CSO Executive Seminar Series on

Securing the Cloud

May 19, 2011

Protecting Your Data in the Cloud

Ulf Mattsson
Chief Technology Officer
ulf.mattsson [at] protegrity.com

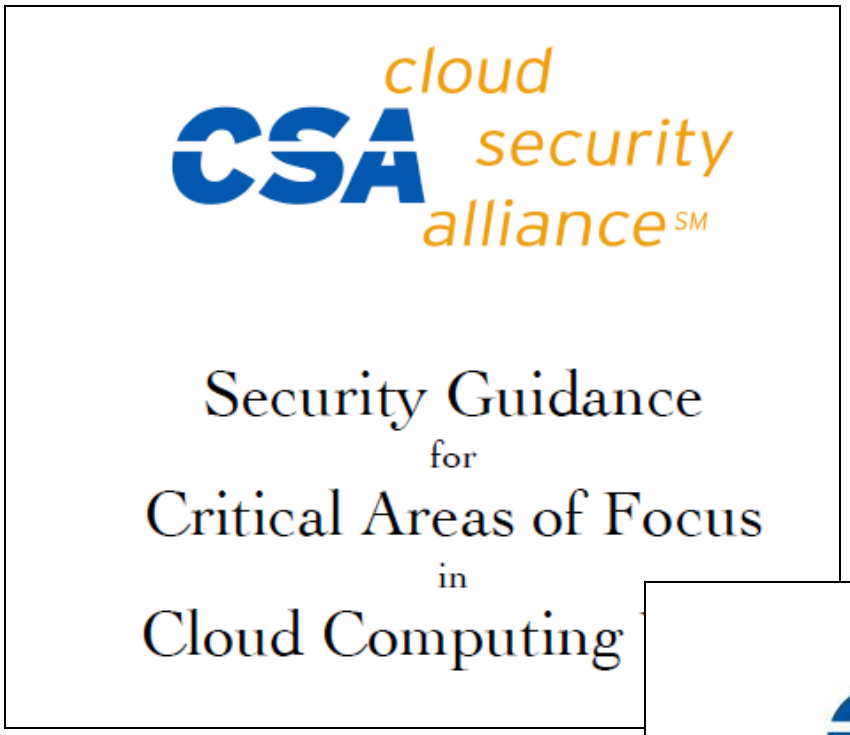
protegrity

protecting your data.
protecting your business.

Ulf Mattsson

- 20 years with IBM Development & Global Services
- Inventor of 22 patents – Encryption and Tokenization
- Co-founder of Protegrity (Data Security)
- Research member of the International Federation for Information Processing (IFIP) WG 11.3 Data and Application Security
- Member of
  - Cloud Security Alliance (CSA)
  - PCI Security Standards Council (PCI SSC)
  - American National Standards Institute (ANSI) X9
  - Information Systems Security Association (ISSA)
  - Information Systems Audit and Control Association (ISACA)

Guidance from Cloud Security Alliance



protegrity

Cloud Security Debate

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Debate >> Encryption is better equipped than tokenization to secure data in the cloud.

October 01 2010

AGAINST

Ulf Mattsson

CTO, Protegrity

One of the biggest
tokenization is a b
transparent, faster,
decreases administ
risk, exposure of e
by replacing sensit
anything with the
remediation costs t
That said, analysts
take shortcuts and
the analysts. Toker

ISSA | PREEMINENT TRUSTED GLOBAL INFORMATION SECURITY COMMUNITY

ISSA Journal | December 2010

Next Generation Tokenization for Compliance and Cloud Data Protection

By Ulf Mattsson – ISSA member, New York Metro, USA Chapter

This article will discuss how next-generation tokenization protects data as it flows across systems while minimizing PCI compliance costs.

ISACA®
Serving IT Governance Professionals
New York Metropolitan Chapter

Metr

Volume 1, Issue 4

Cloud Computing – Assessing Data Security Risks and Solutions

Ulf Mattsson
CTO
Protegrity

Security Mag
AL & PHYSICAL SECURITY MAGAZINE

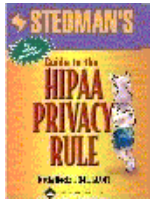
Ulf Mattsson, CTO, Protegrity: Making Sense of the Sony Breach

