

Security Intelligence.
Think Integrated.

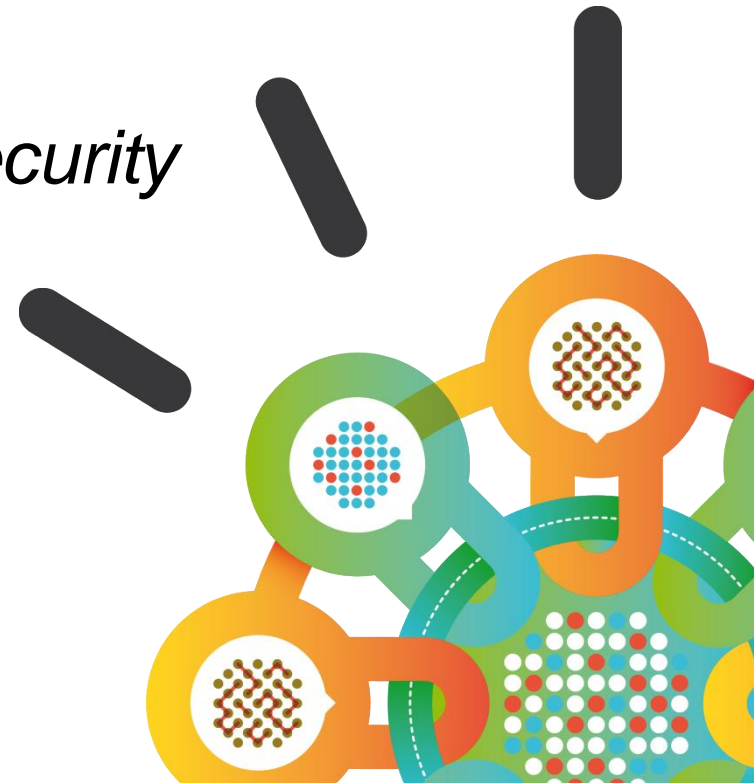
BIG DATA: Big Opportunity, Big Headaches

