Security Intelligence.
Think Integrated.

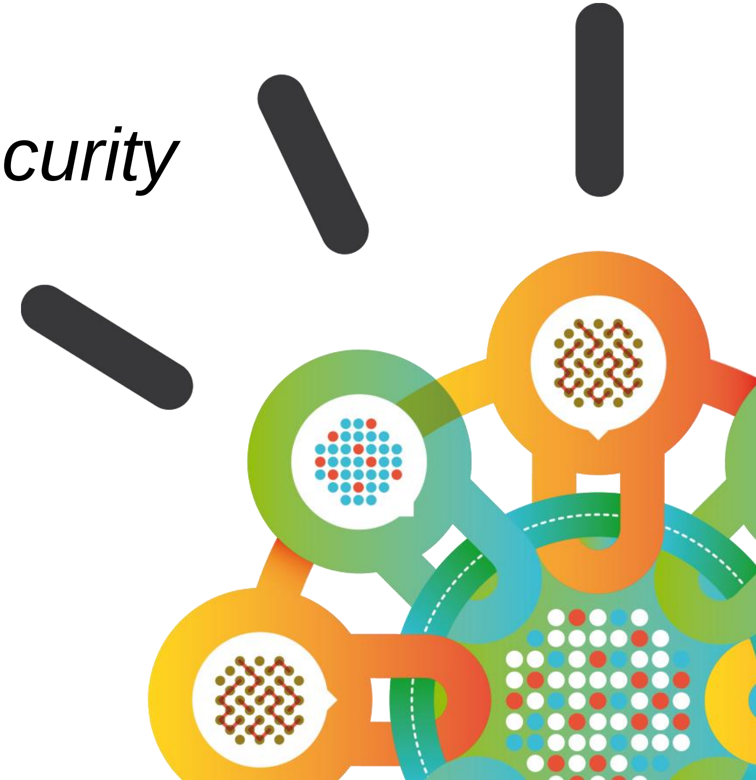
BIG DATA: Big Opportunity, Big Headaches

Protect your Big Data with data security

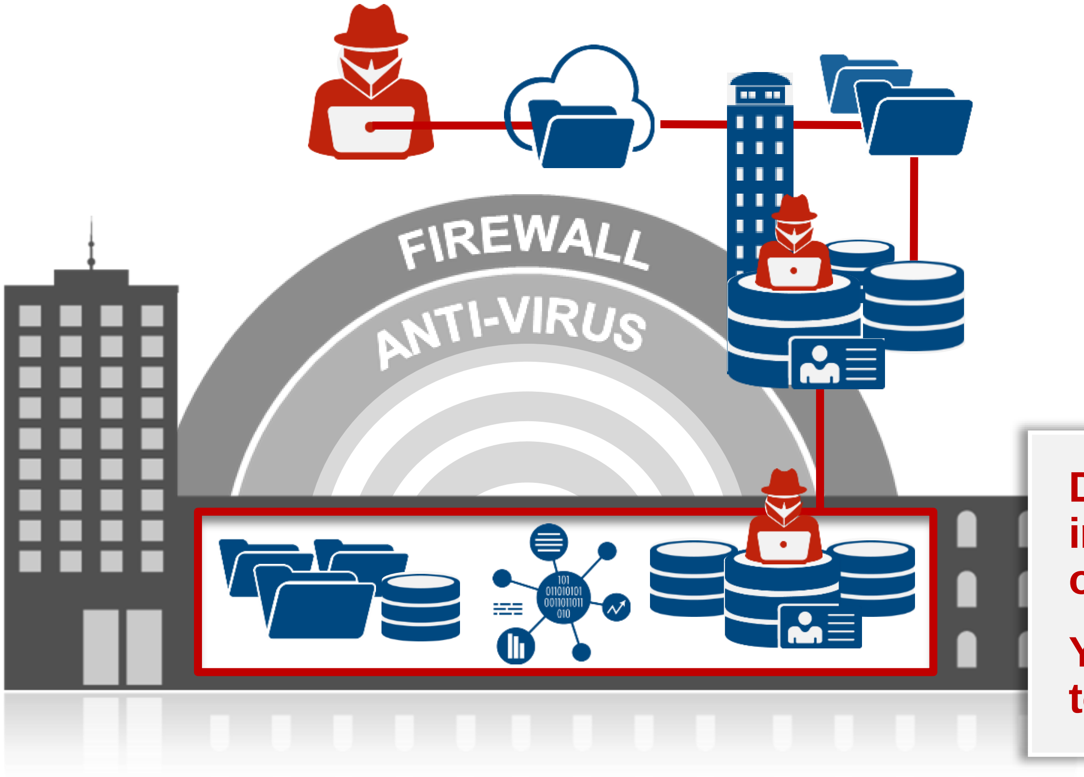
Kathryn Zeidenstein

Guardium Evangelist
IBM Security

October 2015



Are you doing enough to protect data that runs your business?



