Central Pennsylvania User Group
Protecting Big Data

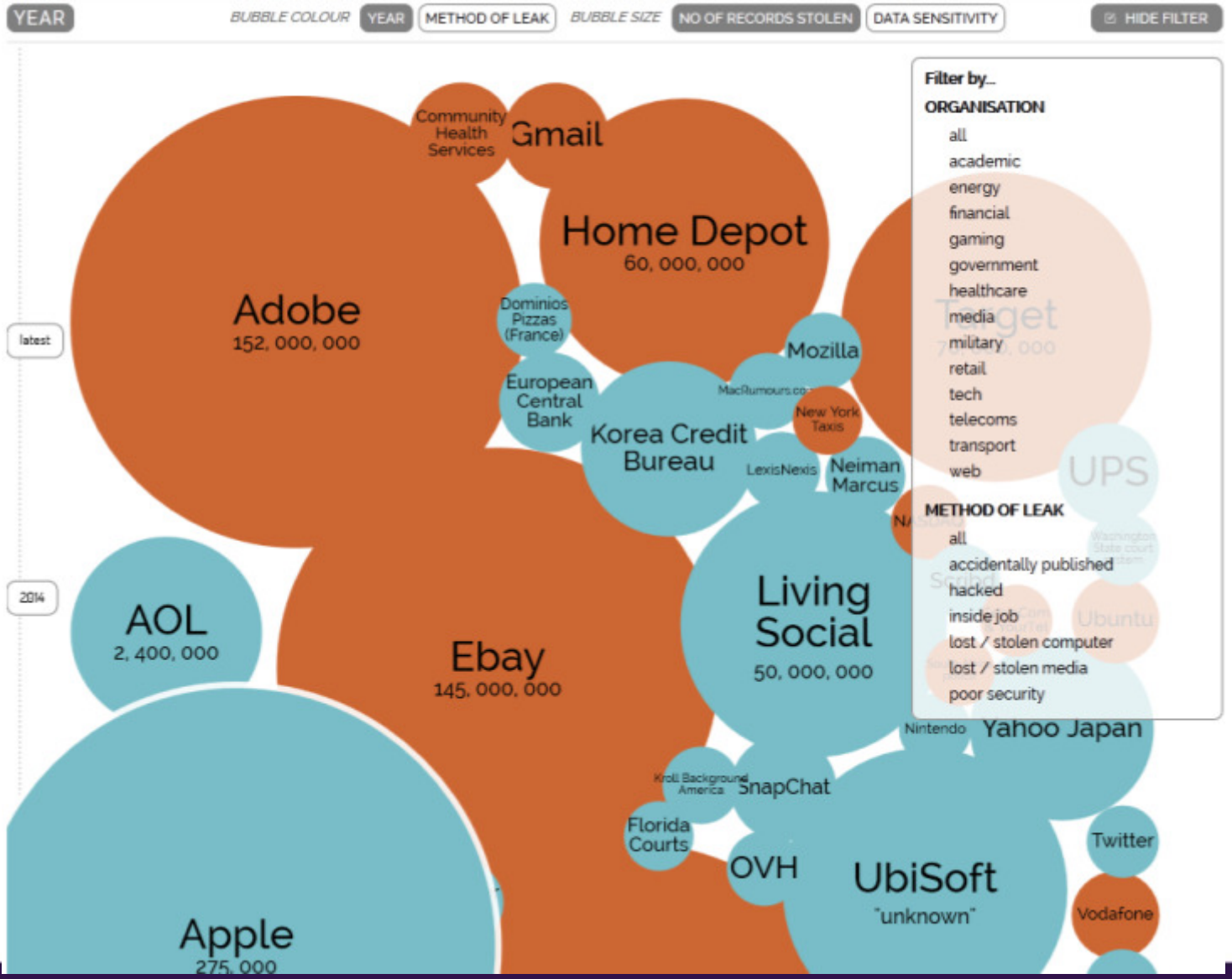
Howie Hirsch –
Senior IT Specialist
IBM Corporation
Valley Forge, PA June 9, 2015

Agenda

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

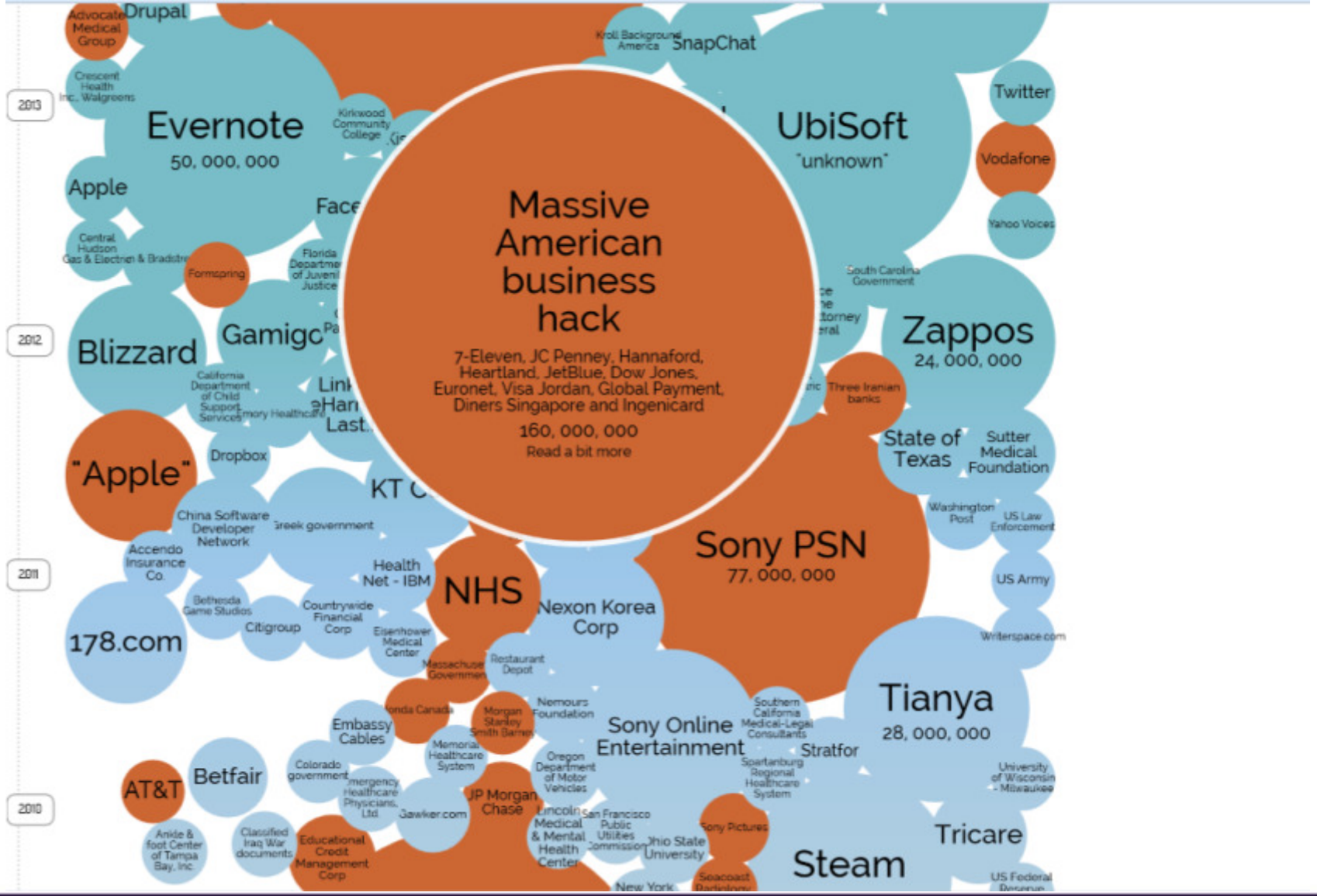
The who's who of the world's biggest data breaches….

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



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 3rd party
- Managed by 3rd 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.

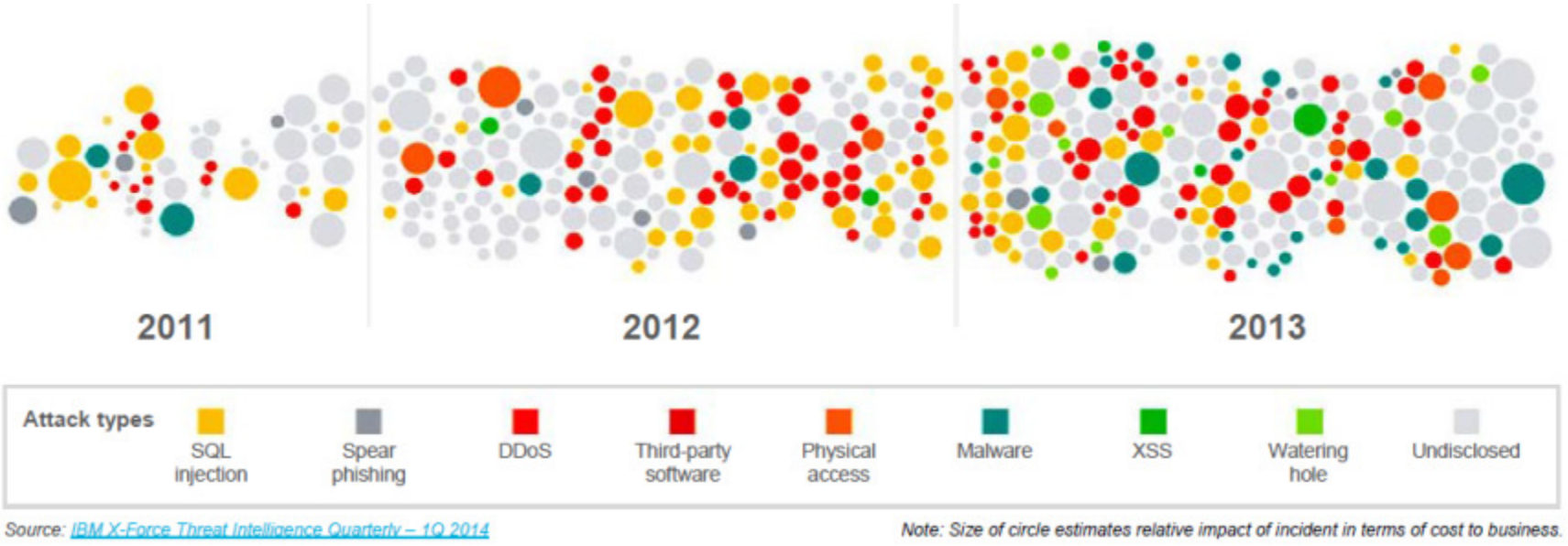
Hackers orchestrated multiple breaches of Sony's PlayStation Network knocking it offline for 24 days and costing the company an estimated $171 million, and significantly damaged brand reputation

