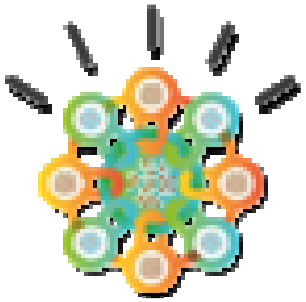
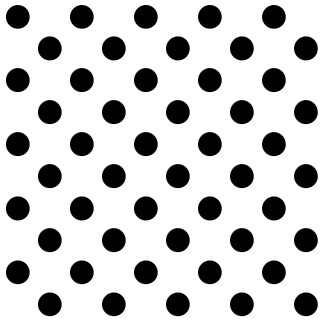


Secure and Protect Enterprise Data in 2013

David Valovcin
dvalovcin@us.ibm.com

Four dimensions of big data

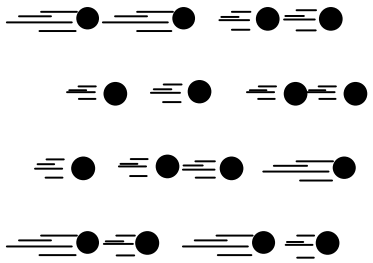
Volume



Data at Rest

Terabytes to exabytes of existing data to process

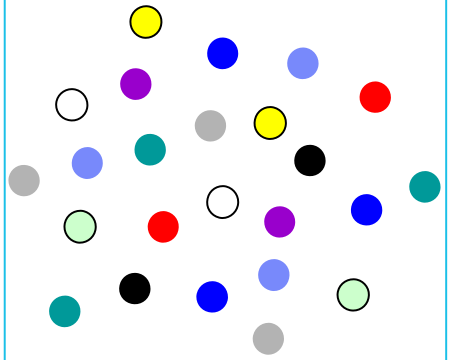
Velocity



Data in Motion

Streaming data, milliseconds to seconds to respond

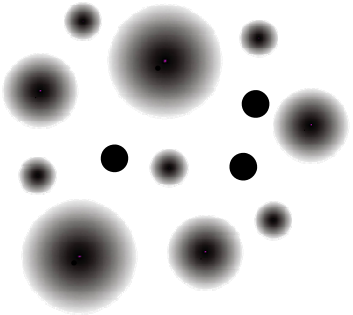
Variety



Data in Many Forms

Structured, unstructured, text, multimedia

Veracity*



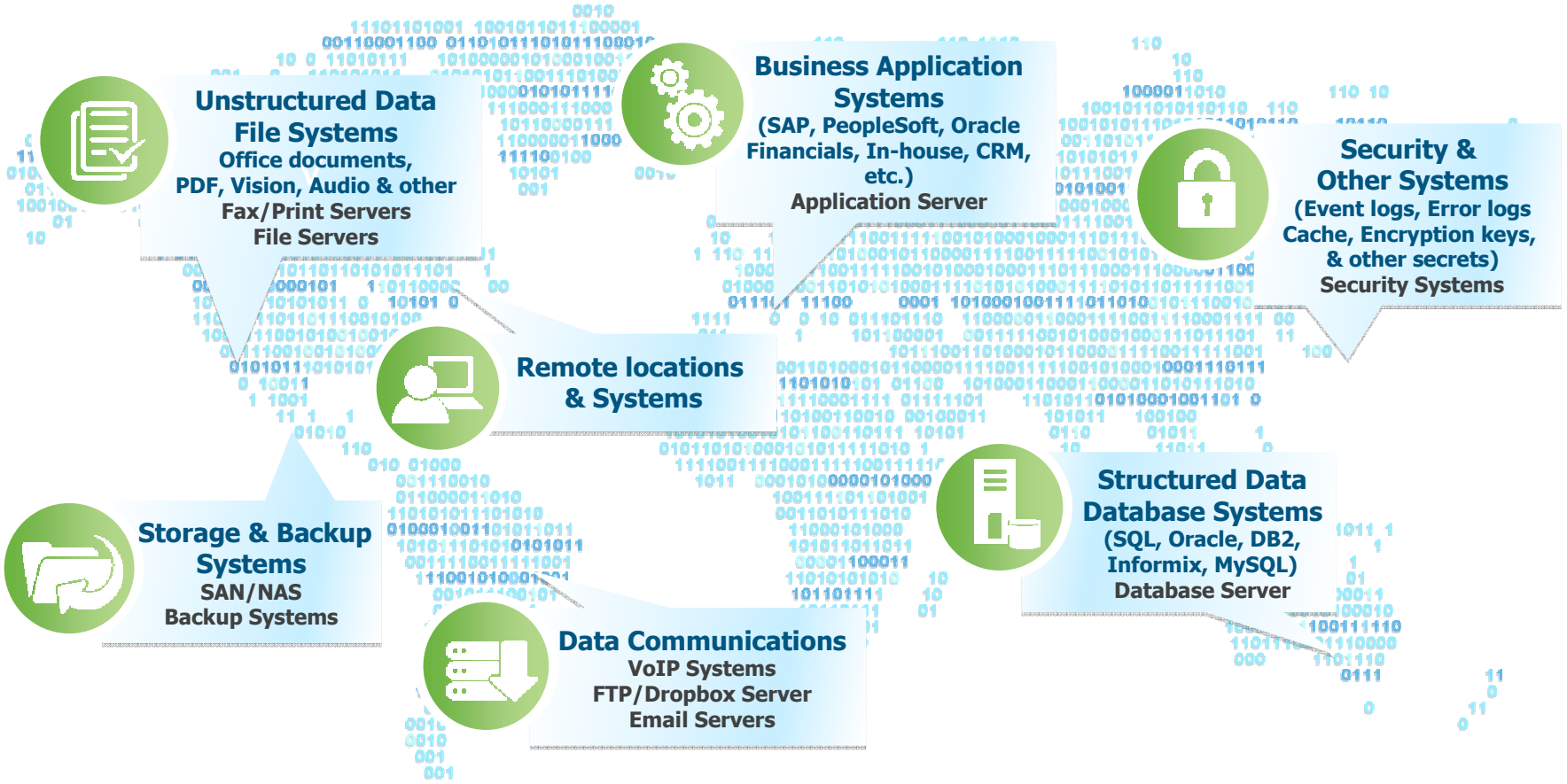
Data in Doubt

Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations

* Truthfulness, accuracy or precision, correctness

What is data security and privacy?