70% of your company's value likely lies in intellectual property

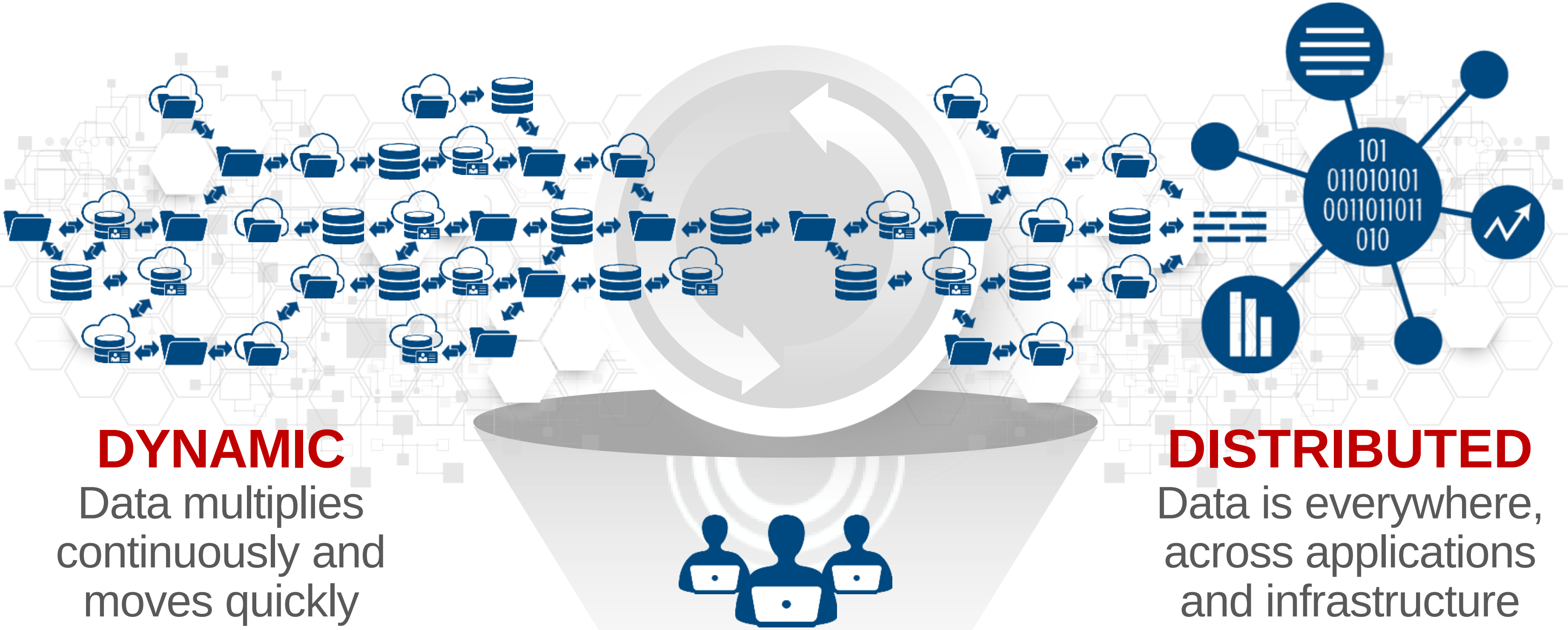
Customer data, product designs, sales information, proprietary algorithms, communications, etc.

Source: TechRadar

Damaging security incidents involve loss or illicit modification or destruction of sensitive data

Yet many security programs forget to protect the data

Data is challenging to secure



DYNAMIC

Data multiplies continuously and moves quickly

IN DEMAND

Users need to constantly access and share data to do their jobs

DISTRIBUTED

Data is everywhere, across applications and infrastructure

The Opportunities from Big Data & Analytics are Infinite

90%
Increased Transaction Capacity
Sprint

98%
Cut in Storage Requirements
LYDEC ليدك

40X
Analysis Performance Gain
Constant Contact

72%
Reduction in Fraudulent Claims
MoneyGram International

98%
Decrease time to analyze data
esri

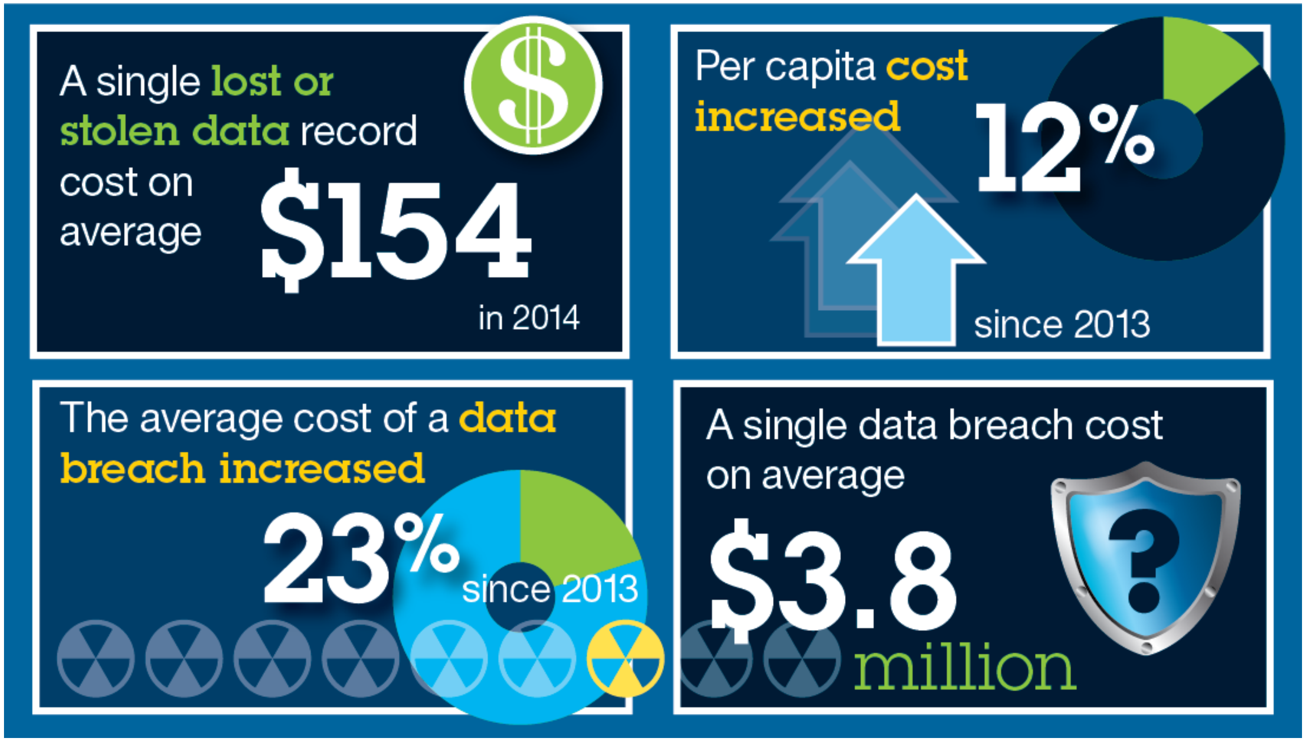
60X
Faster Query Performance
QUALCOMM

$1M
Estimated Cash Savings
CAMERON

Big Data: Look out for the headaches – Organizations are jumping in with both feet

