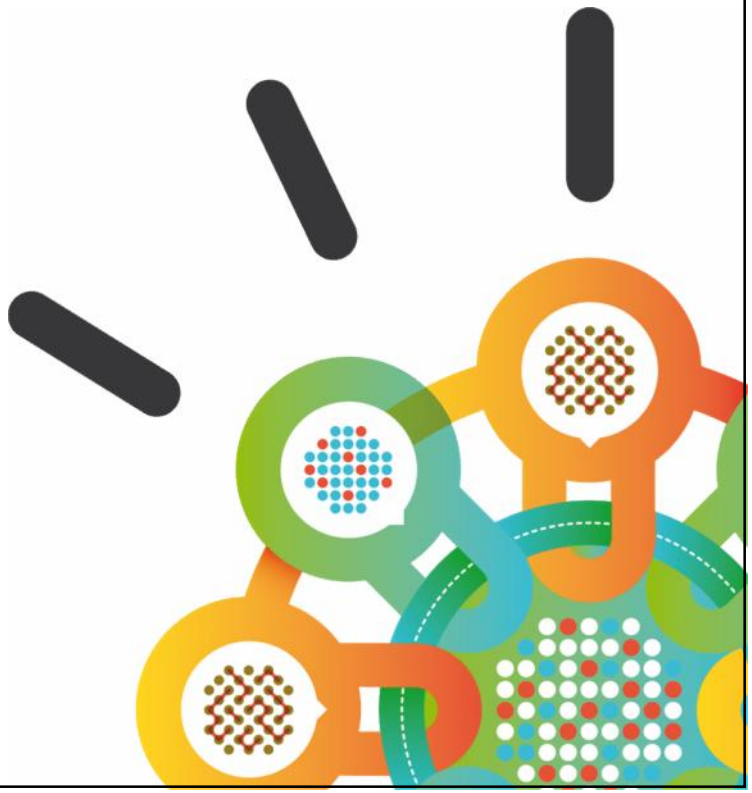
Security Intelligence.
Think Integrated.

Secure Enterprise Data and Ensure Compliance



What we'll discuss

- Protecting Sensitive Data – Challenges
- What's at Stake?
- Ensuring Data Security & Compliance
  - Understand & Define
  - Secure & Protect
  - Monitor & Audit
- Client success with IBM Data Security and Compliance Solutions

Customer Challenges
Data Security

Helping to prevent data breaches

- Mitigate internal and external threats across production and non-production environment.
- Help to prevent disclosure or loss of sensitive data

Maintaining the integrity of sensitive data

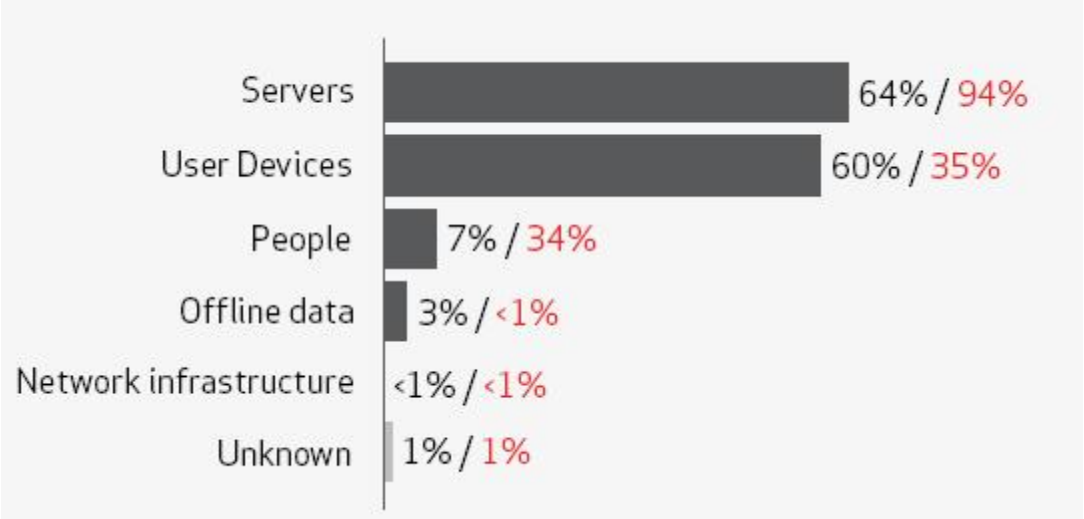
- Help to prevent unauthorized changes to data or structures

Reducing the cost of compliance

- Automate and centralize controls

Database servers are the primary source of breached data

With user devices a close second



Categories of compromised assets by percent of breaches and percent of records

Sources: Verizon Business Data Breach Investigations Report 2011

It's really not surprising that servers seem to have a lock on first place when it comes to the types of assets impacted by data breaches. They store and process data, and that fact isn't lost on data thieves.

Organizations are slow to respond to database attacks

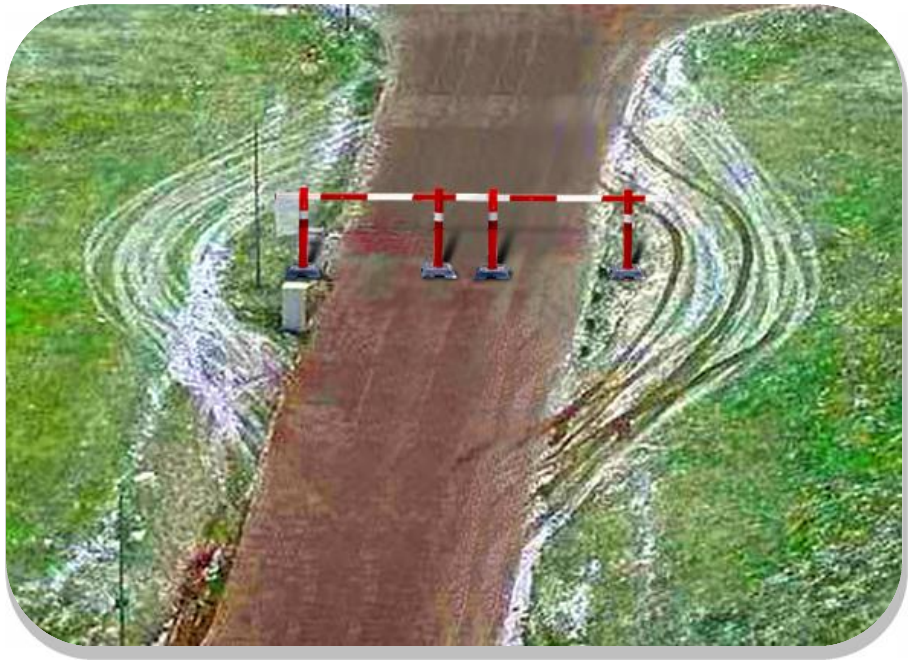
http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z038

Are there ways around your security polices?