Protect your Big Data with data security

Kathryn Zeidenstein

Guardium Evangelist
IBM Security

May 19, 2015



The Opportunities from Big Data & Analytics are Infinite

98%
Cut in Storage Requirements

72%
Reduction in Fraudulent Claims

98%
Decrease time to analyze data

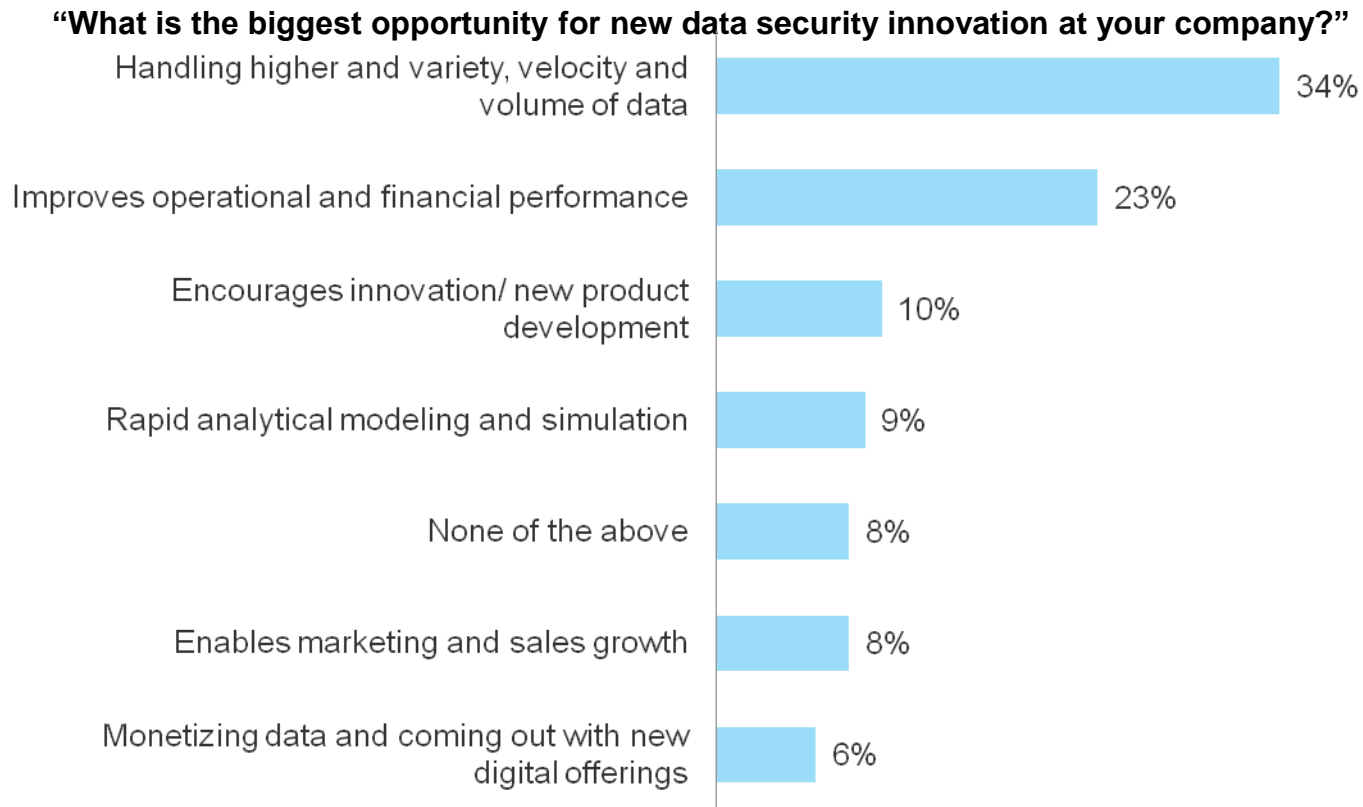
\$1M
Estimated Cash Savings

90%
Increased Transaction Capacity

40X
Analysis Performance Gain

60X
Faster Query Performance

Handling Higher Variety, Velocity and Volume Data as the Biggest Opportunity for Data Security



Base: 200 security decision makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

Organizations are Jumping into Big Data with Both Feet

- Departmental projects
- Rogue IT teams
- Using production data
- Loose user controls
- Impossible to audit



Big Data: Are You Ready for the Headaches?

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

2012

Relentless Use of Multiple Methods

800,000,000+ records were leaked, while the future shows no sign of change

2013

“Insane” Amounts of Records Breached

42% of CISOs claim the risk from external threats increased dramatically from prior years.

2014



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

A historical look at security incidents by attack type, time and impact, 2012 through 2014

Source: IBM X-Force Research and Development

Are You Ready for the Costs?

The average cost of a data breach increased

15%
in 2013

A single lost or stolen data record cost on average



\$145
in 2013

A single breach of sensitive personal data cost

\$3.5
million
in 2013



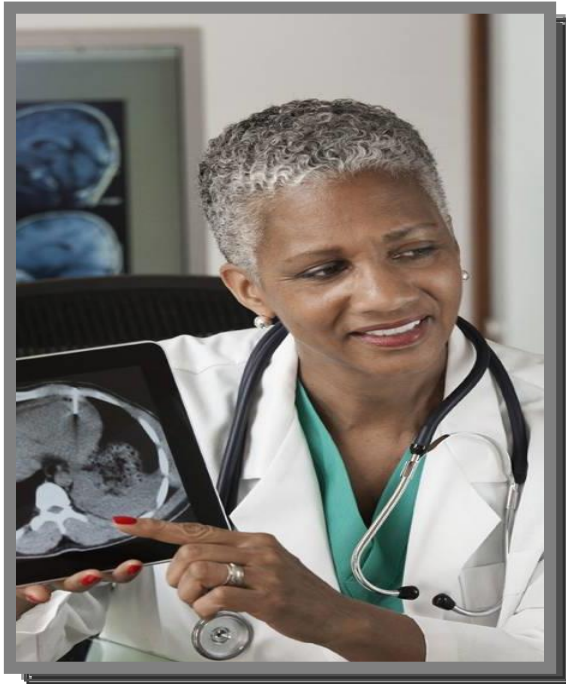
2014 Cost of Data Breach Study
From Ponemon Institute, sponsored by IBM