April 2011 by Ulf Mattsson, CTO, Protegrity Corporation

About Protegrity

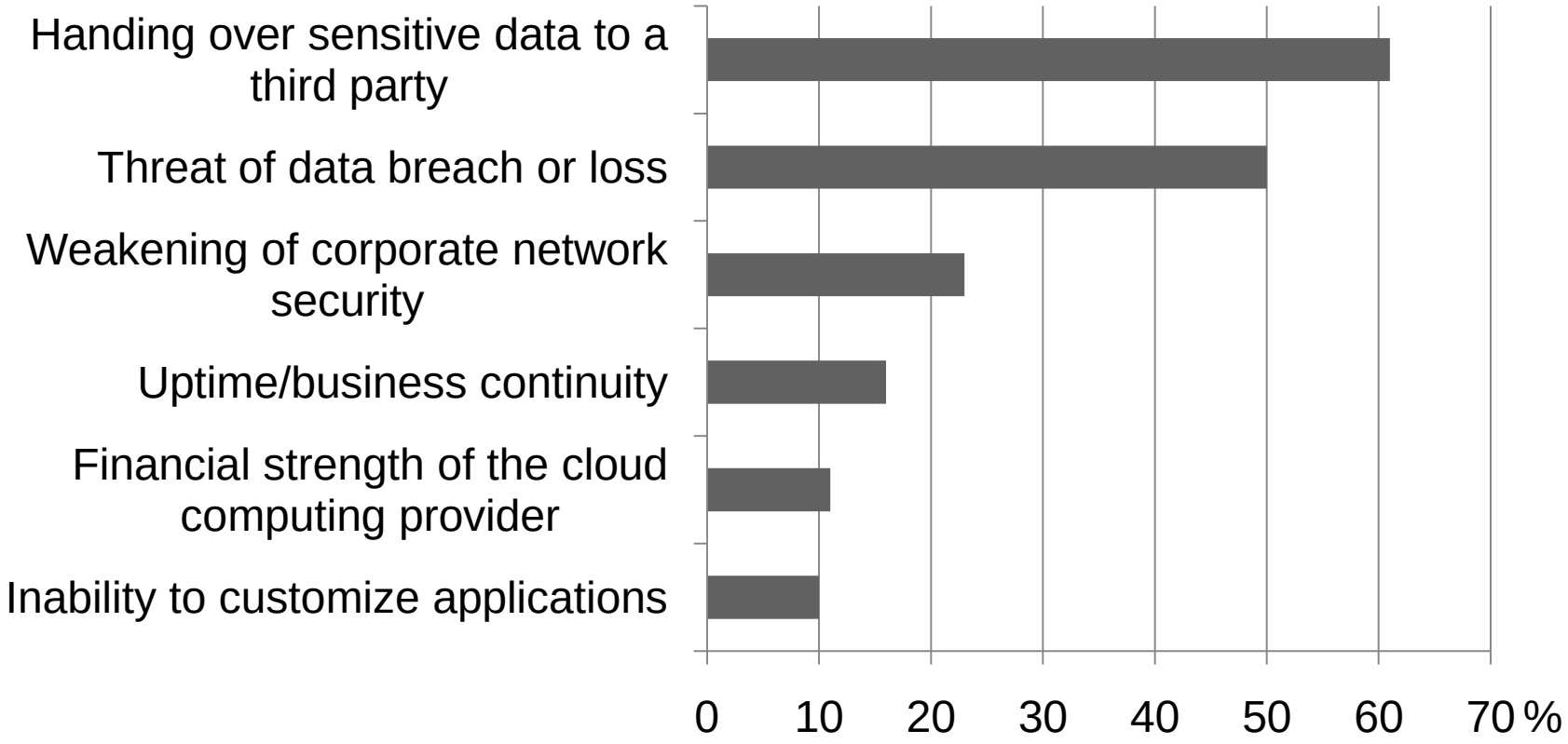
- Proven enterprise data security software and innovation leader
  - Sole focus on the protection of data
  - Patented Technology, Continuing to Drive Innovation
- Growth driven by compliance and risk management
  - PCI (Payment Card Industry)
  - PII (Personally Identifiable Information)
  - PHI (Protected Health Information) – HIPAA
  - State and Foreign Privacy Laws, Breach Notification Laws
  - High Cost of Information Breach ($4.8m average cost), immeasurable costs of brand damage , loss of customers
  - Requirements to eliminate the threat of data breach and non-compliance
- Cross-industry applicability
  - Retail, Hospitality, Travel and Transportation
  - Financial Services, Insurance, Banking
  - Healthcare
  - Telecommunications, Media and Entertainment
  - Manufacturing and Government

PCI Security Standards Council™
PARTICIPATING ORGANIZATION



protegrity

Risks Associated with Cloud Computing



Source: The evolving role of IT managers and CIOs Findings from the 2010 IBM Global IT Risk Study

Best Source of Incident Data

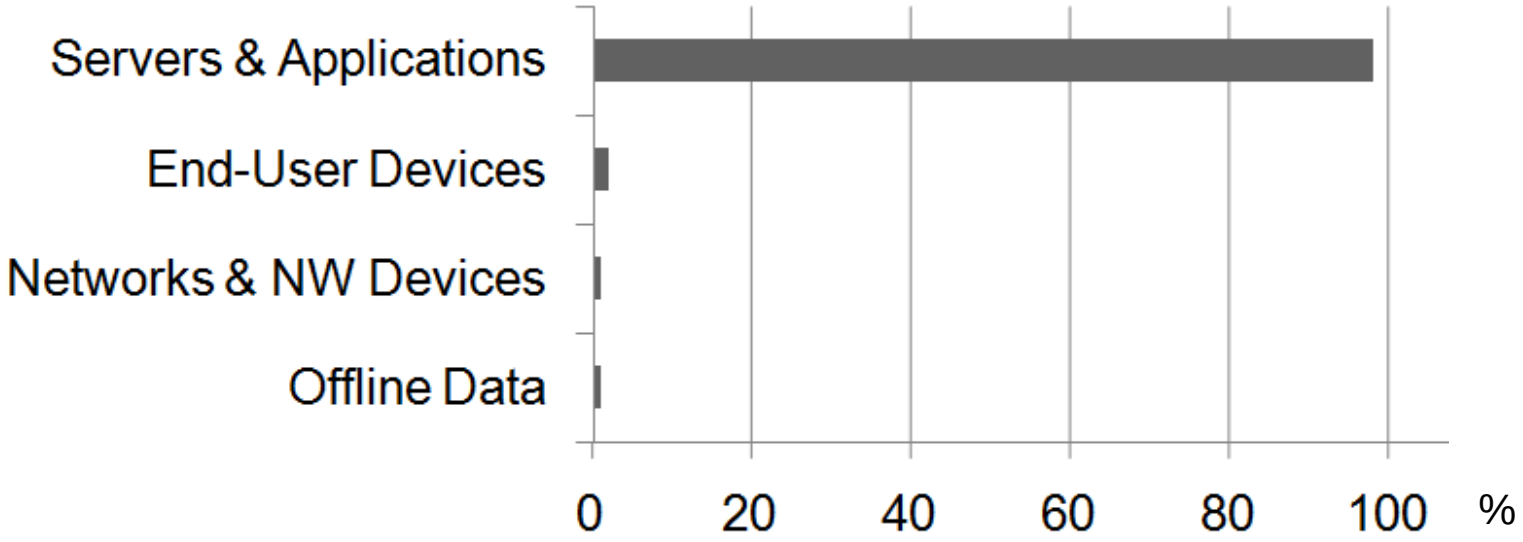
"It is fascinating that the top threat events
in both 2010 and 2011 are the same
and involve external agents hacking and installing malware
to compromise the confidentiality and integrity of servers."

