New York Oracle Users Group, Inc.

Securing Data Today and in the Future

Ulf Mattsson
CTO Protegrity

ulf . mattsson AT protegrity . com

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)

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

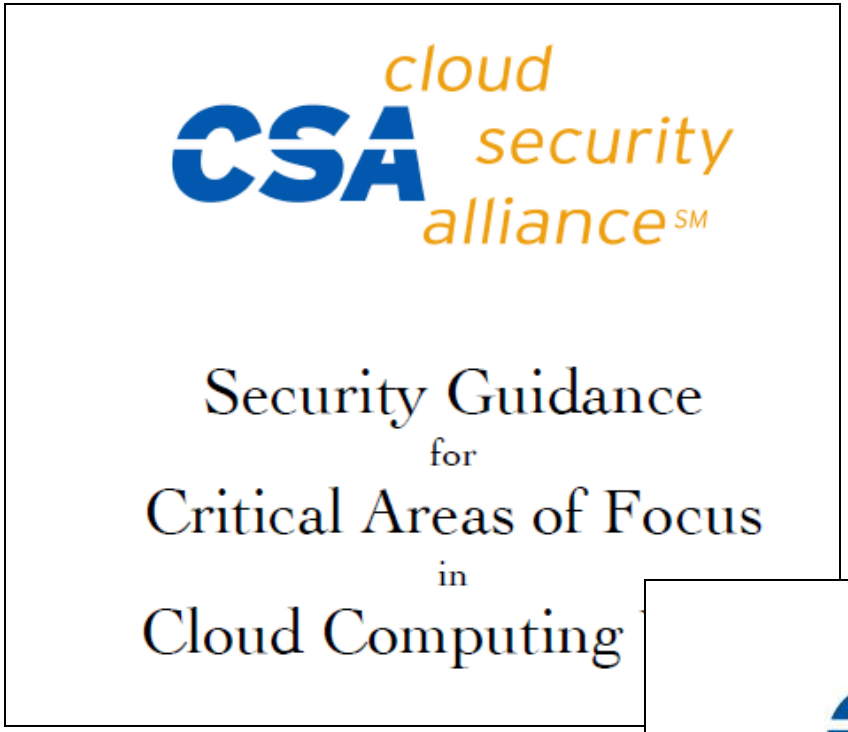
Ulf Mattsson
CTO
Protegrity

Security Mag
AL & PHYSICAL SECURITY MAGAZINE

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

April 2011 by Ulf Mattsson, CTO, Protegrity Corporation

Guidance from Cloud Security Alliance

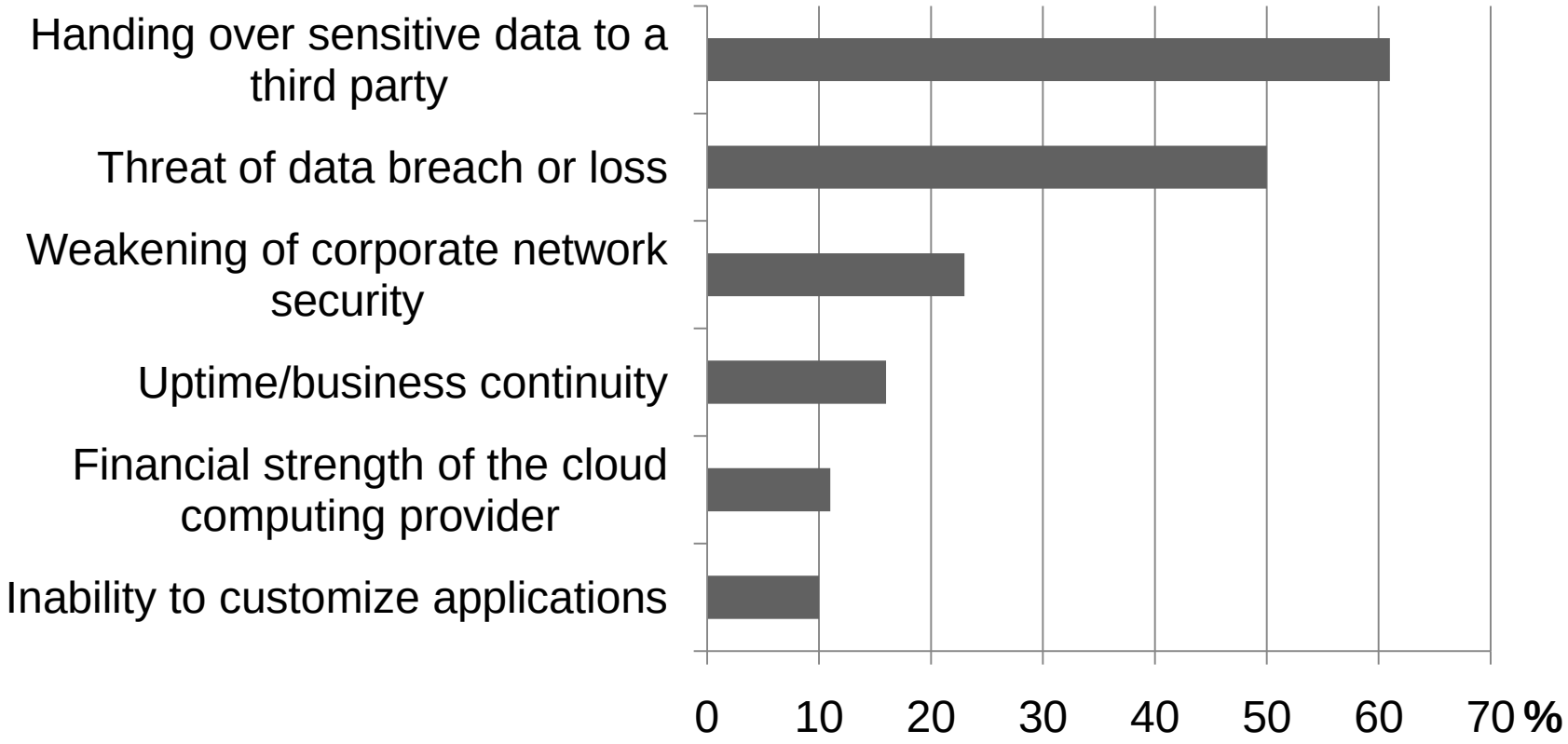


protegrity

“Cloud – Like a Parking Garage”

protegrity

Risks Associated with Cloud Computing



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

protegrity

“Pass Security Before Entering The Cloud”

User

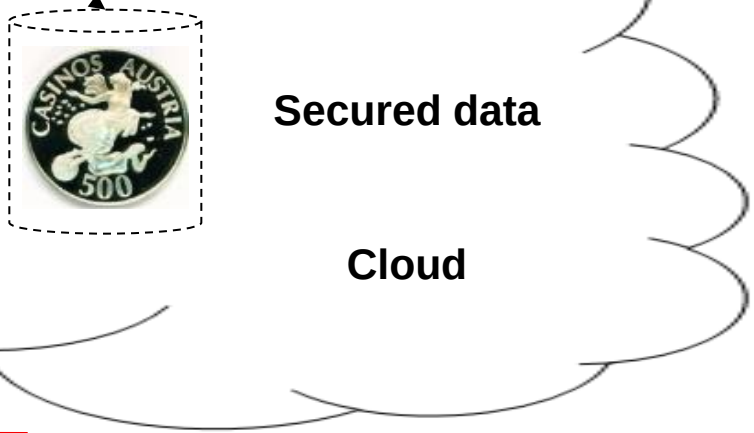
123456 123456 1234

Security
Check Point

123456 123456 1234

Sensitive data

123456 999999 1234



Secured data

Cloud

Unprotected sensitive information:

Protected sensitive information

protegrity

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."

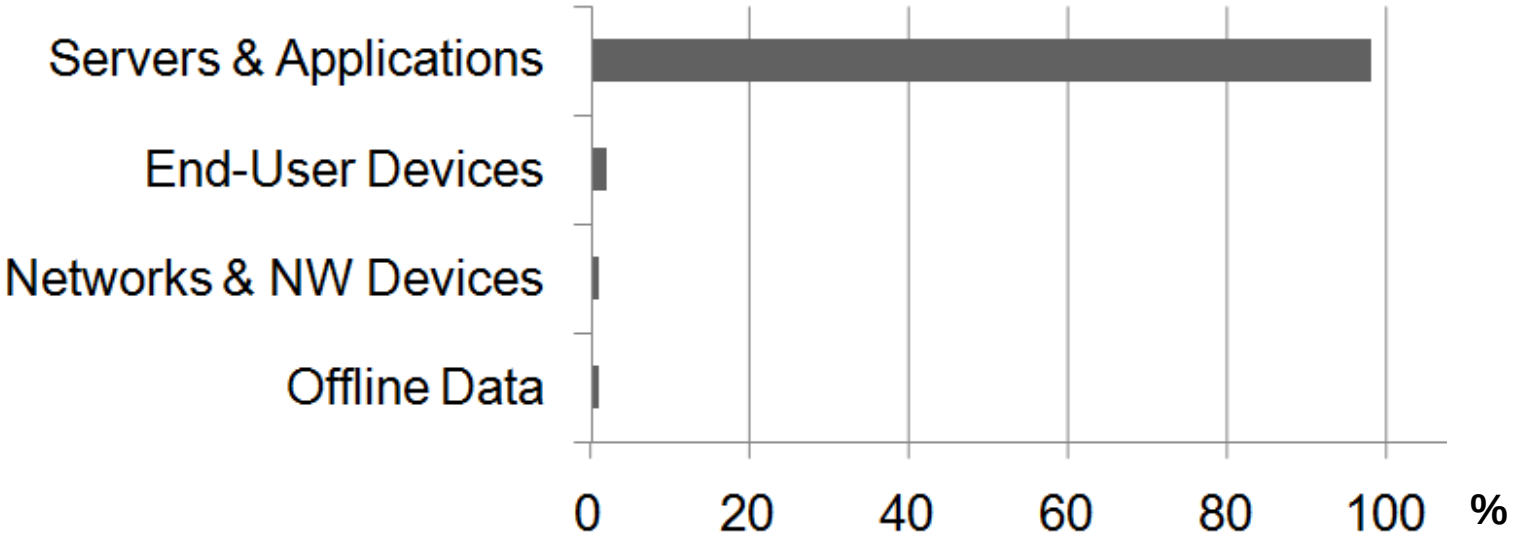
***Source: 2011 Data Breach Investigations Report,* Verizon Business RISK team**