Requirements for data security and compliance

Executives need to:

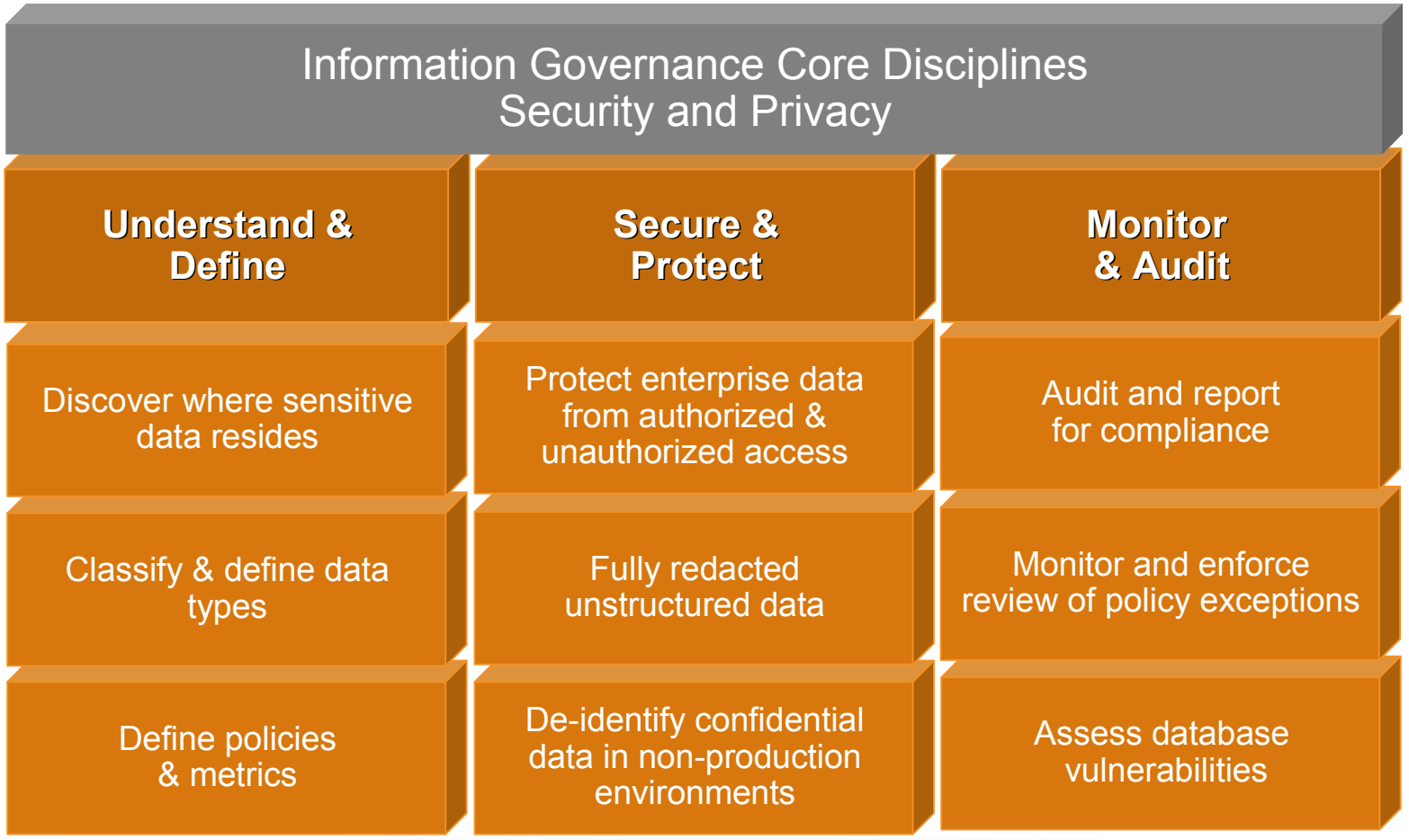
- Lower the cost of compliance
- Avoid audits and fines from regulatory bodies
- Maintain customer satisfaction & brand image



Data security/privacy analysts need to:

- Understand what data exists
- Implement policies based on roles or LOB
- Protect against internal and external threats
- Avoid using confidential data for non-production
- Mitigate vulnerabilities in the data center, on desktops and laptops
- Respond in real time to suspicious activities