Protection of high value data



Sensitive data is EVERYWHERE

METROPOLITAN MUNICIPALITY (Government)

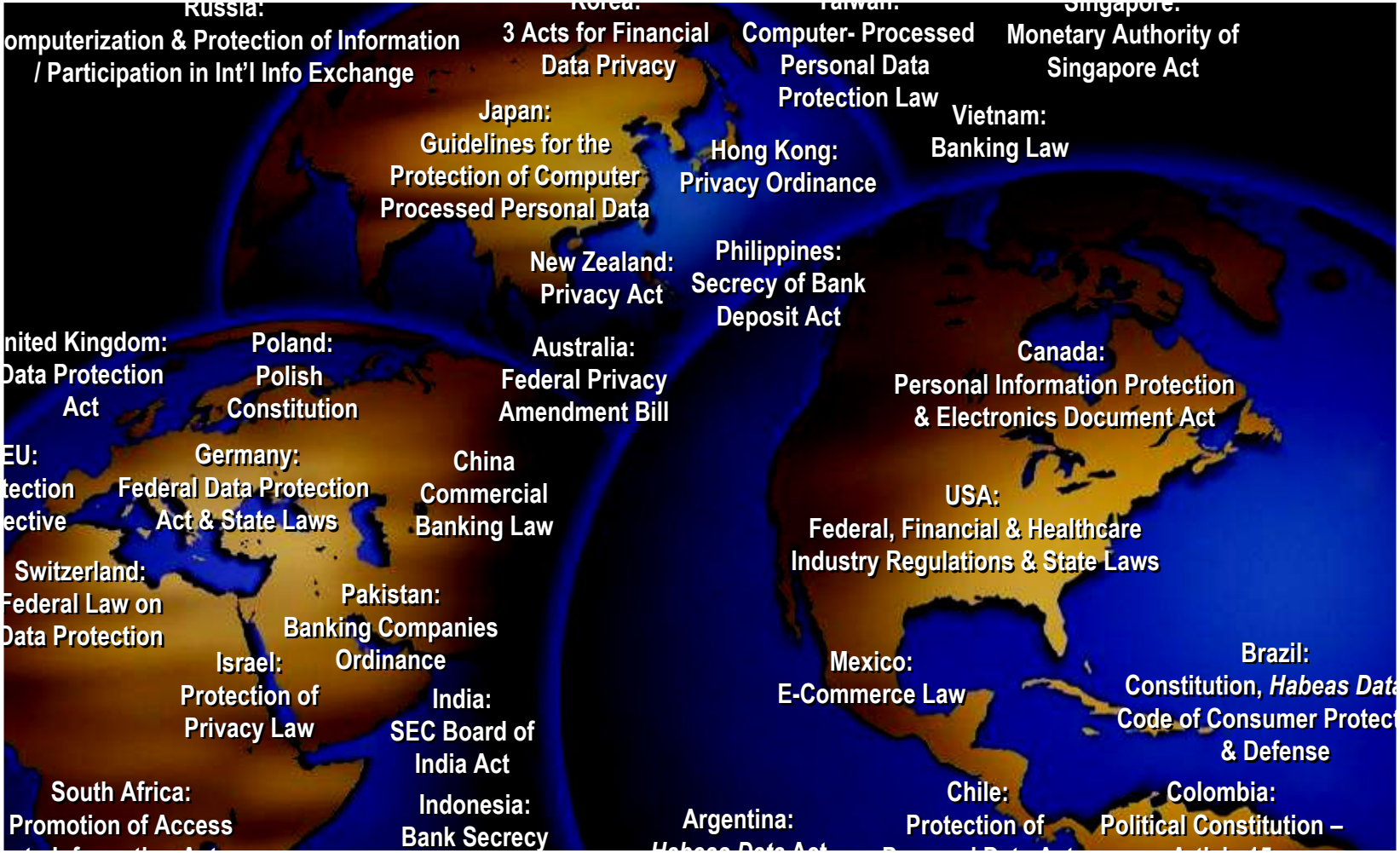
Which Critical Data Asset is Guardium safeguarding:

- *Accounts Payable database (Municipality Expenditures)*
- *Utilities Payment database (water, electricity)*

- **Why ?**
- Expenditure databases holds all the money that goes out. Unauthorized changes can mean **paying more** to vendors.
- Unauthorized changes to customer's bills, can **negatively affect** the municipality's main revenue source.
- Apart from negatively affecting the main revenue source, unauthorized users can get access to **Banking Details** of those customers who pay on-line