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_xg.pdf

Data Governance and Security are changing rapidly

Data Explosion

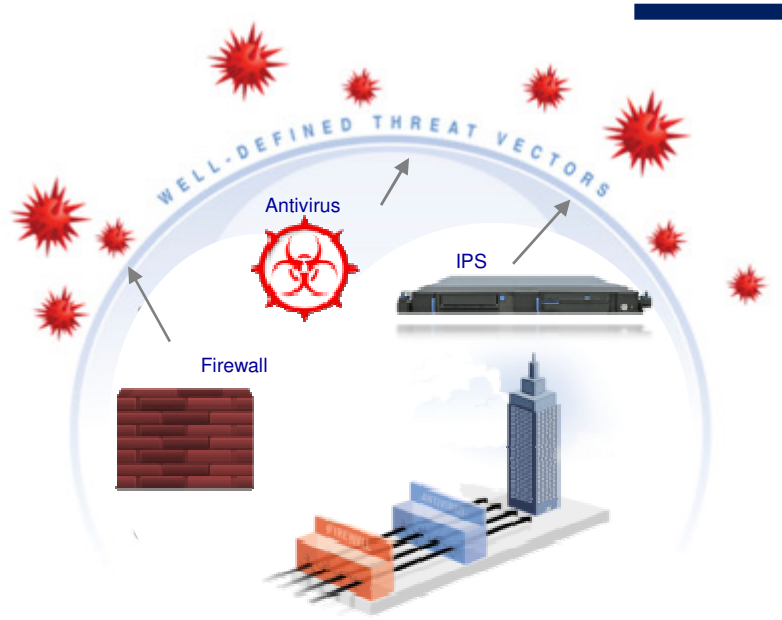
Consumerization of IT

Everything is Everywhere

Attack Sophistication

Extending the perimeter; focus shifts to protecting the DATA

Moving from traditional perimeter-based security…



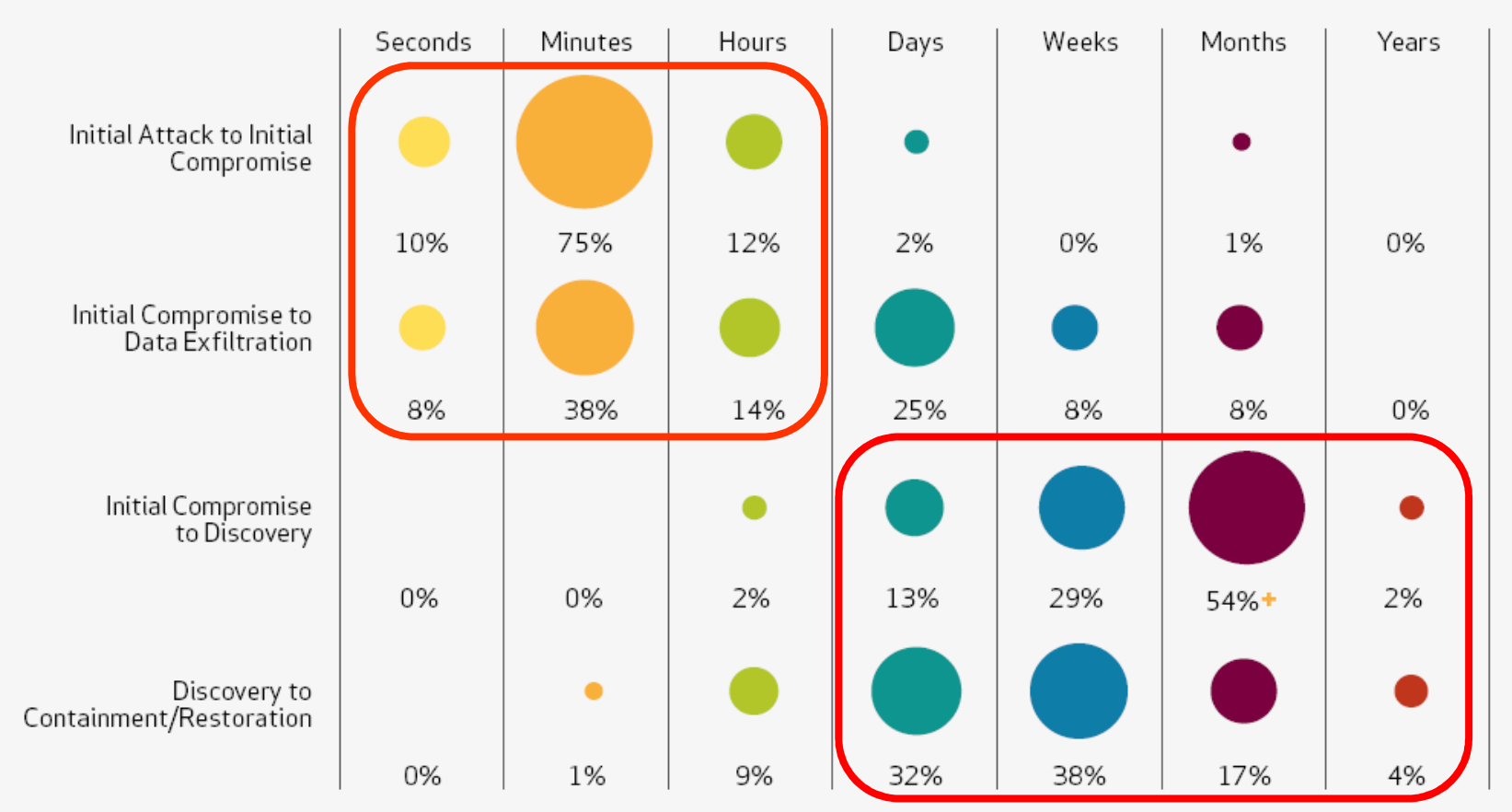
…to logical "perimeter" approach to security—focusing on the data and where it resides

- 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



http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z038

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 = apprx 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 USD[1]
average cost of a data breach

$194 USD[1]
Average cost per Compromised record

28,349[1]
average number of breached records per incident

96%[2]
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.

Data Security Architect
"I need to understand where data is and how it is related to other data. I also need to identify sensitive data and how it is to be classified from a security perspective."

Corp Compliance Officer
"We have to comply with regulatory and industry mandates and must protect the organization from negative external visibility resulting from failed audits and non-compliance."

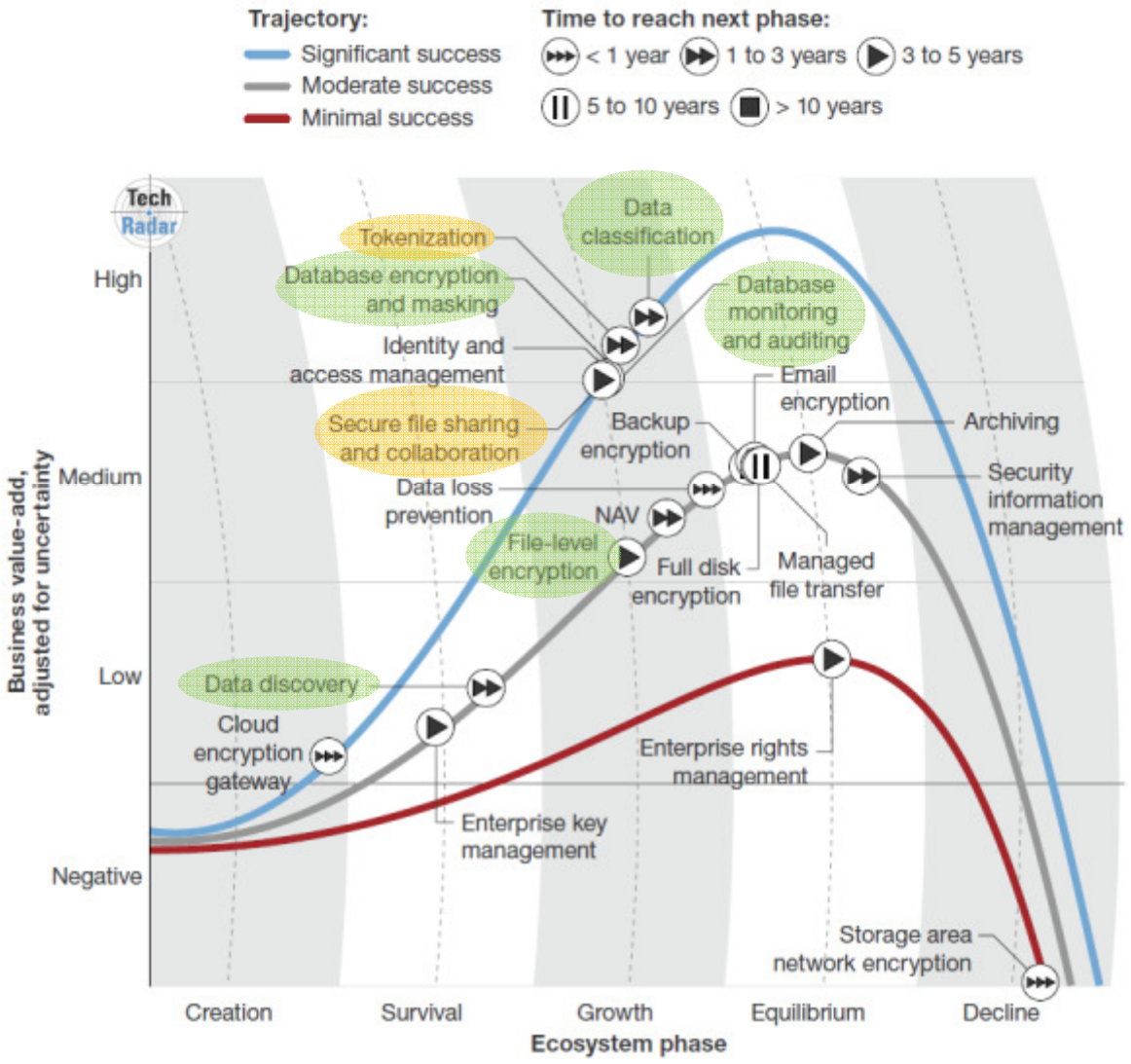
Auditor
"I need 100% visibility and transparency into the who, what, where, why and how of what's been happening with the data."

Chief Security Office
"I need tools that help me interpret and implement security policies into IT deliverables. I also need better ways to manage security and be alerted of potential threats before a breach occurs."

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?

Data at Rest

Discovery
Classification

Masking
Encryption

Configuration Data

Vulnerability
Assessment

Entitlements Reporting

Data in Motion

Activity
Monitoring

Blocking
Quarantine

Dynamic Data
Masking

Where is the sensitive data?

How to protect sensitive data?

How to secure the repository?

Who should have access?

What is actually happening?

How to prevent unauthorized activities?

How to protect sensitive data to reduce risk?