Holistic approach to data security and compliance

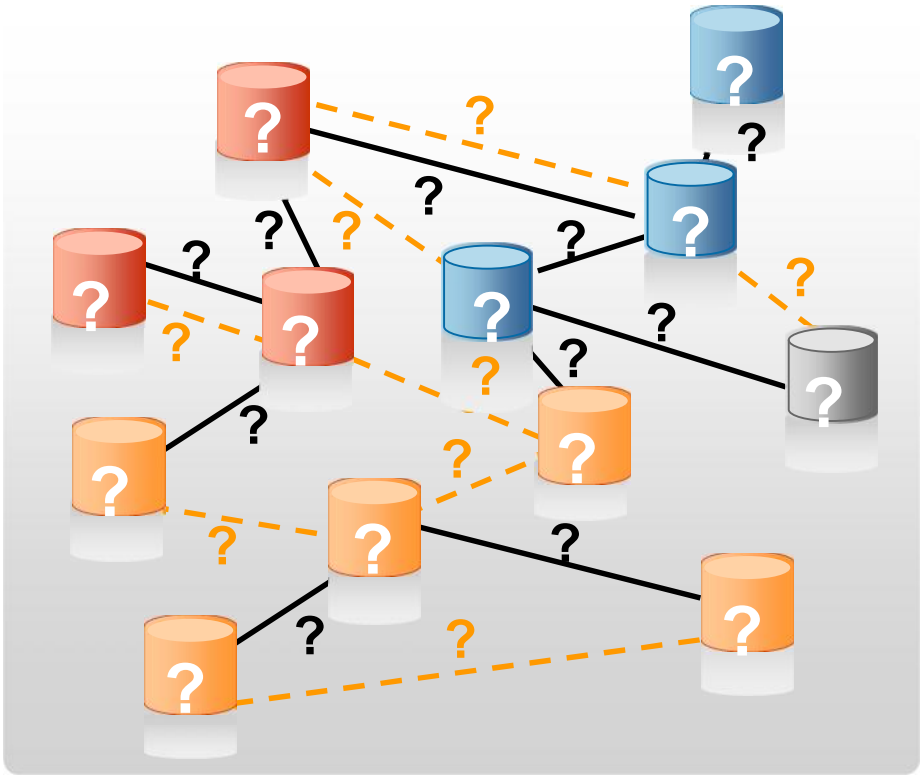


A data security strategy should include database auditing and monitoring, patch management, data masking, access control, discovery/classification, and change management.

-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011

Understand and define your distributed data landscape

- Locate and inventory data sources enterprise
- Identify sensitive data and classify
- Understand relationships
- Centrally document security policies and across the data lifecycle



Start with discovery, classification, and building policies and implementing data security controls.

-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011

Statically mask data in non-production environments

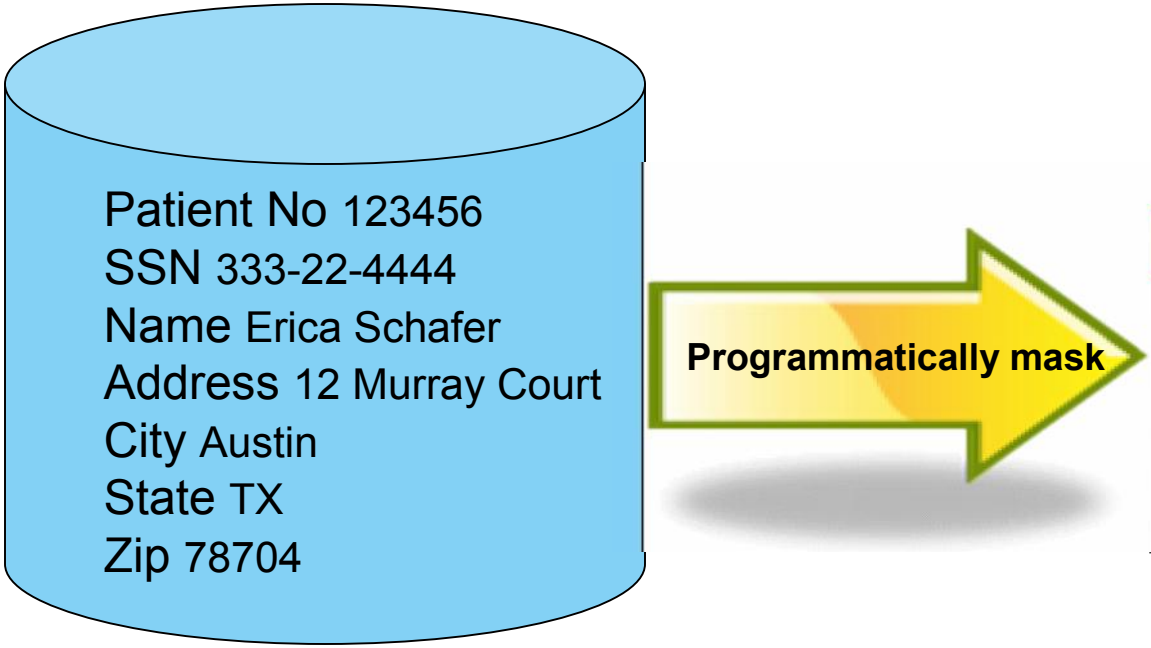
Patient No 123456
SSN 333-22-4444
Name Erica Schafer
Address 12 Murray Court
City Austin
State TX
Zip 78704

Statically mask

Patient No 112233
SSN 123-45-6789
Name Amanda Winters
Address 40 Bayberry Drive
City Elgin
State IL
Zip 60123

- ✓ **Mask data in non-production environments such as test and development**
- ✓ **Improve security of non-production environments**
- ✓ **Facilitate faster testing processes**

Mask data in applications



Programmatically mask

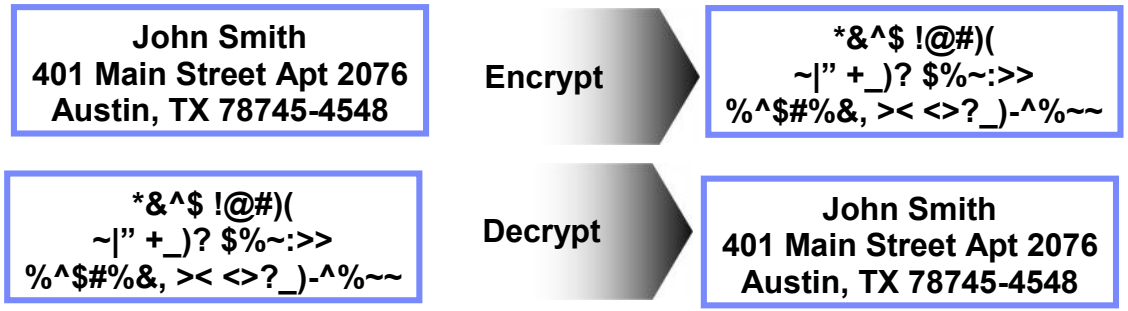
Patient Information

Patient No.	112233	**SSN**	123-45-6789		
Name	Amanda Winters				
Address	40 Bayberry Drive				
City	Elgin	**State**	IL	**Zip**	60123

- ✓ **Ensure valid business need to know to sensitive data**
- ✓ **Mask data access in real time to respond to suspicious activities**
- ✓ **Promote role based approach to data access**

Protect online and offline data with encryption

- Encryption **transforms data to make it unreadable** except to those with a special key
- **Encrypted data is meaningless** so unauthorized access causes no harm
- **Original data is preserved** so encryption is an ideal choice for protecting production environments



Personal identifiable information is encrypted making it meaningless without a proper key.