Compliance with Regulations ≠ Security



Sensitive Data is Common in Big Data Projects



Healthcare



Customer



Citizen

The Need for Data Security and Privacy in Big Data

**The same risks are magnified...
...and big data introduces new challenges**

Data Breach



- Avg cost per breach \$5M'
- It's not *if*, it's *when*

Brand Reputation



- \$100M+ impact to the business

New Users



- Data sharing and new user access

Attractive Target



- Data security hotspot for internal/external threat

Compliance



- Changing and new privacy legislation



Fewer Tools

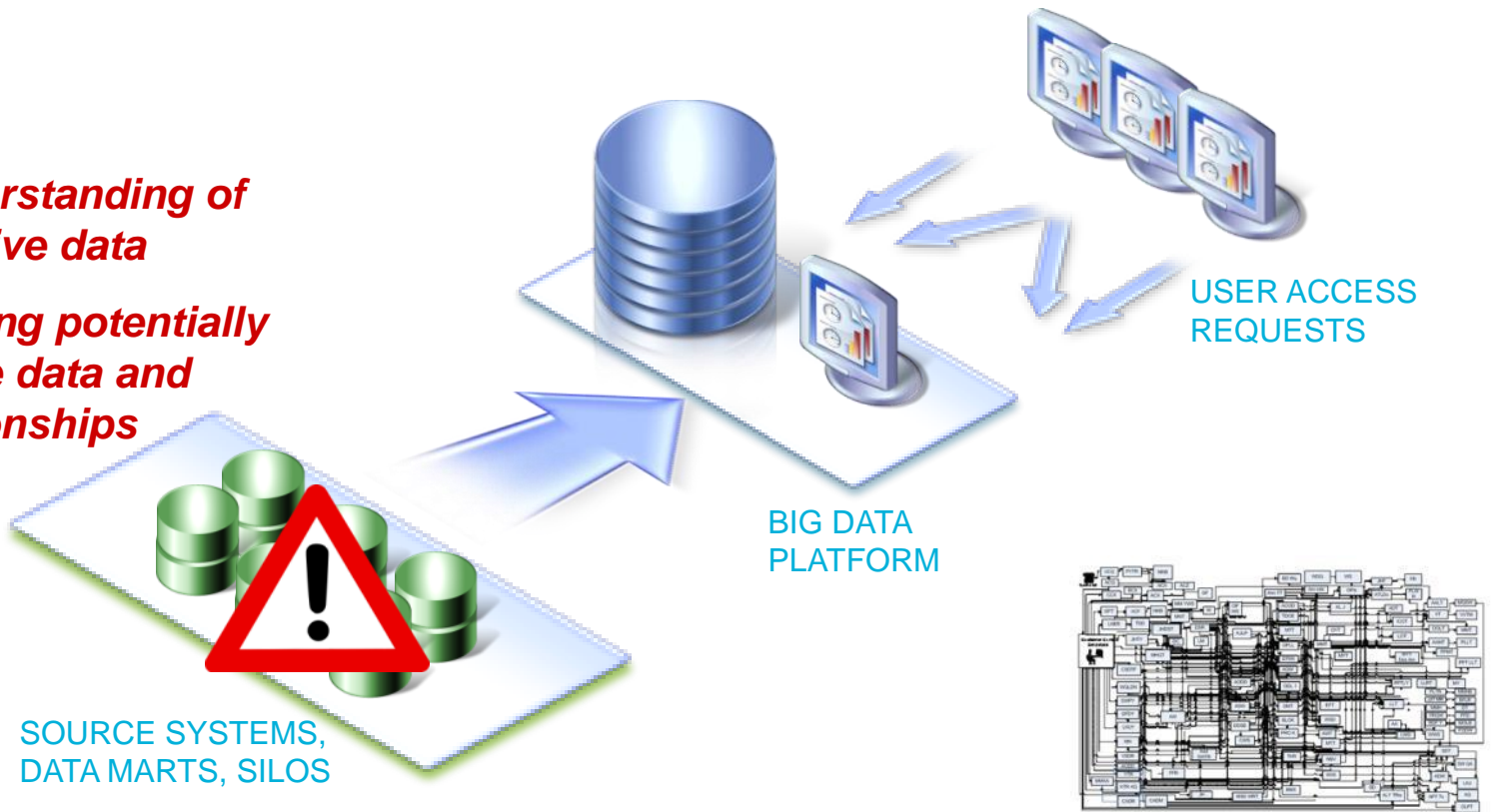


- Traditional tools no longer apply

Big Data Technology Considerations in Security and Privacy

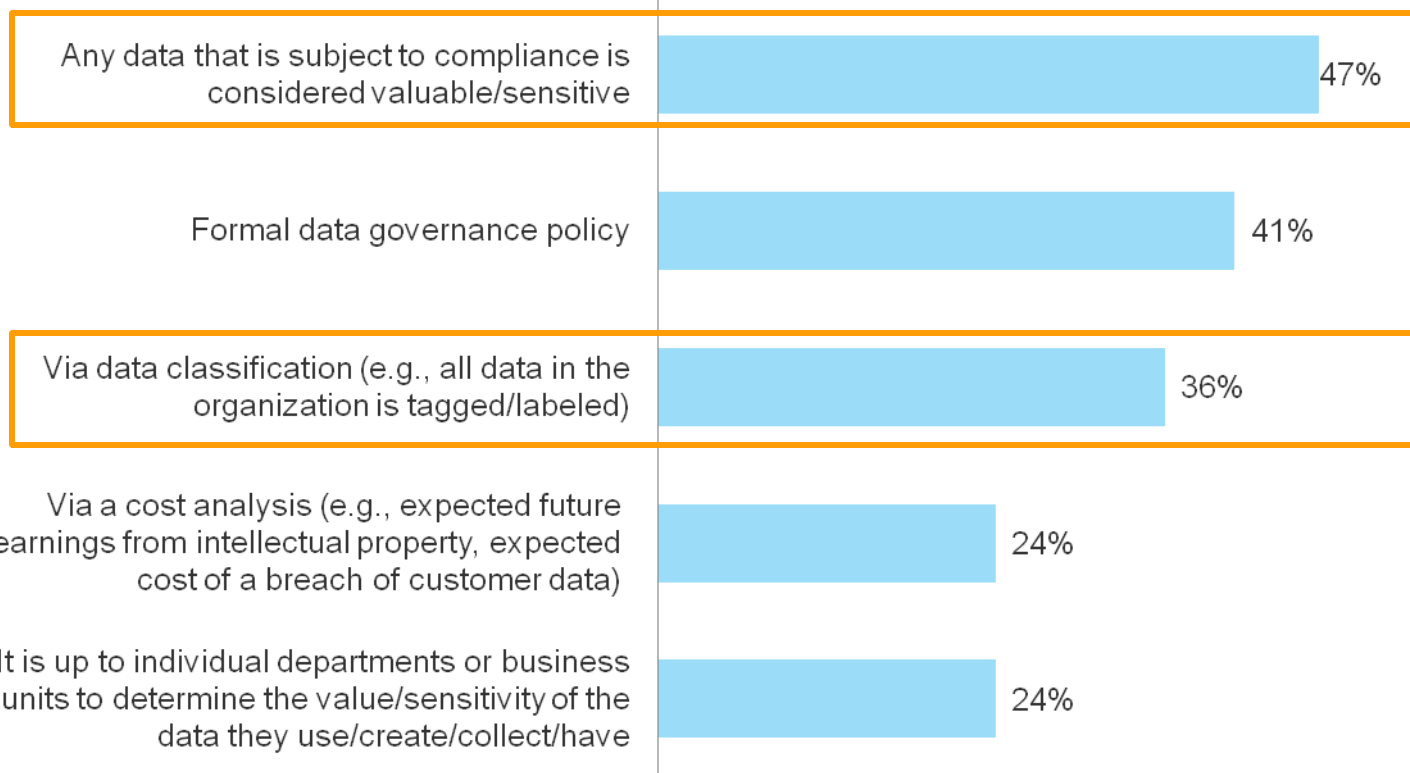
Unclear understanding of sensitive data

Difficulty finding potentially sensitive data and relationships



Only about a Third of Firms Classify their Data

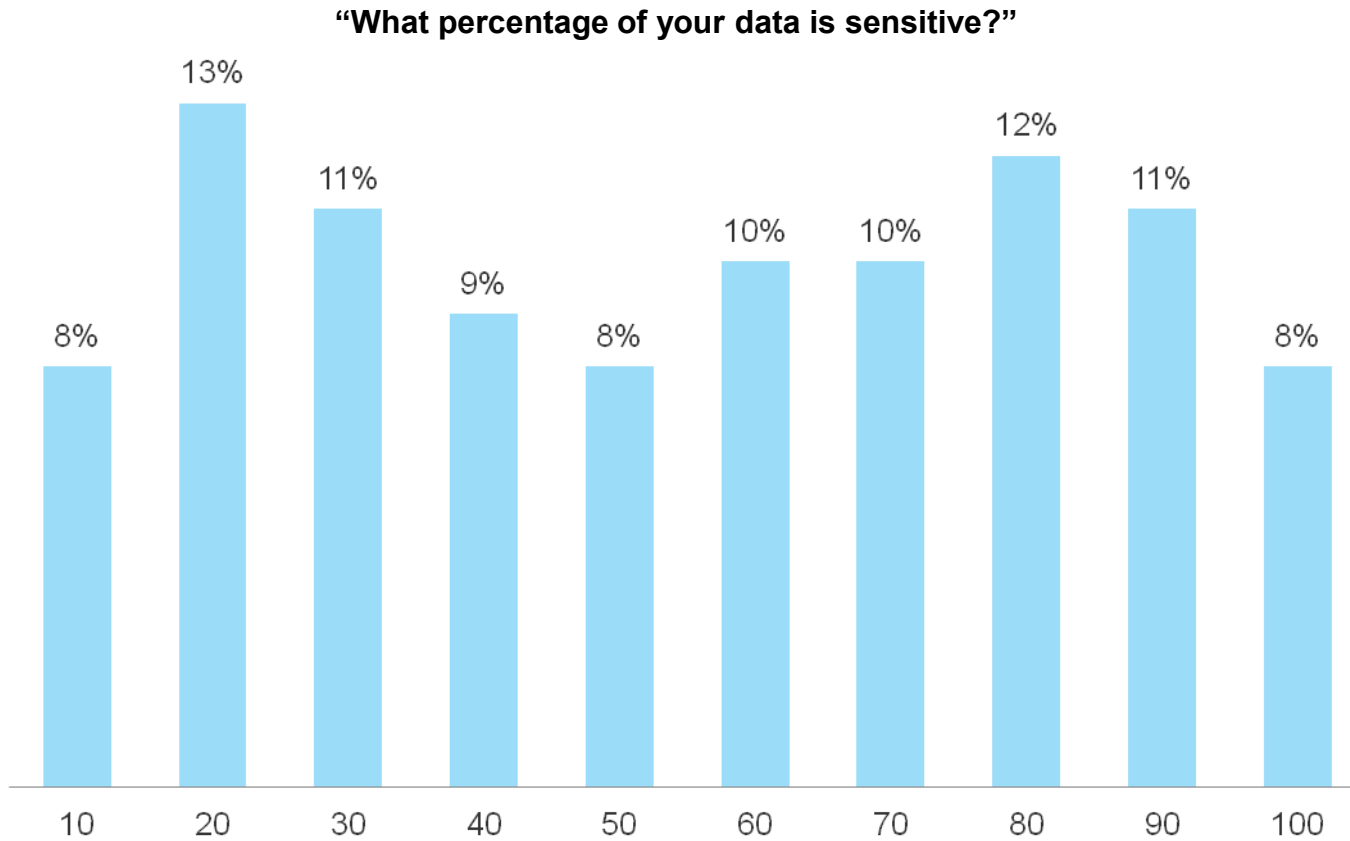
“How does your organization determine the value and/or sensitivity of data to the company?”



