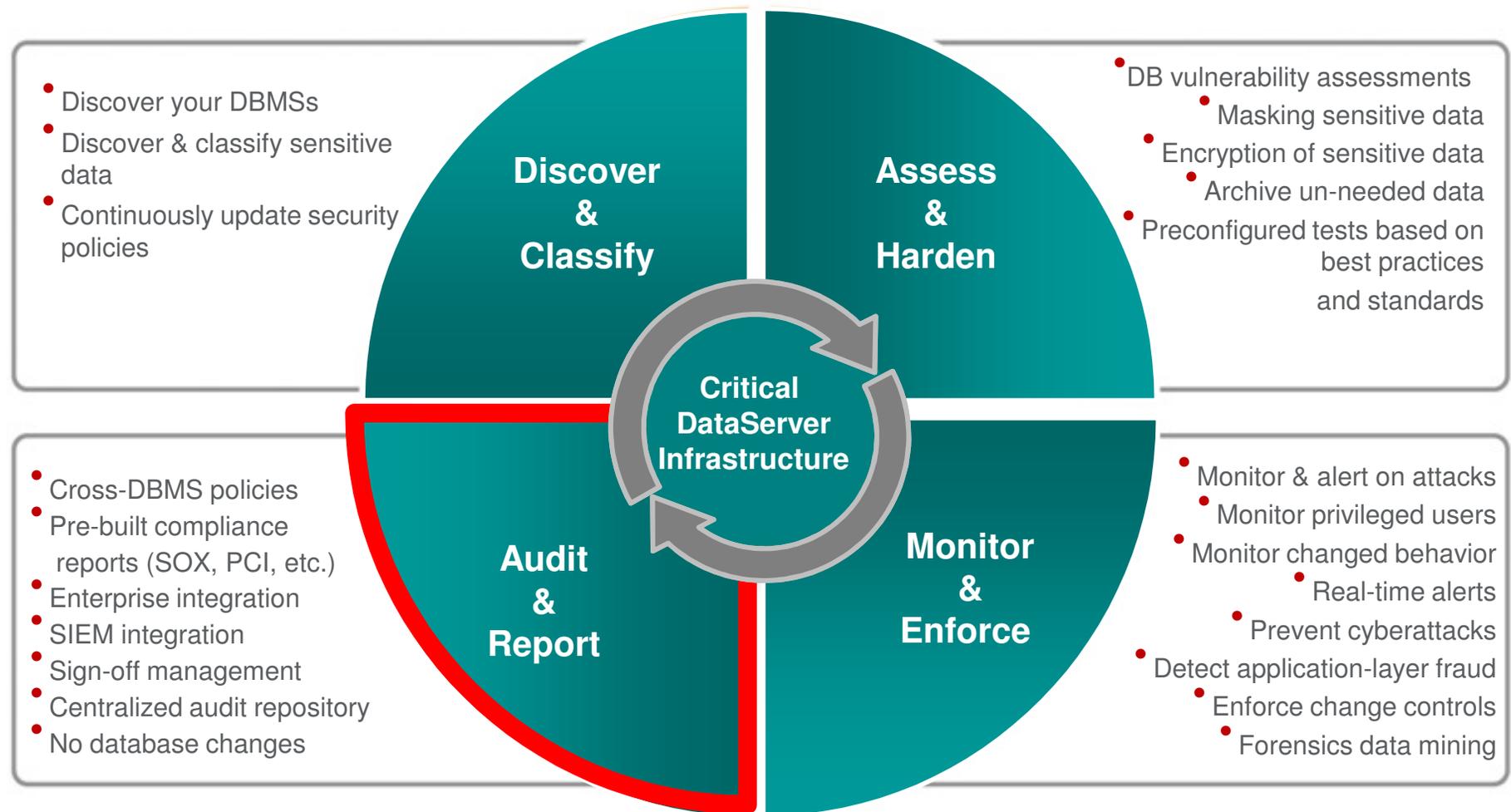
Buttons: Add

Audit Tasks:

- Report: Daily PCI DSS Incident Report [Policy Violations Details] (NOW -1 DAY 1x NOW)