Data loss prevention at the endpoint

Patterns - Regular Expressions

(credit card, social insurance, account numbers)

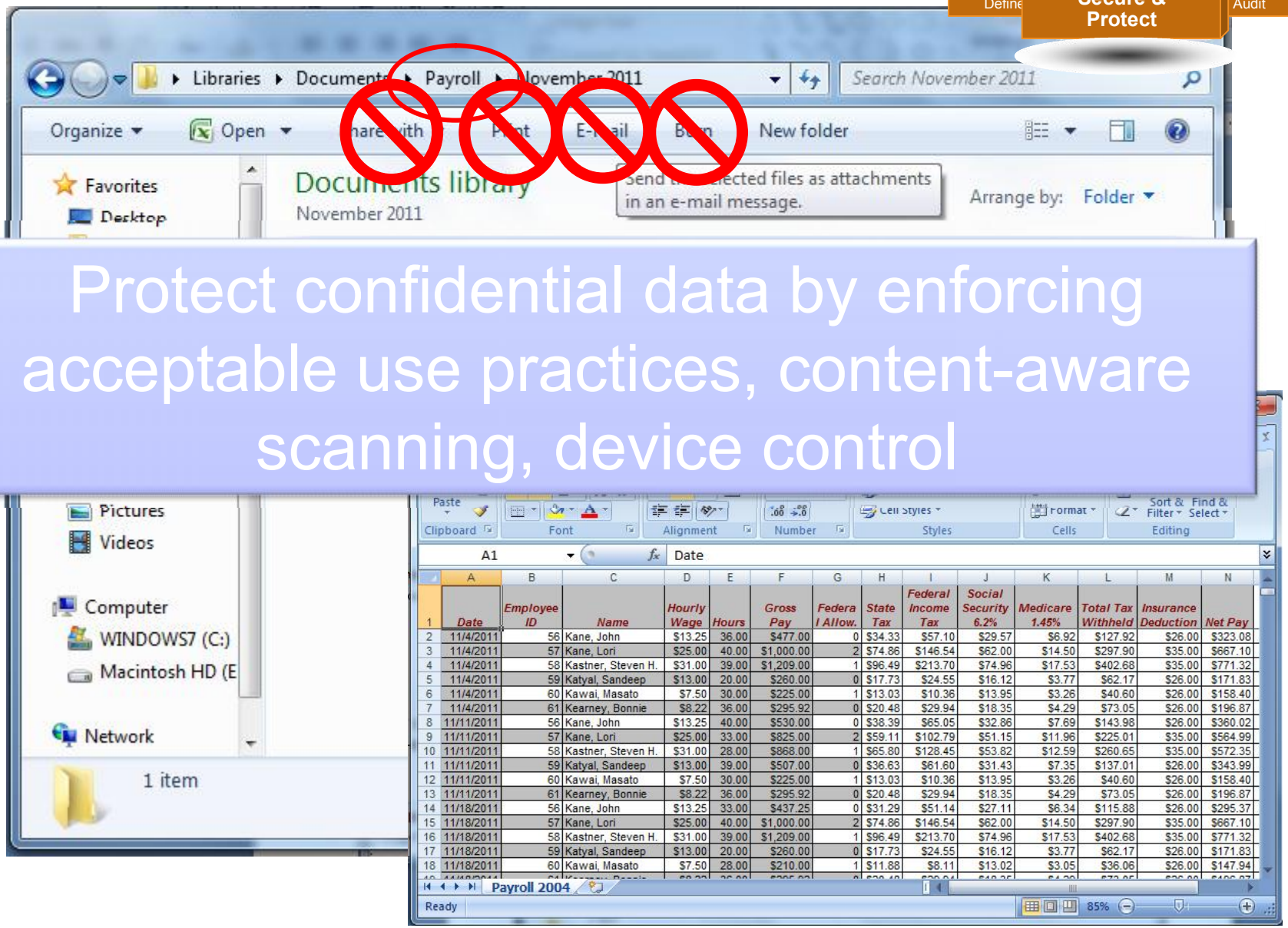
Keywords – Lists of terms

(confidential, internal, project/product names…)

File Attributes – File Name, File Size, File Type

(threshold of acceptable use)