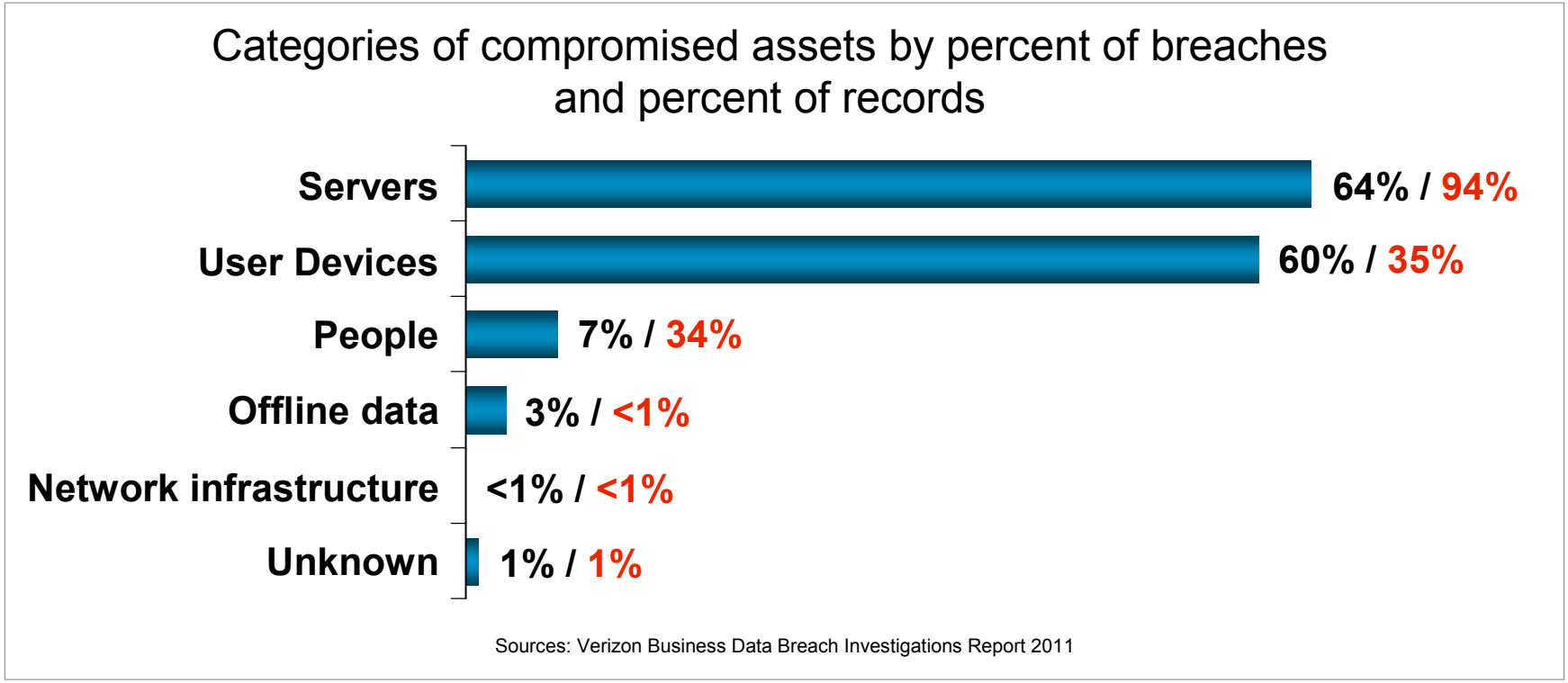
Can you prove that privileged users have not inappropriately accessed or jeopardized the integrity of your sensitive customer, financial and employee data?

Worldwide regulations focus attention on security concerns



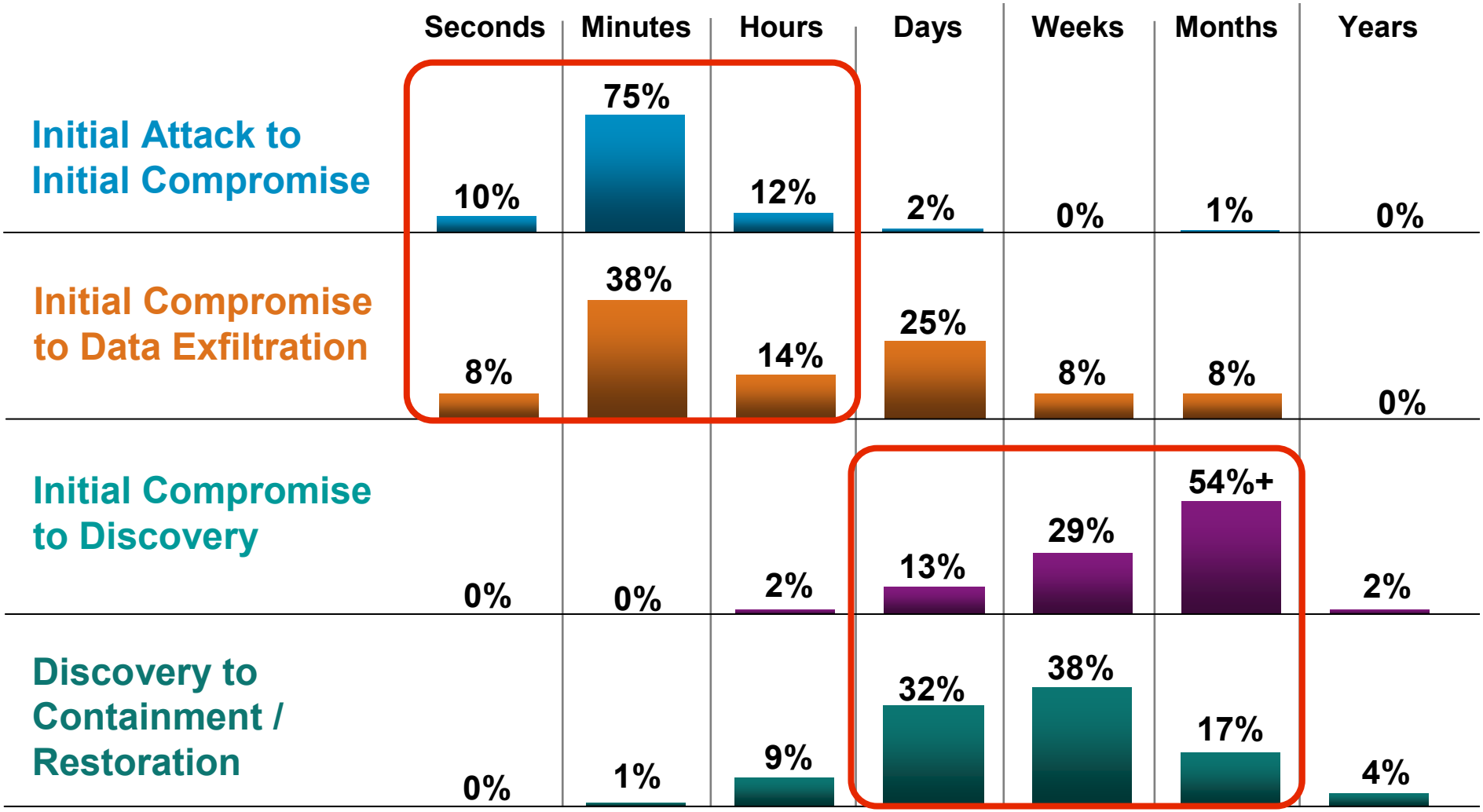
Database servers are the primary source of breached data