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

protegrity

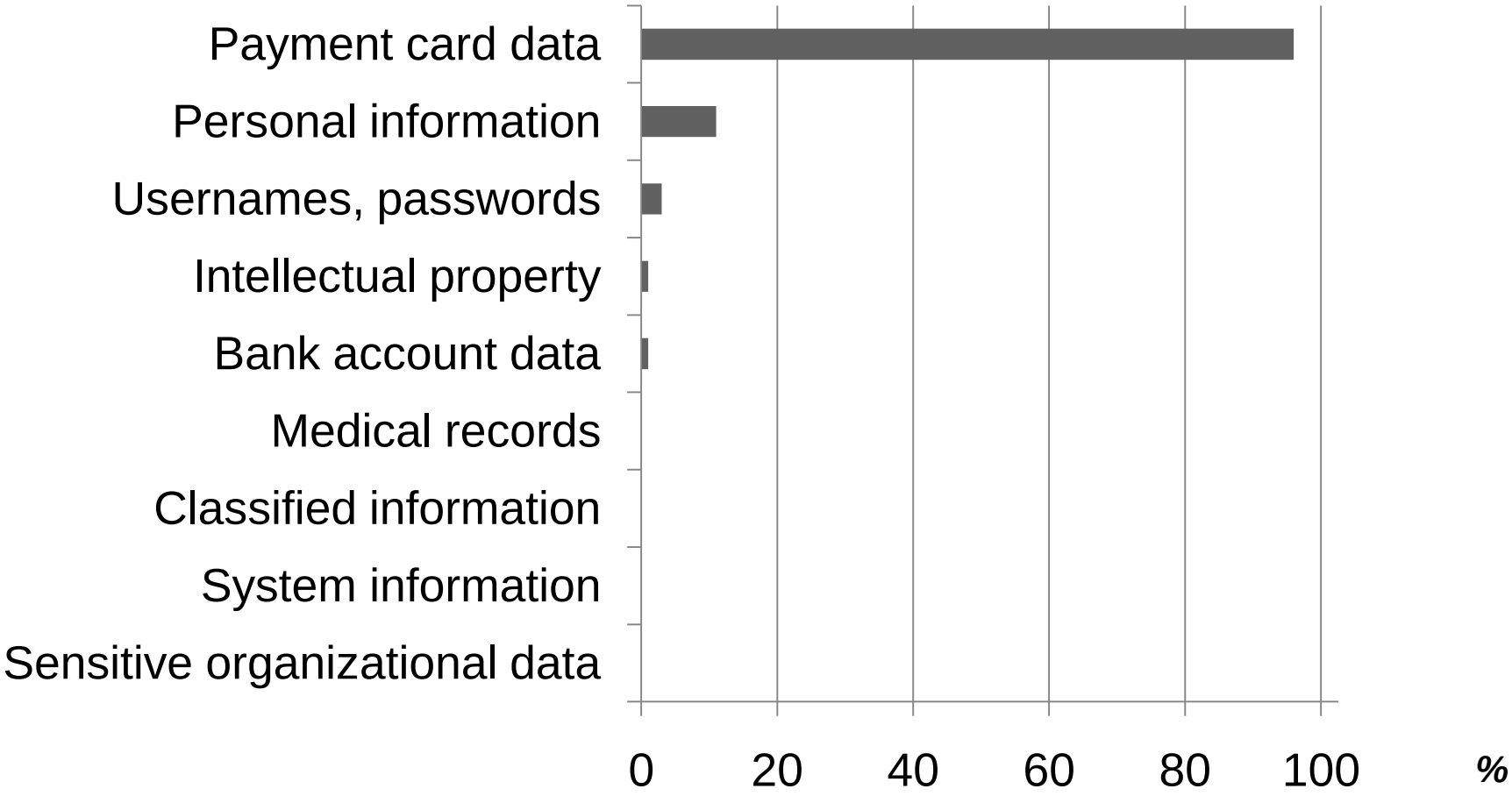
Data Breaches – Mainly Online Data Records

- 900+ breaches
- 900+ million compromised records:



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

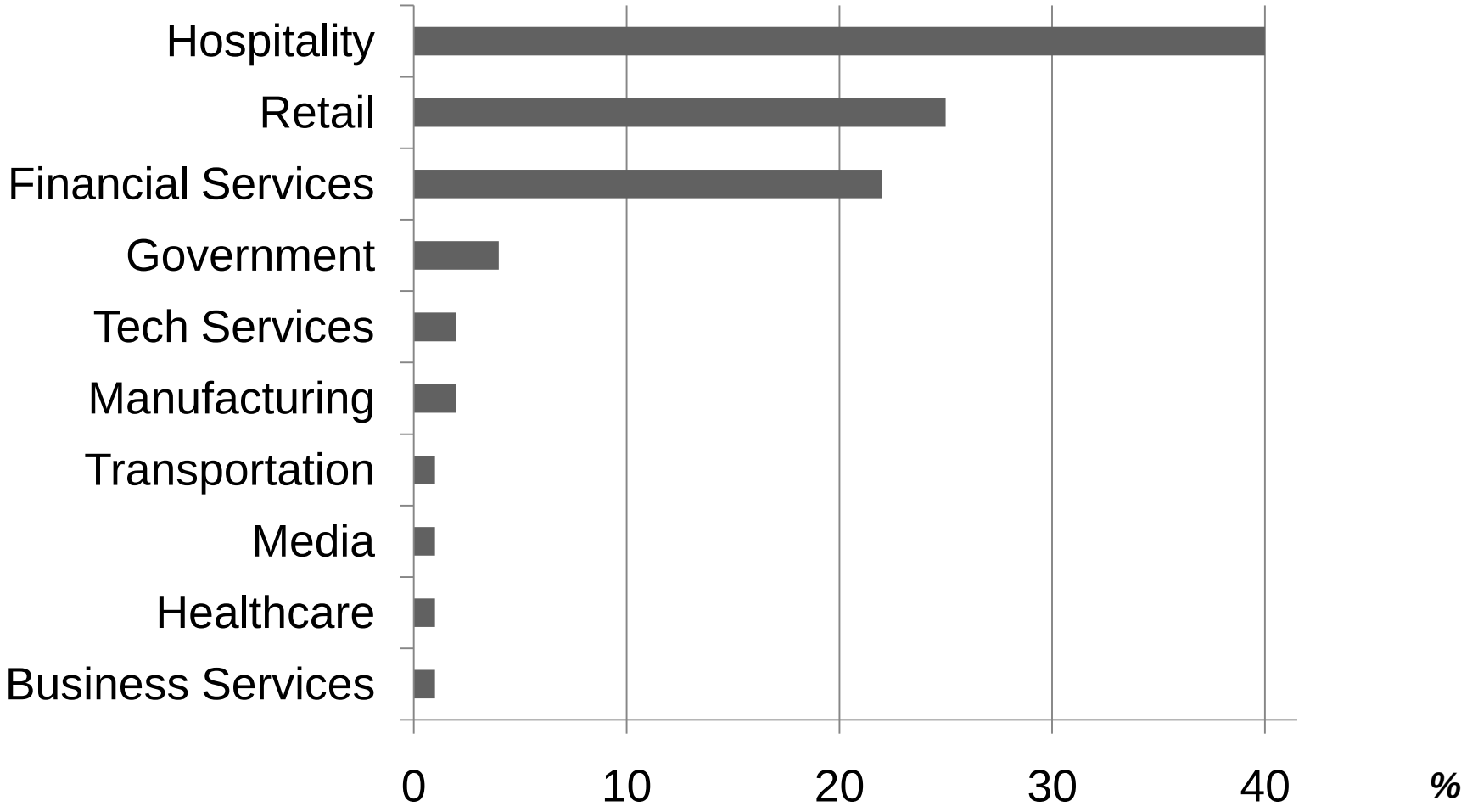
Compromised Data Types - # Records



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

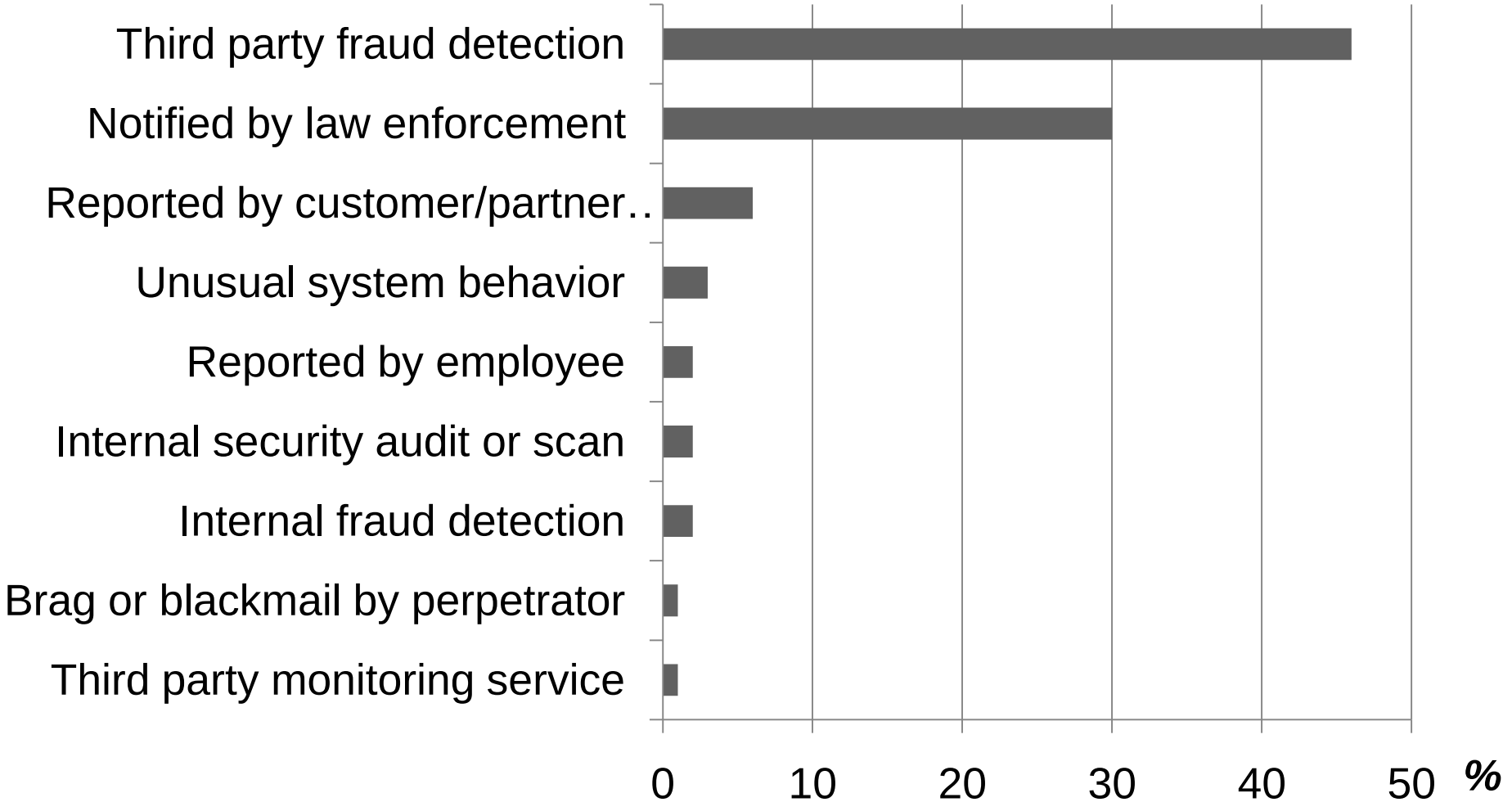
protegrity

Industry Groups Represented - # Breaches



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

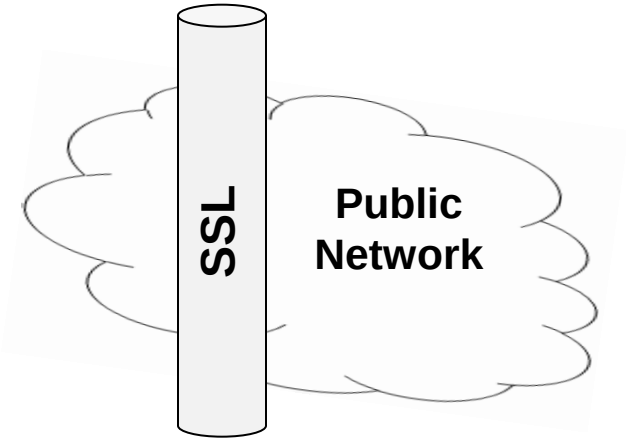
Breach Discovery Methods - # Breaches



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

Example of How the Problem is Occurring – PCI DSS

Encrypt Data on Public Networks (PCI DSS)



Attacker

Clear Text Data

Application

Private Network

Clear Text Data

Database

OS File System

Storage System

Encrypt Data At Rest (PCI DSS)