Source: 2011 Data Breach Investigations Report, Verizon Business RISK team

Source: Securosis, http://securosis.com/

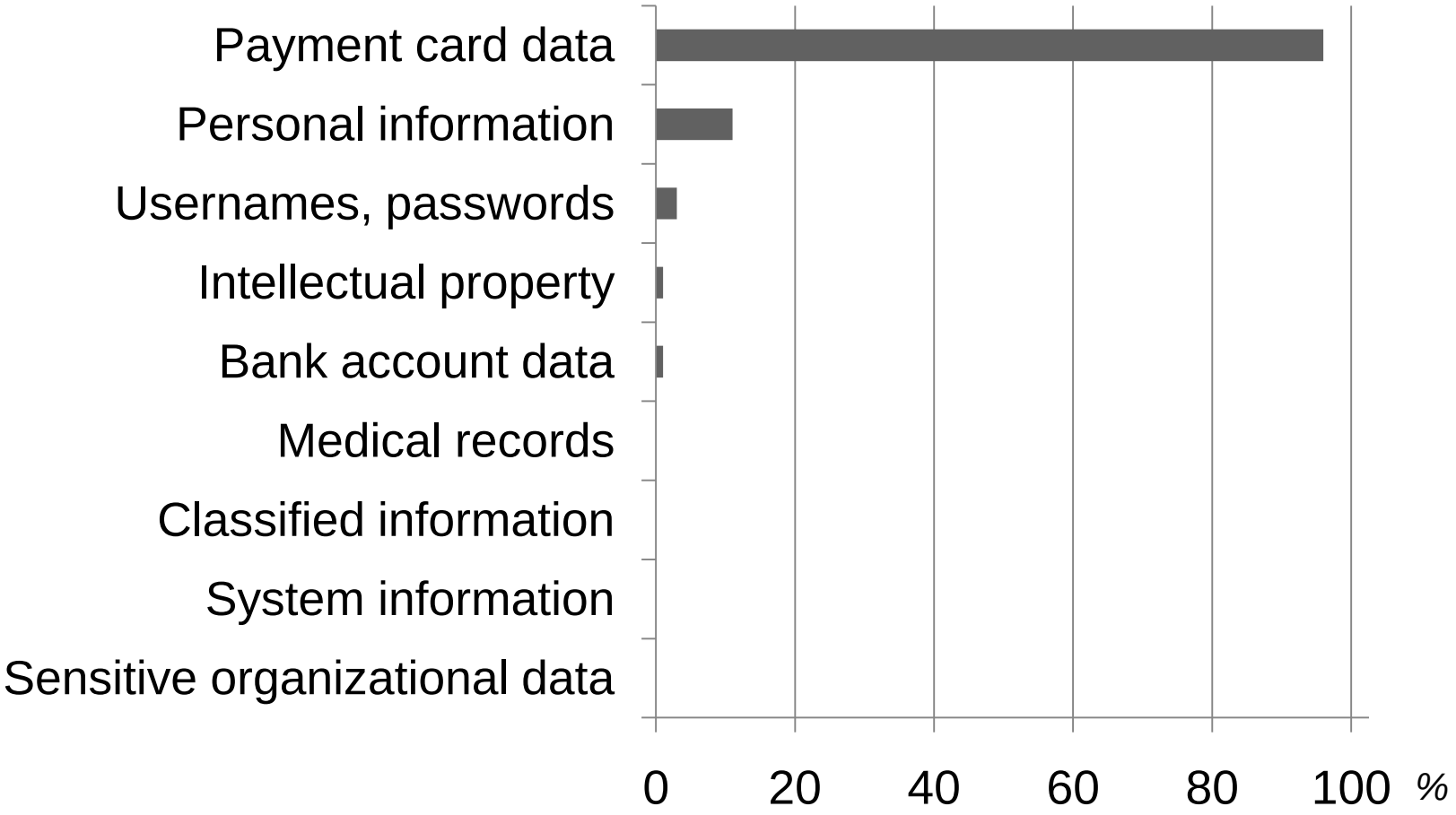
Data Breaches – Mainly Online Data Records

- 900+ breaches
- 900+ million compromised records:



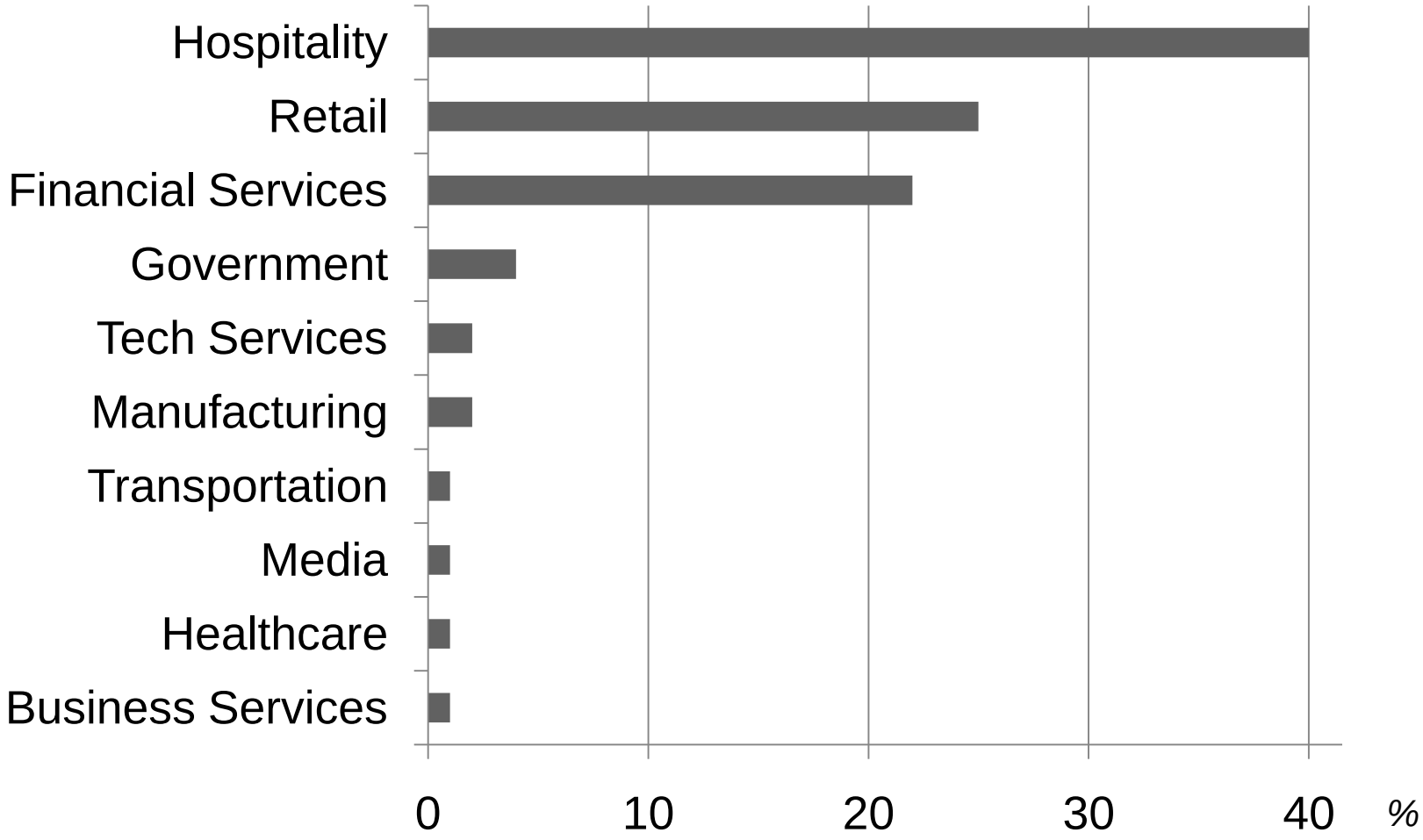
Source: 2010 Data Breach Investigations Report, Verizon Business RISK team and USSS