Base: 200 security decision makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

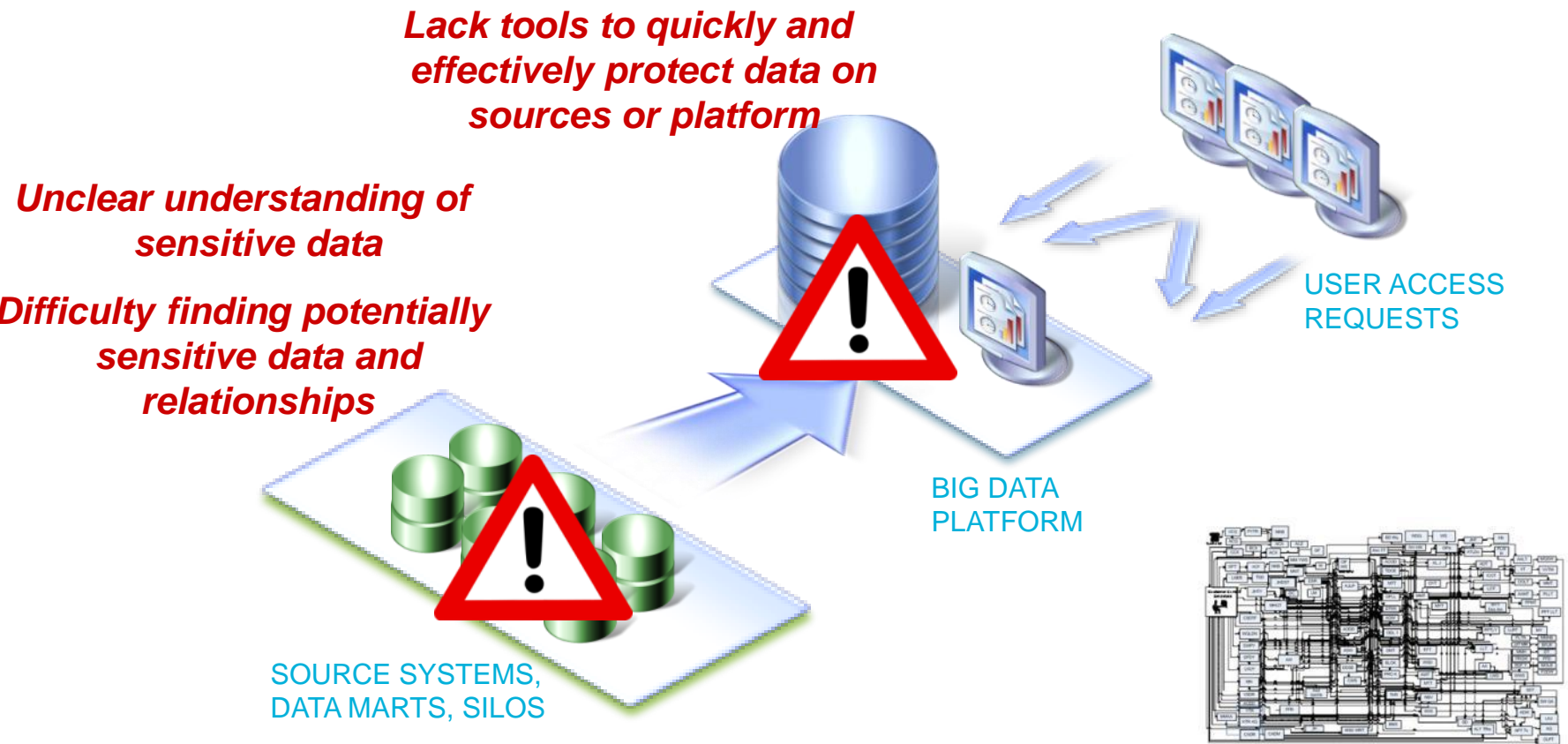
A Lack of Awareness about What Data Is Sensitive