Buttons: Add Audit Task

# Address the Full Data Protection Lifecycle



## Audit and Report

### Custom and Pre-Built Compliance Reports

- Custom reporting
- SOX and PCI accelerators
  - Financial application monitoring (EBS, JD Edwards, Peoplesoft, etc)
  - Authorized application access only
  - Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)

PCI Accelerator

Overview REG 3 Protect REG 6 Maintain REG 7 Restrict REG 8 Assign PCI Req. 10 Track & Monitor REG 11 Test PCI Policy Monitoring

Overview

- Cardholder Server IPs List
- Cardholders DBs
- Cardholder Objects
- Data Access Map
- DB Clients to Servers Map
- Active DB Users
- Cardholder DB Administration
- Source Programs
- Review Groups

**PCI - Cardholder Server IPs**

Start Date: 2007-01-01 00:00:00 End Date: 2007-05-31 00:00:00

Server IP	Server Type	Database Name	Count of Sessions
192.168.1.186	ORACLE	CARD_DATA	8
192.168.2.51	ORACLE	CARD_DATA	140
192.168.200.108	DB2	CARD_DATA	182
192.168.200.108	DB2	DN8DEMO3	258
192.168.200.108	DB2	SAMPLE	44

# Reporting

## DDL and DCL

IBM InfoSphere™ Guardium

13:30 | Edit Account... | Customize | Logout | About | IBM.

Standard Reports | My New Reports | Discover | Assess/Harden | Comply | Protect

G2000 - Standalone Unit

Build Queries and Reports

- Activity Report
- Exceptions Report
- Messages Report
- Policy Violations
- 01 - DDL Commands
- 02 - DDL Commands**
- 03 - Select Statements
- 04 - Detailed SQL
- 07 - PHI Access
- 08 - Activity Source Program
- 09 - Specific DB User
- 12 - Grant Commands
- 13 - Failed Logins
- 14 - SQL Errors
- 15 - Local Access
- 17 - 3rd Party Tool Access
- 19 - DDL by DBA
- Barry Test Report

02 - DDL Commands

Start Date: 2011-11-17 13:30:48 End Date: 2011-11-18 13:30:48

Aliases: OFF ClientIP: LIKE %

DBUsername: LIKE % NetProt: LIKE %

ServerIP: LIKE % ServerType: LIKE %

Timestamp	Server IP	Service Name	Network Protocol	OS User	DB User Name	App User Name	Sql
2011-11-18 12:05:46.0	172.21.248.9	DSNZ	TSO BATCH	K250151K250151	PLAN=DSNTEP2 ; SQLID= ; PROG=		REVOKE SELECT ON ADHUSER.ADHRULE FROM GHOST
2011-11-18 12:05:46.0	172.21.248.9	DSNZ	TSO BATCH	K250151K250151	PLAN=DSNTEP2 ; SQLID= ; PROG=		GRANT SELECT ON ADHUSER.ADHRULE TO GHOST
2011-11-18 12:05:46.0	172.21.248.9	DSNZ	TSO BATCH	K250151K250151	PLAN=DSNTEP2 ; SQLID= ; PROG= ; DB_NAME=ADHDB		GRANT SELECT ON ADHUSER.ADHRULE TO GHOST
2011-11-17 17:28:22.0	172.21.248.9	DSNZ	CALL.DB2CALL	SYSSLG	SYSSLG	PLAN=ACT930DM ; SQLID=DB2ADMG ; PROG=ACTQ9SQL	DROP TABLE DB2SLG.DSN_PREDICAT_TABLE
2011-11-17 17:29:05.0	172.21.248.9	DSNZ	CALL.DB2CALL	SYSSLG	DB2ADMG	PLAN=ACT930DM ; SQLID=DB2ADMG ; PROG=ACSNQSP	DROP TABLE SESSION .SYSPRINT
2011-11-17 17:28:28.0	172.21.248.9	DSNZ	CALL.DB2CALL	SYSSLG	SYSSLG	PLAN=ACT930DM ; SQLID=DB2ADMG ; PROG=ACTQ9SQL	CREATE TABLE DB2SLG.DSN_PREDICAT_TABLE ( "QUERYNO" INTEGER NOT NULL ,OBLOCKNO SMALLINT NOT
2011-11-17 17:28:22.0	172.21.248.9	DSNZ	CALL.DB2CALL	SYSSLG	DB2ADMG	PLAN=ACT930DM ; SQLID=SYSSLG ; PROG=ACSNQSP	DROP TABLE SESSION .SYSPRINT
2011-11-17 17:28:20.0	172.21.248.9	DSNZ	CALL.DB2CALL	SYSSLG	DB2ADMG	PLAN=ACT930DM ; SQLID=SYSSLG ; PROG=ACSNHDD	DROP TABLE SESSION .MXLIST