Compromised Data Types - # Records



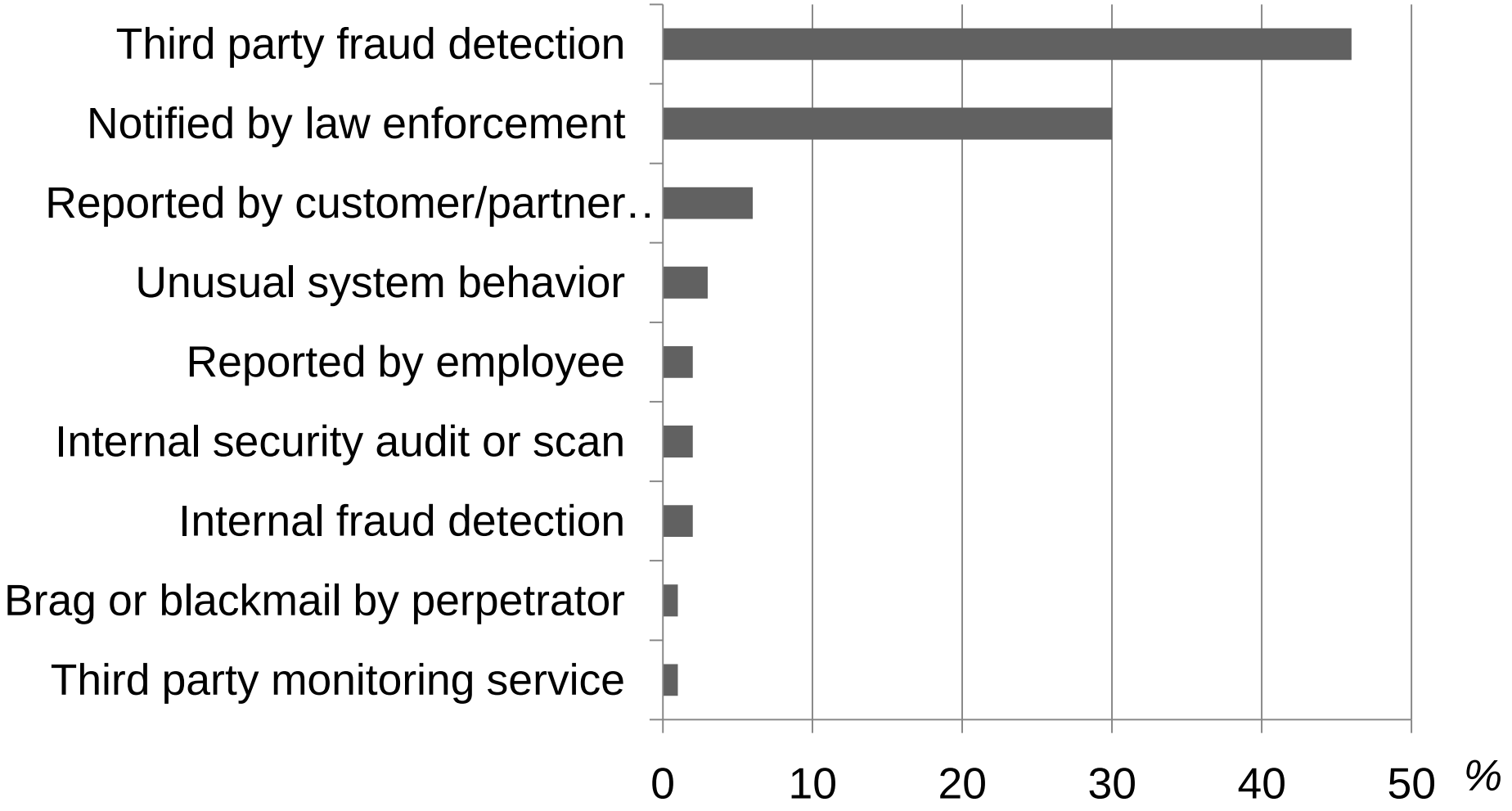
Source: Data Breach Investigations Report, Verizon Business RISK team and USSS

Industry Groups Represented - # Breaches



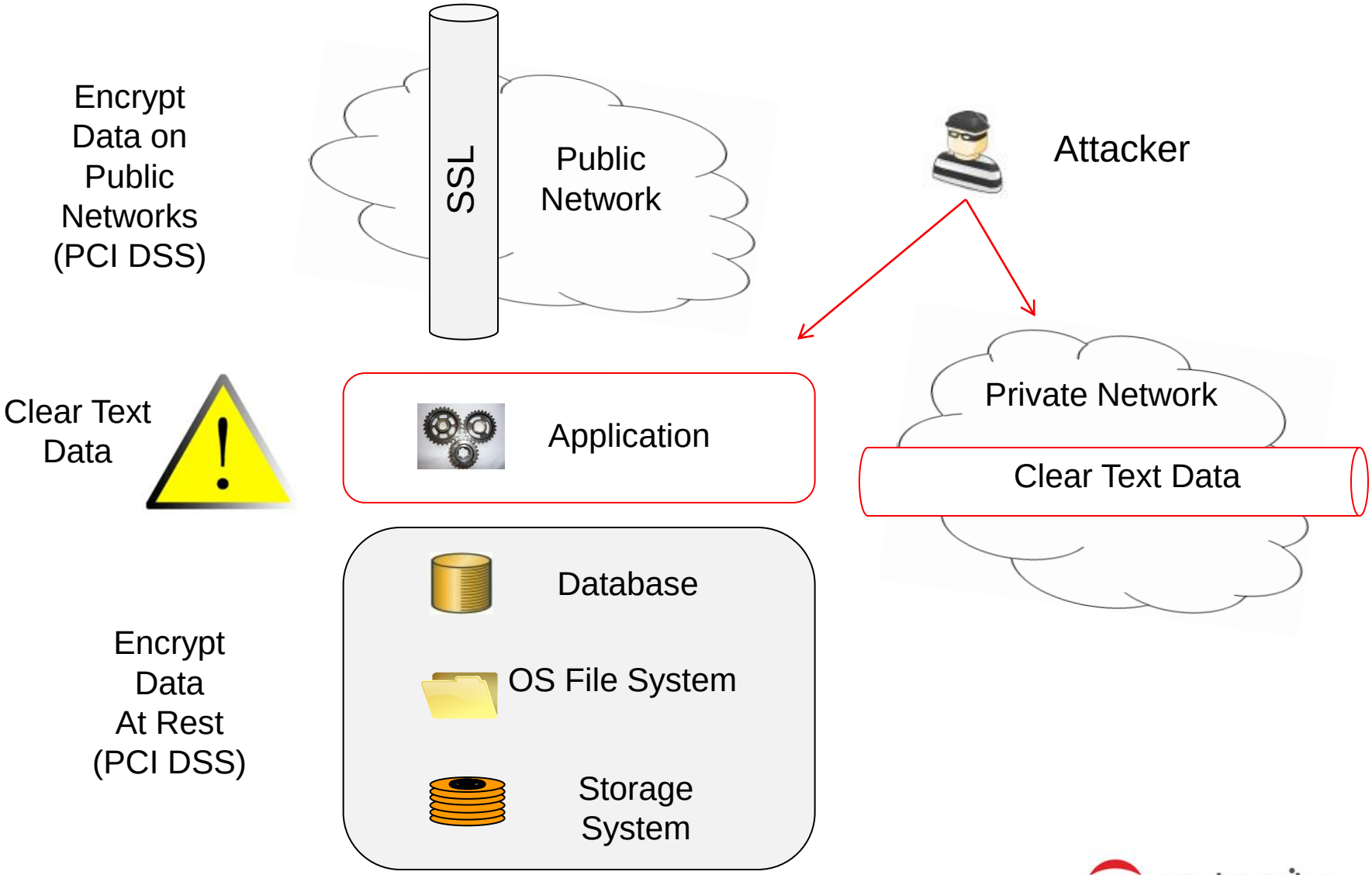
Source: Data Breach Investigations Report, Verizon Business RISK team and USSS