Focus limited resources on the most threatened data source



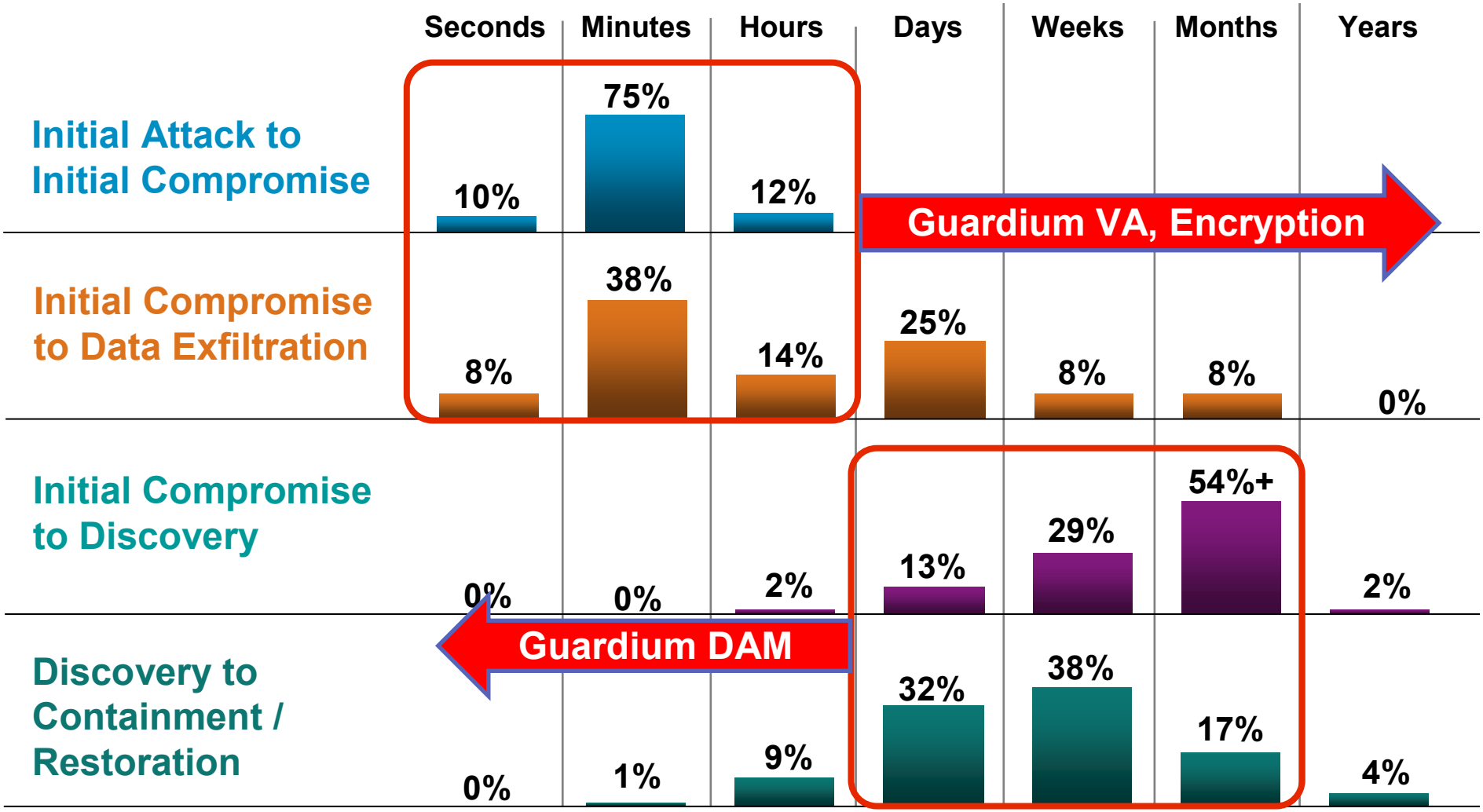
> *It's really not surprising that servers seem to have a lock on first place when it comes to the types of assets impacted by data breaches. They store and process data, and that fact isn't lost on data thieves.*