Source: PCI Security Standards Council, 2011

protegrity

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

Source: PCI Security Standards Council, 2011

protegrity

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

Evaluating Options

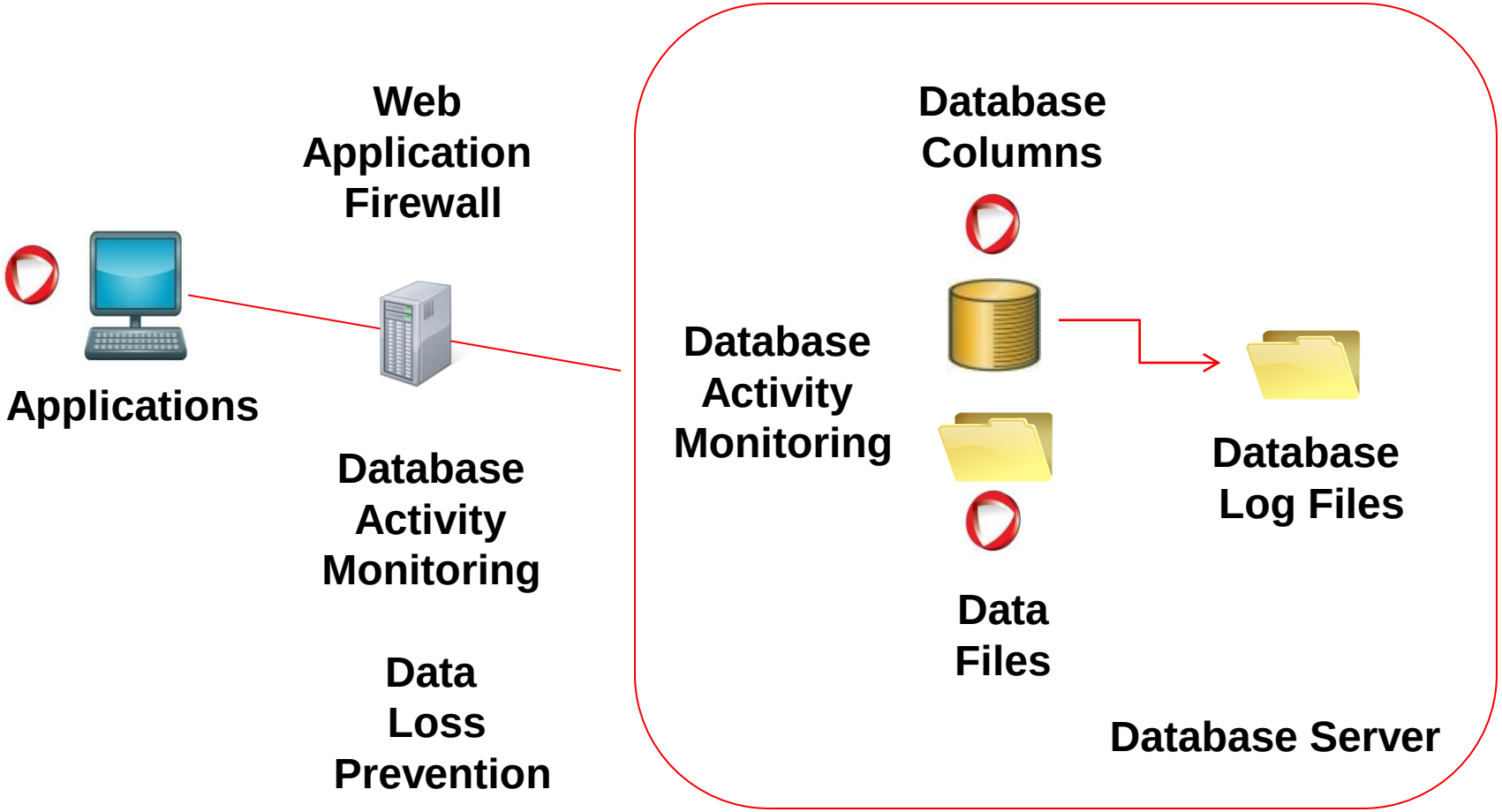
Evaluating Field Encryption & Tokenization

Evaluation Criteria	Strong Field Encryption	Formatted Encryption	Tokenization (distributed)
Disconnected environments	●	●	●
Distributed environments	●	●	●
Performance impact when loading data	●	◔	●
Transparent to applications	●	◒	◒
Expanded storage size	◒	●	◔
Transparent to databases schema	◒	●	●
Long life-cycle data	◔	◕	●
Unix or Windows mixed with “big iron” (EBCDIC)	●	◕	●
Easy re-keying of data in a data flow	◒	◕	●
High risk data	●	○	●
Security - compliance to PCI, NIST	●	○	●

Best ● ◔ ◒ ◕ ○ Worst

protegrity

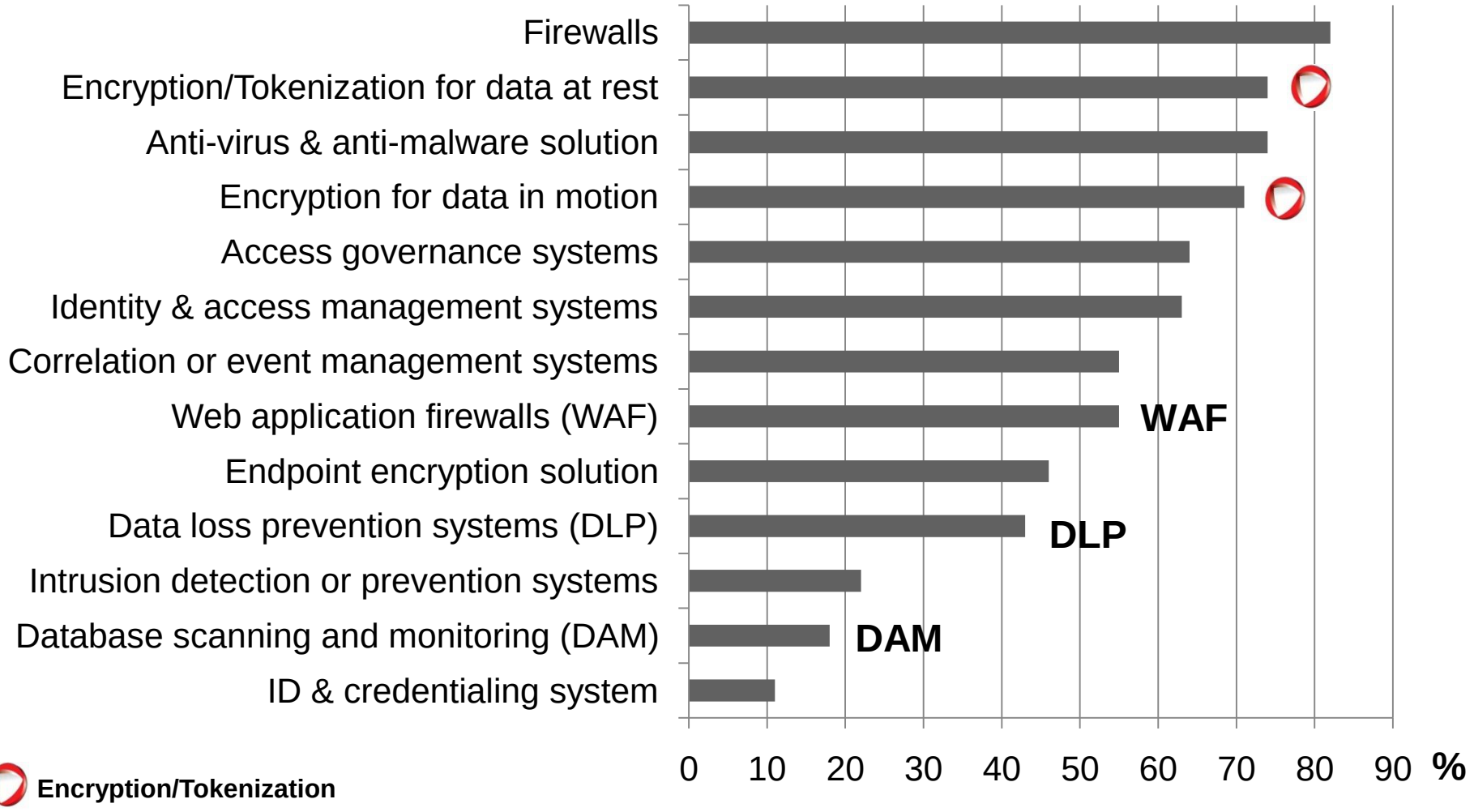
Choose Your Defenses – Different Approaches



Encryption/Tokenization

protegrity

Choose Your Defenses – Cost Effective PCI DSS

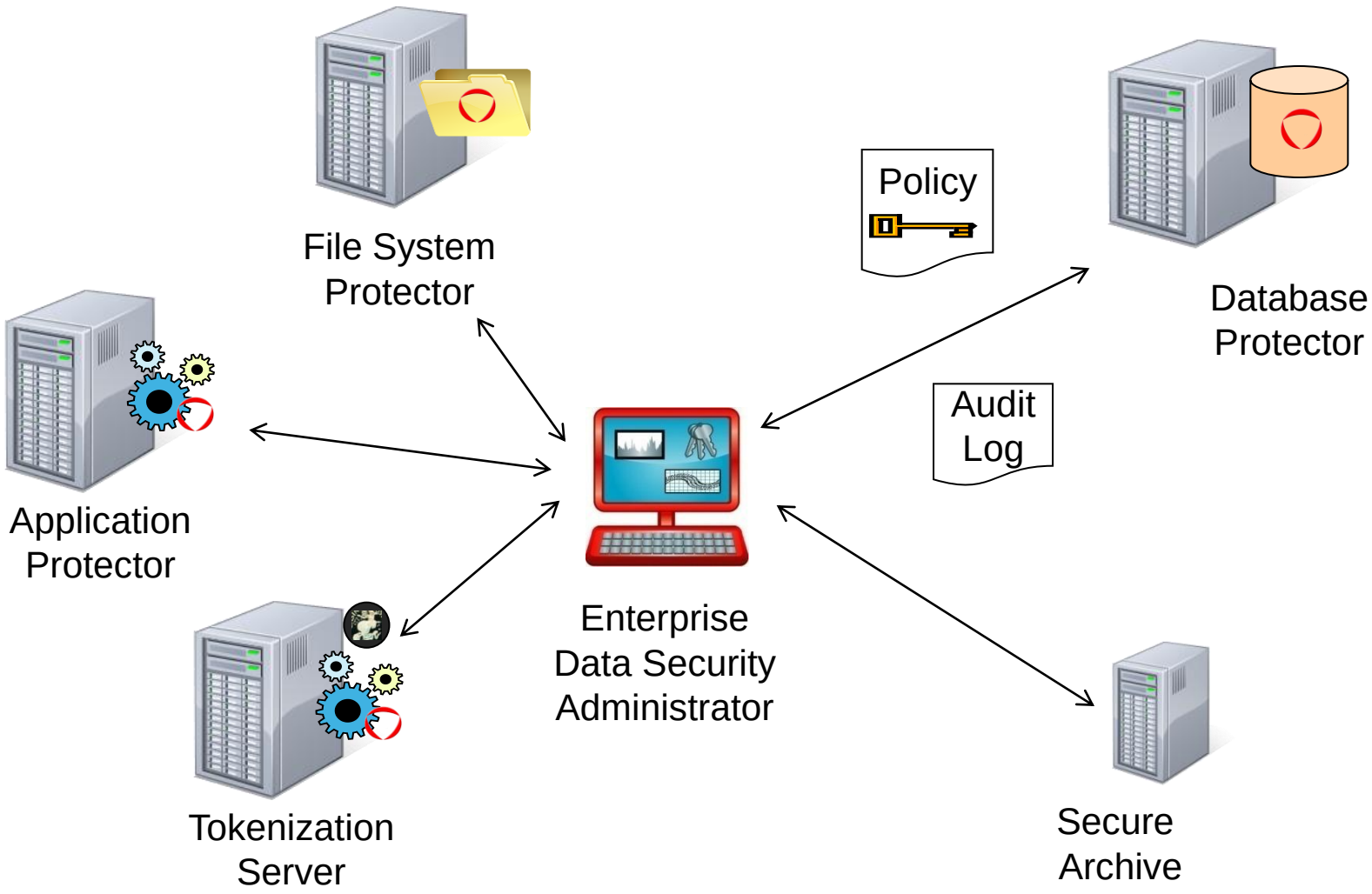


Encryption/Tokenization

Source: 2009 PCI DSS Compliance Survey, Ponemon Institute

protegrity

Best Practices - Data Security Management



: Encryption service

protegrity

Vendors/Products Providing Database Protection

Feature	3rd Party	Oracle 9	Oracle 10	Oracle 11	IBM DB2	MS SQL
Database file encryption	●	○	○	●	●	◒
Database column encryption	●	●	●	●	●	◒
Column encryption adds 32-52 bytes (10.2.0.4, 11.1.0.7)	●	○	○	○	○	◒
Formatted encryption	●	○	○	○	○	○
Data tokenization	●	○	○	○	○	○
Database activity monitoring	◔	○	○	○	●	○
Multi vendor encryption	●	○	○	○	○	○
Data masking	●	○	◒	●	●	○
Central key management	●	○	○	○	●	◒
HSM support (11.1.0.7)	●	○	○	●	◒	◒
Re-key support (tablespace)	●	○	○	○	○	○