Security Policies

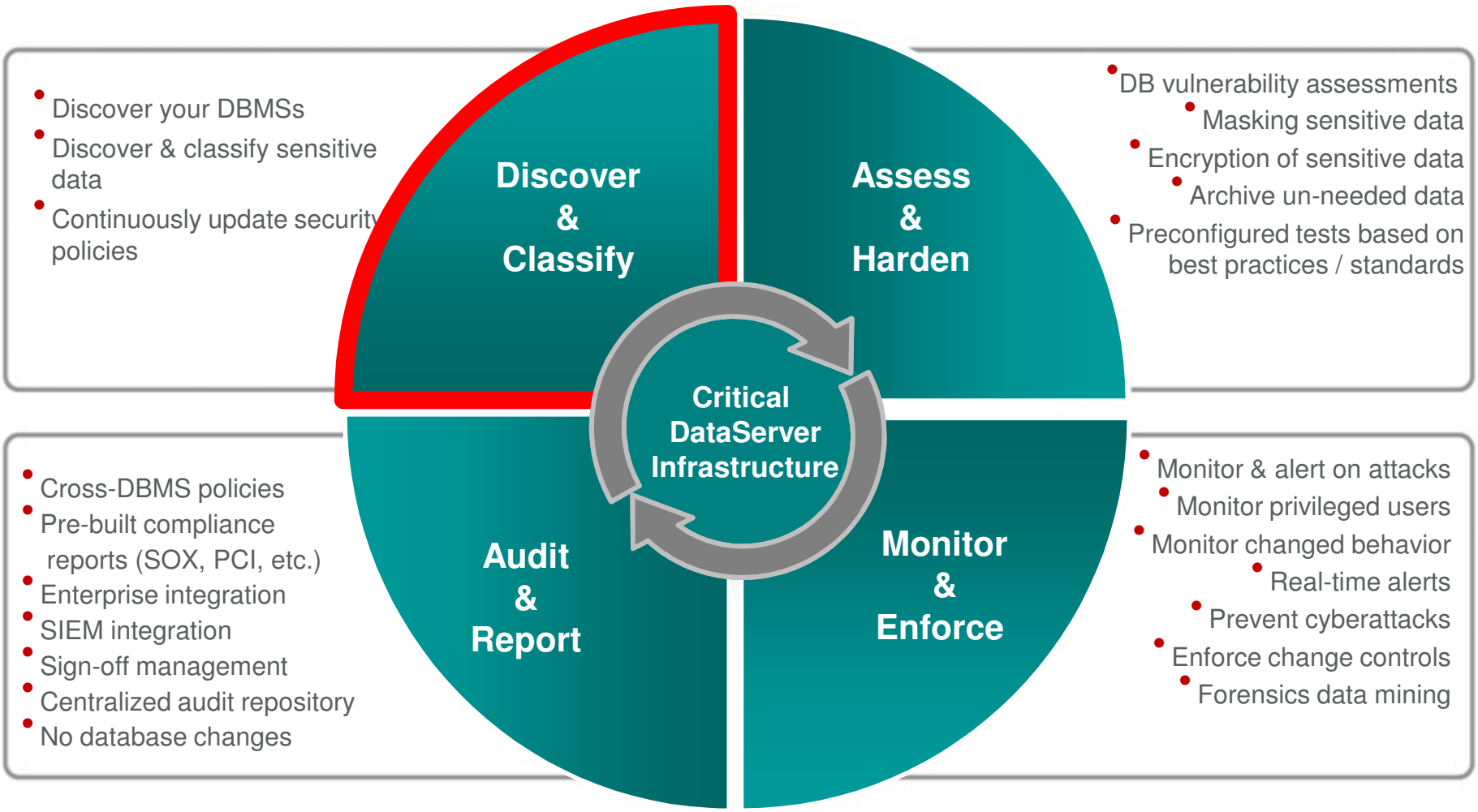
Dormant Data

Security Alerts / Enforcement

Dormant Entitlements

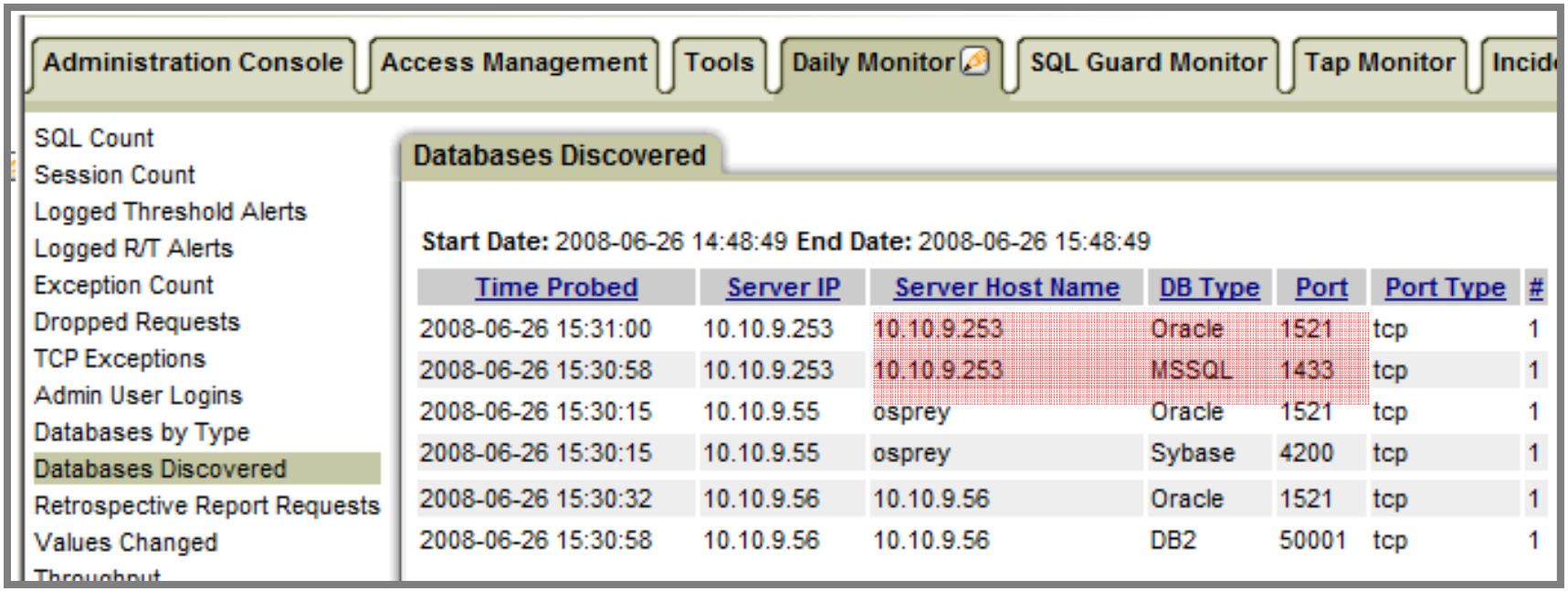
Compliance Reporting

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



Sensitive Data Discovery

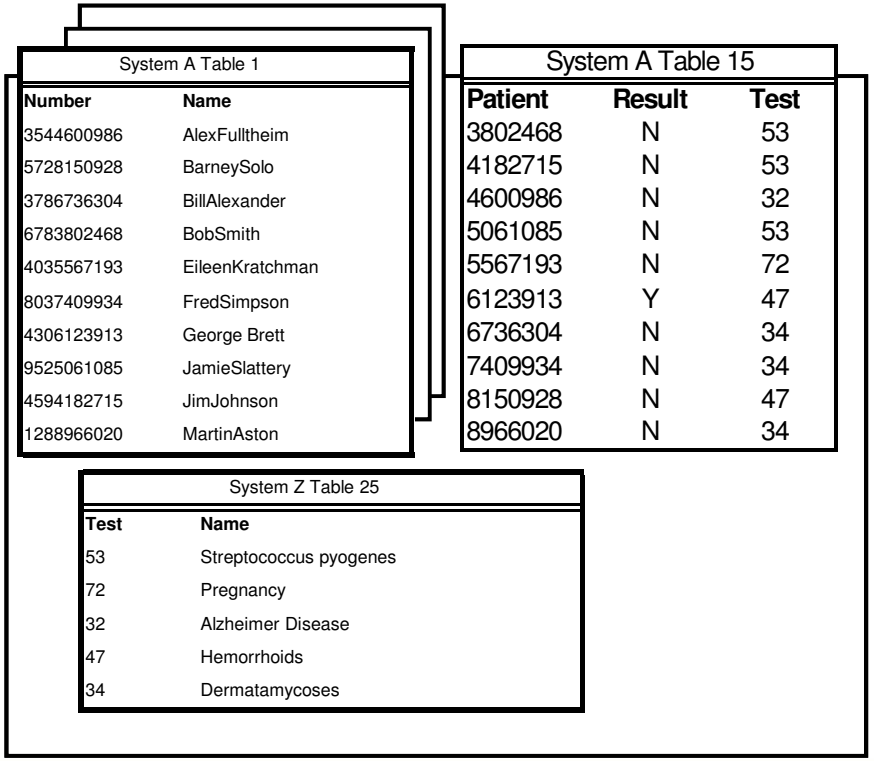
The Problem: Finding Sensitive Data can be difficult:

- 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

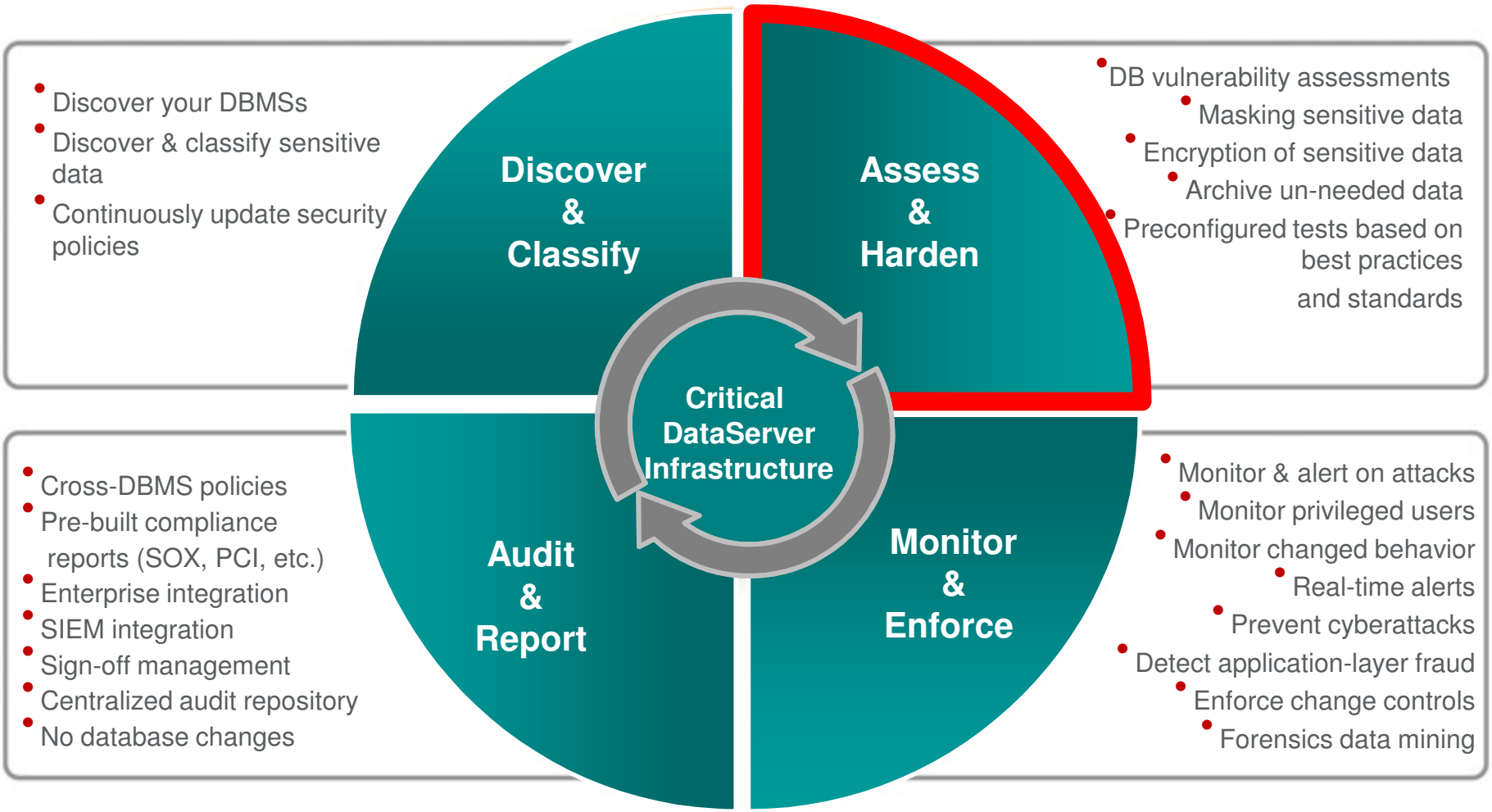
The Solution:

- 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



Address the Full Data Protection Lifecycle



Vulnerability Assessment

Based on best practices

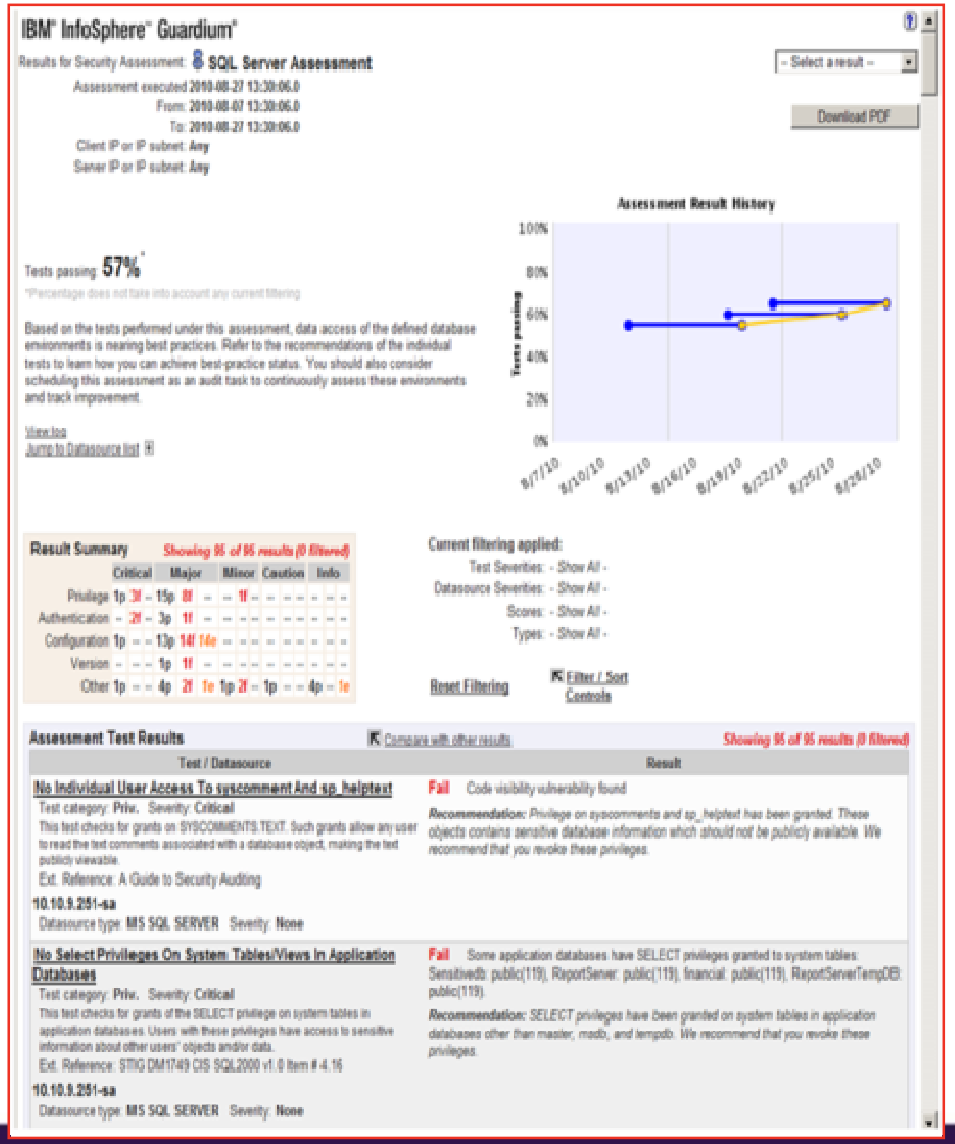
- Cost effectively improve the security of data servers by conducting automated database vulnerability assessment tests
  - Packaged tests to detect vulnerabilities including inappropriate privileges, grants, default accounts and passwords, security exposures, patches, etc.
  - Capabilities enabling 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

Prioritized Breakdown

Detailed Test Results



Result History

Filters and Sort Controls

Detailed Remediation Suggestions

Eliminate inappropriate privileges

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Priv.	Access To The UTL_FILE Package is restricted	ORACLE: Oracle EE - Joe	Fail	Major	Found Exec UTL_FILE privilege granted to public *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.*
Conf.	LOG_ARCHIVE_DUPLEX_DEST Set	ORACLE: Oracle EE - Joe	Fail	Major	Parameter: 'LOG_ARCHIVE_DUPLEX_DEST' is not set. *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.*
Conf.	MAX_ENABLED_ROLES is not greater than 30	ORACLE: Oracle EE - Joe	Fail	Major	Parameter: 'MAX_ENABLED_ROLES' with a value of '150' has been obsoleted for version 10.2. *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)*
Priv.	No 'Catalog' Role Assignments	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. *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'.*
Priv.	No Authority To Create Libraries	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. *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.*
Priv.	No Roles With The Admin Option	ORACLE: Oracle EE - Joe	Fail	Major	Found roles granted WITH ADMIN option *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*