Breach Discovery Methods - # Breaches



Source: Data Breach Investigations Report, Verizon Business RISK team and USSS

Example of How the Problem is Occurring – PCI DSS



Source: PCI Security Standards Council, 2011

How can the problem be solved? -Tokenization and other options can reduce the risk

Source: PCI Security Standards Council, 2011

Amazon Cloud & PCI DSS

- Just because AWS is certified doesn't mean you are
  - You still need to deploy a PCI compliant application/service and anything on AWS is still within your assessment scope
- PCI-DSS 2.0 doesn't address multi-tenancy concerns
- You can store PAN data on S3, but it still needs to be encrypted in accordance with PCI-DSS requirements
  - Amazon doesn't do this for you
  - You need to implement key management, rotation, logging, etc.
- If you deploy a server instance in EC2 it still needs to be assessed by your QSA (PCI auditor)
  - Organization's assessment scope isn't necessarily reduced
- Tokenization can reduce your handling of PAN data

Source: Securosis, http://securosis.com/

Tokenization Use Case Example

- A leading retail chain
  - 1500 locations in the U.S. market
- Simplify PCI Compliance
  - 98% of Use Cases out of audit scope
  - Ease of install (had 18 PCI initiatives at one time)
- Tokenization solution was implemented in 2 weeks
  - Reduced PCI Audit from 7 months to 3 months
  - No 3rd Party code modifications
  - Proved to be the best performance option
  - 700,000 transactions per days
  - 50 million card holder data records
  - Conversion took 90 minutes (plan was 30 days)
  - Next step – tokenization server at 1500 locations

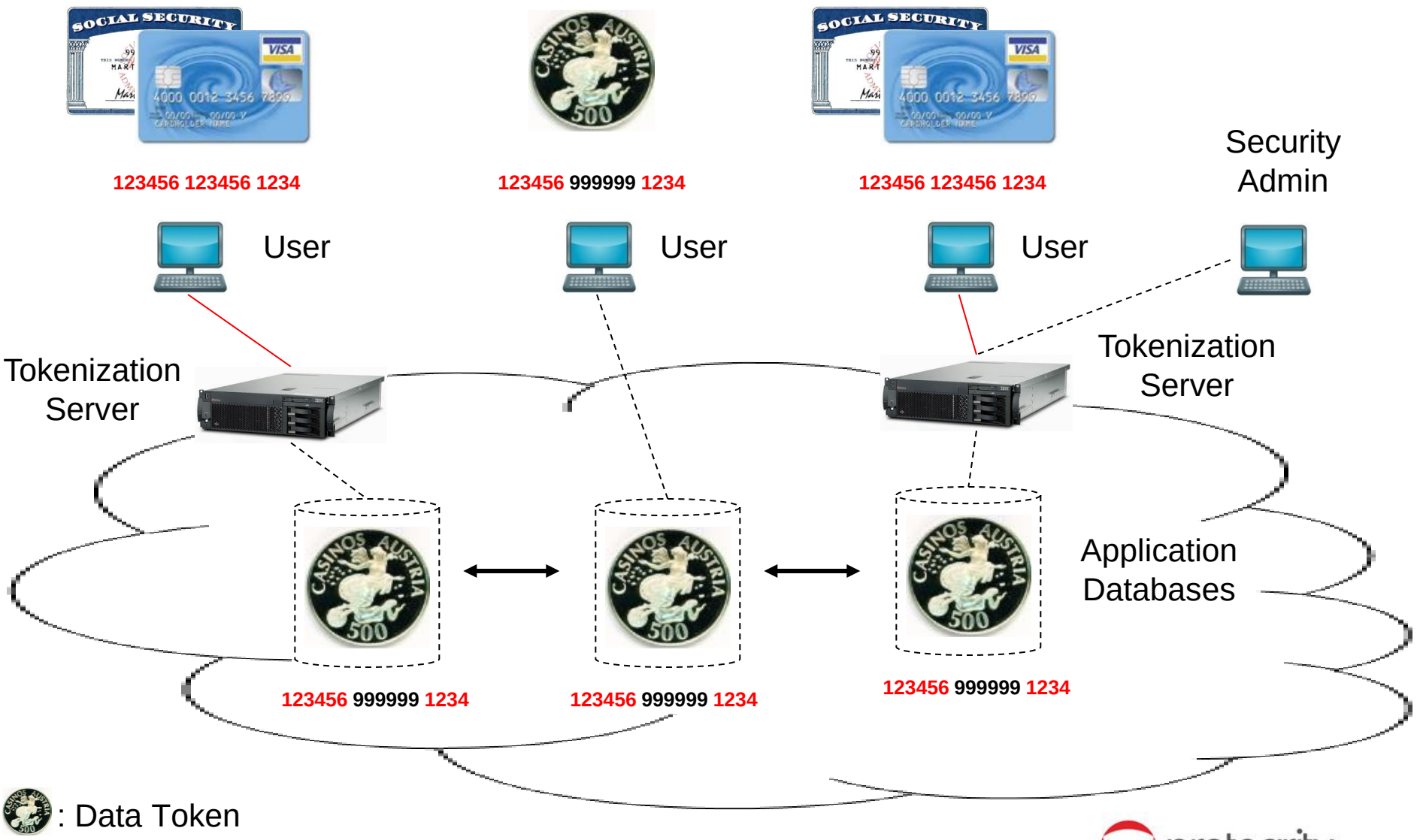
What is Tokenization and what is the Benefit?