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

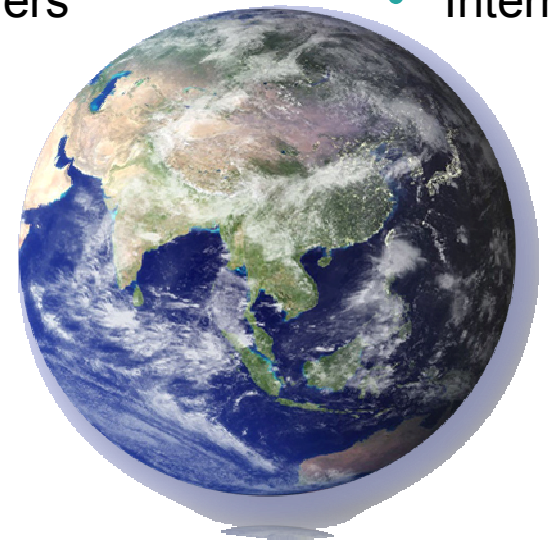
Organizations are slow to respond to database attacks



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

Chosen by Leading Organizations Worldwide

- 8 of the top 10 global banks
- 5 of the top 6 global insurers
- 4 of the top 4 health care providers
- 9 of the top 10 telecoms
- 3 of the top 4 auto makers
- 3 of the world's favorite beverage brands
- 2 of the top 3 global retailers
- Top government agencies
- Top global cardholder brand
- Top energy suppliers
- The most recognized name in PCs
- #1 dedicated security company
- Media & entertainment brands
- International airline brands



The Choice of Financial Services

JPMorgan Chase & Co.	HSBC	ICBC	citi	BNP PARIBAS
Santander	Allianz	AIG	ING	BARCLAYS
SOCIETE GENERALE Corporate & Investment Banking	AXA Rosenberg An AXA Investment Managers Company	MUFG Bank of Tokyo-Mitsubishi UFJ	BBVA Compass	UniCredit
INTESA SANPAOLO	MetLife	ANZ	SMFG Sumitomo Mitsui Financial Group	Scotiabank
MIZUHO	Prudential 保德信	PRUDENTIAL	Itaú	AVIVA

The Choice of Telecommunications

vodafone	Telefónica	ASPire Holdings	NTT Communications	verizon
adquira	orange	telcel	T-Systems	TELECOM ITALIA
Maroc Telecom Un monde nouveau vous appelle	Tre.it	Designing The Future KDDI	ERICSSON	SoftBank
telenor group	MTS	VimpelCom	Chunghwa Telecom	Sprint
zain	TÜRK TELEKOM	vtr	Otel	TURKCELL