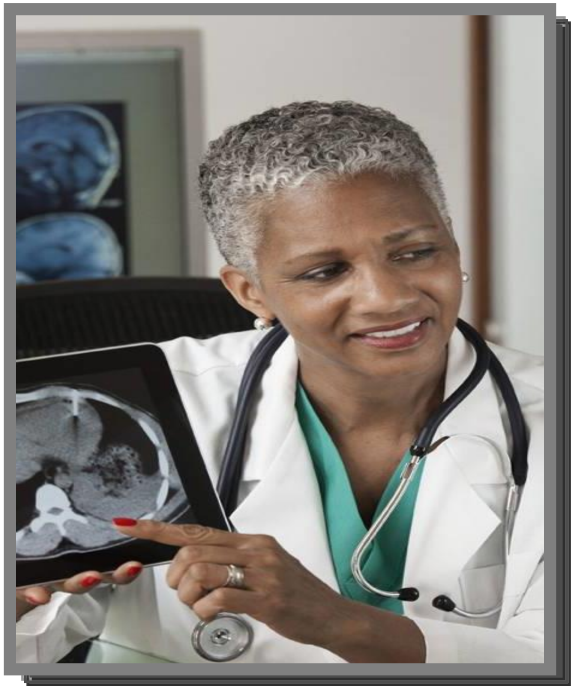
- Departmental projects
- Rogue IT teams
- Using production data
- Loose user controls
- Impossible to audit

Big Data: Watch out for the costs

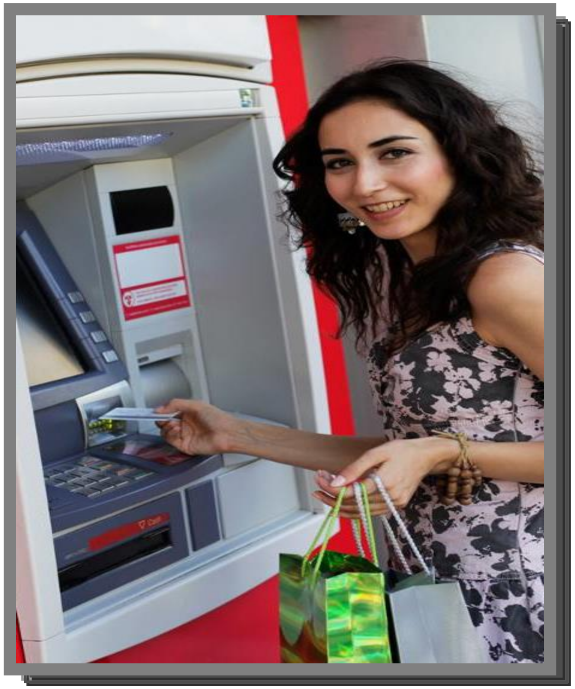


Source: “2015 Cost of a Data Breach Study: Global Analysis,” Ponemeon Institute, May 2015

Watch out: Sensitive Data is Common in Big Data Projects



Healthcare



Customer

Citizen

Why is the Big Data Security Headache is 'Bigger' than usual?