Base: 200 security decision makers

Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, June 2014

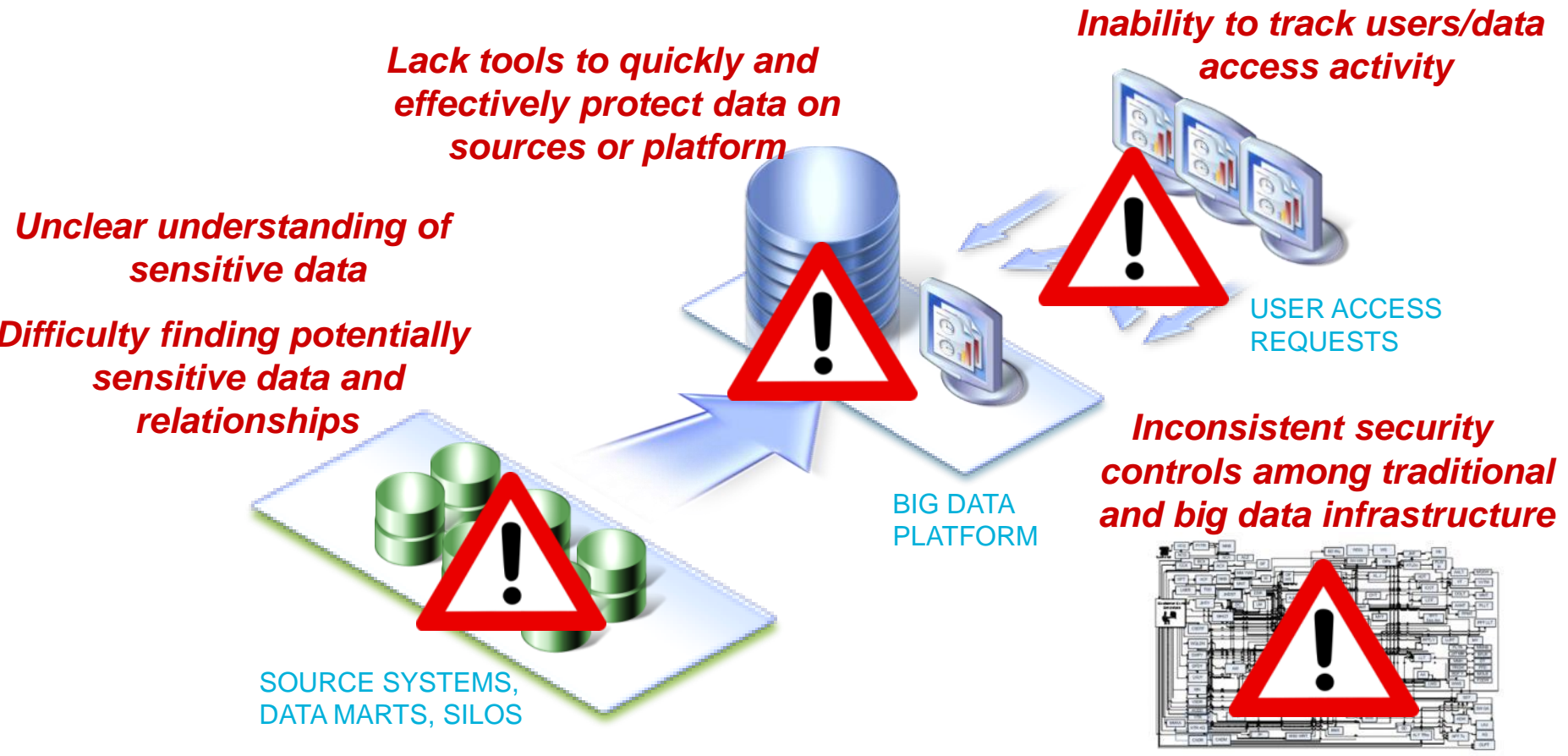
Big Data Technology Considerations in Security and Privacy



Big Data: Critical Data Security Capabilities

<i>Critical Capabilities</i>	<i>Hadoop/NoSQL</i>	<i>IBM Data Security</i>
Auditing with minimal performance impact		
Real-time alerts, so you can take action before it's too late.		
Separation of duties, so the security/auditing person is not the same as the Hadoop administrator		
Data encryption & masking		
Data scalability, performance & the ability to integration across diverse traditional and big data environments		

Big Data Technology Considerations in Security and Privacy



The Inability to Track Users and Data Access Leaves Organizations Open to Attack

What can you do? Continuously monitor access to sensitive data including databases, data warehouses, big data environments and file shares to...

1

Prevent data breaches

- Avoiding disclosure or leakage of sensitive data



2

Ensure the integrity of sensitive data

- Prevent unauthorized changes to data, database structures, configuration files and logs



3

Reduce cost of compliance

- Automate and centralize controls
- Simplify the audit review processes



Inconsistent Security Controls across Big Data and Traditional Environments Elevates Risk – A Lot

What can you do? Protect your data in an efficient, scalable and cost-effective way to...