Best ● ◔ ◒ ◕ ○ **Worst**

protegrity

Vendors Providing Strong Encryption

Feature	Vendor A	Vendor B	Vendor C	Oracle	Vendor D	Vendor E
Software solution	●	●	●	●	○	○
HSM support	●	●	○	●	●	●
Database support	●	◔	●	◔	◒	◔
File encryption support	●	◔	●	○	◔	◕
Performance	●	◒	◕	●	◔	●
FIPS	◒	◒	○	◒	●	●
Availability	●	◒	●	●	○	◒
Central key management	●	●	●	○	●	●

Best ● ◕ ◒ ◔ ○ Worst

protegrity

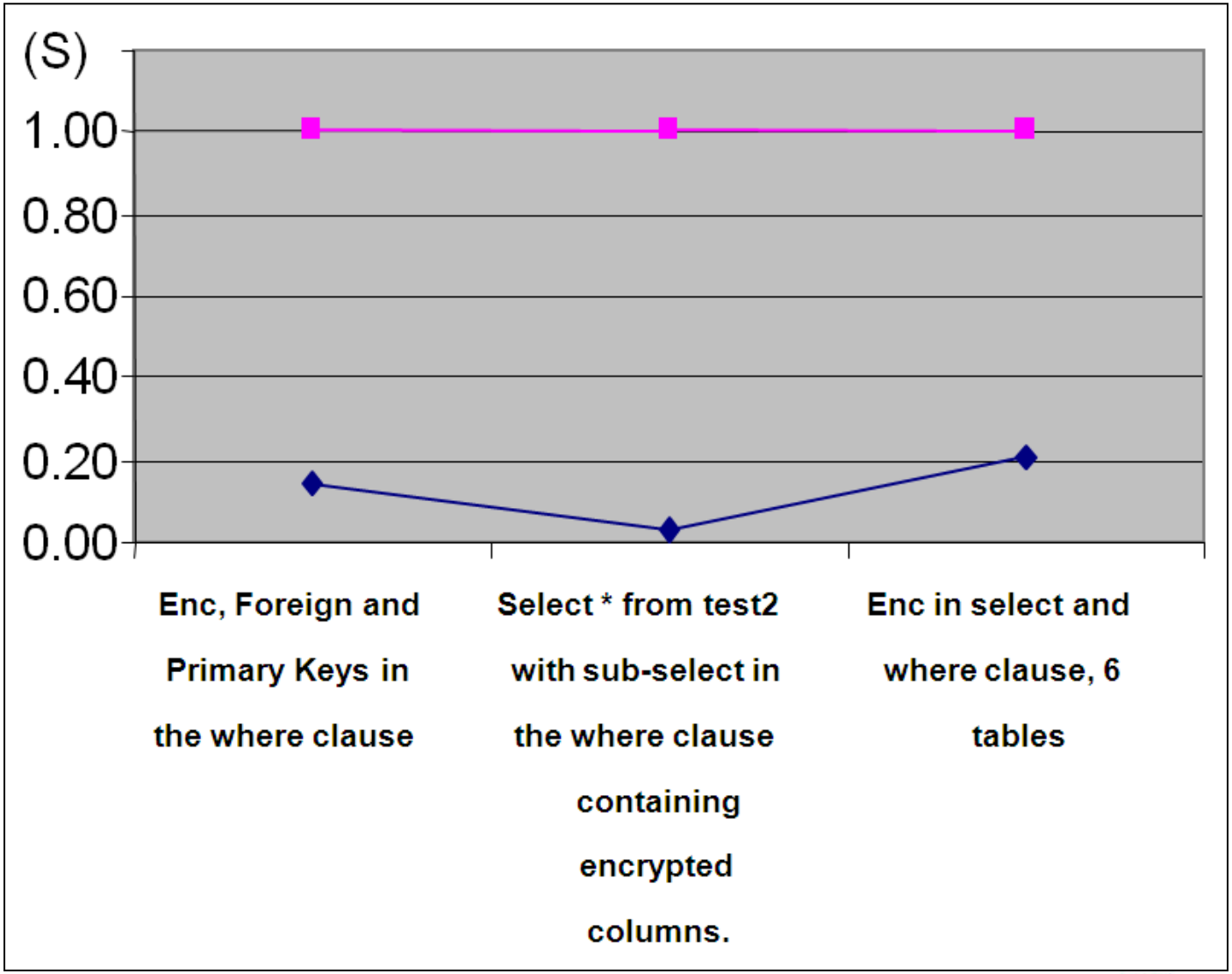
Column Encryption Solutions – Some Considerations

Area of Evaluation	3rd Party	Oracle 10 TDE	Oracle 11 TDE
Performance, manage UDT or views/triggers	◔	●	●
Support for both encryption and replication	●	○	○
Support for Oracle Domain Index for fast search	◒	○	○
Keys are local; re-encryption if moving A -> B	●	○	○
Separation of duties/key control vector	●	○	○
Encryption format specified	●	○	○
Data type support	●	◒	◒
Index support beyond equality comparison	●	○	○
HSM (hardware crypto) support (11.1.0.6)	●	○	●
HSM password not stored in file	●	○	○
Automated and secure master key backup procedure	●	○	○
Keys exportable	●	○	○