The same risks are magnified…

…and big data introduces new challenges

Brand Reputation

•$100M+ impact to the business

New Users

•Data sharing and new user access

Data Breach

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

Attractive Target

•Data security hotspot for internal/external threat

BIG DATA PLATFORM

Compliance

•Changing and new privacy legislation

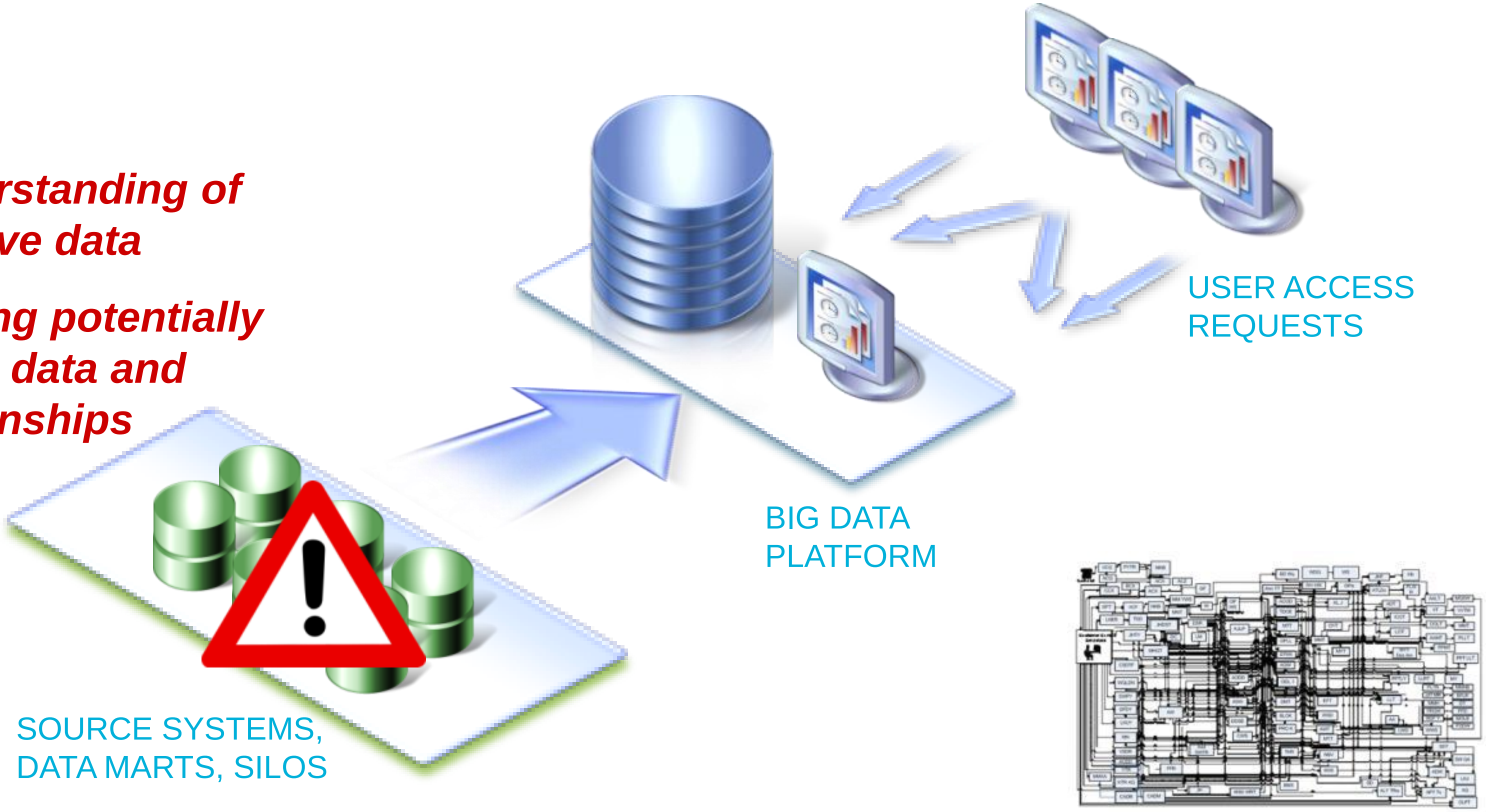
Fewer Tools