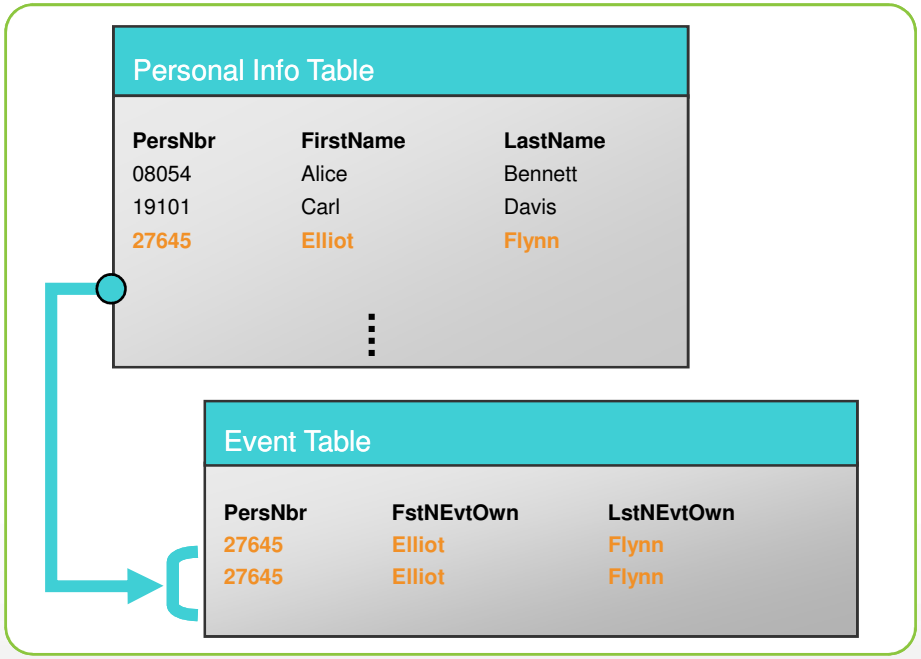
Sensitive Data Masking

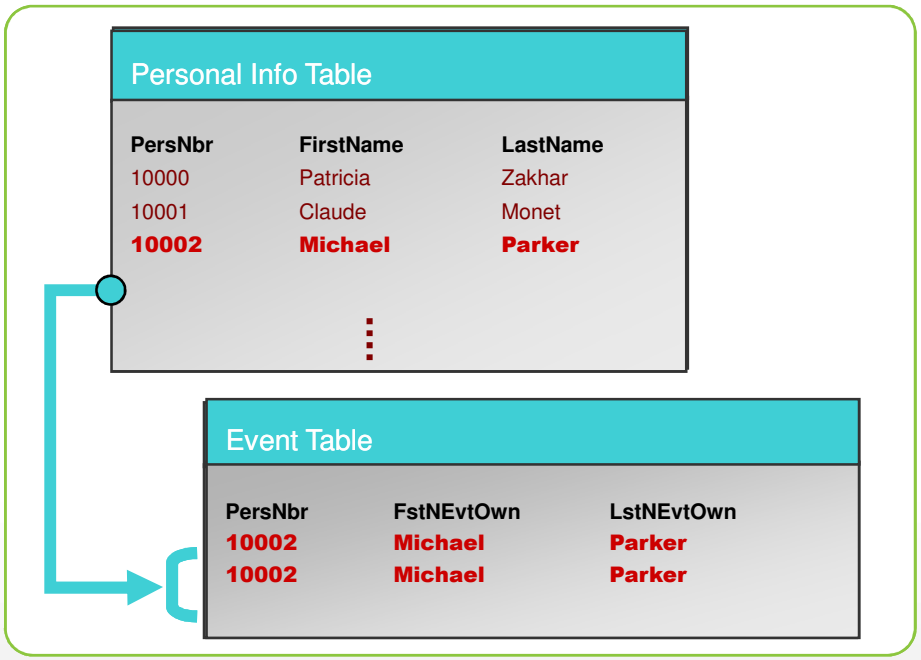
Masked or transformed data must be appropriate to the context:

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

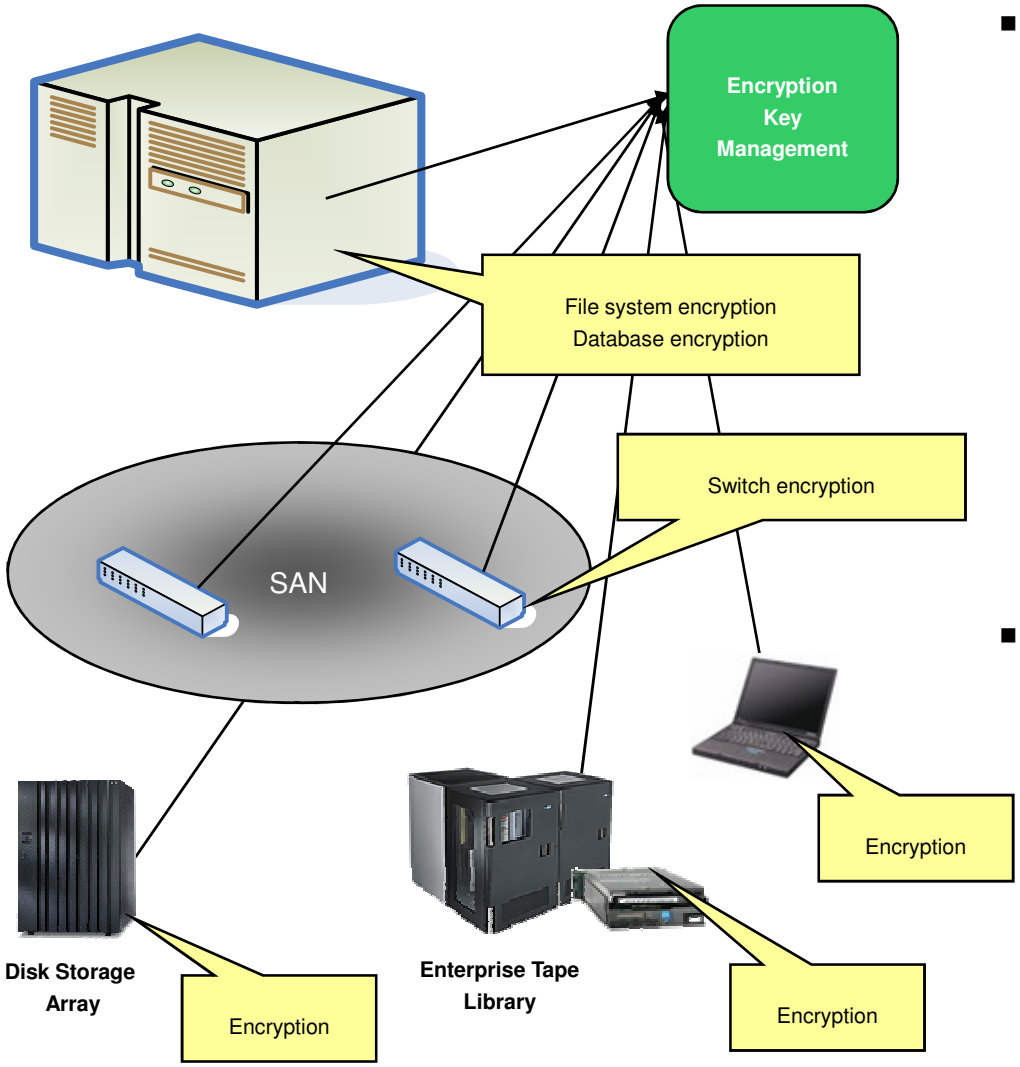
A comprehensive set of data masking techniques to transform or de-identify data, including:

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



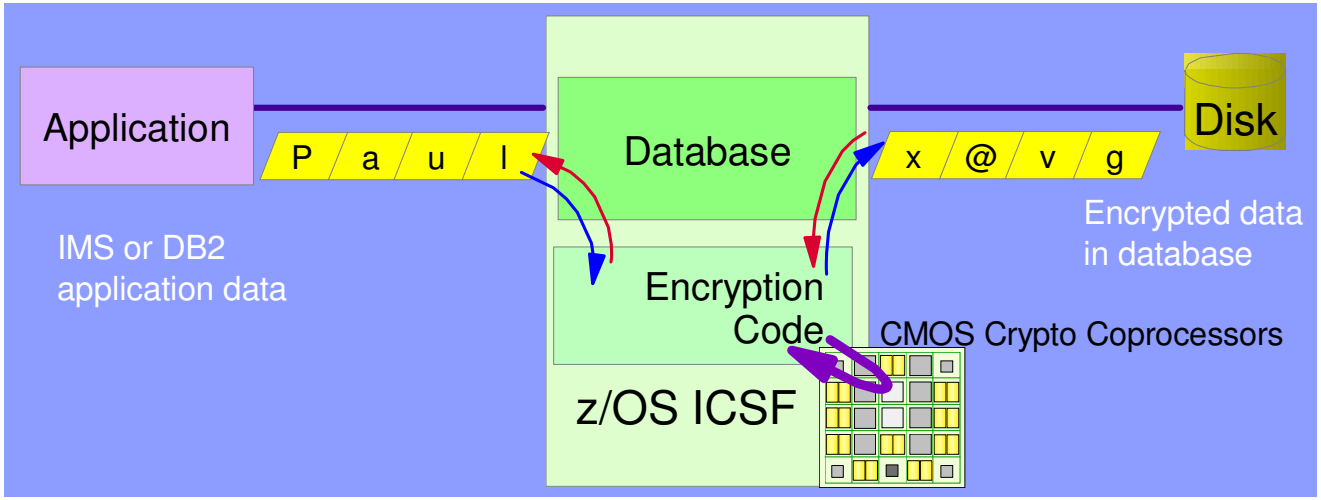


Encryption is everywhere – but where and how makes a difference



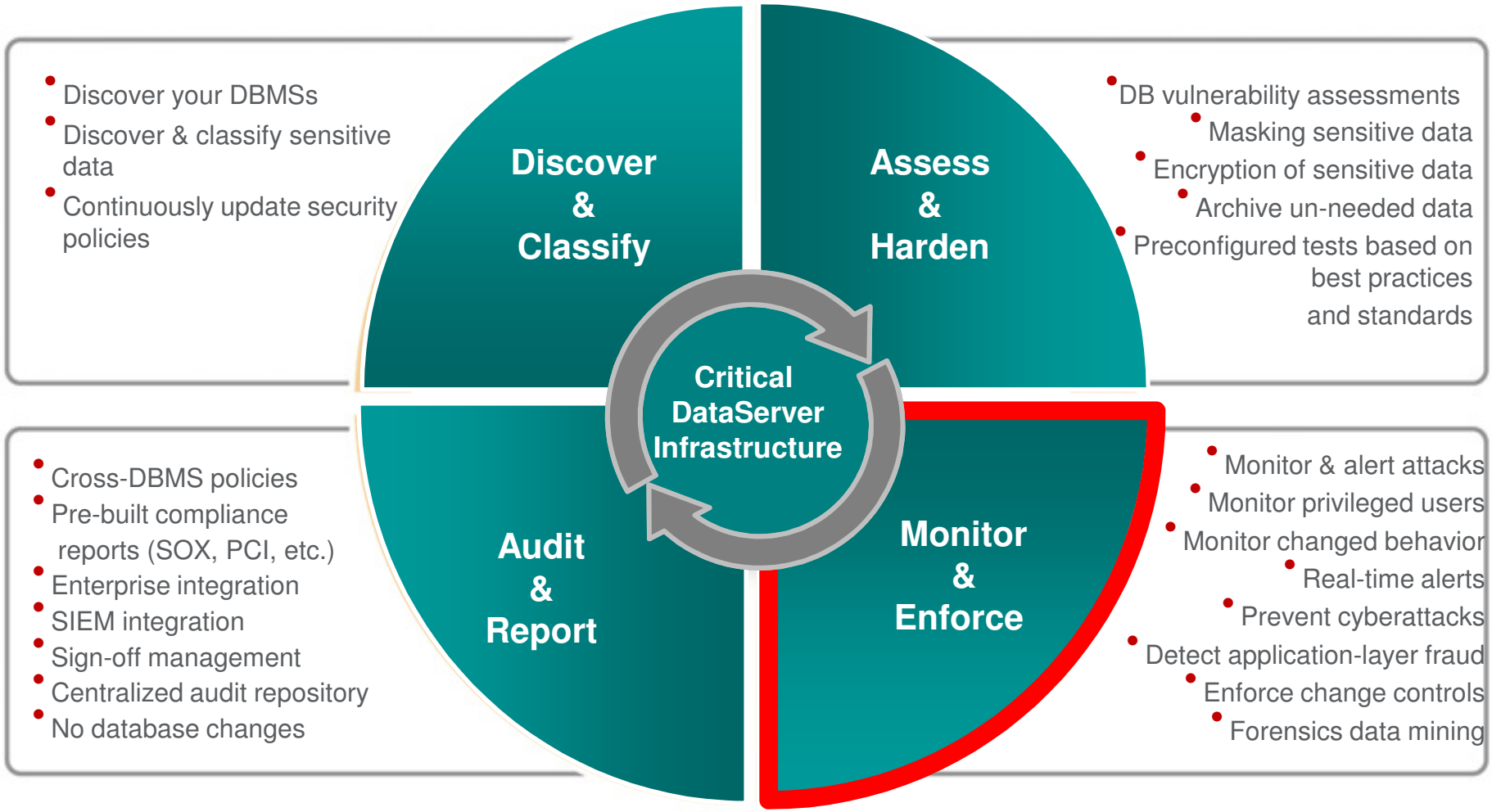
- **Encryption choices – why should encryption be built into storage**
  - Performance – cryptography can be computationally intensive
  - Efficiency - encrypted data is not able to be compressed or de-duplicated
  - Security - Data in transit should use temporary keys, data at rest should have long 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