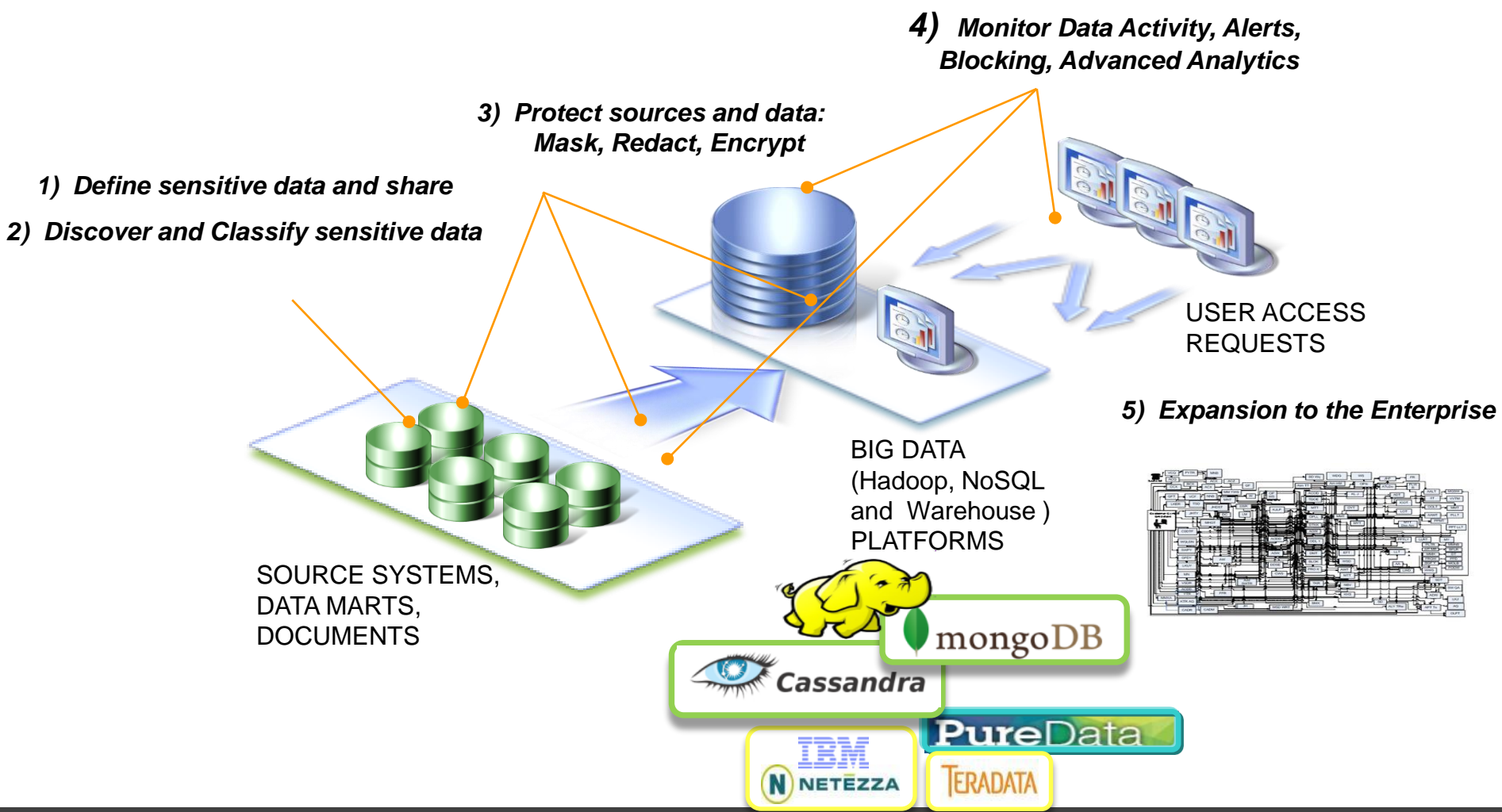
Increase operational efficiency

- ✓ Automate & centralize internal controls
- ✓ Across heterogeneous & distributed environments
- ✓ Identify and help resolve performance issues & application errors
- ✓ Highly-scalable platform, proven in most demanding data center environments worldwide
- ✓ Infrastructure & business processes perform consistently