•Traditional tools no longer apply

Big Data Technology Considerations in Security and Privacy

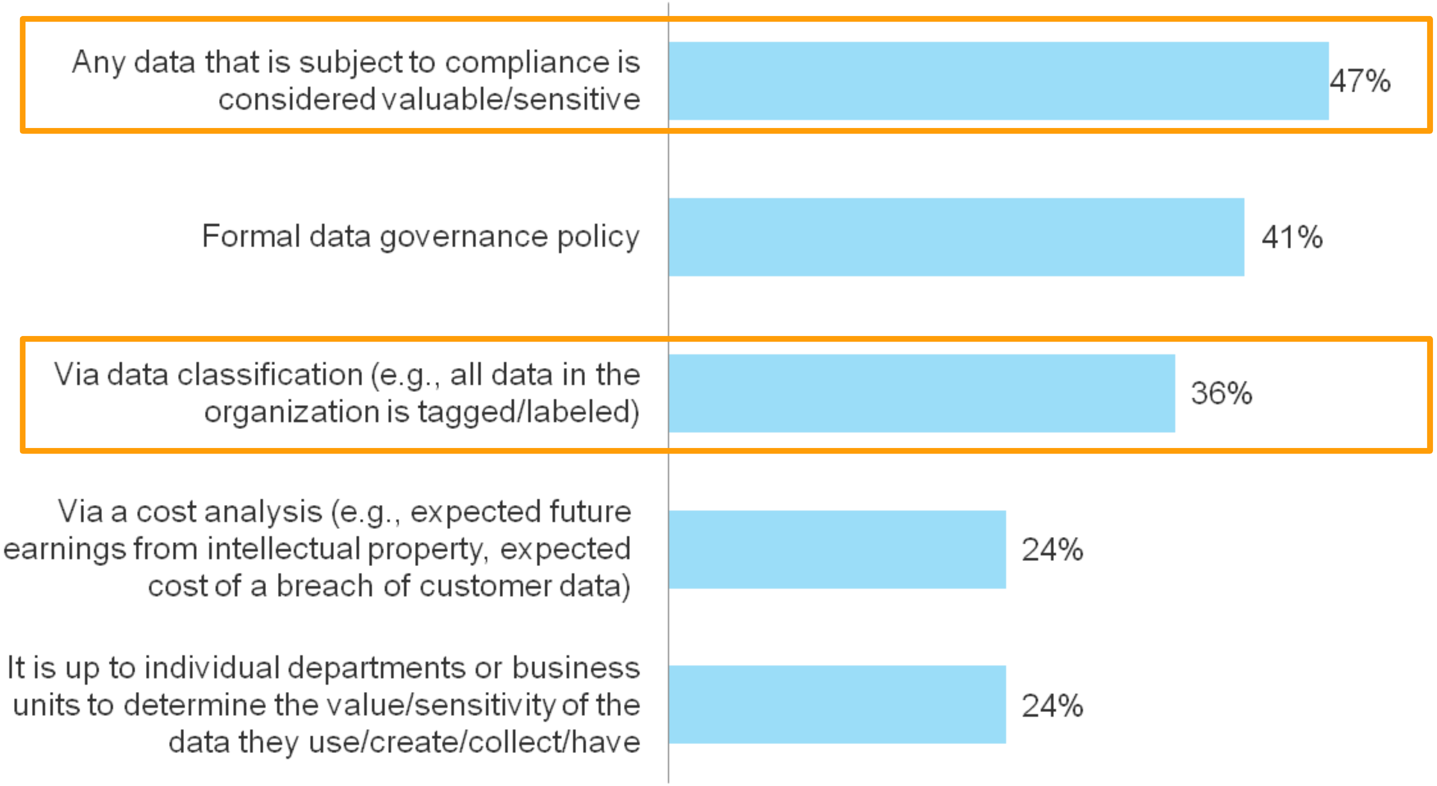
Unclear understanding of sensitive data

Difficulty finding potentially sensitive data and relationships



Only about a Third of Firms Classify their Data

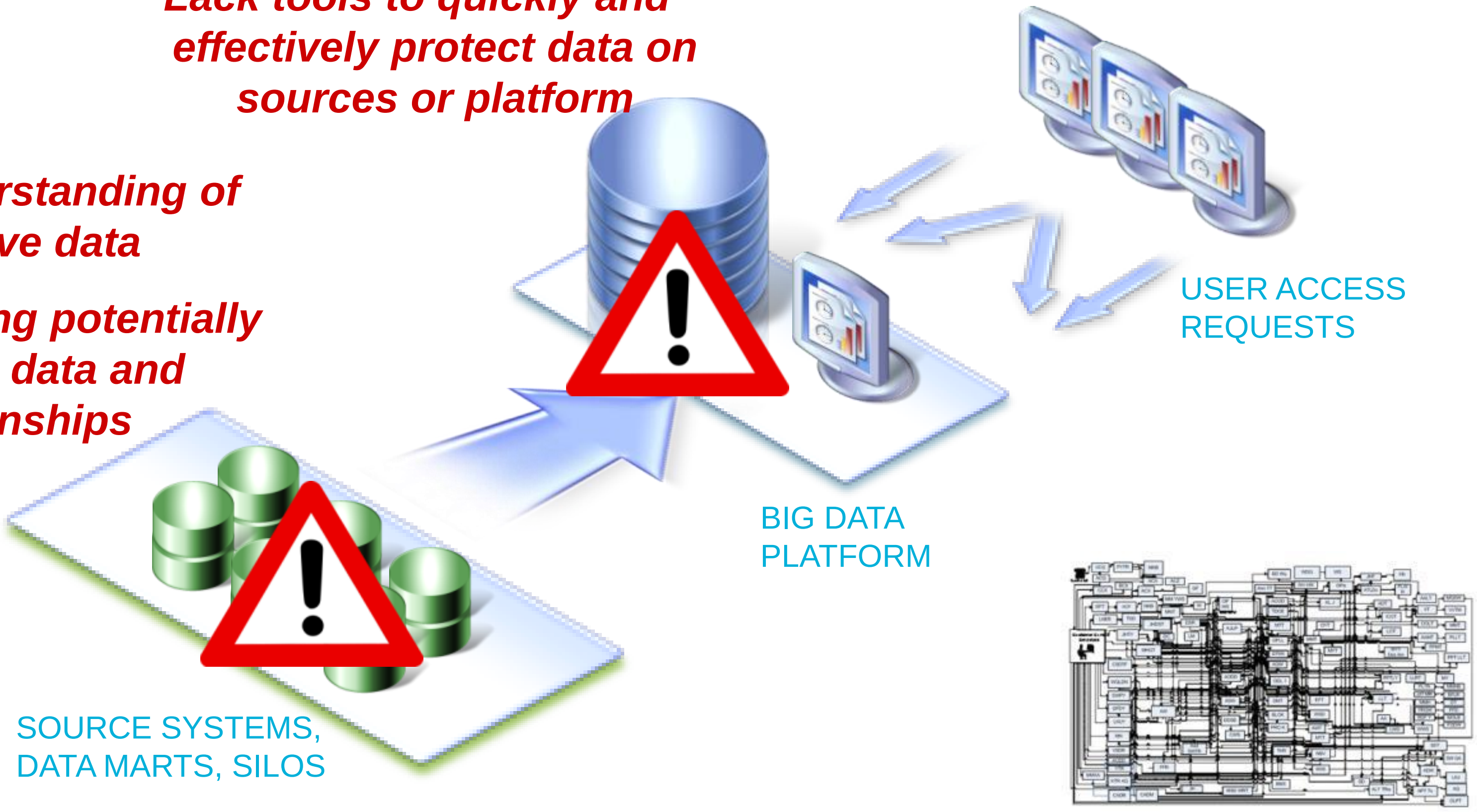
“How does your organization determine the value and/or sensitivity of data to the company?”