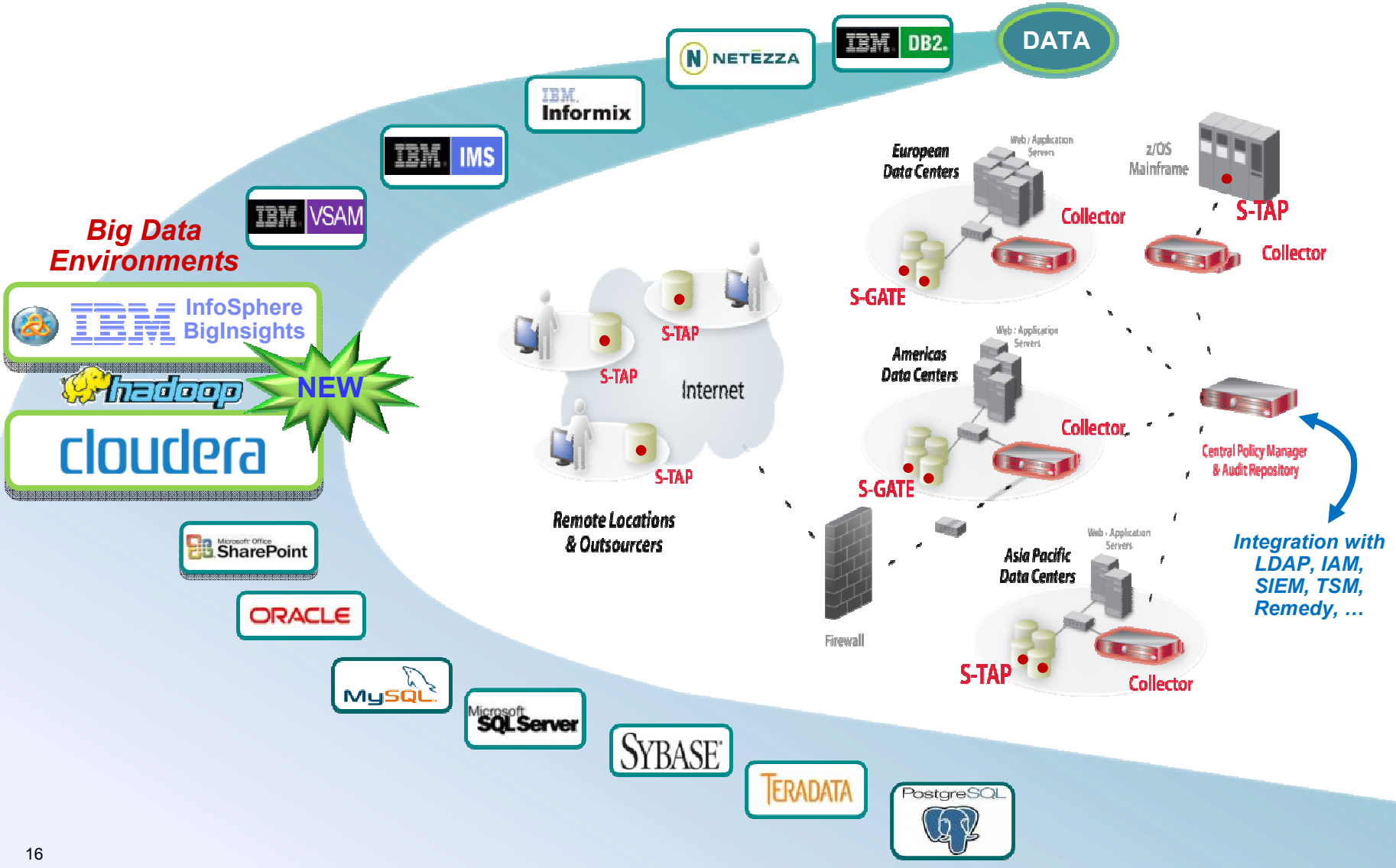
The Choice of Energy & Utilities

GAZPROM NEFT	e·on		nationalgrid THE POWER OF ACTION	THE KANSAI ELECTRIC POWER CO.,INC.
FPL	PG&E	encana natural gas	SOUTHERN CALIFORNIA EDISON® An EDISON INTERNATIONAL® Company	cenovus ENERGY
Progress	TALISMAN ENERGY	Ameren	SCANA POWER FOR LIVING	CIMAREX
pepco	SK	USEC A Global Energy Company	DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA	Government of South Australia Department for Transport, Energy and Infrastructure
NVEnergy	EPCOR	Gexa ENERGY	Yanchang Petroleum	ISO

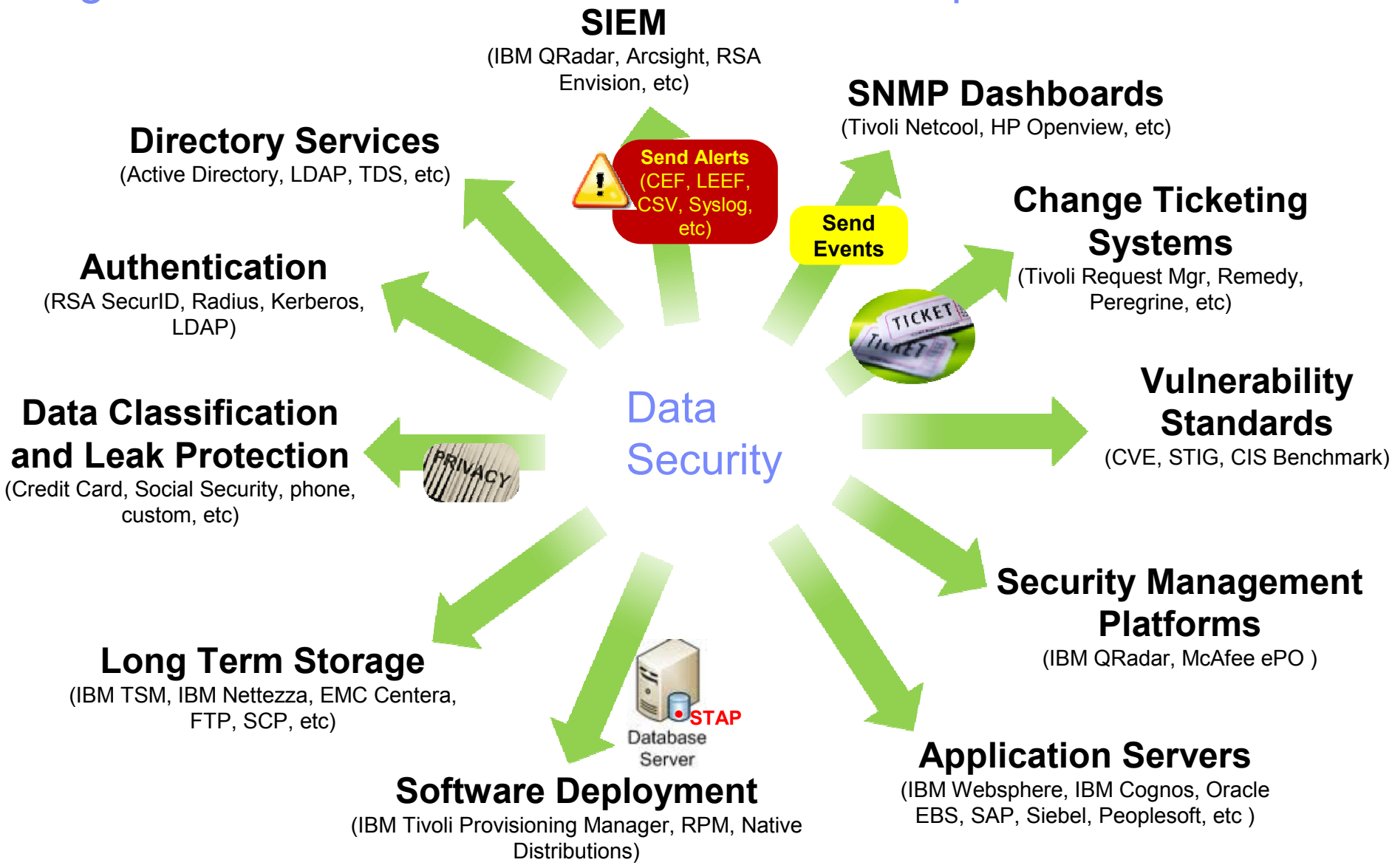
The Choice of Middle East & Africa

The Choice of Local Organizations

Extend real-time Data Activity Monitoring to protect sensitive data in databases, data warehouses, Big Data environments and file shares



Integrate with IT Infrastructure for seamless operations



Reports and Workflow

Failed User Login Attempts

User Name	Client IP	Server IP	Number of Exceptions
ajhernandez	10.10.10.88	10.10.10.60	4
apreciado	10.80.10.132	10.10.10.60	4
bpetty	10.10.10.88	10.10.10.60	4
des	10.80.22.107	10.10.10.79	4
dpieratt	10.10.10.88	10.10.10.60	6
fandalon	10.10.10.171	10.10.10.79	1
gonzalez	10.80.10.93	10.10.10.60	2
hgonzalez			
hgonzalez			
hgonzalez			
ktom			
ohernandez			
sa			
sa			
sa			
sa			
sa			
sa			