Records 1 to 8 of 8

Ability to Monitor Data Definition Language Commands  
 Create, Alter, Drop, etc.

Ability to Monitor Data Control Language Commands  
 Grant, Revoke, etc.

# Reporting

## Sensitive Data Access

IBM InfoSphere™ Guardium

15:42 | [Edit Account.poc](#) | [Customize](#) | [Logout](#) | [About](#) | IBM.

G2000 - Standalone Unit

Standard Reports | My New Reports | Discover | Assess/Harden | Comply | Protect

Build Queries and Reports

- Activity Report
- Exceptions Report
- Messages Report
- Policy Violations
- 01 - DML Commands
- 02 - DDL Commands
- 03 - Select Statements
- 04 - Detailed SQL
- 07 - PHI Access**
- 08 - Activity Source Program
- 09 - Specific DB User
- 12 - Grant Commands
- 13 - Failed Logins
- 14 - SQL Errors
- 15 - Local Access
- 17 - 3rd Party Tool Access
- 19 - DDL by DBA
- Barry Test Report

07 - PHI Access

Start Date: 2011-11-18 12:34:21 End Date: 2011-11-18 15:34:21

Aliases: OFF Lastaccess: < NOW

ObjectName: LIKE %

Timestamp	Service Name	Object Name	Field Name	OS User	DB User Name	App User Name	Sql
2011-11-18 15:32:45.0	DT31	KDINDV4V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTG ; SQLID=CQUAL5 ; PROG=KDI01 ; DB_NAME=KDQ50000	SELECT XVRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:32:45.0	DT31	KDINDV1V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTG ; SQLID=CQUAL5 ; PROG=MSM02 ; DB_NAME=KDQ50000	SELECT PHNM_DISPL_NM , INDV_KSR_MBR_IND , XVRSE
2011-11-18 15:32:35.0	DT31	KDINDV4V	INDV_SSN	KS01197	KS01197	PLAN=DISTSERV ; SQLID=KS01197 ; PROG=IRMSP041 ; DB_NAME=KDQ50000	SELECT INDV_KSR_MBR_IND , INDV_SSN , INDV_DOB II
2011-11-18 15:32:35.0	DT31	KDINDV4V	INDV_SSN	KS01197	KS01197	PLAN=DISTSERV ; SQLID=KS01197 ; PROG=IRMSP041 ; DB_NAME=KDQ50000	DECLARE KINDCD-CSR CURSOR WITH RETURN FOR SE
2011-11-18 15:31:20.0	DT31	KDPHNM2V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTG ; SQLID=CQUAL5 ; PROG=KDI02 ; DB_NAME=KDQ50000	DECLARE EZEUCRSOR1 CURSOR FOR SELECT PHNM_
2011-11-18 15:31:15.0	DT31	KDINDV1V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTG ; SQLID=CQUAL5 ; PROG=KDI011 ; DB_NAME=KDQ50000	SELECT XVRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:31:15.0	DT41	KDINDV1V	INDV_SSN	MSDB2QMSDB2Q	MSDB2Q	PLAN=MSFM00 ; SQLID=MSDB2Q ; PROG=MSFH1 ; DB_NAME=PKD00000	DECLARE EZEUCRSOR2 CURSOR FOR SELECT PHNM_
2011-11-18 15:31:10.0	DT41	KDINDV4V	INDV_SSN	MSDB2QMSDB2Q	MSDB2Q	PLAN=MSFM00 ; SQLID=MSDB2Q ; PROG=KDI01 ; DB_NAME=PKD00000	SELECT XVRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:31:10.0	DT41	KDINDV1V	INDV_SSN	MSDB2QMSDB2Q	MSDB2Q	PLAN=MSFM00 ; SQLID=MSDB2Q ; PROG=MSF02 ; DB_NAME=PKD00000	DECLARE EZEUCRSOR5 CURSOR FOR SELECT PHNM_
2011-11-18 15:30:45.0	DT41	KDLIND3V	INDV_SSN	MSDB2QMSDB2Q	MSDB2Q	PLAN=MSFM00 ; SQLID=MSDB2Q ; PROG=KDIH1 ; DB_NAME=PKD00000	DECLARE EZEUCRSOR1 CURSOR FOR SELECT XVRGN_
2011-11-18 15:30:40.0	DT41	KDINDV1V	INDV_SSN	MSDB2QMSDB2Q	MSDB2Q	PLAN=MSFM00 ; SQLID=MSDB2Q ; PROG=KDI011 ; DB_NAME=PKD00000	SELECT XVRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:30:35.0	DT41	KDPHNM2V	INDV_SSN	MSDB2QMSDB2Q	MSDB2Q	PLAN=MSFM00 ; SQLID=MSDB2Q ; PROG=KDI02 ; DB_NAME=PKD00000	DECLARE EZEUCRSOR1 CURSOR FOR SELECT PHNM_
2011-11-18 15:30:30.0	DT31	KDINDV1V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTG ; SQLID=CQUAL5 ; PROG=MSME1 ; DB_NAME=KDQ50000	SELECT XVRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:30:05.0	DT41	KDINDV3V	INDV_SSN	IWE8000	IWE8000	PLAN=DISTSERV ; SQLID=IWE8000 ; PROG=IREH007 ; DB_NAME=PKD00000	SELECT INDV_HRN , PHNM_DISPL_NM , INDV_KSR_MBI