Base: 200 security decision makers

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

Big Data Technology Considerations in Security and Privacy



Lack tools to quickly and effectively protect data on sources or platform

Unclear understanding of sensitive data

Difficulty finding potentially sensitive data and relationships

USER ACCESS
REQUESTS

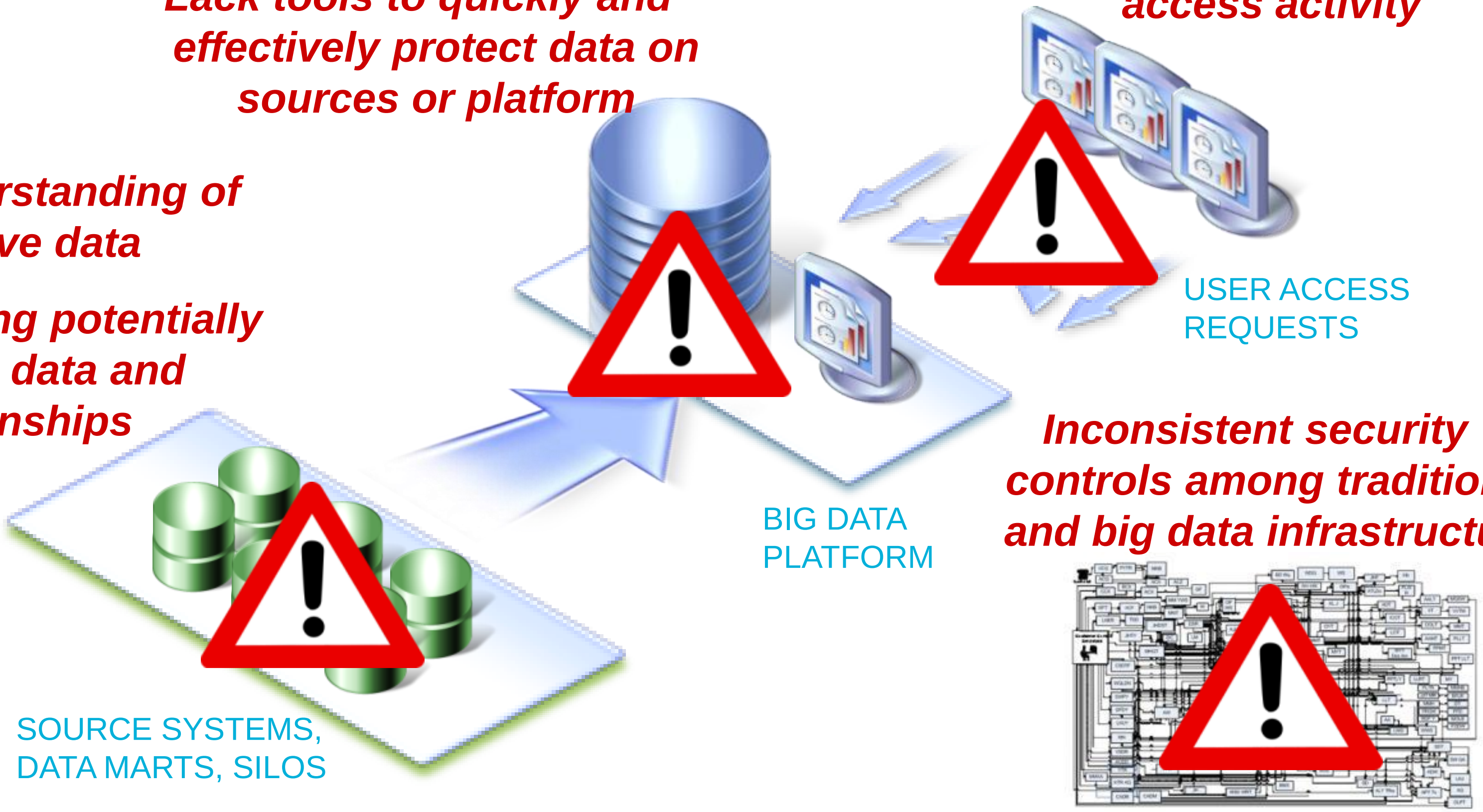
BIG DATA
PLATFORM

SOURCE SYSTEMS,
DATA MARTS, SILOS

What key capabilities are missing from Big Data platforms?

	Missing	Why it's Important
1.	Auditing with minimal impact	Improve performance, reduce costs
2.	Real-time alerts	Stop data loss in real-time, taking action before it's too late
3.	Separation of duties	There's too much risk if the same person has all the access
4.	Advanced role behavior & data usage analytics	You need to monitor everyone – including the watchers, to avoid risk
5.	Data scalability, performance & the ability to integrate	Closes loopholes, reduces costs, increases efficiencies

Big Data Technology Considerations in Security and Privacy



Lack tools to quickly and effectively protect data on sources or platform

Inability to track users/data access activity

Unclear understanding of sensitive data

Difficulty finding potentially sensitive data and relationships

Inconsistent security controls among traditional and big data infrastructure

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 files 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

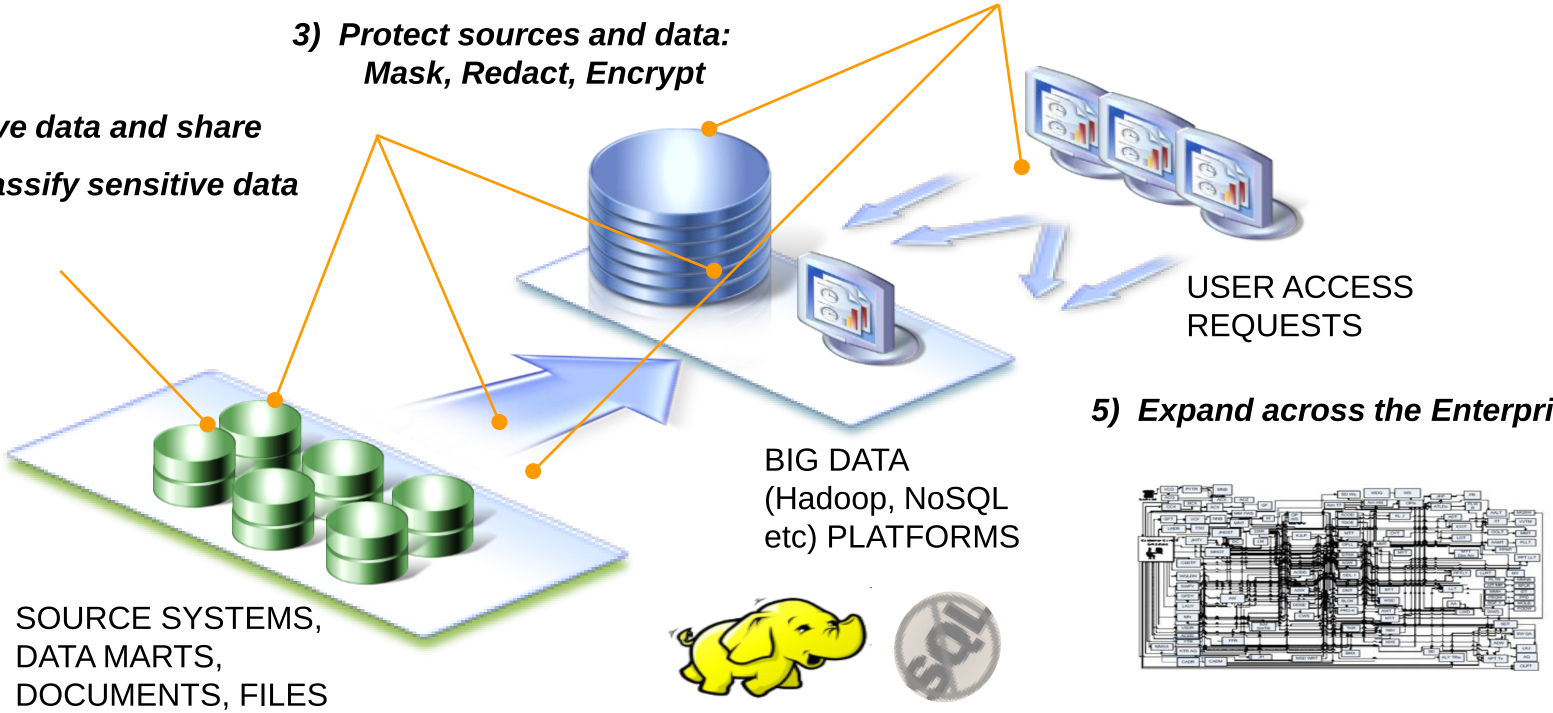
What can you do? *Protect your data in an efficient, scalable and cost-effective way to...*