Detailed SQL Audit by Client IP

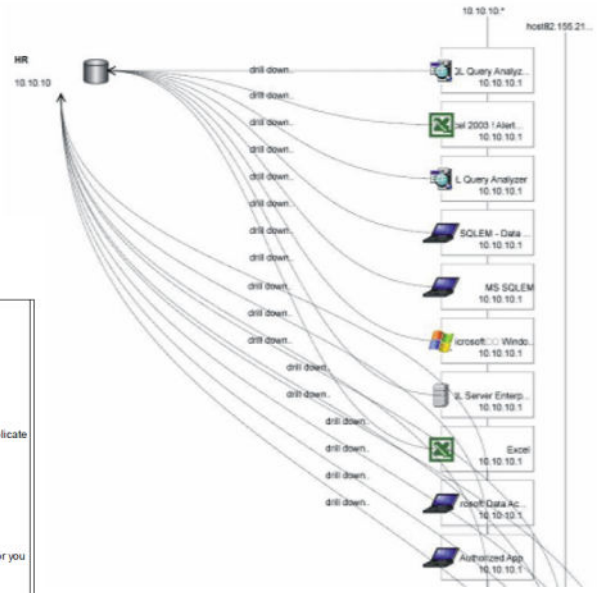
Client IP	Count Of SQL Verb	Count Of Object	Total access
10.10.10.20	26	1132	6399656
10.80.10.128	19	363	349909
10.10.10.171	7	179	104835
10.80.10.93	23	1405	81969
10.10.10.88	14	771	61629
10.80.10.136	8	290	46012
10.80.10.132	19	568	24259
10.80.10.96	18	575	13106
10.80.15.98	13	440	11163
10.10.10.102	24	446	11041
10.10.10.65	21	408	8583
10.80.25.56	9	99	7 960

8. Data Access Map Viewed by Database

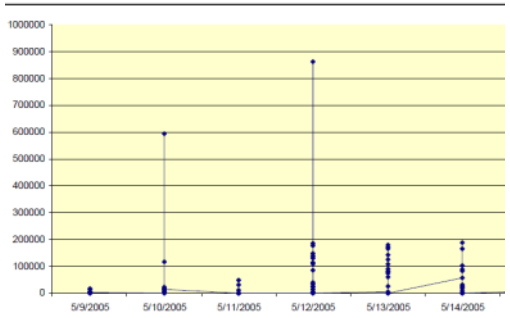
The following table shows a partial set of databases accessed for server 10.10.10.60

Server IP	Database Name	Source Programs	Sessions
10.10.10.60	CARDS	2	6
10.10.10.60	ConcurExpense	2	11
10.10.10.60	CPI	2	2
10.10.10.60	dynamics	4	151
10.10.10.60	EFM	1	1
10.10.10.60	EGL	1	1
10.10.10.60	ELV	1	1
10.10.10.60	GP_ICENTER	1	1
10.10.10.60	H5720		
10.10.10.60	ICENTER		
10.10.10.60	Interchang		
10.10.10.60	Interchang		
10.10.10.60	Interchang		
10.10.10.60	M4150		

Visual Data Access Map

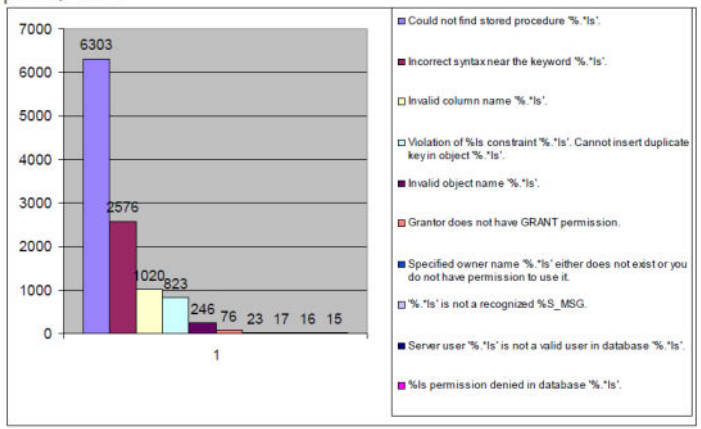


Throughput



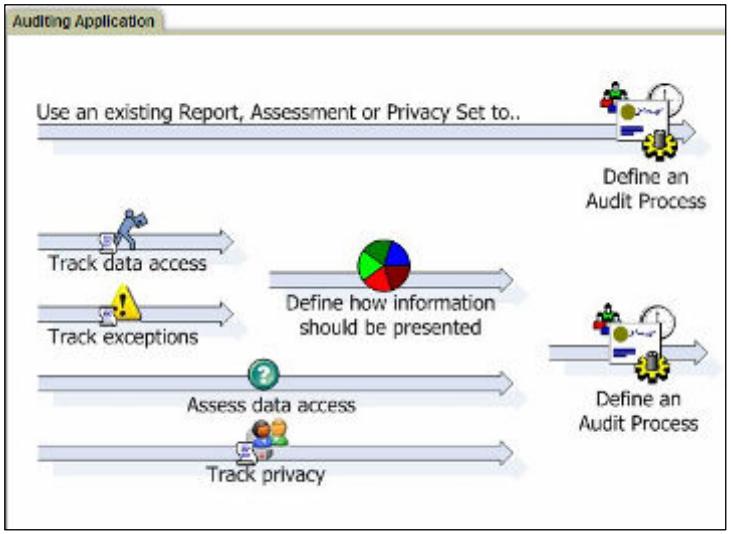
Errors and Exceptions

1. Top 10 SQL Errors



Workflow Automation

- Scheduled & automated tasks
- Find sensitive data as it "migrates" due to ongoing changes
  - Find by pattern, table name, etc. – and then:
  - Assign classification, alert, add to group, etc. (policy-based)
  - Run on regular basis to keep security policies updated
- Compliance reporting
  - Automatically generate reports
  - Distribute to oversight team
  - Track electronic sign-offs
  - Escalate when required
  - Store process trail in secure repository
  - *Demonstrates oversight process for auditors*



Large Regional Bank

Monitors database activity to support compliance regulations

The need:

Prevent users from inappropriately accessing or jeopardizing the integrity of enterprise data. Protect financial and transactional data including: payment card primary account numbers (PAN data), automatic cleansing house (ACH) transaction data and human resources (HR) data. Comply with Sarbanes-Oxley, Payment Card Industry Data Security Standard (PCI-DSS) and other financial privacy and audit regulations.