Ability to Monitor Access to Objects and Fields Containing Sensitive Data

# Reporting

## Specific User Activity

IBM InfoSphere™ Guardium

15:50 | Edit Account, doc | Customize | Logout | About | IBM

G2000 - Standalone Unit

Standard Reports | My New Reports | Discover | Assess/Harden | Comply | Protect

Build Queries and Reports

- Activity Report
- Exceptions Report
- Messages Report
- Policy Violations
- 01 - DML Commands
- 02 - DDL Commands
- 03 - Select Statements
- 04 - Detailed SQL
- 07 - DB Access
- 08 - Activity Source Program**
- 09 - Specific DB User
- 12 - Grant Commands
- 13 - Failed Logins
- 14 - SQL Errors
- 15 - Local Access
- 17 - 3rd Party Tool Access
- 19 - DDL by DBA
- Barry Test Report

09 - Specific DB User

Start Date: 2011-11-15 15:50:40 End Date: 2011-11-18 15:50:40

Aliases: OFF ClientIP: LIKE %

DBUsername: LIKE K250151 NetProt: LIKE %

SQL: LIKE % ServerP: LIKE %

ServerType: LIKE %

Timestamp	Server Type	Server IP	Service Name	Client IP	Network Protocol	DB User Name	Sql
2011-11-15 16:54:30.0	DB2	172.21.248.13D011		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR, TBNAME, TBCreator FROM SYSIBM.SYSINDEXES WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:53:40.0	DB2	172.21.248.13D02		127.0.0.1	TSO: BATCH	K250151	SELECT BPOOL, NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?
2011-11-15 16:53:40.0	DB2	172.21.248.13D02		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR, BPOOL FROM SYSIBM.SYSTABLESPACE WHERE DBNAME IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?)
2011-11-15 16:53:40.0	DB2	172.21.248.13D02		127.0.0.1	TSO: BATCH	K250151	SELECT NAME, CREATOR FROM SYSIBM.SYSDATABASE WHERE BPOOL = ? AND NAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?
2011-11-15 16:53:40.0	DB2	172.21.248.13D02		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR FROM SYSIBM.SYSTABLESPACE WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:53:40.0	DB2	172.21.248.13D02		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR, TBNAME, TBCreator FROM SYSIBM.SYSINDEXES WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:48:13.0	DB2	172.21.248.13D01		127.0.0.1	TSO: TSO	K250151	DB2_COMMAND -ds trace
2011-11-15 16:46:03.0	DB2	172.21.248.13D02		127.0.0.1	TSO: TSO	K250151	DB2_COMMAND -DIS LOG
2011-11-15 16:07:05.0	DB2	172.21.248.13D01		127.0.0.1	TSO: BATCH	K250151	SELECT BPOOL, NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?
2011-11-15 16:07:05.0	DB2	172.21.248.13D01		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR, BPOOL FROM SYSIBM.SYSTABLESPACE WHERE DBNAME IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?)
2011-11-15 16:07:05.0	DB2	172.21.248.13D01		127.0.0.1	TSO: BATCH	K250151	SELECT NAME, CREATOR FROM SYSIBM.SYSDATABASE WHERE BPOOL = ? AND NAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?
2011-11-15 16:07:05.0	DB2	172.21.248.13D01		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR FROM SYSIBM.SYSTABLESPACE WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:07:05.0	DB2	172.21.248.13D01		127.0.0.1	TSO: BATCH	K250151	SELECT DBNAME, NAME, CREATOR, TBNAME, TBCreator FROM SYSIBM.SYSINDEXES WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:03:58.0	DB2	172.21.248.13D01		127.0.0.1	TSO: TSO	K250151	DB2_COMMAND -ds ddf