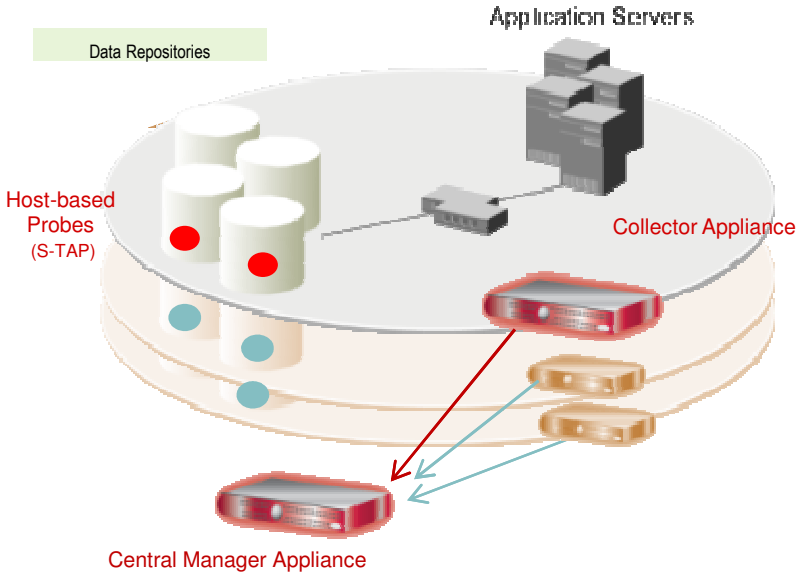


Data Activity Monitoring

Activity Monitoring
Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users

Blocking & Masking
Data protection compliance automation

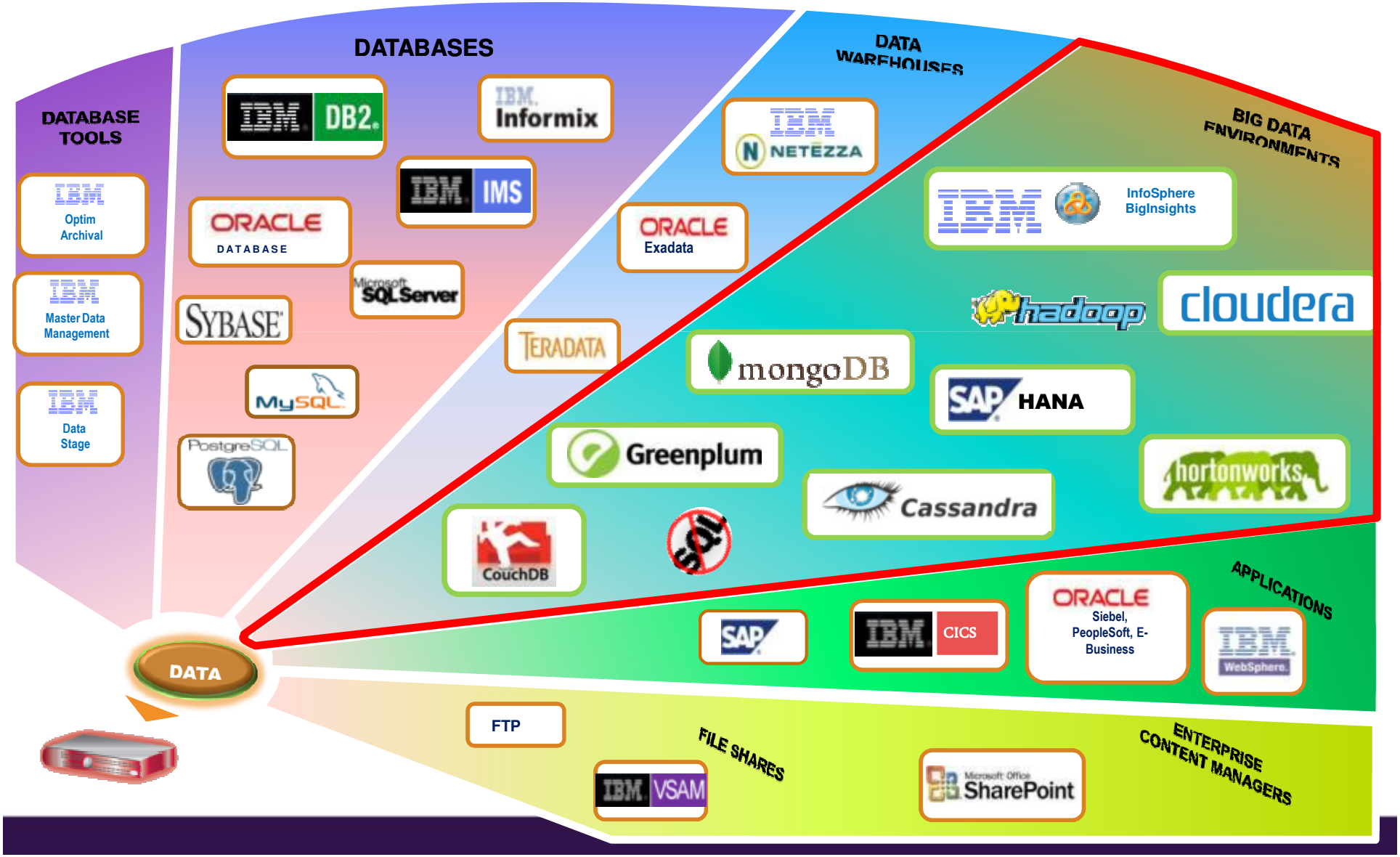
Vulnerability Assessment
Database infrastructure scanning for missing patches, mis-configured privileges and other vulnerabilities



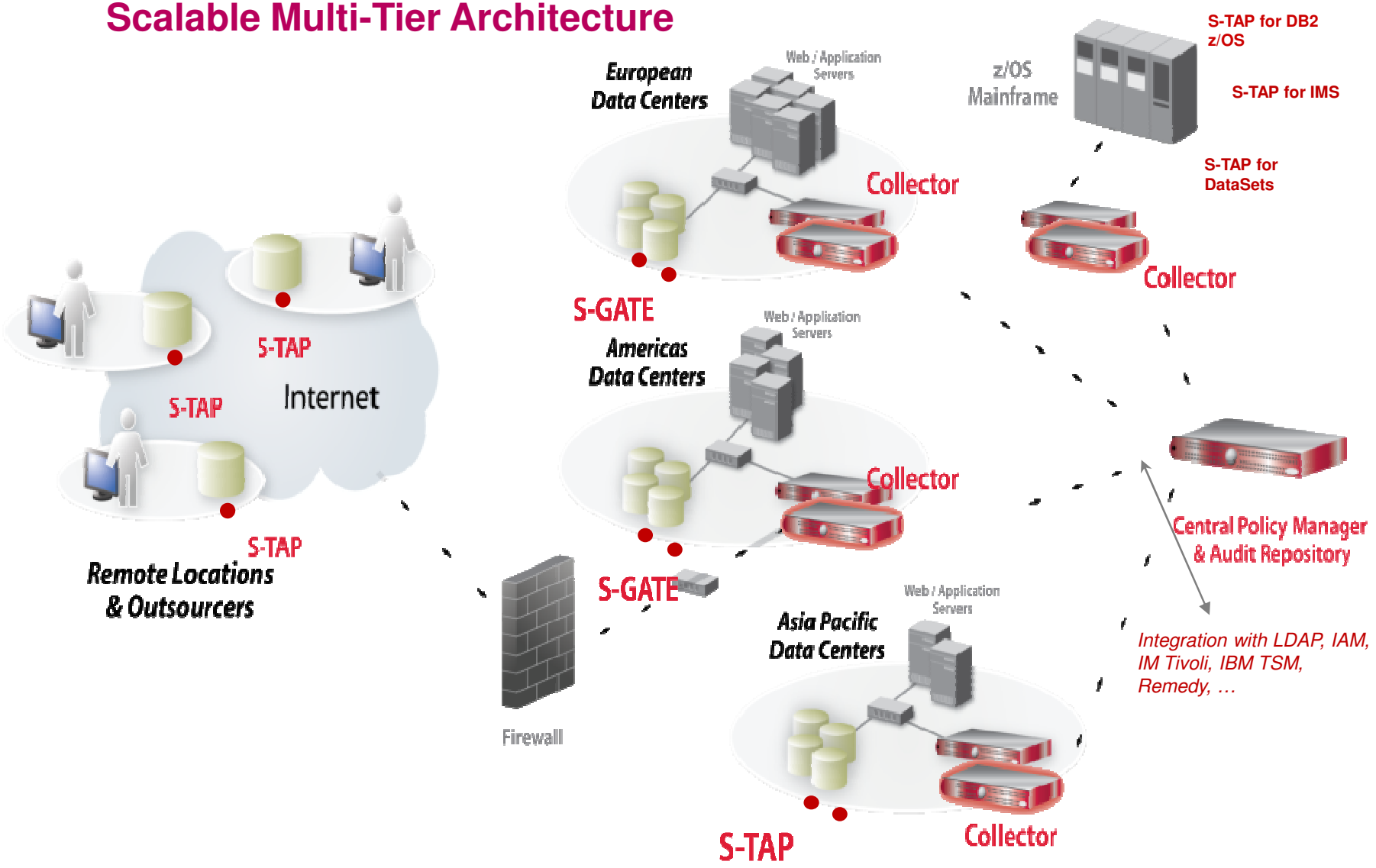
Key Characteristics

- 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

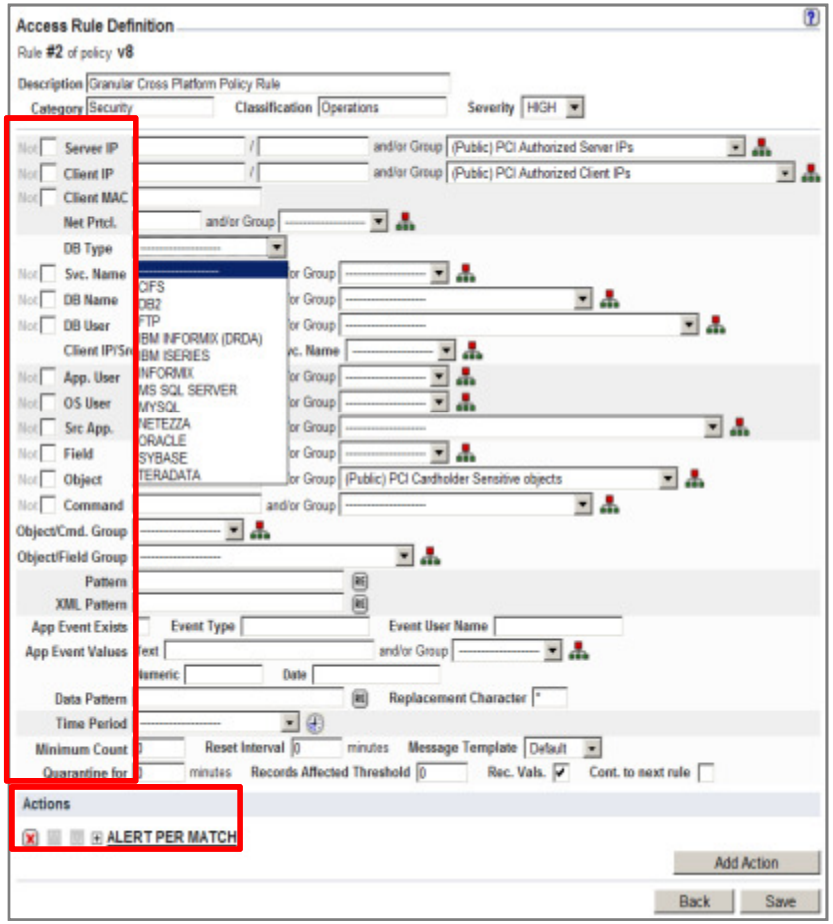


Cross-platform policies and auditing across enterprise

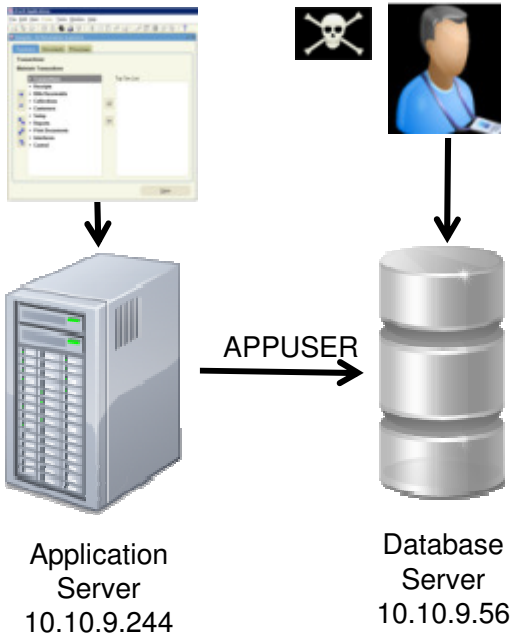
Unified cross-platform policies easily defined

Responsive actions defined within policies

Single audit repository enables enterprise-wide compliance reporting and analytics