The solution:

Implemented IBM InfoSphere Guardium Database Activity Monitor to monitor end-user and privileged user activity across the **IBM DB2, Oracle Database, MS SQL Server, and MySQL** databases in the **AIX, Solaris, Windows and Linux** environments.

The benefits:

- Effectively monitors database activity for over 800 banking branches and supports compliance with privacy and audit regulations
- Helps prevent fraud and delivers return on investment with capabilities to identify suspicious database activities
- Supports data governance by preventing unauthorized changes to critical database values and structures

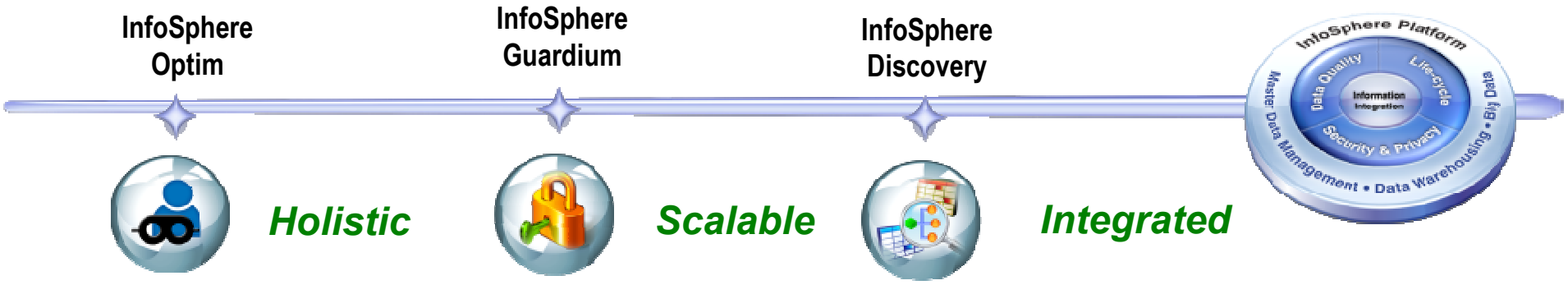
"Monitoring database activity with IBM Guardium is helping us support compliance with our privacy and audit requirements without impacting database performance."

-- Source: Senior DBA, Large Regional Bank

Solution components:

- **IBM InfoSphere Guardium Database Activity Monitor**

InfoSphere Platform for data security and compliance



Allows you to …

Reduce the cost of compliance

- Customer streamlines testing and protects test data **saving $240K/year** in administrative costs

Prevent data breaches

- Organizations complete audits **20% faster** saving about **$50,000** per year

Ensure data integrity

- Monitoring database activity protects data and provides **239%** ROI

The Difference

- Completely protects across diverse data types and environments
- Scales across small and large heterogeneous enterprises
- Delivers both processes and technologies

Understand the SCOPE of your project

DATA

- ❑ What data repositories I have?
- ❑ Where does my sensitive date reside?

Credentials

- ❑ Who has access to what data
- ❑ Who should have access

Stakeholders

- ❑ Who owns Security?
- ❑ Who owns Compliance?
- ❑ Who views the audit reports?
- ❑ Who reacts to security incidents?
- ❑ Who updates security policies?

Audit Requirements

- ❑ What regulations or requirement?
- ❑ What activity should be logged?
  - ▪ Which users to audit?
  - ▪ What granularity to log?
  - ▪ What is the retention period?
- ❑ What are the archive requirements?

Security Policies

- ❑ What activity to monitor?
  - ▪ Requests
  - ▪ Replies
  - ▪ Exception
- ❑ What action to take when policy violated?
  - ▪ Trigger an alert
  - ▪ Block / Terminate / Quarantine
  - ▪ Mask

Reduce costs through integrations and automation

IT Changes

- New data center
- New Servers
- Consolidation/Virtualization projects
- New Database Instance

Failover
Load Balancing
Guardium Grid

Discovery
Classification

Personnel Changes

- Employee leaving the company
- New DBA hired
- Roles Rotation / Change of responsibilities

Data Level Security
Users Hierarchies
LDAP Integration

Regulatory/Policy changes

- New Audit Requirements
- New Security Threats
- New Regulation put in place

Automation of
- Group generation
- Audit Reports
- Security Policies

What's the business value?

Profitability

- Reduce fraudulent transactions
- Speed audits
- Increase customer satisfaction
- Protect brand reputation
- Reduce operational costs
  1. Labor
  2. Power
  3. Data Center Space
  4. Hardware / Software

Business Agility & Resiliency

- Increase ability to meet SLA
- Increase application performance
- Reduce downtime
- Automate repetitive tasks
- Increase visibility and clarity

Data Security & Risk Mitigation

- Improve visibility to risk exposure
- Implement controls to mitigate risk
- Demonstrate compliance
  1. Sox
  2. PCI
  3. Data Privacy
  4. Other/Corporate regulations

David Valovcin
dvalovcin@us.ibm.com