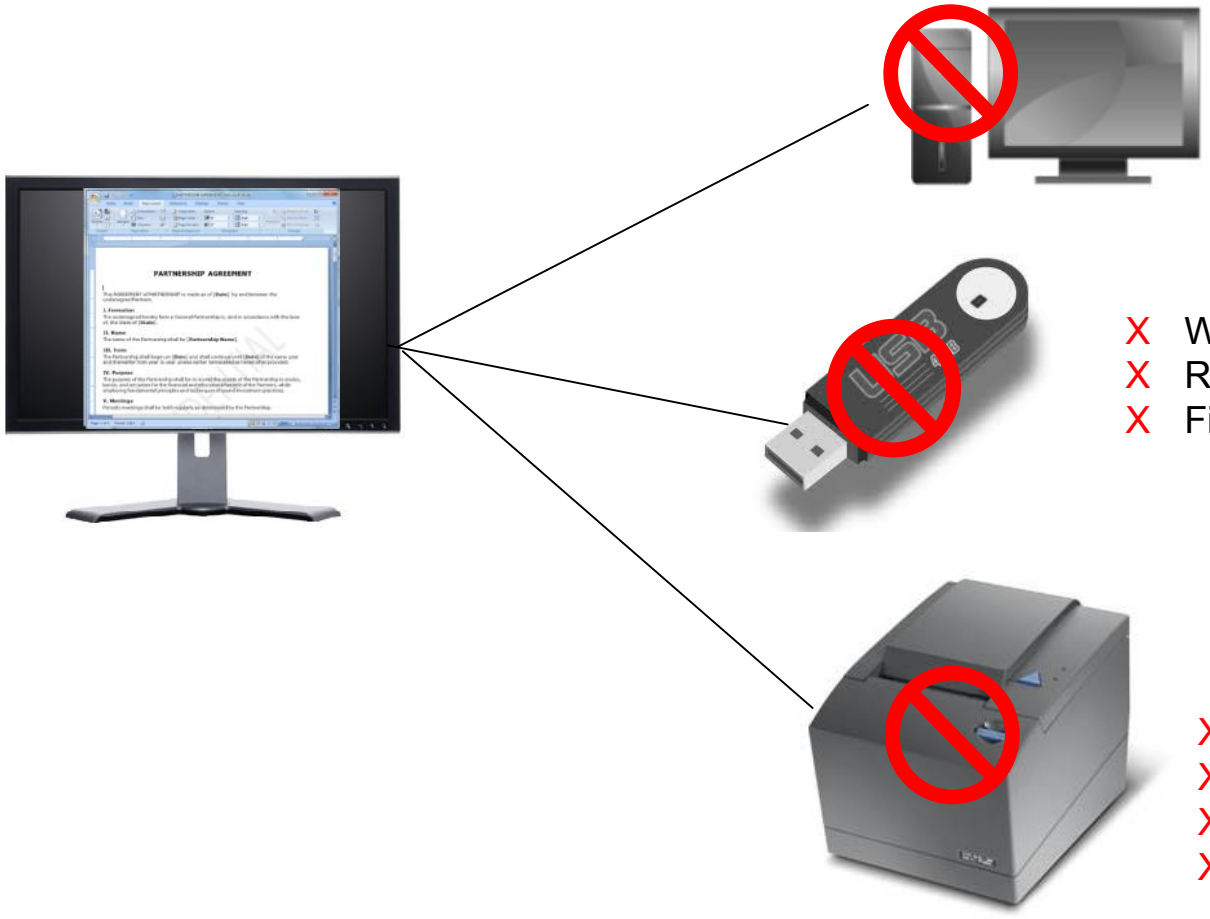
Data loss prevention: e-mail, browser, network



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Date	Employee ID	Name	Hourly Wage	Hours	Gross Pay	Federal Allow.	State Tax	Federal Income Tax	Social Security 6.2%	Medicare 1.45%	Total Tax Withheld	Insurance Deduction	Net Pay
2	11/4/2011	56	Kane, John	$13.25	36.00	$477.00	0	$34.33	$57.10	$29.57	$6.92	$127.92	$26.00	$323.08
3	11/4/2011	57	Kane, Lori	$25.00	40.00	$1,000.00	2	$74.86	$146.54	$62.00	$14.50	$297.90	$35.00	$667.10
4	11/4/2011	58	Kastner, Steven H.	$31.00	39.00	$1,209.00	1	$96.49	$213.70	$74.96	$17.53	$402.68	$35.00	$771.32
5	11/4/2011	59	Katyal, Sandeep	$13.00	20.00	$260.00	0	$17.73	$24.55	$16.12	$3.77	$62.17	$26.00	$171.83
6	11/4/2011	60	Kawai, Masato	$7.50	30.00	$225.00	1	$13.03	$10.36	$13.95	$3.26	$40.60	$26.00	$158.40
7	11/4/2011	61	Kearney, Bonnie	$8.22	36.00	$295.92	0	$20.48	$29.94	$18.35	$4.29	$73.05	$26.00	$196.87
8	11/11/2011	56	Kane, John	$13.25	40.00	$530.00	0	$38.39	$65.05	$32.86	$7.69	$143.98	$26.00	$360.02
9	11/11/2011	57	Kane, Lori	$25.00	33.00	$825.00	2	$59.11	$102.79	$51.15	$11.96	$225.01	$35.00	$564.99
10	11/11/2011	58	Kastner, Steven H.	$31.00	28.00	$868.00	1	$65.80	$128.45	$53.82	$12.59	$260.65	$35.00	$572.35
11	11/11/2011	59	Katyal, Sandeep	$13.00	39.00	$507.00	0	$36.63	$61.60	$31.43	$7.35	$137.01	$26.00	$343.99
12	11/11/2011	60	Kawai, Masato	$7.50	30.00	$225.00	1	$13.03	$10.36	$13.95	$3.26	$40.60	$26.00	$158.40
13	11/11/2011	61	Kearney, Bonnie	$8.22	36.00	$295.92	0	$20.48	$29.94	$18.35	$4.29	$73.05	$26.00	$196.87
14	11/18/2011	56	Kane, John	$13.25	33.00	$437.25	0	$31.29	$51.14	$27.11	$6.34	$115.88	$26.00	$295.37
15	11/18/2011	57	Kane, Lori	$25.00	40.00	$1,000.00	2	$74.86	$146.54	$62.00	$14.50	$297.90	$35.00	$667.10
16	11/18/2011	58	Kastner, Steven H.	$31.00	39.00	$1,209.00	1	$96.49	$213.70	$74.96	$17.53	$402.68	$35.00	$771.32
17	11/18/2011	59	Katyal, Sandeep	$13.00	20.00	$260.00	0	$17.73	$24.55	$16.12	$3.77	$62.17	$26.00	$171.83
18	11/18/2011	60	Kawai, Masato	$7.50	28.00	$210.00	1	$11.88	$8.11	$13.02	$3.05	$36.06	$26.00	$147.94

Protect confidential data by enforcing acceptable use practices, content-aware scanning, device control