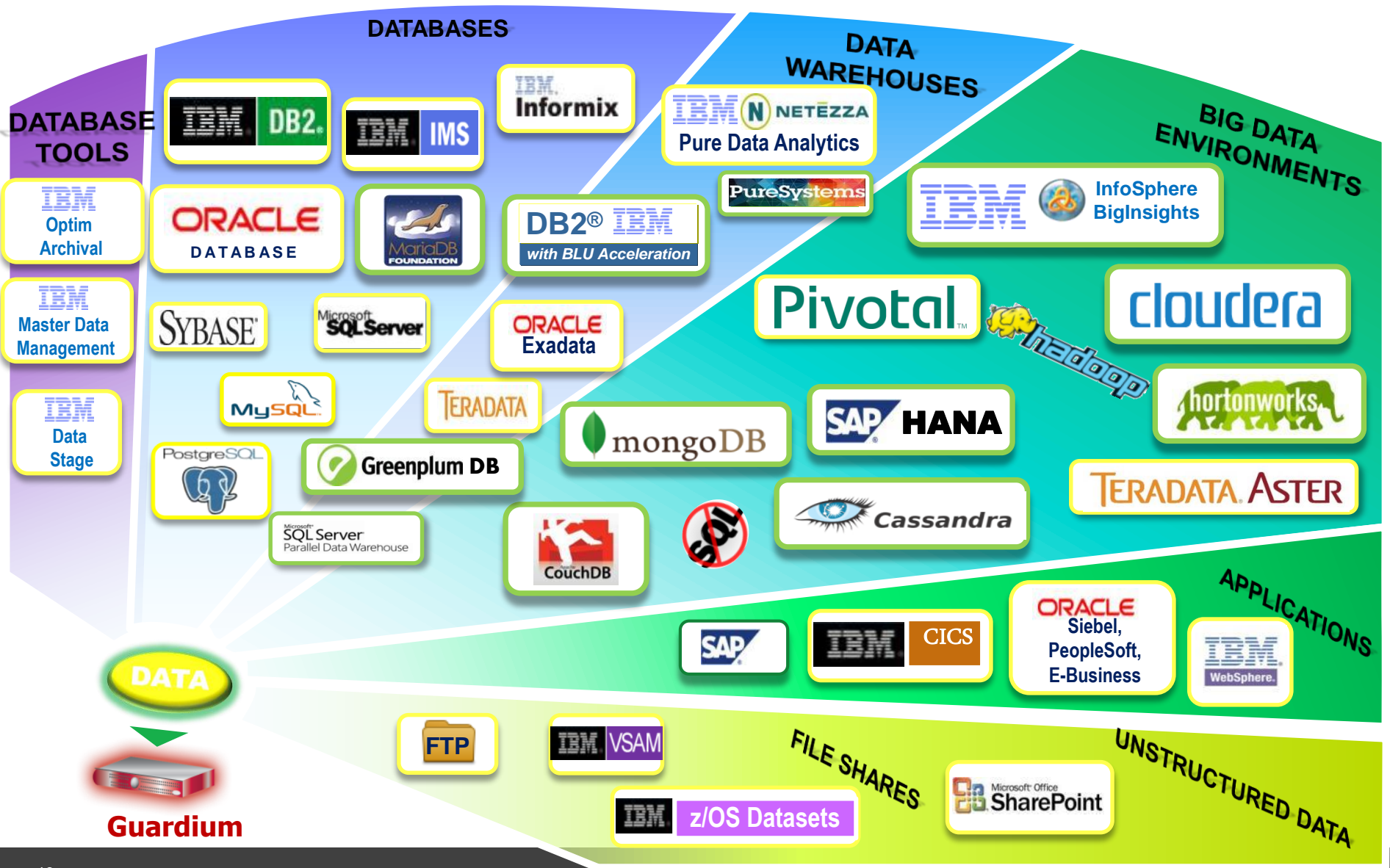
... while making your data security platform smarter and more efficient at detecting threats



IBM's Approach to Data Security and Privacy for Big Data



IBM Has You Covered for Protecting All Your Data



Guardium

Consistent, comprehensive data security across traditional and big data environments



UNCOVER DATA RISKS

Define and find sensitive data and relationships so you know what you need to protect



PROTECT DATA

Secure and protect sensitive structured and unstructured from breach or misuse



MONITOR & ACT AGAINST ATTACKS

Address both external attacks AND block unauthorized access by privileged users



A Private Bank in the UAE automates security compliance reporting in a big data environment

Need

- The bank processes several terabytes of data daily and required a solution which addressed the new security risks evolving around the world, especially with respect to protecting big data environments.

Benefits

- Achieves ROI in 8 months
- A scalable security monitoring solution that supports diverse database environment and does not impact application performance
- The time required to produce audit and compliance reports has gone from two months to near real-time

Next Steps in Big Data Security?

Get Educated

- Download educational pieces:
 - [Top Tips for Securing Big Data eBook](#)
 - [Planning a Hadoop Data Security Deployment](#)
- Analyst Reports: [Control and Protect Sensitive Information in the Era of Big Data](#)
- Visit the [InfoSphere Data Security and Privacy for Big Data webpages](#)

Schedule a Client Value Engagement (CVE)

- Business and IT: Narrow the communication gap
- Easy to follow programmatic client-centric approach – determine possible benefits from solution
- Fast time to completion: Less than 2 weeks – deliverables easy to follow and understand



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2015. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.