A simple policy example: *Application bypass*



Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

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

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

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

Not ☐ DB Name

Not ☐ DB User: APPUSER

Field Name

Object: EmployeeTable

Command: Select

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

Continue to next Rule ☐ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

☒ Notification Type MAIL Mail User marc_gamache@guardium.com

Sample Alert

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

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

Identify inappropriate use by authorized users

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

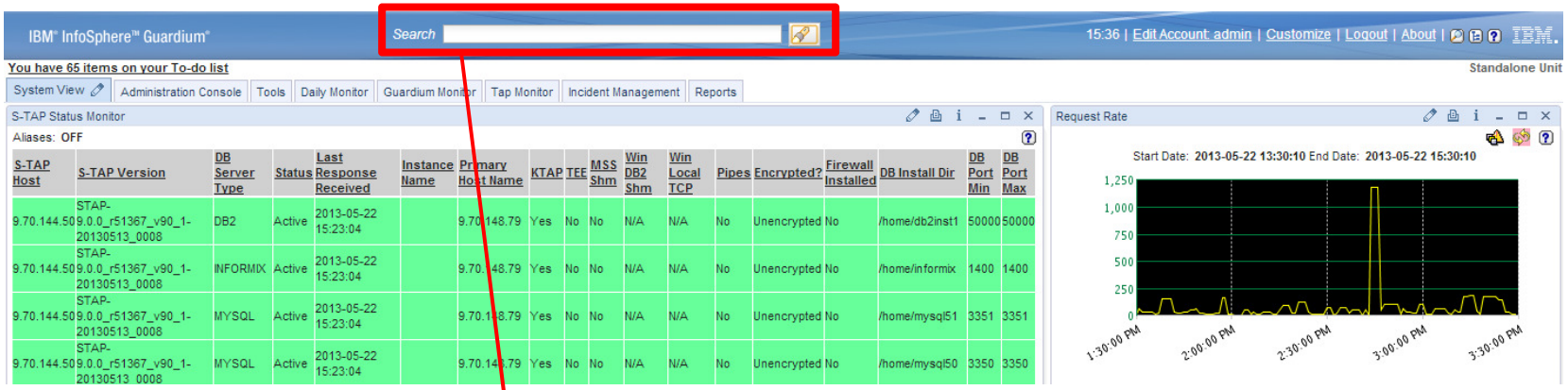
DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

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)

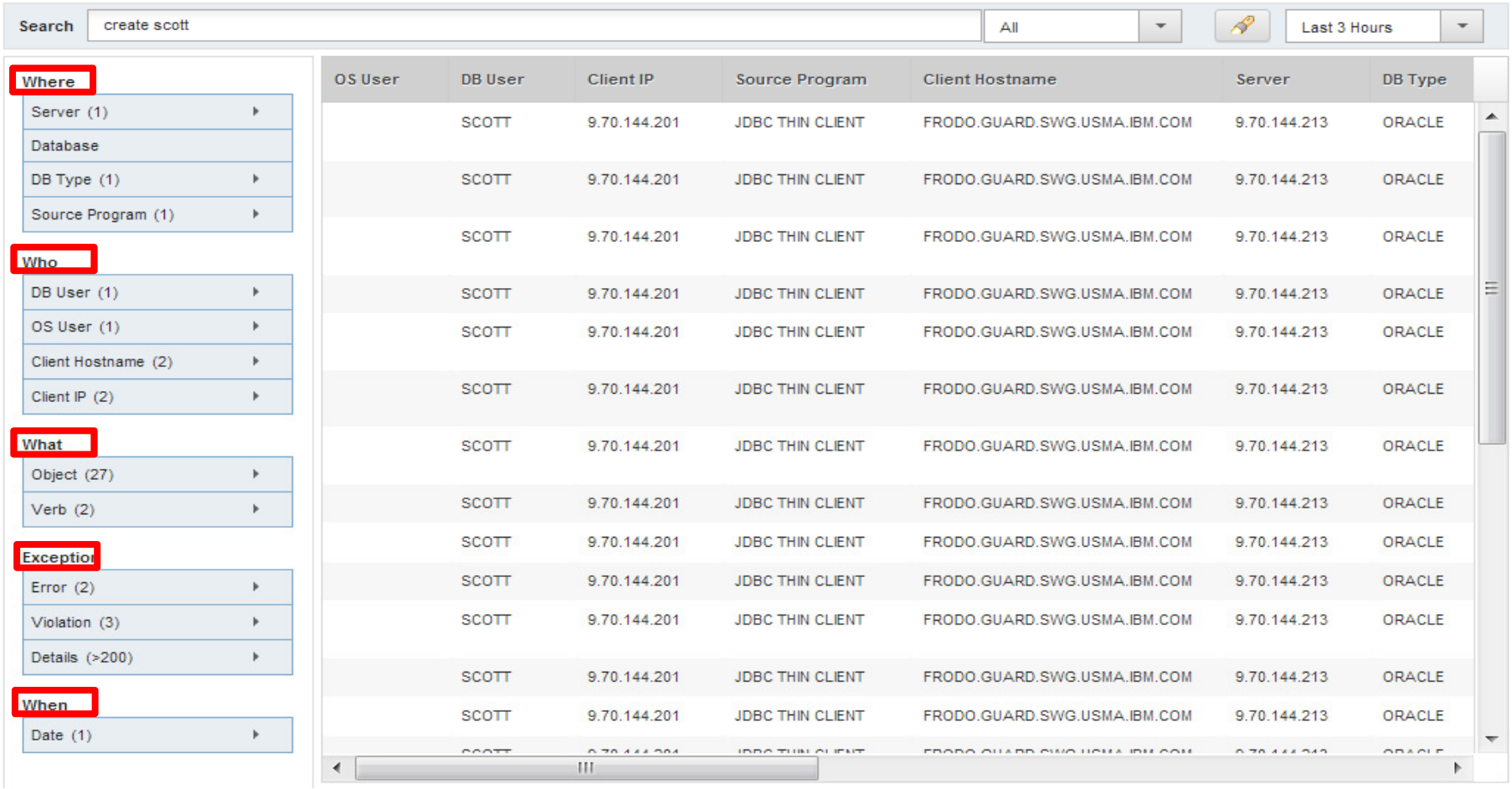


S-TAP Host	S-TAP Version	DB Server Type	Status	Last Response Received	Instance Name	Primary Host Name	KTAP	TEE	MSS Shm	Win DB2 Shm	Win Local TCP	Pipes	Encrypted?	Firewall Installed	DB Install Dir	DB Port Min	DB Port Max
9.70.144.50	STAP-9.0.0_r51367_v90_1-20130513_0008	DB2	Active	2013-05-22 15:23:04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

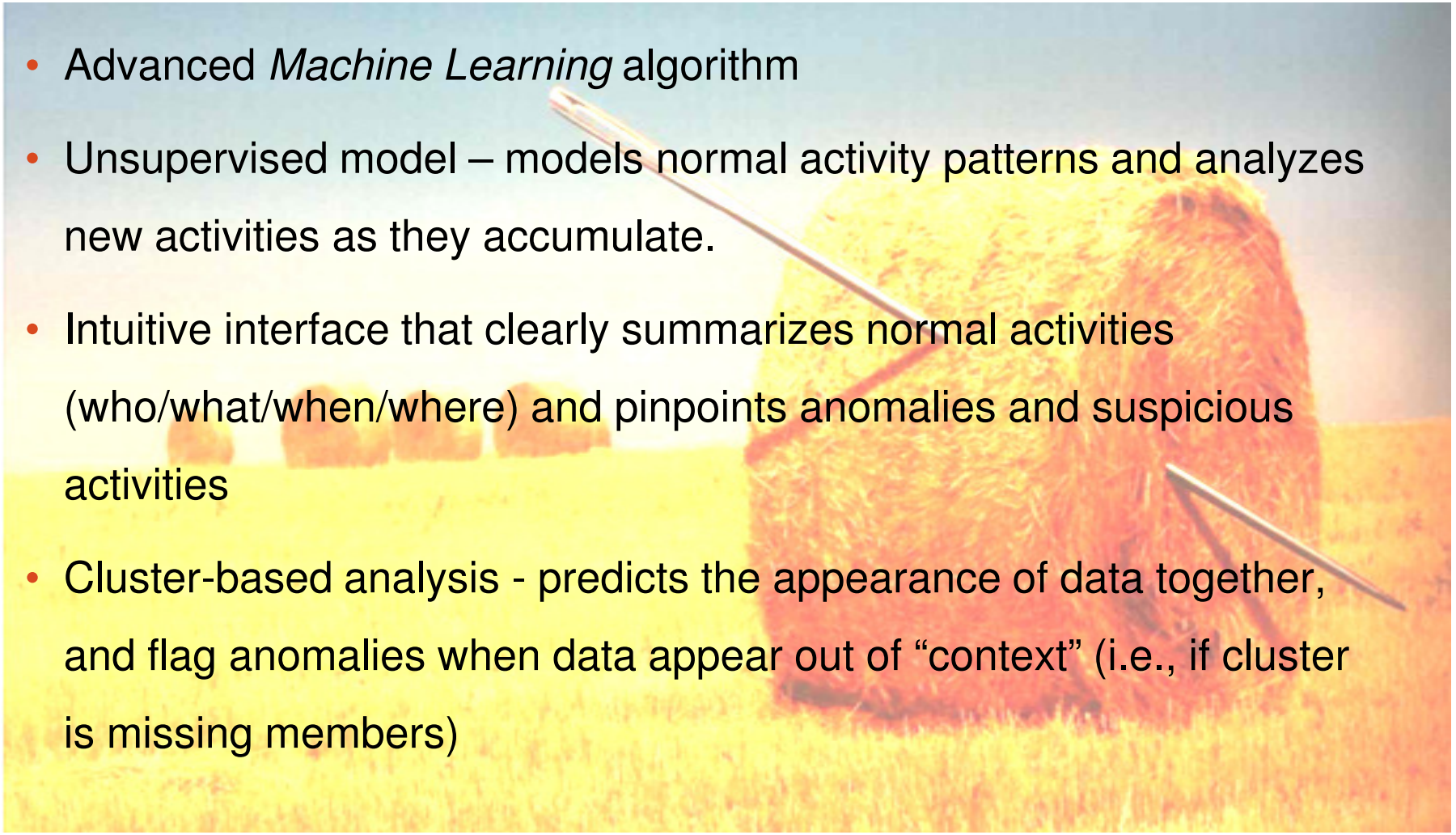
For manually entered search terms, the following rules apply:

- 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

Quick Search (cont)



Outliers – finding the needle in the security haystack



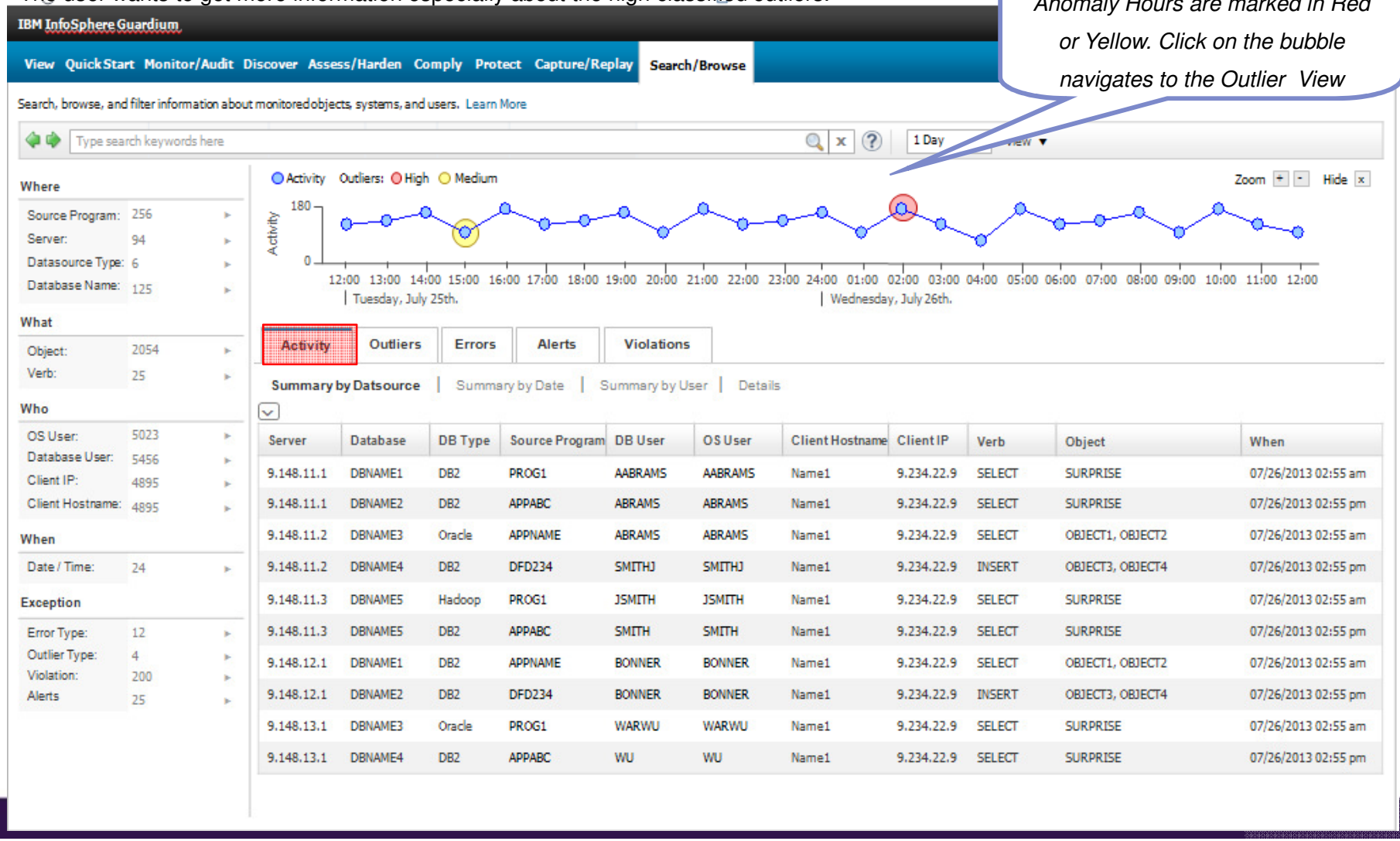
- Advanced *Machine Learning* algorithm
- Unsupervised model – models normal activity patterns and analyzes new activities as they accumulate.
- Intuitive interface that clearly summarizes normal activities (who/what/when/where) and pinpoints anomalies and suspicious activities
- Cluster-based analysis - 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.