Data loss prevention: external devices

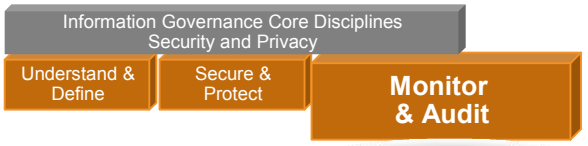


X Port restrictions
X Restricted keyword
X File size restricted

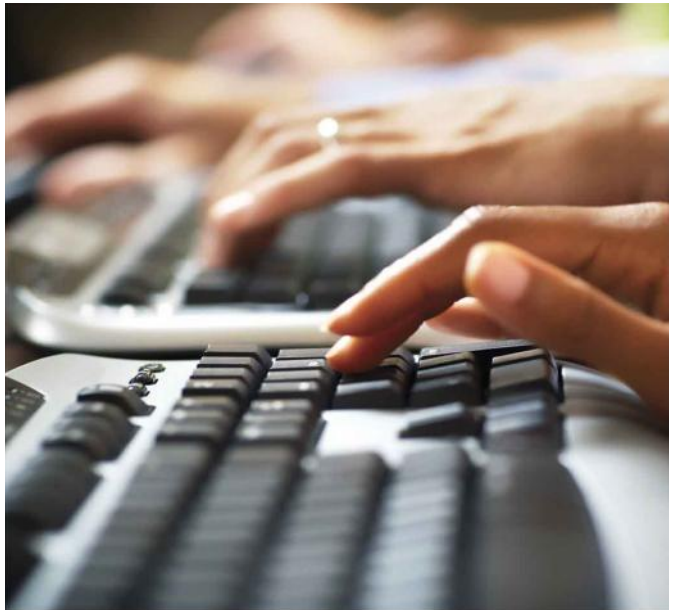
X Wrong USB serial number
X Restricted keyword
X File size restricted

X Access/Print restriction
X Restricted keyword
X Pattern restriction
X Print port restriction

What happens with compliance complacency?



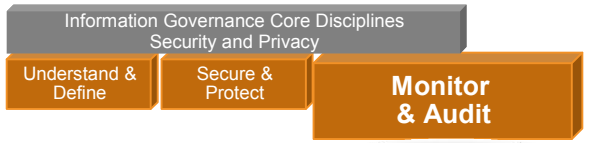
- Regulatory fines
  - No audit report mechanism
  - No fine grain audit trail of database activities
- Inability to detect data breaches
  - Lack of awareness of suspicious access patterns
  - On-going vs. single-invent: problems identifying patterns of unauthorized use
- Not able to monitor super user activity
  - Unable to detect intentional and unintentional events

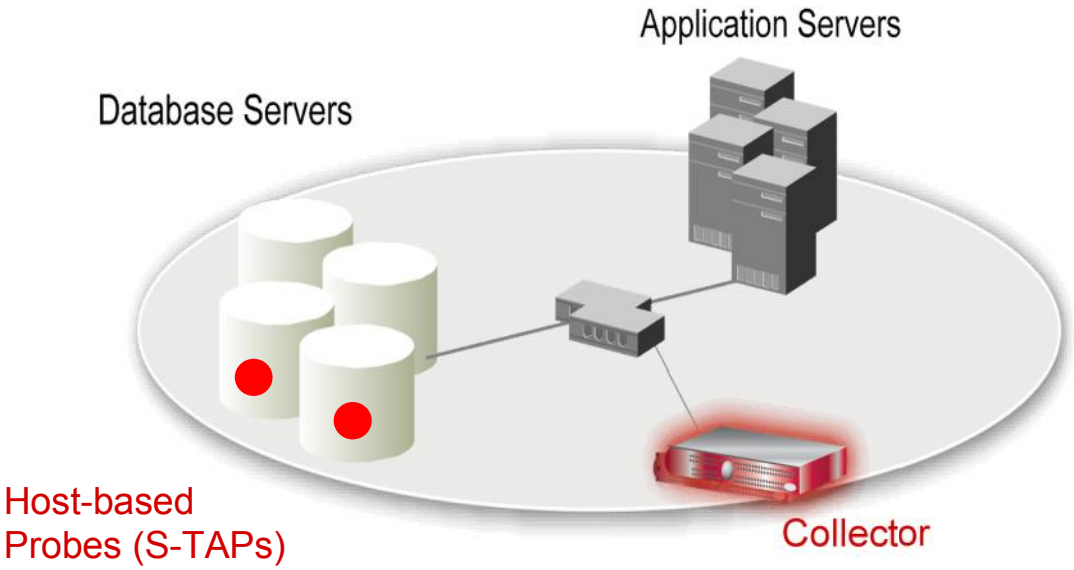


Most organizations do not have mechanisms in place to prevent database administrators and other privileged database users from reading or tampering with sensitive information [in business applications] … Fewer than two out of five respondents said they could prevent such tampering by super users.