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 Big Data Security



4) *Monitor Data Activity, Alerts, Blocking, Advanced Analytics*

3) *Protect sources and data: Mask, Redact, Encrypt*

1) *Define sensitive data and share*

2) *Discover and Classify sensitive data*

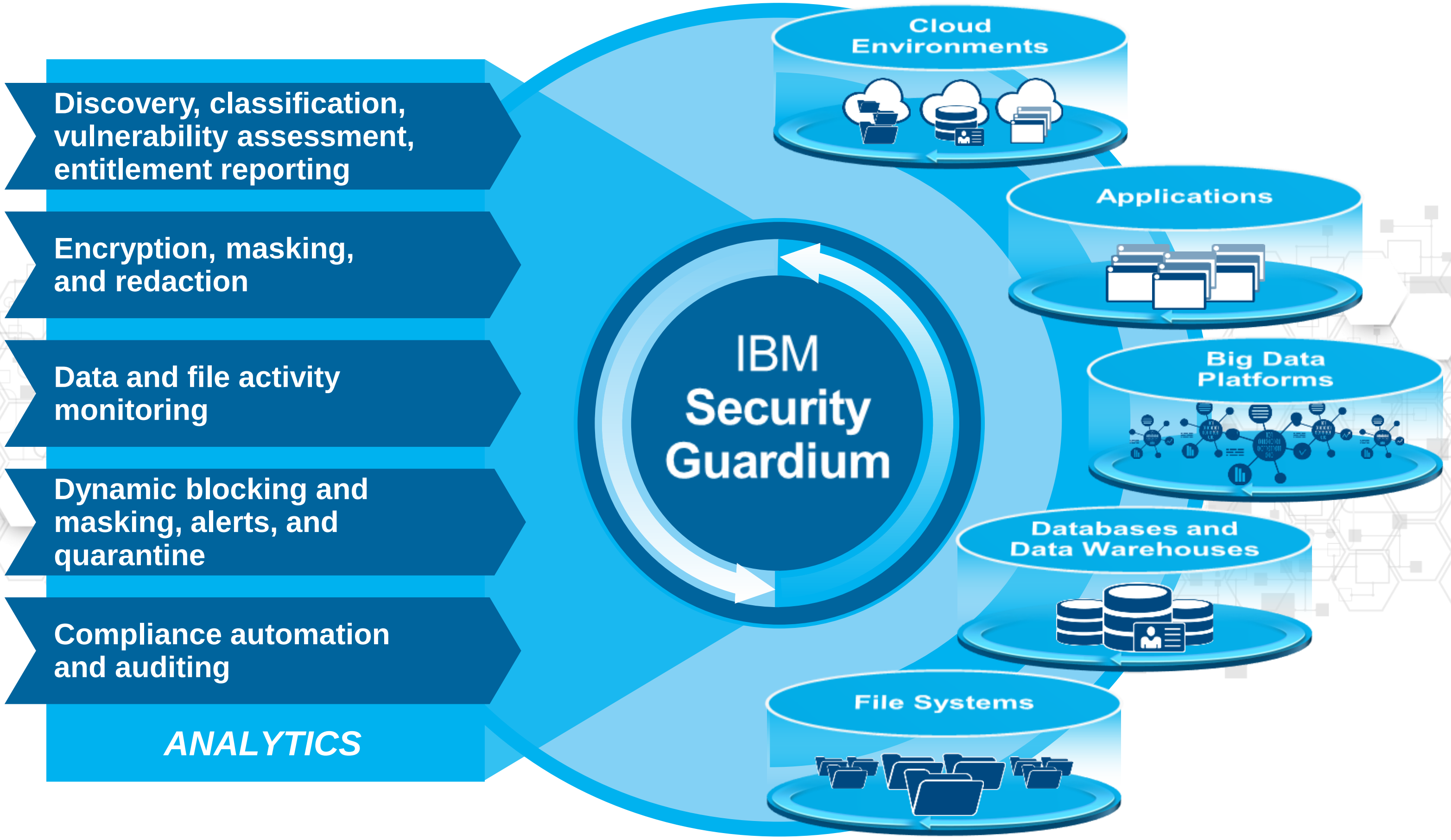
USER ACCESS REQUESTS

5) *Expand across the Enterprise*

BIG DATA (Hadoop, NoSQL etc) PLATFORMS

SOURCE SYSTEMS, DATA MARTS, DOCUMENTS, FILES

ANALYZE. PROTECT. ADAPT.


Discovery, classification, vulnerability assessment, entitlement reporting
Encryption, masking, and redaction
Data and file activity monitoring
Dynamic blocking and masking, alerts, and quarantine
Compliance automation and auditing
ANALYTICS
IBM Security Guardium
Cloud Environments
Applications
Big Data Platforms
Databases and Data Warehouses
File Systems

IBM Security Guardium efficiently secures sensitive data and reduces risk

Executive Summary

- Forrester was commissioned by IBM to examine the financial benefit of IBM Security Guardium.
- Forrester performed analysis, based on a composite organization created from feedback from different IBM customers, that quantified benefits, costs, risks, and flexibility of the product.
- Based on that composite organization, Forrester determined that Guardium has a three-year risk-adjusted **ROI of 218%** with a **net present value of $1.8M**