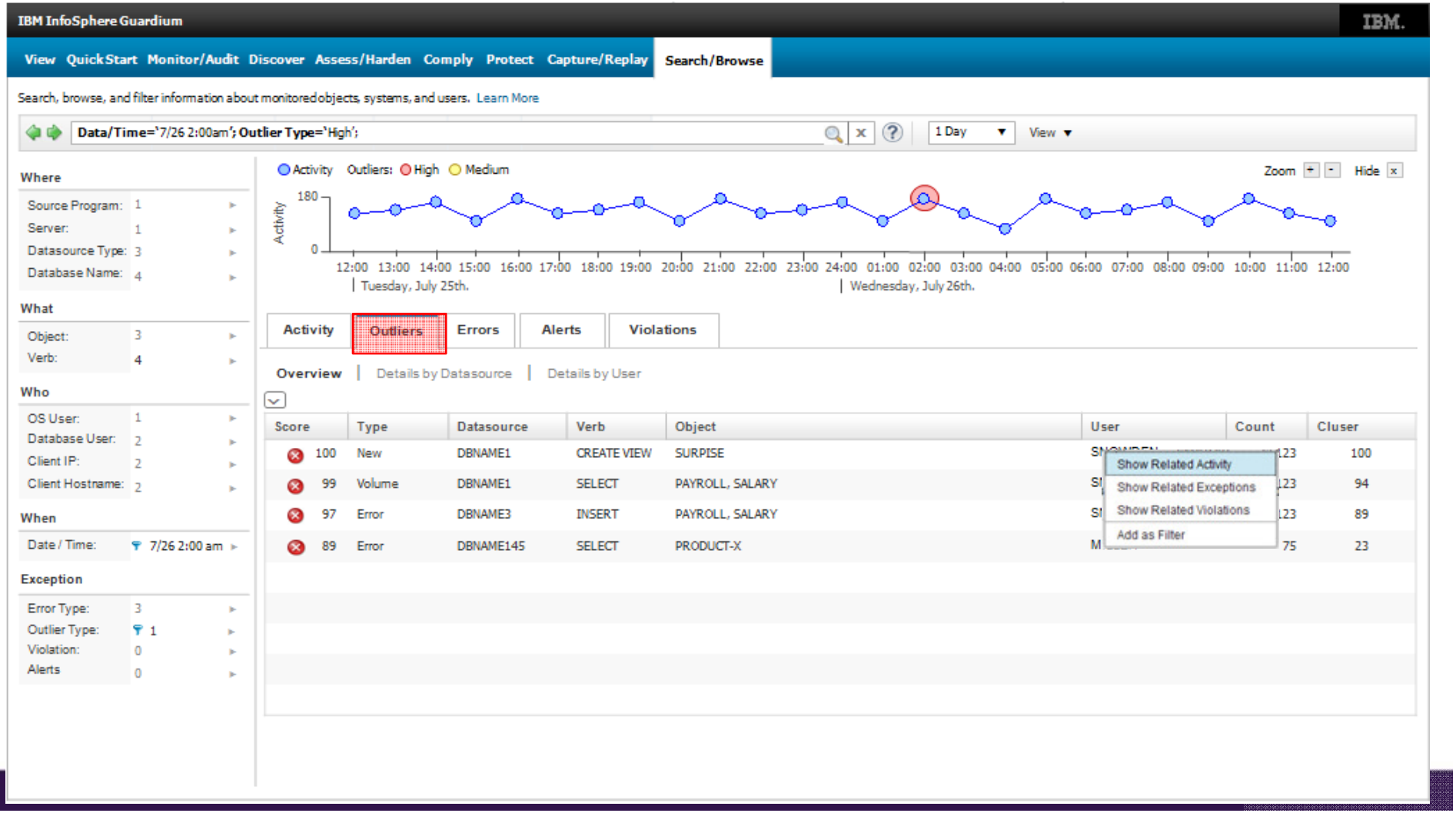


Outliers Details

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.



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

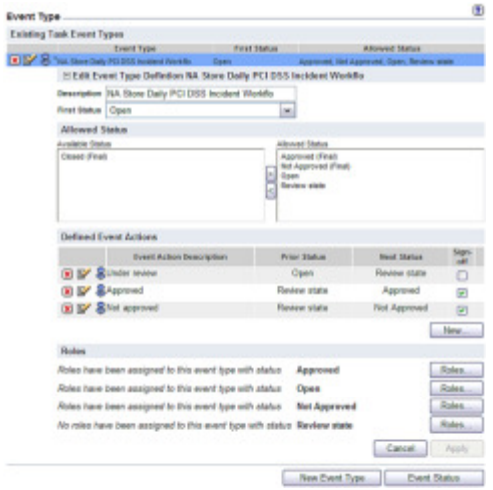
Automate oversight processes to ensure compliance and reduce operational costs

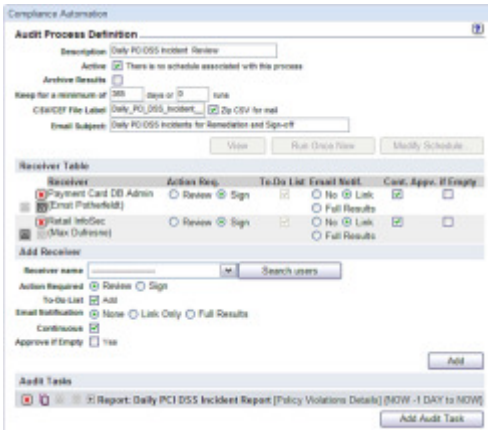
Easily create custom processes by specifying unique combination of workflow steps, actions and users

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

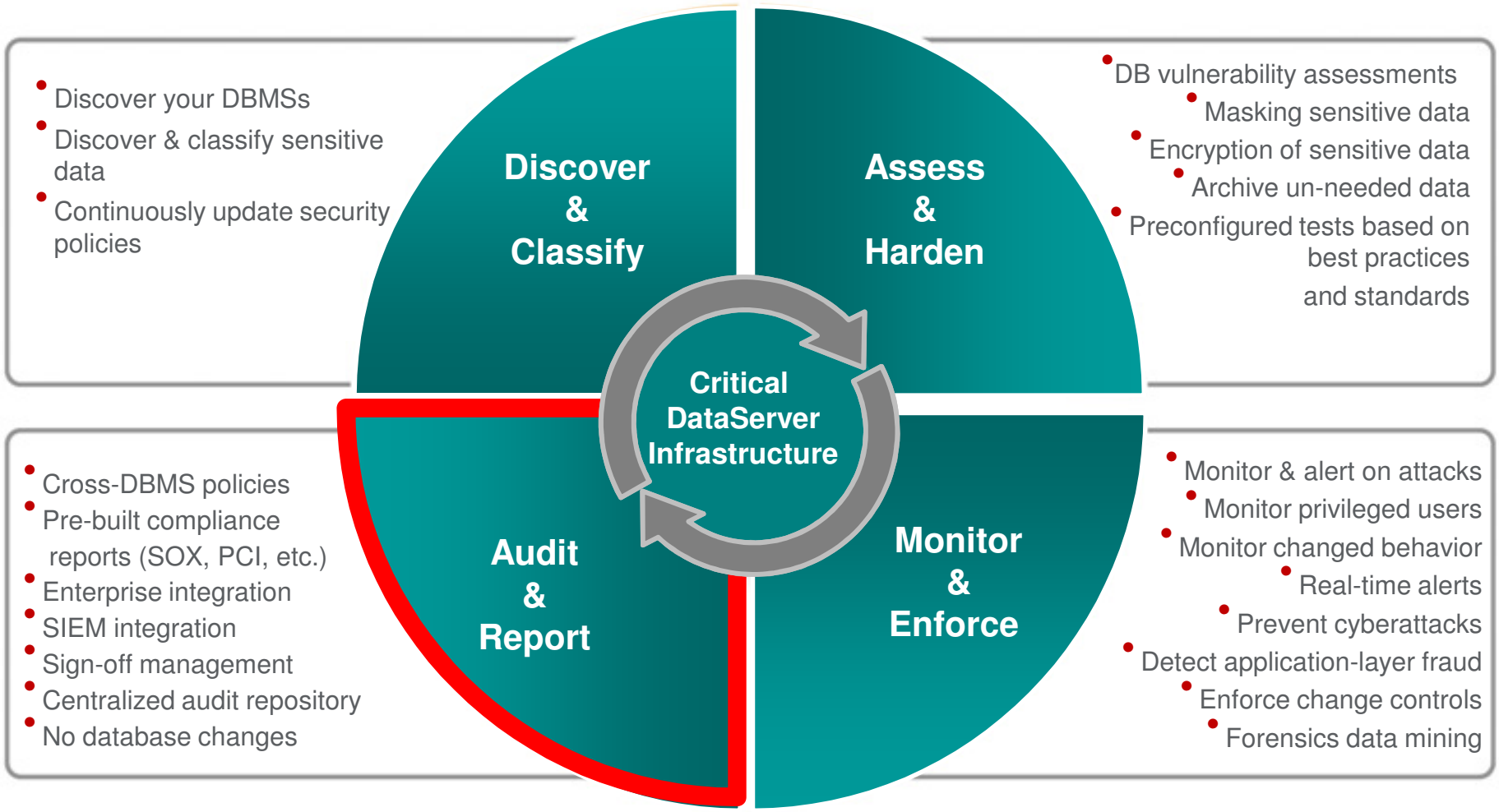
Supports automated execution of oversight processes on a report line item basis, maximizing efficiency without sacrificing security

- 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





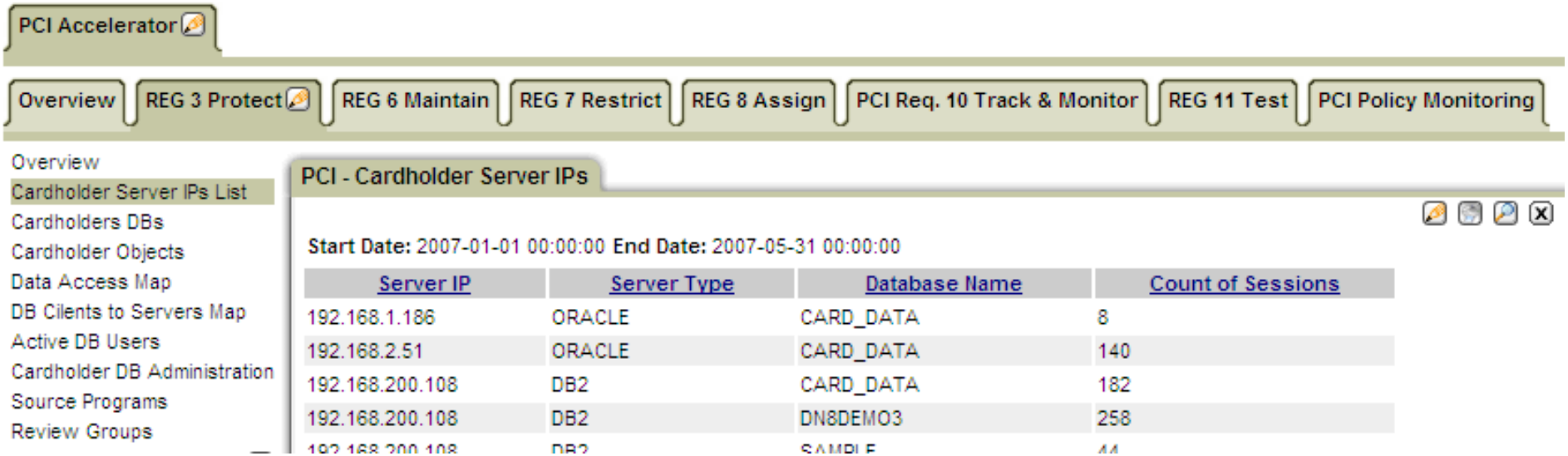
Address the Full Data Protection Lifecycle