-- Independent Oracle User Group

Real time database monitoring and protection with InfoSphere Guardium

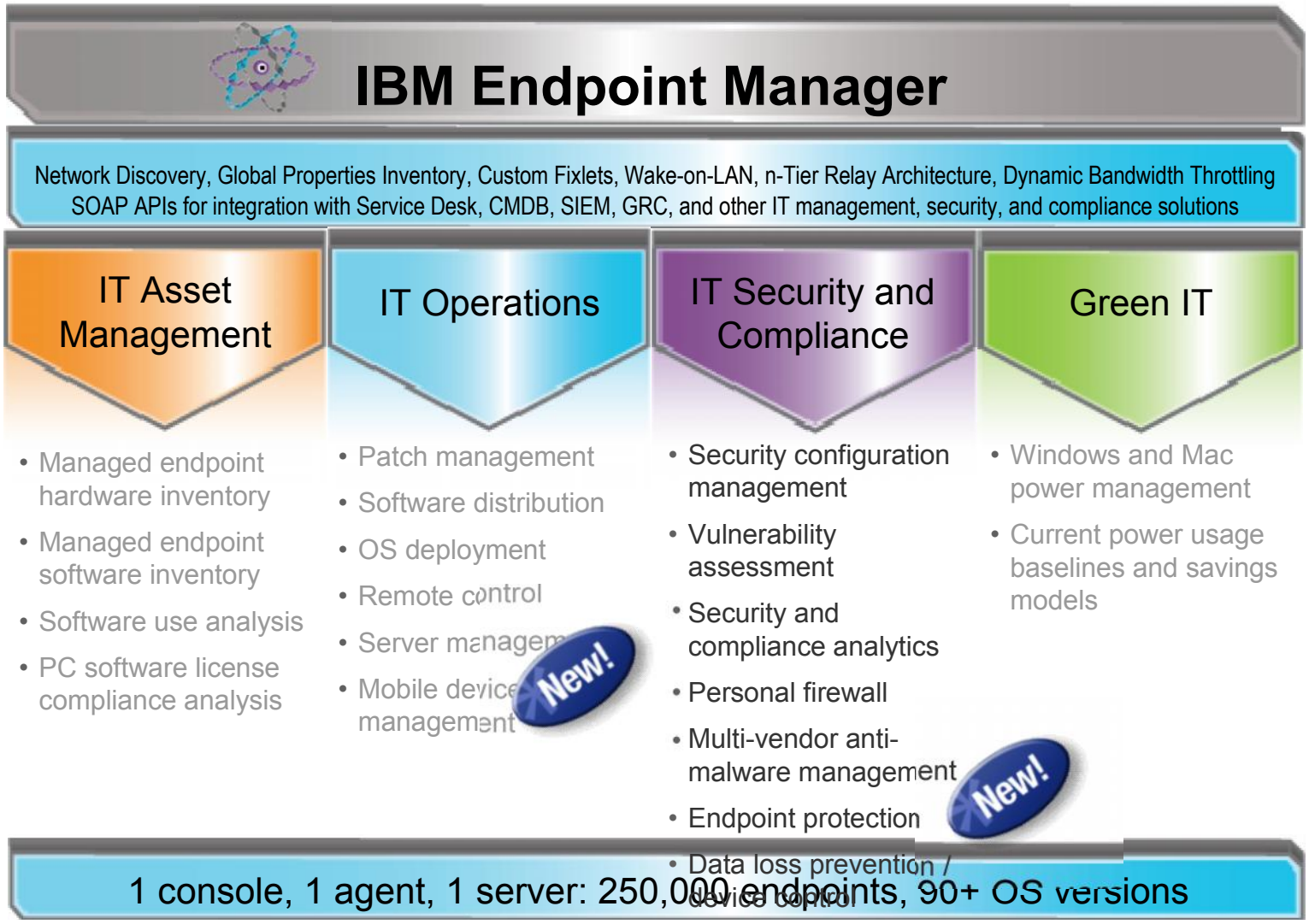




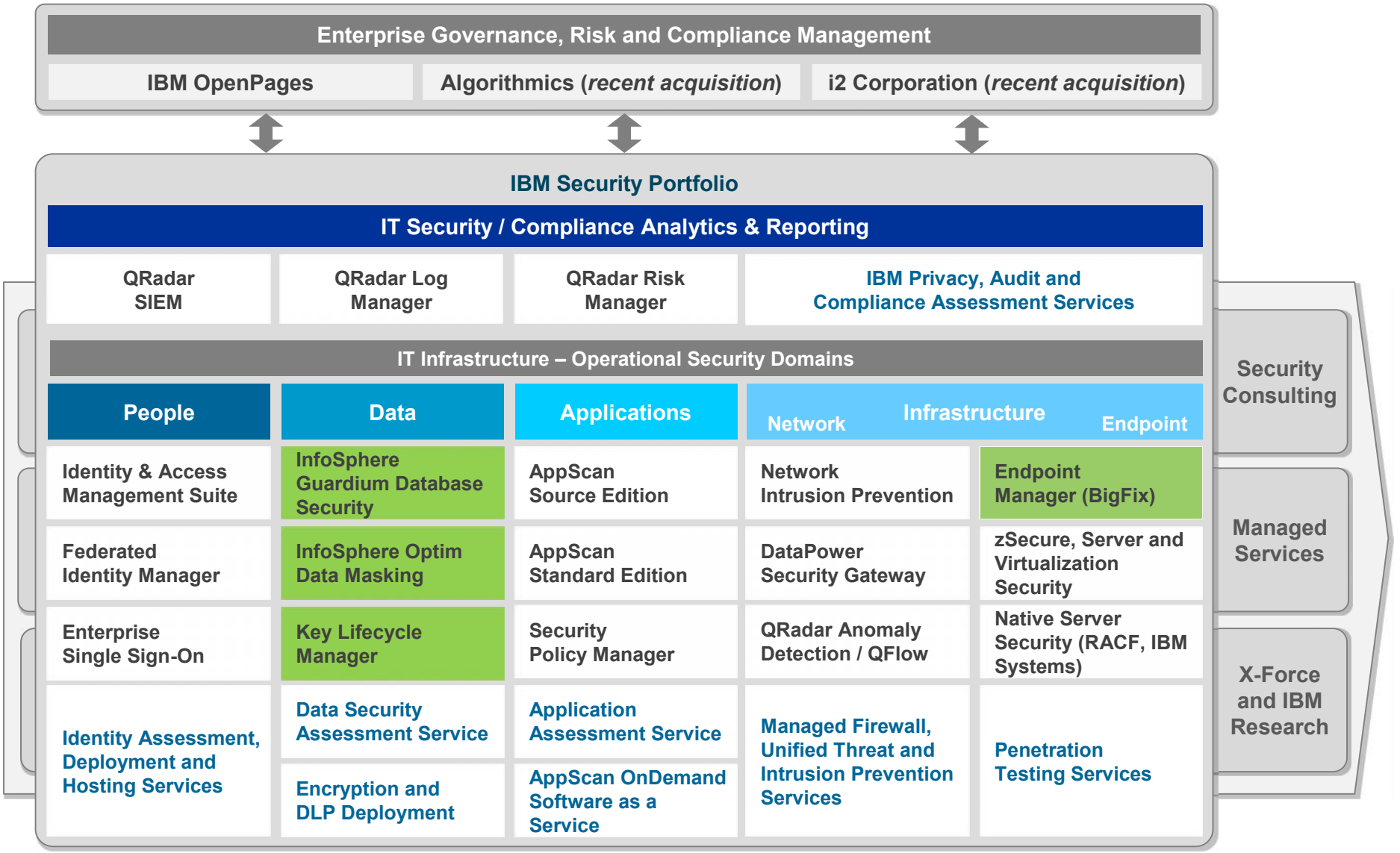
- No DBMS or application changes
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- 100% visibility including local DBA access
- Minimal performance impact