Three-Year Risk-Adjusted Financial Snapshot

ROI

218%

TOTAL BENEFITS

$2.6M

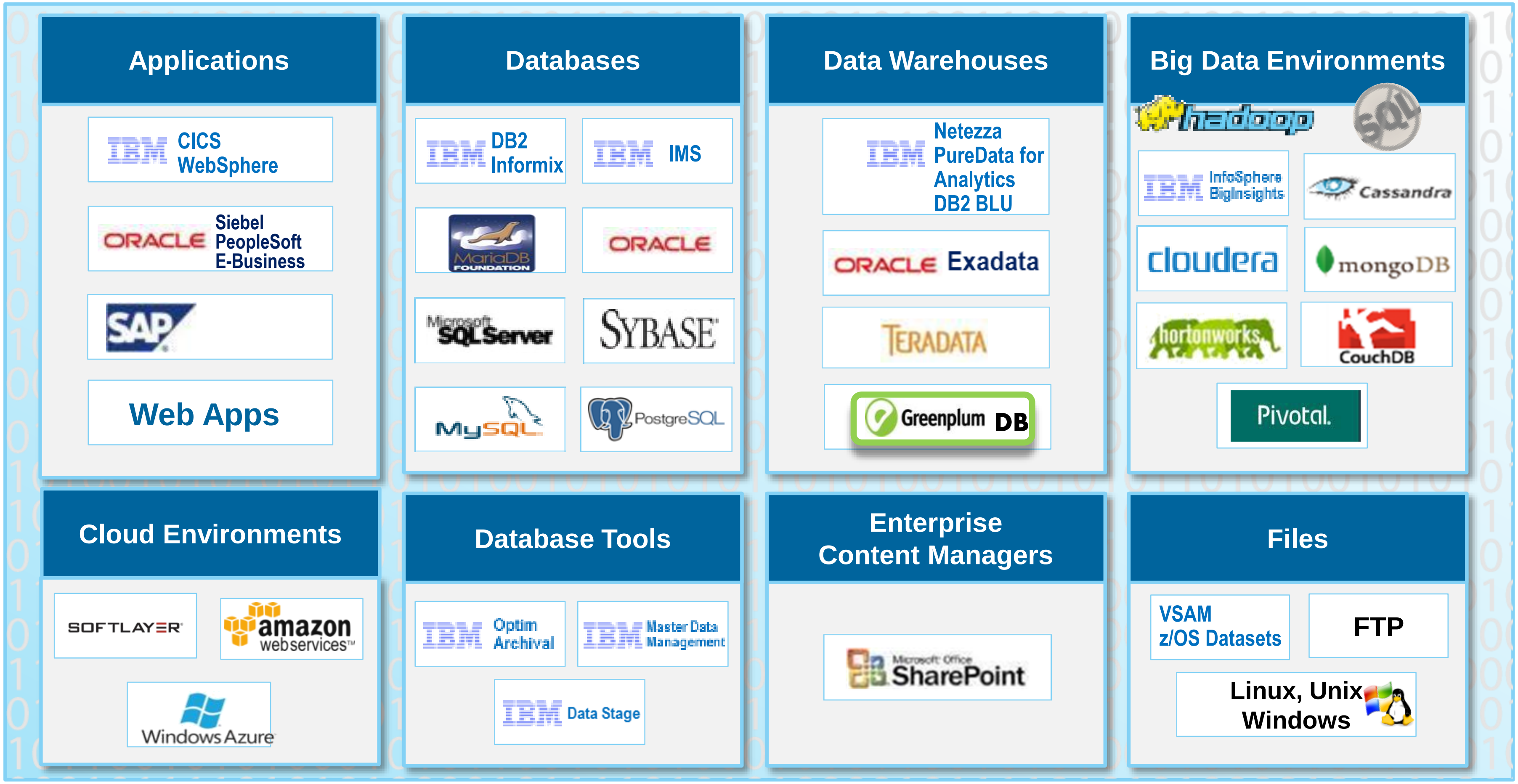
NPV

$1.8M

The Total Economic Impact Of IBM Guardium, a commissioned study conducted by Forrester Consulting on behalf of IBM, September 2015

Guardium helps support the most complex of IT environments

Examples of supported databases, Big Data environments, file systems, etc



Applications

- IBM CICS WebSphere
- ORACLE Siebel PeopleSoft E-Business
- SAP
- Web Apps

Databases

- IBM DB2 Informix
- IBM IMS
- MariaDB FOUNDATION
- ORACLE
- Microsoft SQL Server
- SYBASE
- MySQL
- PostgreSQL

Data Warehouses

- IBM Netezza PureData for Analytics DB2 BLU
- ORACLE Exadata
- TERADATA
- Greenplum DB

Big Data Environments

- hadoop
- SQL
- IBM InfoSphere BigInsights
- Cassandra
- cloudera
- mongoDB
- hortonworks
- CouchDB
- Pivotal.

Cloud Environments

- SOFTLAYER
- amazon webservices™
- Windows Azure

Database Tools

- IBM Optim Archival
- IBM Master Data Management
- IBM Data Stage

Enterprise Content Managers

- Microsoft Office SharePoint

Files

- VSAM z/OS Datasets
- FTP
- Linux, Unix Windows

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

Learn More about IBM Security Guardium

Independent study: **Total Economic Impact™ of IBM® Security Guardium®**

218% Your Potential **ROI** with the **Right Data Security Solution**

[Read the Guardium TEI Report]

Top tips for securing big data environments

Why big data doesn't have to mean big security challenges

[Read the Big Data ebook]

What does it take to win the **Data Security Triple Crown?**

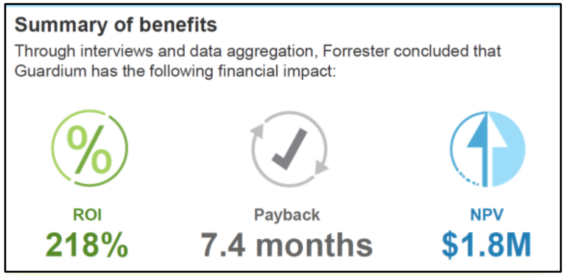
Analyze

Protect

Adapt

Read the Solution Brief

[Read the new Solution Brief]



Summary of benefits

Through interviews and data aggregation, Forrester concluded that Guardium has the following financial impact:

ROI	Payback	NPV
218%	7.4 months	$1.8M

[Check out the Infographic]

Go to: *ibm.com/Guardium* for more information

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