- Tokenization
  - Tokenization is process that replaces sensitive data in systems with inert data called tokens which have no value to the thief.
  - Tokens resemble the original data in data type and length
- Benefit
  - Greatly improved transparency to systems and processes that need to be protected
- Result
  - Reduced remediation
  - Reduced need for key management
  - Reduce the points of attacks
  - Reduce the PCI DSS audit costs for retail scenarios

Token Flexibility for Different Categories of Data

Type of Data	Input	Token	Comment
Token Properties			
Credit Card	3872 3789 1620 3675	8278 2789 2990 2789	Numeric
Medical ID	29M2009ID	497HF390D	Alpha-Numeric
Date	10/30/1955	12/25/2034	Date
E-mail Address	bob.hope@protegrity.com	empo.snaugs@svtiensnni.snk	Alpha Numeric, delimiters in input preserved
SSN delimiters	075-67-2278	287-38-2567	Numeric, delimiters in input
Credit Card	3872 3789 1620 3675	8278 2789 2990 3675	Numeric, Last 4 digits exposed
Policy Masking			
Credit Card	3872 3789 1620 3675	clear, encrypted, tokenized at rest 3872 37## #### ####	Presentation Mask: Expose 1st 6 digits

Data Tokenization – Reducing the Attack Surface



Unprotected sensitive information:

Protected sensitive information

PCI DSS - Ways to Render the PAN Unreadable

- Two-way cryptography with associated key management processes
- One-way cryptographic hash functions
- Index tokens and pads
- Truncation (or masking – xxxxxx xxxxxx 6781)

PCI Security Standards Council
PARTICIPATING ORGANIZATION

protegrity

Positioning Different Protection Options

Evaluation Criteria	Strong Encryption	Formatted Encryption	Tokens
Security & Compliance			
Total Cost of Ownership			
Use of Encoded Data			

Best  Worst

Different Approaches for Tokenization

- Traditional Tokenization
  - Dynamic Model or Pre-Generated Model
  - 5 tokens per second - 5000 tokenizations per second
- Protegrity Next Generation Tokenization
  - Memory-tokenization
  - 200,000 - 9,000,000+ tokenizations per second
  - “The tokenization scheme offers excellent security, since it is based on fully randomized tables.” *
  - “This is a fully distributed tokenization approach with no need for synchronization and there is no risk for collisions.“ *

*: Prof. Dr. Ir. Bart Preneel, Katholieke University Leuven, Belgium

Tokenization Summary

	Traditional Tokenization	Protegrity Tokenization
Footprint	**Large, Expanding.** The large and expanding footprint of Traditional Tokenization is it's Achilles heal. It is the source of poor performance, scalability, and limitations on its expanded use.	**Small, Static.** The small static footprint is the enabling factor that delivers extreme performance, scalability, and expanded use.
High Availability, DR, and Distribution	**Complex replication required.** Deploying more than one token server for the purpose of high availability or scalability will require complex and expensive replication or synchronization between the servers.	**No replication required.** Any number of token servers can be deployed without the need for replication or synchronization between the servers. This delivers a simple, elegant, yet powerful solution.
Reliability	**Prone to collisions.** The synchronization and replication required to support many deployed token servers is prone to collisions, a characteristic that severely limits the usability of traditional tokenization.	**No collisions**. Protegrity Tokenizations' lack of need for replication or synchronization eliminates the potential for collisions .
Performance, Latency, and Scalability	**Will adversely impact performance & scalability.** The large footprint severely limits the ability to place the token server close to the data. The distance between the data and the token server creates latency that adversely effects performance and scalability to the extent that some use cases are not possible.	**Little or no latency. Fastest industry tokenization.** The small footprint enables the token server to be placed close to the data to reduce latency. When placed in-memory, it eliminates latency and delivers the fastest tokenization in the industry.
Extendibility	**Practically impossible.** Based on all the issues inherent in Traditional Tokenization of a single data category, tokenizing more data categories may be impractical.	**Unlimited Tokenization Capability.** Protegrity Tokenization can be used to tokenize many data categories with minimal or no impact on footprint or performance.