Audit and Report

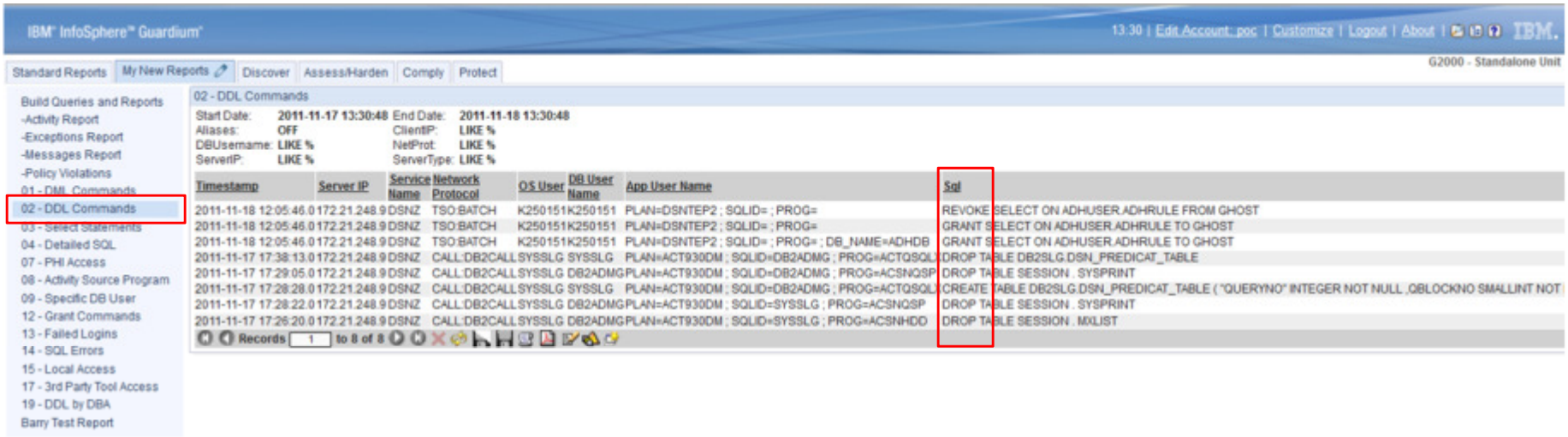
Custom and Pre-Built Compliance Reports

- 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.)



Reporting

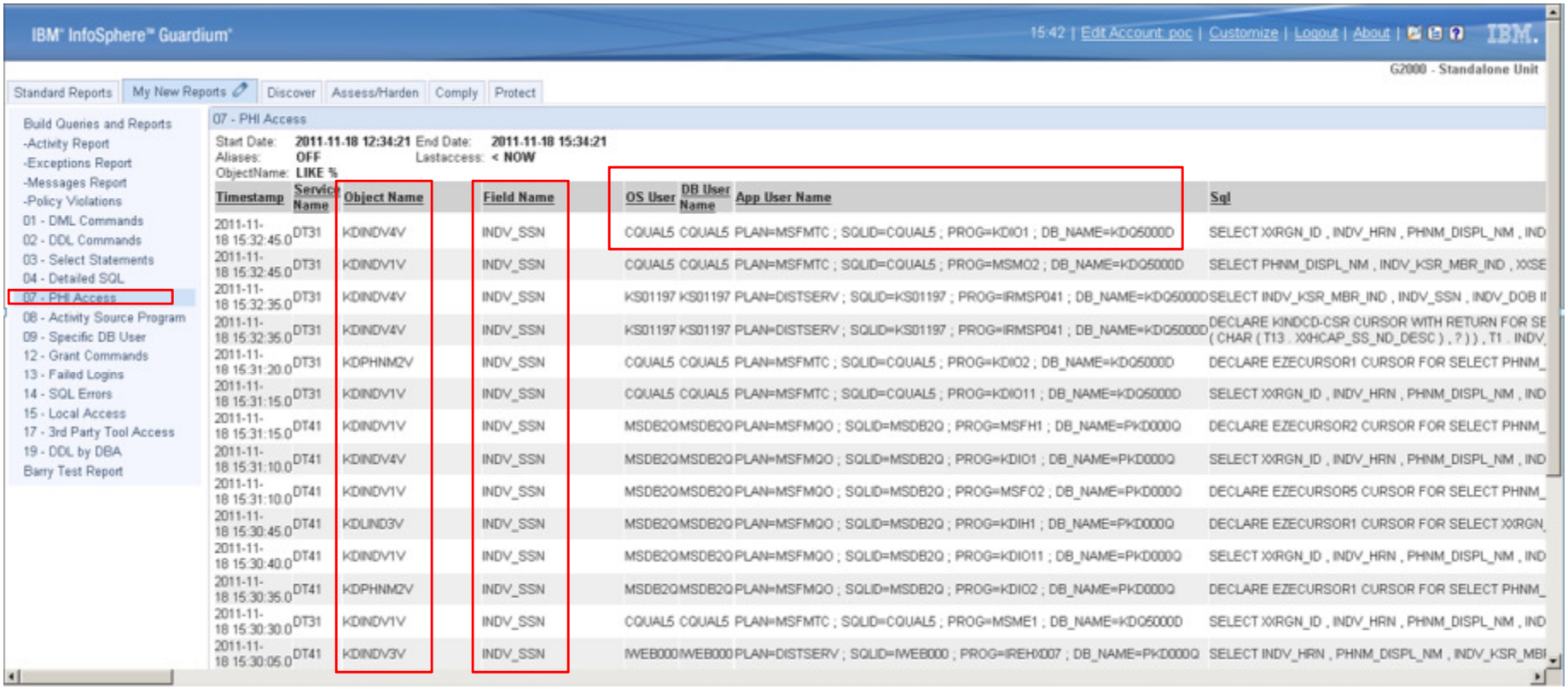
DDL and DCL



- Ability to Monitor Data Definition Language Commands
  - Create, Alter, Drop, etc.
- Ability to Monitor Data Control Language Commands
  - Grant, Revoke, etc.

Reporting

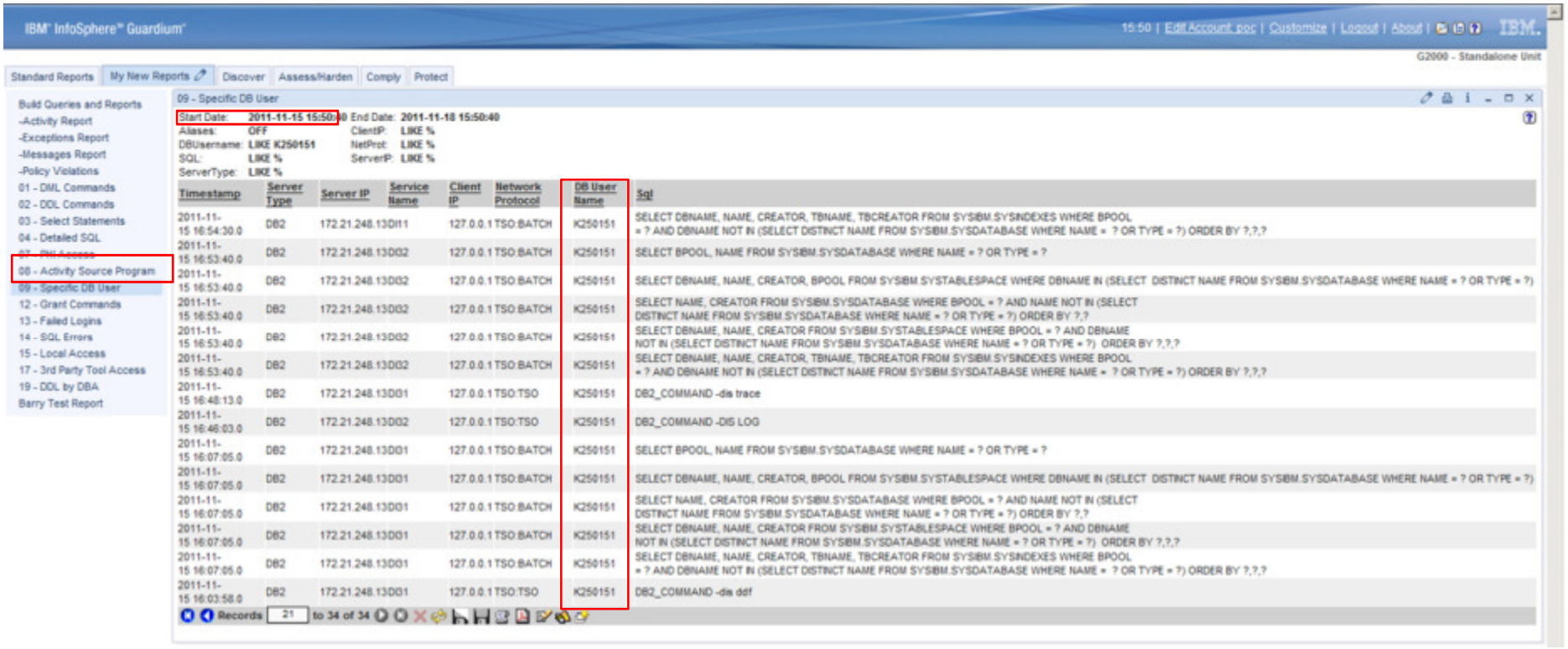
Sensitive Data Access



Ability to Monitor Access to Objects and Fields Containing Sensitive Data

Reporting

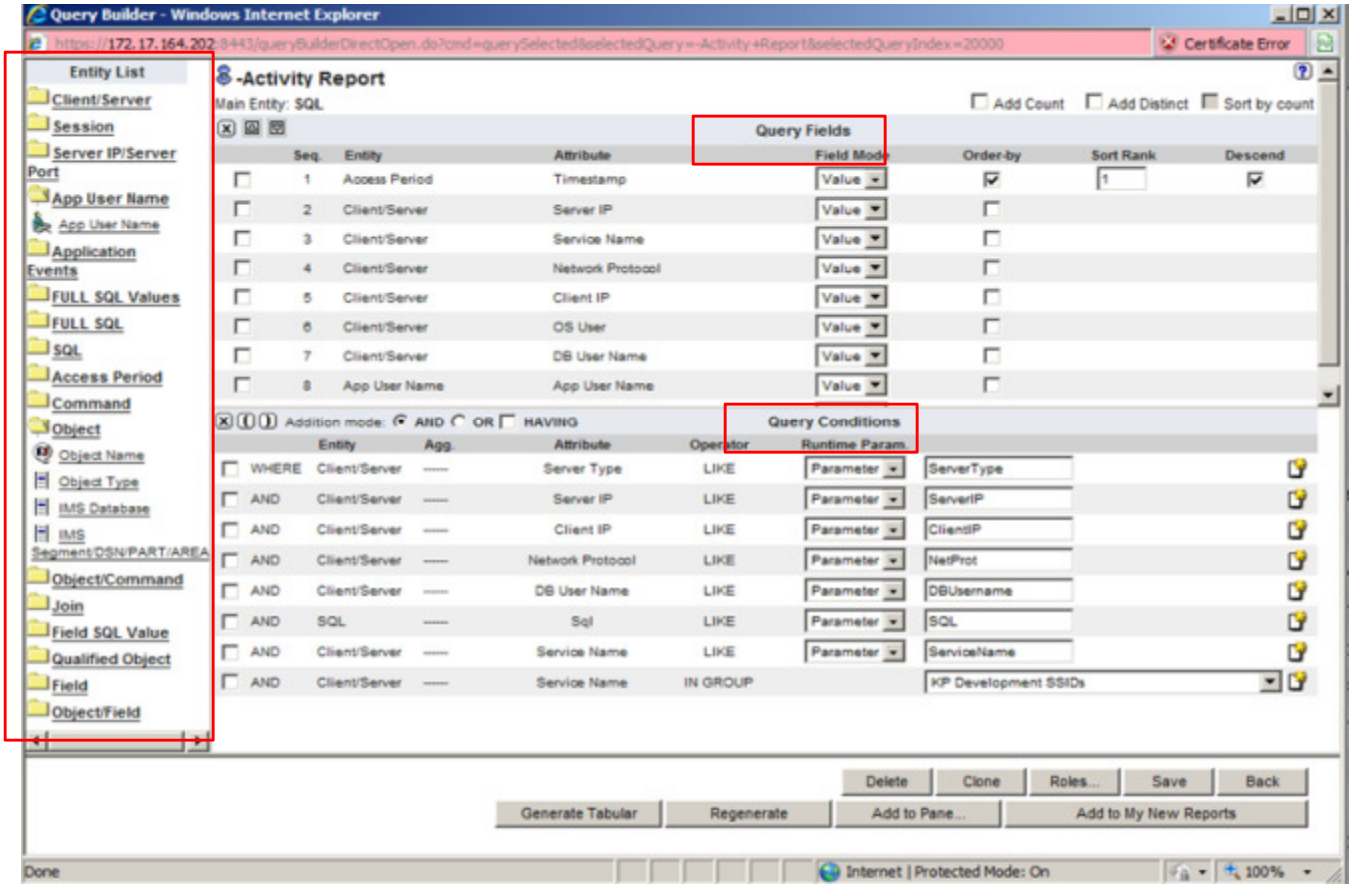
Specific User Activity



Ability to Report on a Specific User's Activity

Reporting

Custom Report Building



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/*
- *www.ibm.com/guardium*
- *www.ibm.com/bigdata/z*
- *www.infogovcommunity.com*


THINK
BIG

THINK

Z

Thank You