- Cross-DBMS solution
- Granular, real-time policies & auditing
  - *Who, what, when, how*
- Automated compliance reporting, sign-offs and escalations (financial regulations, PCI DSS, data privacy regulations, etc.)

Functional Overview



IBM's security product and service portfolio



Aviva UK Health

Data redaction supports payment card and privacy compliance

The need:

Aviva UK Health was challenged to satisfy incompatible PCI-DSS and DPA compliance requirements that threatened its ability to maintain credit card payment options for its customers.

The solution:

IBM InfoSphere Guardium Data Redaction supports both PCI-DSS and DPA requirements by automatically identifying and protecting sensitive data in unstructured documents and forms.

The benefits:

- Satisfied challenging PCI-DSS and DPA compliance requirements
- Avoided costly fines and protects sensitive customer data managed in document files
- Eliminated error-prone manual redaction processes and achieved a 97 average accuracy rate

"We are thoroughly impressed with IBM InfoSphere Guardium Data Redaction, its capabilities and accuracy rates. This technology is helping us comply with PCI-DSS requirements for historical content management of documents and forms."

— Leslie Ross, Head of BCIT, Aviva UK Health

Solution components:

- IBM Content Manager for z/OS
- IBM InfoSphere Guardium Data Redaction

AVIVA

Aviva Case Study

Global Online Financial Services Firm

Automates audit & change control processes to support compliance

The need:

Support compliance with Sarbanes-Oxley requirements and enhance data governance initiatives in four data centers managed by IBM Global Services. Phase 1 – Monitor all privileged user activities, especially database changes. Phase 2 – Protect customer privacy. Native auditing was not practical because of performance overhead and database servers at 99% capacity.

The solution:

IBM InfoSphere Guardium solutions monitor activity and protect privacy in four data centers comprising PeopleSoft plus 75 in-house applications, 122 database instances on 100 plus servers, and across Oracle Database, IBM DB2, Sybase and SQL Server on AIX, HP-UX, Solaris and windows.

The benefits:

- Automates auditing and reporting capabilities for monitoring over one million sessions per day (GRANTs, DDL, etc.) and successfully passed several external audits
- Supports daily audit reporting compliance for Sarbanes Oxley with sign-off by oversight teams
- Monitors all privileged user activities to prevent mishandling of client confidential and transaction sensitive information and to protect privacy

"We are confident that the IBM InfoSphere Guardium solutions are effectively monitoring all user activities and helping us comply with privacy and audit requirements."

—Online Financial Services Firm

Solution components:

- IBM InfoSphere Guardium Database Activity Monitor
- IBM InfoSphere Database Vulnerability Assessment Solution
- IBM Global Services manages four data centers

CSFi
Complies with PCI DSS

The need:
CSFi needed to satisfy PCI DSS. This meant ensuring that no devise or system retains cardholder data while trying to grow in new overseas markets to beat the competition and increase revenues.

The solution:
CSFi used InfoSphere Guardium Data Encryption to satisfy PCI DSS rather than using column level encryption which can slow performance and is difficult to implement.

The benefits:
- Ensure compliance with Payment Card Industry Data Security Standard (PCI DSS)
- Allow IT staff to focus on value recreation and not tedious manual tasks
- Achieve all security and privacy requirements while maximizing system throughput
- Meet SLAs for processing transactions in just a few milliseconds

Solution components:
- IBM InfoSphere Guardium Data Encryption
- IBM Informix Dynamic Server

Arek Oy

Deploys a pension earnings and accrual system in 30 months

The need:

Pension laws (TyEL) in Finland changed radically in 2007. In response, Arek Oy had to develop and deliver a tested and reliable Pension Earnings and Accrual System within 30 months. Arek Oy had to protect confidential employee salary and pension information in multiple non-production (development and testing) environments. Failure to satisfy requirements would result in loss of customer good will and future business opportunities.

The solution:

Using IBM InfoSphere Optim subsetting capabilities rather than cloning large production databases made it possible for Arek Oy staff to create robust, realistic test databases that supported faster iterative testing cycles. In addition, InfoSphere Optim offered proven capabilities for performing complex data masking routines, while preserving the integrity of the pension data for development and testing purposes.

The benefits:

- Improved development and testing efficiencies, enabling Arek Oy to promote faster deployment of new pension application functionality and enhancements
- Protected confidential data to strengthen public confidence and support TyEL compliance requirements

"We see Optim as an integral part of our development solution set. Optim's data masking capabilities help ensure that we can protect privacy in our development and testing environments."

— Katri Savolainen, Project Manager, Arek Oy

Solution components:

- IBM InfoSphere Optim Data Masking Solution
- IBM InfoSphere Optim Test Data Management Solution

arek

Arek Oy Case Study

Learn more

Understand compliance mandates

- Whitepaper: Protect payment card data with InfoSphere
- Whitepaper: Help ensure HIPAA compliance with InfoSphere
- Whitepaper: Understanding encryption requirements of PCI DSS
- ebook: Managing compliance to protect enterprise data

Talk to your sales rep about holistic data security

- Whitepaper: Secure Enterprise Data & Ensure Compliance
- ROI Study: Forrester Total Economic Impact of InfoSphere Guardium
- Website: InfoSphere Guardium Database Security