Records: 21 to 34 of 34

Ability to Report on a Specific User's Activity

# Reporting

## Custom Report Building

The screenshot displays the Query Builder interface in a browser window. The main area is titled '-Activity Report' and shows a configuration for a query. The 'Query Fields' table lists various attributes and their field modes. The 'Query Conditions' table lists logical conditions for filtering the data.

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
<input type="checkbox"/>	1	Access Period	Timestamp	Value	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	Client/Server	Server IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	Client/Server	Service Name	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	4	Client/Server	Network Protocol	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	5	Client/Server	Client IP	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	6	Client/Server	OS User	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	7	Client/Server	DB User Name	Value	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	8	App User Name	App User Name	Value	<input type="checkbox"/>	<input type="checkbox"/>

	Entity	Agg.	Attribute	Operator	Runtime Param.	
<input type="checkbox"/>	WHERE	Client/Server	---	Server Type	LIKE	Parameter ServerType
<input type="checkbox"/>	AND	Client/Server	---	Server IP	LIKE	Parameter ServerIP
<input type="checkbox"/>	AND	Client/Server	---	Client IP	LIKE	Parameter ClientIP
<input type="checkbox"/>	AND	Client/Server	---	Network Protocol	LIKE	Parameter NetProt
<input type="checkbox"/>	AND	Client/Server	---	DB User Name	LIKE	Parameter DBUsername
<input type="checkbox"/>	AND	SQL	---	Sql	LIKE	Parameter SQL
<input type="checkbox"/>	AND	Client/Server	---	Service Name	LIKE	Parameter ServiceName
<input type="checkbox"/>	AND	Client/Server	---	Service Name	IN GROUP	KP Development SSIDs

Ability to Easily Create Custom Reports Through Point and Click Interface

## Agenda

- **Big Data opportunities and threats**
- **Proactive and preventative measures to information protection**
- **Summary and Call to Action**

## Summary and call to action..

- **Enterprise wide protection across many databases, platforms and data streams**
  - *Preventative and proactive data security controls*
  - *Real-time data threat detection and monitoring alerts*
  - *Support for many data streams – not just transactional*
  - *Extensive integration capabilities*
  - *Fast implementation with automated workflows, predefined compliance reports and policies*
  - *Data Masking, Encryption and vulnerability assessment.*
- **Sign up for future related papers in 2015 “The world of DB2 for z/OS” on LinkedIn and Facebook**

## Useful URLs

- [www.ibm.com/software/os/systemz/security/](http://www.ibm.com/software/os/systemz/security/)
- [www.ibm.com/guardium](http://www.ibm.com/guardium)
- [www.ibm.com/bigdata/z](http://www.ibm.com/bigdata/z)
- [www.infogovcommunity.com](http://www.infogovcommunity.com)

THINK

BIG

THINK

Z

**Thank You**