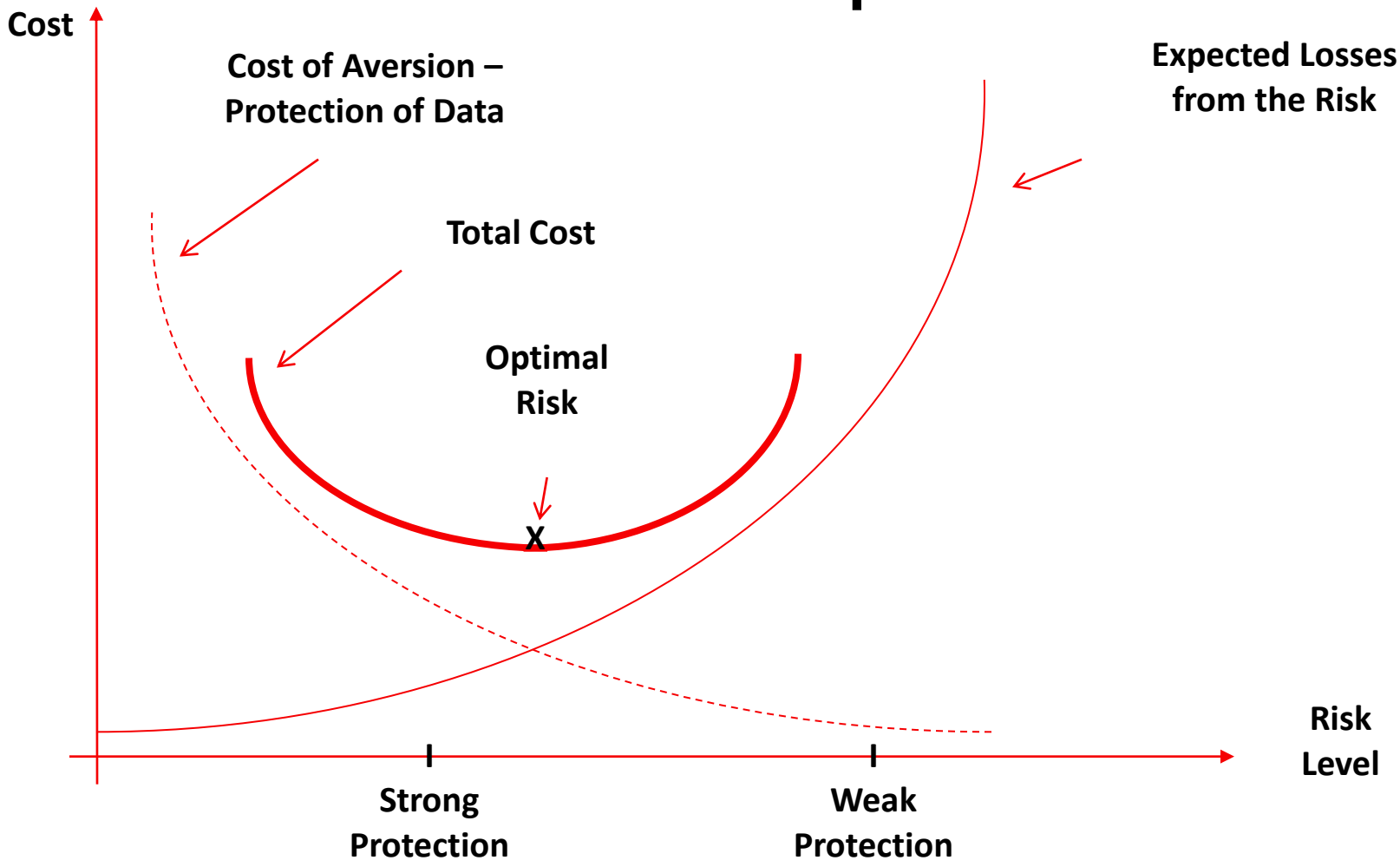
Best ● ◔ ◒ ◕ ○ **Worst**

protegrity

Oracle Domain Index



Choose Your Defenses – Total Cost of Ownership



Case Studies – Retail Environments

Point of Sale

E-Commerce

Branch Office

Aggregation

Operations

Analysis

Archive

‘Information in the wild’
- Short lifecycle / High risk

Temporary information
- Short lifecycle / High risk

Operating information
- Typically 1 or more year lifecycle

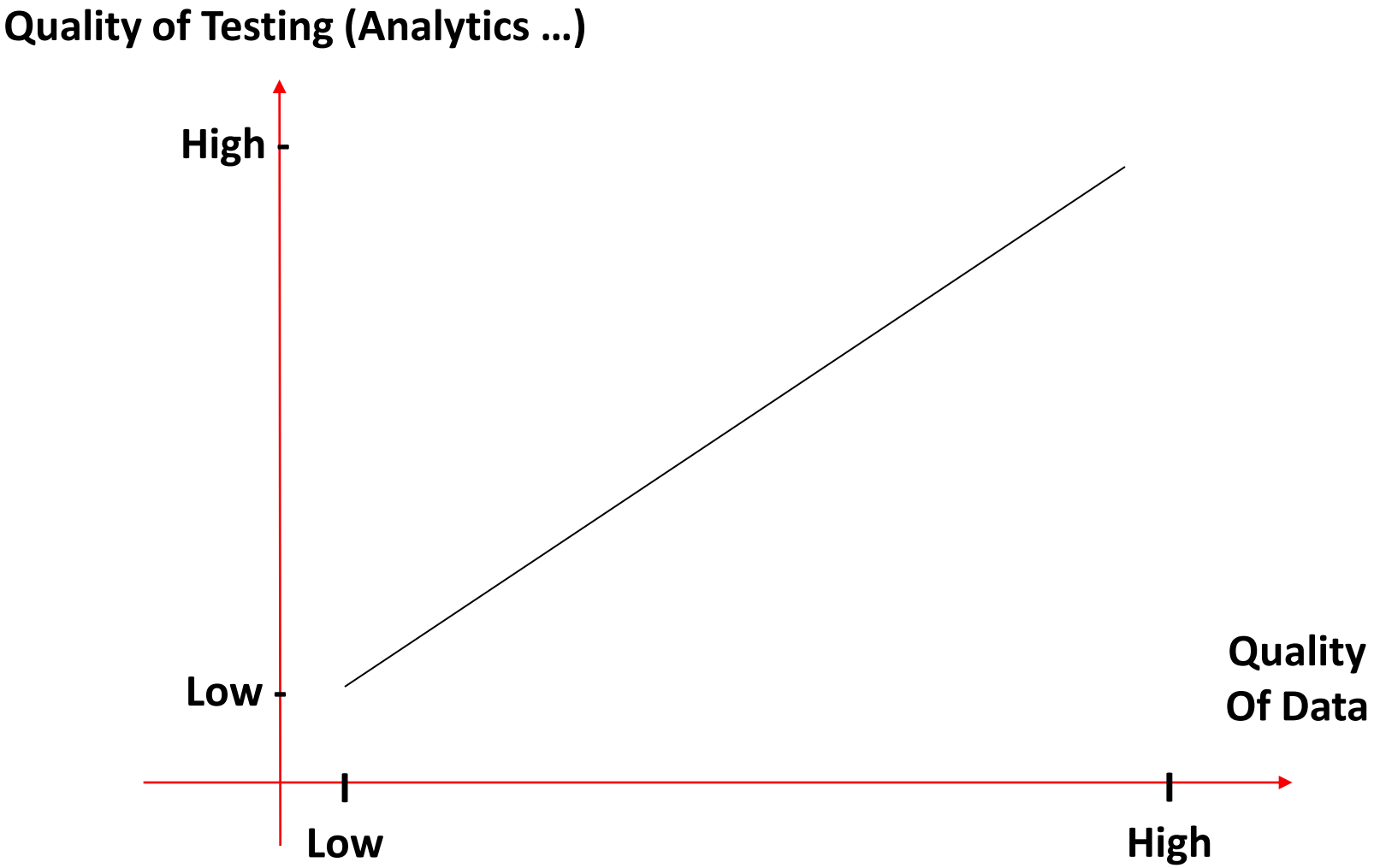
Decision making information
- Typically multi-year lifecycle
- High volume database analysis
- Wide internal audience with privileges

Archive
- Typically multi-year lifecycle

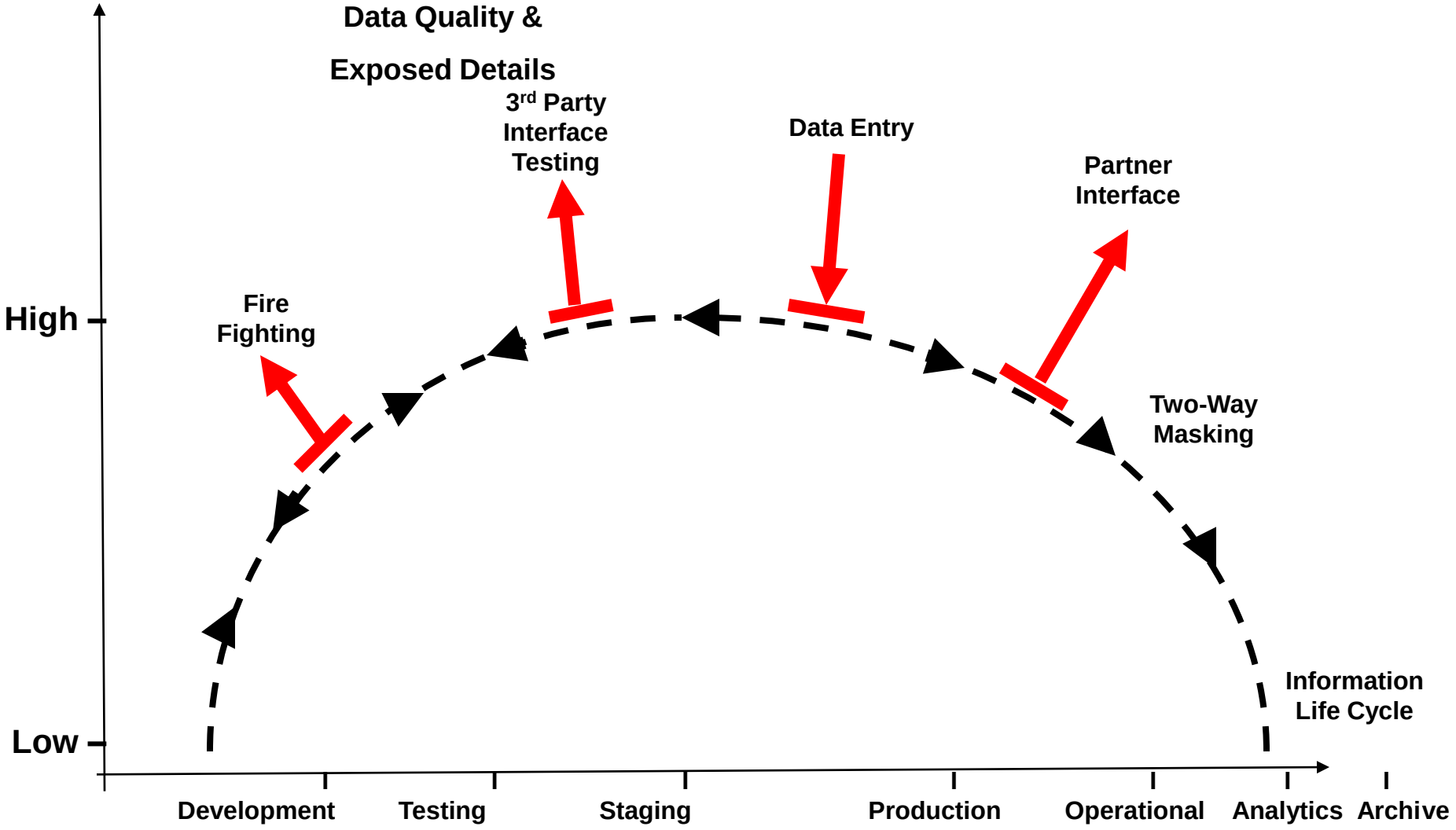
: Encryption service

protegrity

Quality of Systems Testing vs. Data Exposure



Data Security Life Cycle – Reversible Protection

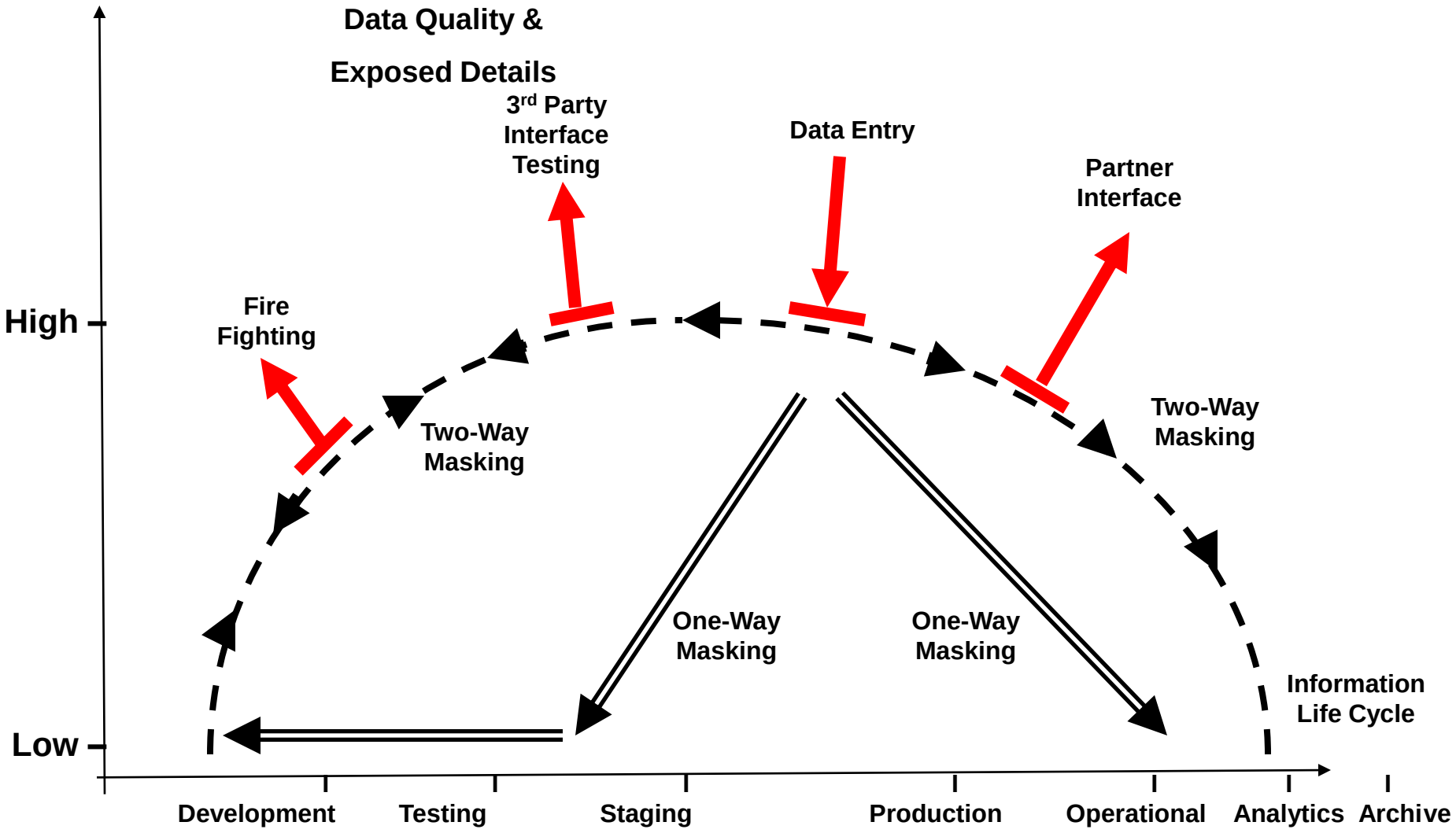


Unprotected sensitive information:

Protected sensitive information

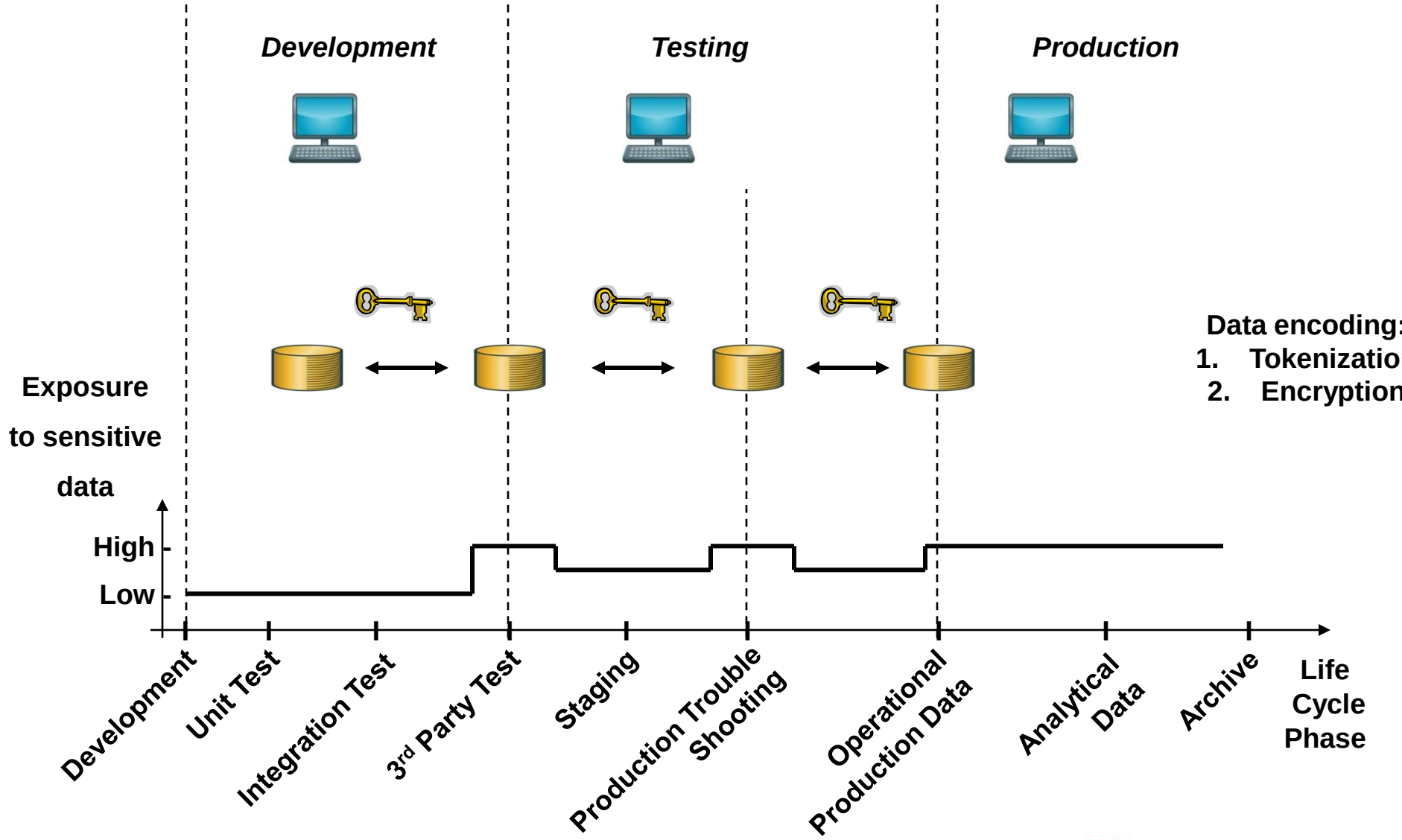
protegrity

Data Protection – Reversible or Not



protegrity

Limit Exposure to Sensitive Data



protegrity

Data Tokens in a Cloud Environment – Integration Example

990-23-1013

4000 0012 3456 7899

123-45 -1013

40 12 3456 7890 7899

Tokenization Gateway

123-45 -1013

40 12 3456 7890 7899

Application Databases

Cloud Environment

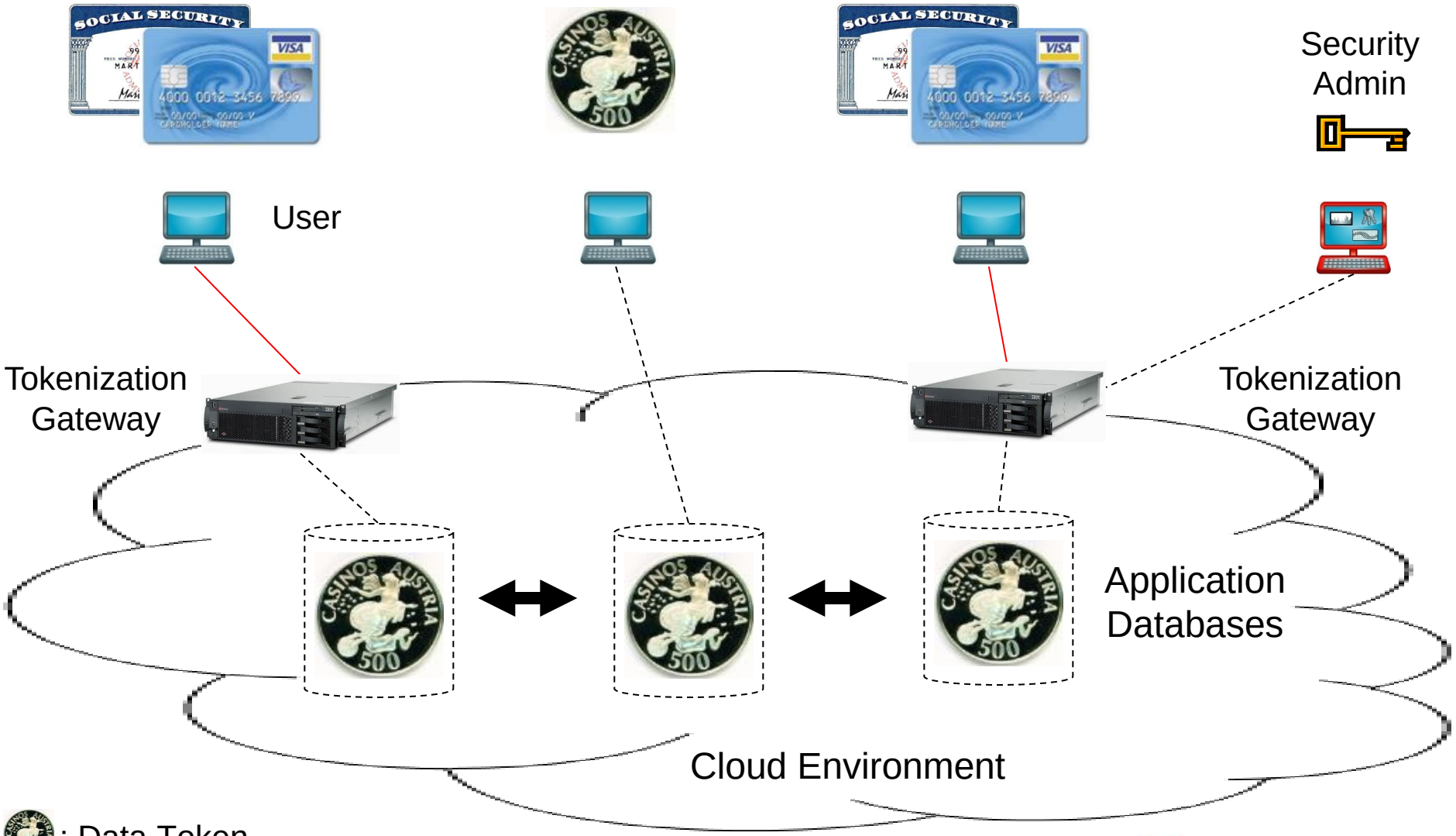
: Data Token

Unprotected sensitive information: ——————

Protected sensitive information – – – – – – – – –

protegrity

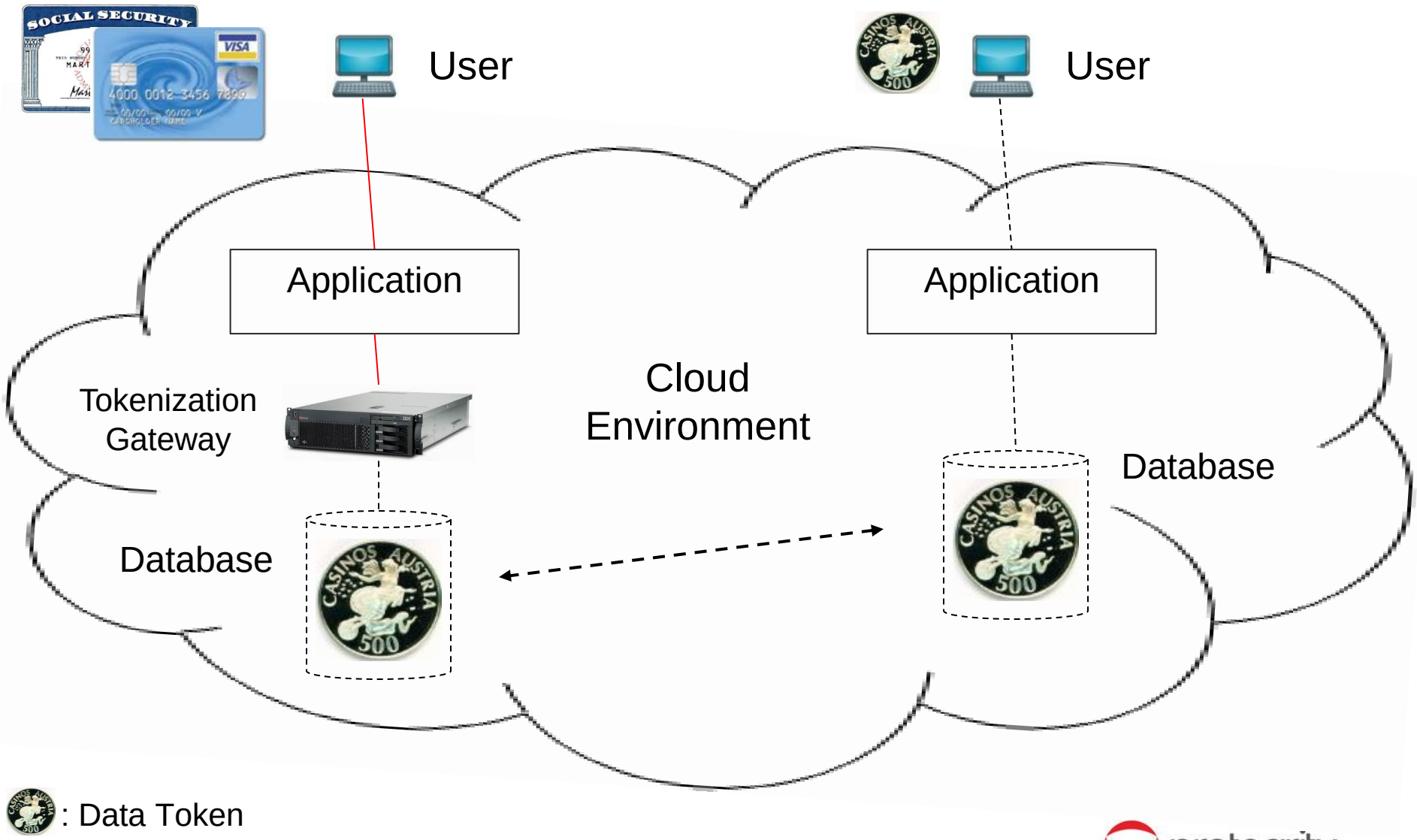
Data Tokens in a Cloud Environment – Integration Example



Unprotected sensitive information:

Protected sensitive information

Data Tokenization at the Gateway Layer



Unprotected sensitive information:

Protected sensitive information

protegrity

Data Tokenization at the Gateway Layer

User

User

Application

Application

Tokenization Gateway

Database

Cloud Environment

Database

: Data Token

Unprotected sensitive information:

Protected sensitive information

protegrity

Data Tokenization at the Application Layer

User

Security Admin

Application

Token Server

Database

Cloud

: Data Token

Unprotected sensitive information:

Protected sensitive information

protegrity

Data Tokenization at the Database Layer

User

Security Admin

Application

Token Server

Database

Cloud

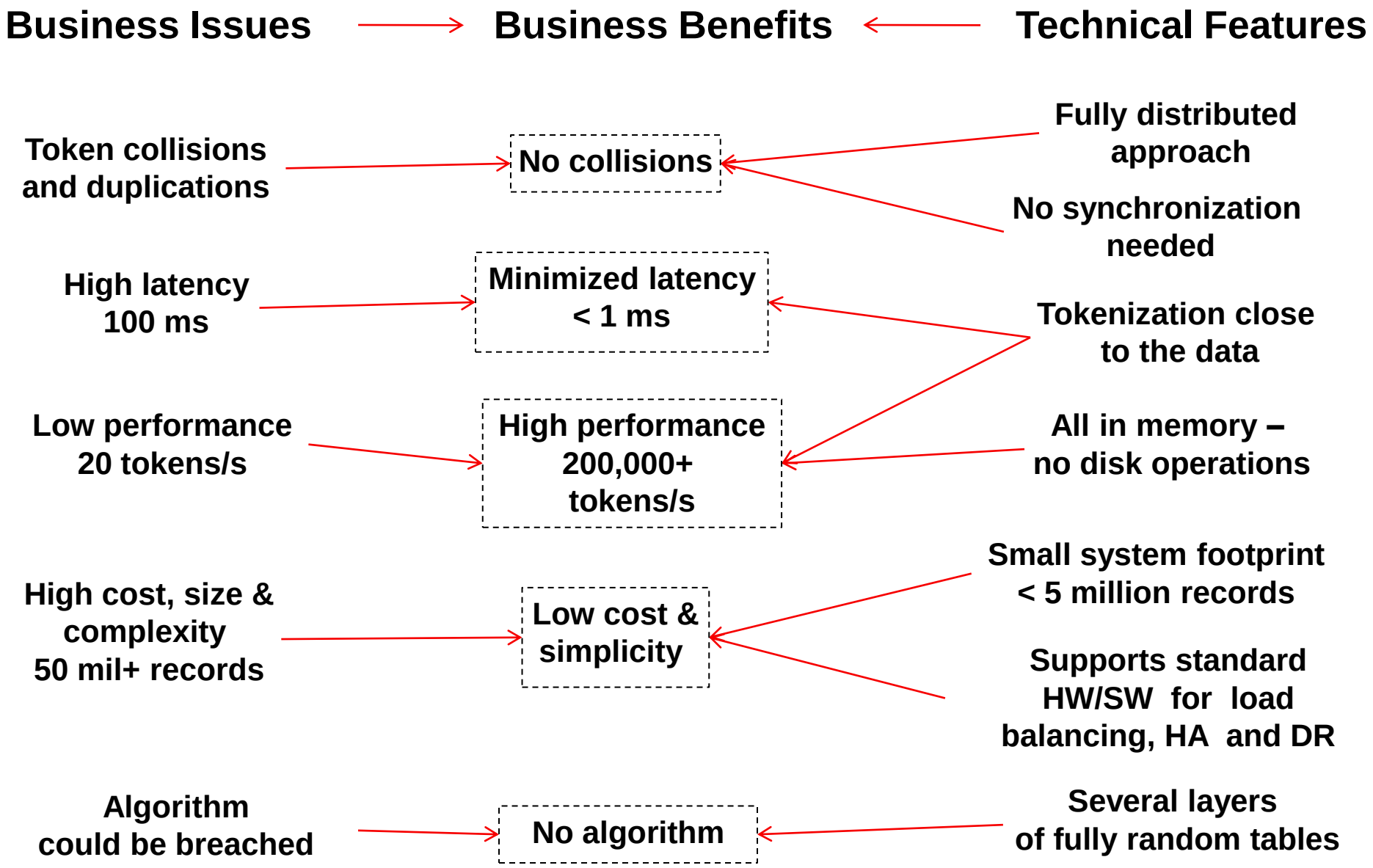
: Data Token

Unprotected sensitive information:

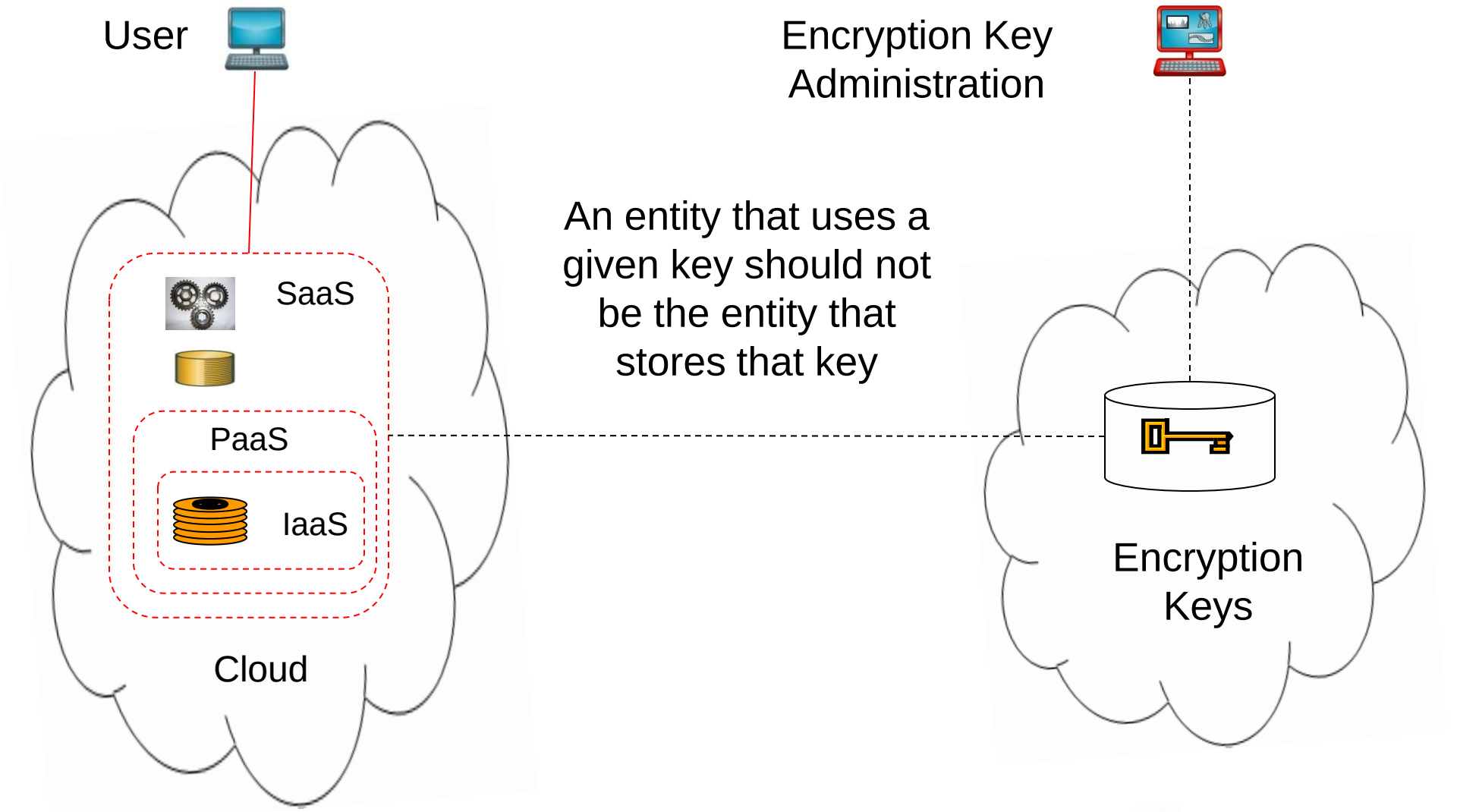
Protected sensitive information

protegrity

Solving 5 Business Issues with 7 Technical Features



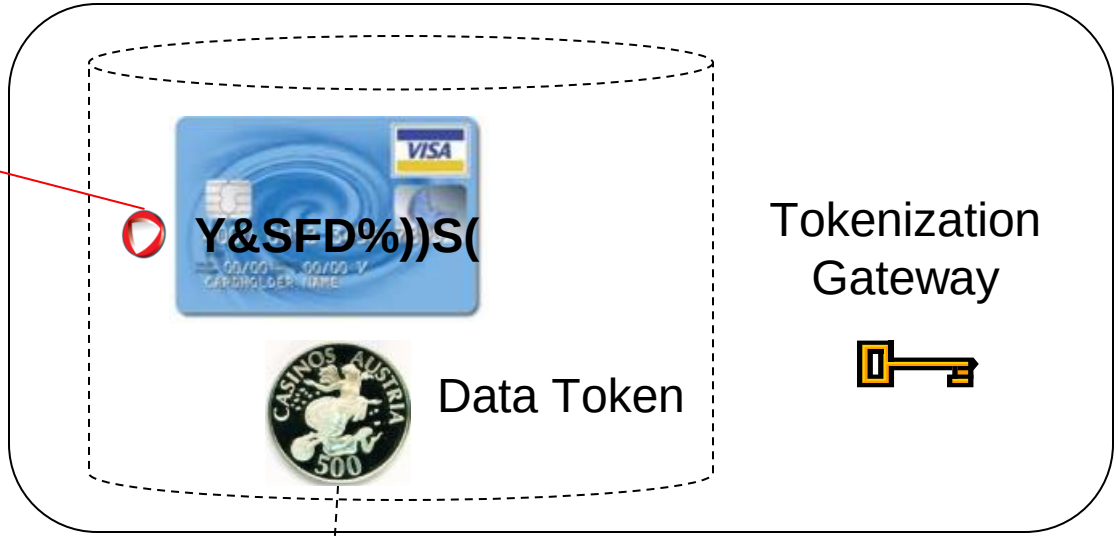
Securing Encryption Keys



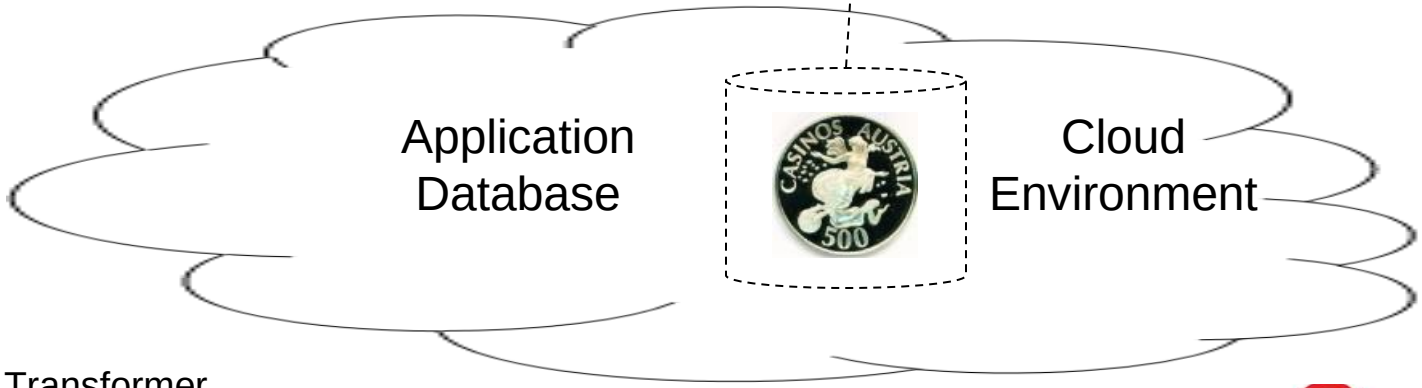
Source: http://csrc.nist.gov/groups/SNS/cloud-computing/

Hiding Data in Plain Sight – Data Tokenization

4000 0012 3456 7899



40 *12 3456 7890* 7899



: Data Transformer

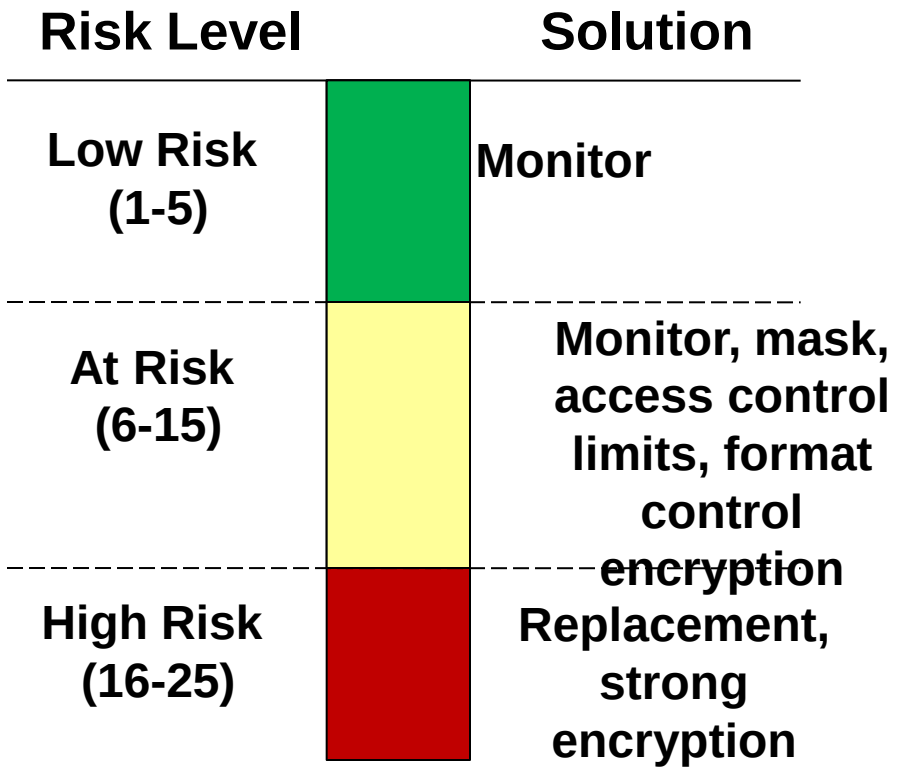
Unprotected sensitive information: ——————

Protected sensitive information: - - - - - - - -

Deploy Defenses

Matching Data Protection Solutions with Risk Level

Data Field	Risk Level
Credit Card Number	25
Social Security Number	20
CVV	20
Customer Name	12
Secret Formula	10
Employee Name	9
Employee Health Record	6
Zip Code	3



protegrity

Please contact me for more information

Ulf Mattsson

Ulf . Mattsson AT protegrity . com

protegrity

protecting your data.
protecting your business.