Evaluating Encryption & Tokenization Approaches

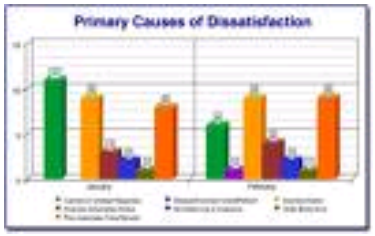
Evaluation Criteria		Encryption		Tokenization	
Area	**Impact**	**Database File Encryption**	**Database Column Encryption**	**Traditional Tokenization**	**Memory Tokenization (Protegrity)**
Scalability	Availability	●	●	○	●
	Latency	◔	◒	○	●
	CPU Consumption	○	◒	◒	●
Security	Data Flow Protection	○	◒	◔	●
	Compliance Scoping	◒	◔	●	●
	Key Management	○	○	●	●
	Data Collisions	●	●	◒	●
	Separation of Duties	◔	◒	●	●

Best ● ◔ ◒ ◔ ○ Worst

protegrity

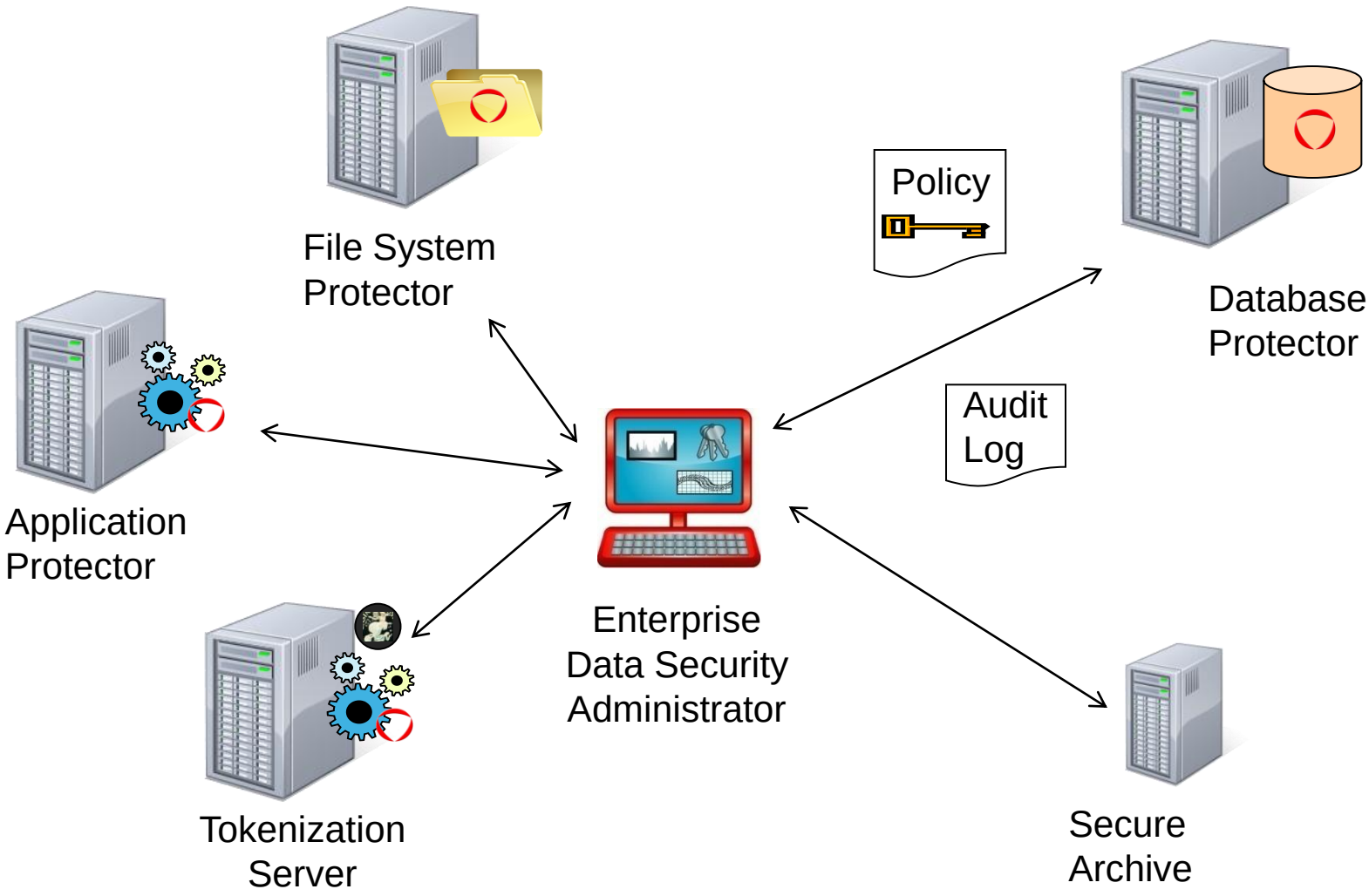
Data Protection Challenges

- The actual protection of the data is not the challenge
- Centralized solutions are needed to managed complex security requirements
  - Based on Security Policies with Transparent Key management
  - Many methods to secure the data
  - Auditing, Monitoring and Reporting
- Solutions that minimize the impact on business operations
  - Highest level of performance and transparency
- Rapid Deployment
- Affordable with low TCO
- Enable & Maintaining compliance



protegrity

Protegrity Data Security Management



: Encryption service

Protegrity Data Protection Platform

- Coverage
  - Supports heterogeneous environments across operating systems, applications, file systems and databases
- Protection Methods
  - Encryption, Tokenization, DTP2 (data type/format preserving encryption), Masking and Monitoring
- Packaged Data Protectors for Databases, Files and Applications
- Next Generation Tokenization
- Separation of Duties/Roles
  - IT Security resource responsible for defining policy is different than Administrator's managing the sensitive data
- Policy and Key Management
  - Central and secure solution to manage the keys to the data across the enterprise
- Central Reporting
  - Reporting for security management compliance assessment

Please contact me for more information

ulf.mattsson [at] protegrity.com

Visit our table

protegrity

protecting your data.
protecting your business.