Summary

1. With the rising cost of data security breaches and their increasing frequency, companies are starting to reevaluate how they protect their data.

2. External and internal breaches have highlighted the need for companies to understand the flow of data within the enterprise and the need to take a more granular approach in terms of how it is secured.

3. This session will discuss recent breaches and review different options for data protection strategies in a cloud and outsourced environment.

US Laws - Privacy and Data Security Risks in Cloud

- HIPAA Restrictions on Health Data
  - Covered entity would risk a HIPAA violation by using such a provider for data storage.
- Breach Provisions Under HITECH Act
  - To the extent a HIPAA covered entity discloses PHI to a cloud provider, it risks exposure to federal data security breach notification requirements under the HITECH Act.
- Gramm-Leach-Bliley Act - GLBA
  - GLB's Privacy and Safeguards Rules restrict financial institutions from disclosing consumers' nonpublic personal information to non-affiliated third parties
- State Information Security Laws
  - For example, California requires businesses that disclose personal information to nonaffiliated third parties to include contractual obligations that those entities maintain reasonable security procedures
- State Breach Notification Laws
  - Over 45 U.S. states and other jurisdictions have data security breach notification laws that require data owners to notify individuals whose computerized personal information has been subject to unauthorized access
- Massachusetts regulations
  - Must determine whether the cloud provider maintains appropriate security measures to protect the data to be stored

US Legislation

US Laws - Privacy and Data Security Risks in Cloud

- HIPAA Restrictions on Health Data
  - Covered entity would risk a HIPAA violation by using such a provider for data storage.
- Breach Provisions Under HITECH Act
  - To the extent a HIPAA covered entity discloses PHI to a cloud provider, it risks exposure to federal data security breach notification requirements under the HITECH Act.
- Gramm-Leach-Bliley Act - GLBA
  - GLB's Privacy and Safeguards Rules restrict financial institutions from disclosing consumers' nonpublic personal information to non-affiliated third parties
- State Information Security Laws
  - For example, California requires businesses that disclose personal information to nonaffiliated third parties to include contractual obligations that those entities maintain reasonable security procedures
- State Breach Notification Laws
  - Over 45 U.S. states and other jurisdictions have data security breach notification laws that require data owners to notify individuals whose computerized personal information has been subject to unauthorized access
- Massachusetts regulations
  - Must determine whether the cloud provider maintains appropriate security measures to protect the data to be stored

Best Practices and Regulations

Case Study: Global Investment Banking and Securities

Investment banking division

- Encryption of Deal related attributes and other MNPI data (i.e. company name, company identifier, etc)
- Prevented development and technology people to identify entities involved in deals

Compliance department

- Compliance has TWO copies of Deal data – one for the Conflicts Process and one for the Control Room
- Encryption KEYS are DIFFERENT in Banking and Compliance

Encryption of compensation data

Encryption of firewall rules

- Managed in a standalone application

Platforms:

- Oracle, DB2, SQL Server, UNIX, Linux and Windows

Best Practices from NIST on PII Data - SP800-122

Examples of PII Data

1. Name
2. Personal identification number, such as social security number (SSN), passport number, driver‘s license number, taxpayer identification number, patient identification number, and financial account or credit card number
3. Address information
4. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address
5. Telephone numbers
6. Personal characteristics, including photographic image
7. Information identifying personally owned property
8. Information about an individual that is linked or linkable to one of the above

Source: National Institute of Standards & Technology - NIST (http://csrc.nist.gov/)

SEC Adopted Regulation S-P to Address Privacy

1. Like GLB (*Gramm-Leach-Bliley* Act), compliance with Regulation S-P (17 CFR Part 248) is mandatory since July 1, 2001
2. Regulation S-P provides the means of implementing GLB
3. Every broker, dealer, and investment company, and every investment adviser registered with the SEC must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information
4. Insure the security and confidentiality of customer records and information
5. Protect against any anticipated threats or hazards to the security or integrity of customer records and information
6. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer

HIPAA / HITECH Act – Title IV Legislation

[1] Establishes a Federal Breach Notification requirement for health information that is not encrypted or otherwise made indecipherable. It requires that an individual be notified if there is an unauthorized disclosure or use of their health information.

[2] Ensures that new entities that were not contemplated when the Federal privacy rules were written, as well as those entities that do work on behalf of providers and insurers, are subject to the same privacy and security rules as providers and health insurers.

[3] Provide transparency to patients by allowing them to request an audit trail showing all disclosures of their health information made through an electronic record.

[4] Shutting down the secondary market that has emerged around the sale and mining of patient health information by prohibiting the sale of an individual's health information without their authorization.

[5] Requires that providers attain authorization from a patient in order to use their health information for marketing and fundraising activities.

[6] Strengthening enforcement of Federal privacy and security laws by increasing penalties for violations.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Health Information Technology for Economic and Clinical Health Act (HITECH Act), of 2009

Example: HIPAA – 18 Direct Identifiers

1. Names
2. Geographic subdivisions smaller than a state, including
3. All elements of dates (e.g., date of birth, admission)
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal locators (URLs)
15. IP address numbers
16. Biometric identifiers, including fingerprints and voice prints
17. Full-face photographic images and any comparable images
18. Other unique identifying numbers, characteristics or codes

MA 201 Privacy Law

The Massachusetts law is the first in the nation to require specific technology when protecting personal information. Both "**data at rest**" and "data in transit" over a public network, such as the Internet, that contain personal information must be **encrypted**.

- Personal information is defined as a Massachusetts resident's **name** in combination with one of the following :

  Social Security number , Driver's license number or state-issued identification card number and Financial **account number or credit/debit card number**

Visa Best Practices for Tokenization Version 1

Published July 14, 2010.

Token Generation		Token Types	
		Single Use Token	Multi Use Token
Algorithm and Key **Reversible**	Known strong algorithm (NIST Approved)	✓	-
One way **Irreversible** Function	Unique Sequence Number	✓	✓
	Hash	Secret per transaction	Secret per merchant
	Randomly generated value	✓	✓

Best Practices Summary

- Reduce attack surface and compliance scope
  - Separation of System Components
- Separation of Duties: DBA, Risk Manager, etc.
  - Get the DBA off the hook – Not a Suspect
- Security can be highly transparent to developers
- Less documentation necessary

Making Data Unreadable – Protection Methods (Pro's & Con's)

IO Interface		Protection Method				
System Layer	**Granularity**	**AES/CBC, AES/CTR …**	**Formatted Encryption**	**Data Tokenization**	**Hashing**	**Data Masking**
Application	Column/Field	●	●	●	●	●
	Record	●	●	●	●	●
Database	Column	●	●	●	●	●
	Table	●	○	○	○	○
	Table Space	●	○	○	○	○
OS File	IO Block	●	◒	◒	◒	◒
Storage System	IO Block	●	○	○	○	○

Best ● ◔ ◒ ◕ ○ **Worse**

protegrity

Best Practices from NIST on PII Data - SP800-122

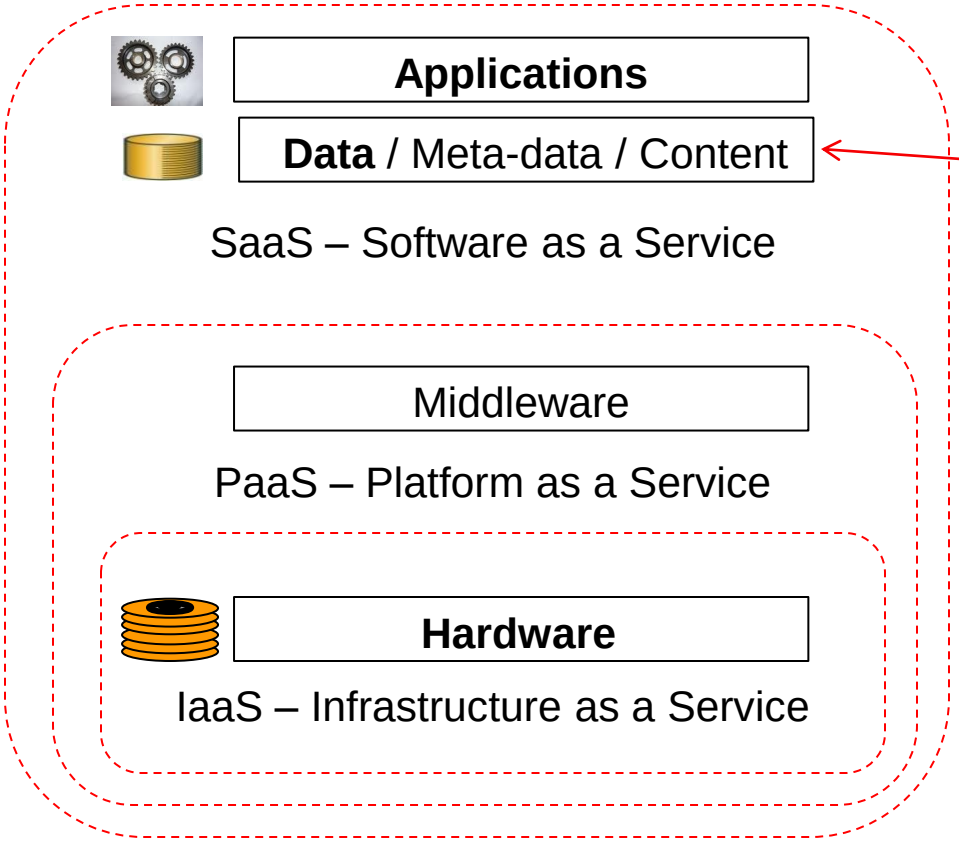
De-identified information can be assigned a PII confidentiality impact level of *low, as long as the following are both true:*

- The re-identification algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access to the re-identification information.
- The data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data.

Source: National Institute of Standards & Technology - NIST (http://csrc.nist.gov/)

Mapping the Cloud to Compliance – PCI DSS

Cloud Service Models



Compliance Model – PCI DSS

1.	Install and maintain a firewall configuration to protect data
2.	Do not use vendor-supplied defaults for system passwords and other security parameters
3.	Protect stored data
4.	Encrypt transmission of cardholder data and sensitive information across public networks
5.	Use and regularly update anti-virus software
6.	Develop and maintain secure systems and applications
7.	Restrict access to data by business need-to-know
8.	Assign a unique ID to each person with computer access
9.	Restrict physical access to cardholder data
10.	Track and monitor all access to network resources and cardholder data
11.	Regularly test security systems and processes
12.	Maintain a policy that addresses information security

Source: http://csrc.nist.gov/groups/SNS/cloud-computing/