New York Oracle Users Group, Inc.

Database Security Solutions in Cloud and Outsourced Environments

l f . att sson
. rot egri t y

ul f . mat t sson . pr ot egri t y . com

Ulf Mattsson

- 20 years with IBM Development & Global Services
- Inventor of 22 patents – Encryption and Intrusion Prevention
- 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
  - PCI Security Standards Council (PCI SSC)
  - American National Standards Institute (ANSI) X9
  - Cloud Security Alliance (CSA)
  - Information Systems Security Association (ISSA)
  - Information Systems Audit and Control Association (ISACA)
  - Institute of Electrical and Electronics Engineers (IEEE)
- Received Industry's 2008 Most Valuable Performers (MVP) award together with technology leaders from IBM, Google and other leading companies

Cloud Security Alliance (CSA): http://www.cloudsecurityalliance.org/

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 concerns
tokenization is a better opti
transparent, faster, more sec
decreases administrators' ab
risk, exposure of encryption
by replacing sensitive data
anything with the data if the
remediation costs to applica
That said, analysts recomme
take shortcuts and don't con
the analysts. Tokenization n

Ulf Mattsson, CTO, Protegrity Corporation

June 4, 2009

MasterCard Worldwide

How to Evaluate Encryption Technologies

Achieving PCI Compliance & Protecting Cardholder Data

Abstract

1. One of the biggest concerns about the cloud is the threat of data being stolen

2. The cloud is a high risk environment that decreases the database administrators' ability to control the flow of sensitive data

3. Because cloud introduces risk, exposure of database encryption keys becomes particularly vulnerable

4. Data security in today's business world is a classic Catch-22

5. We need to protect both data and the business processes that rely on that data, but in order to do so we need to move from a reactive, fear (or compliance) driven mode to a proactive data security plan

Summary

1. How to secure Oracle database and application environments by using a risk adjusted methodology for determining appropriate solutions

2. Address external and internal threats, including threats from DBAs and developers

3. Review case studies in protecting against internal and external threats

4. How to be compliant to PCI DSS and State Legislation by utilizing different data protection options including data encryption, enterprise key management, tokenization and database activity monitoring

5. How to provide cost effective protection of data throughout the entire data flow in production, test, outsourced and virtualized environments

6. How to balance the requirements for security, performance and administration

No Confidence in Cloud Security (Oct 2010)

CSO Magazine Survey: Cloud Security Still a Struggle for Many Companies

A recent article written by Bill Brenner, senior editor at CSO Magazine, reveals that companies are still a bit scared of putting critical data in the cloud. Results from the 8th Annual Global Information Security Survey conducted by CSO, along with CIO and PriceWaterhouseCoopers, cites: 62% of companies have little to no confidence in their ability to secure any assets put in the cloud. Also, of the 49% of respondents who have ventured into cloud computing, 39% have major qualms about security.

Source, CSO. October, 2010 : http://www.csoonline.com/

Cloud Computing to Fuel Security Market (Oct 2010)

1. "Concerns about cloud security have grown in the past year”

2. "In 2009, the fear was abstract: a general concern as there is with all new technologies when they're introduced ...

3. “Today, however, concerns are both more specific and more weighty”

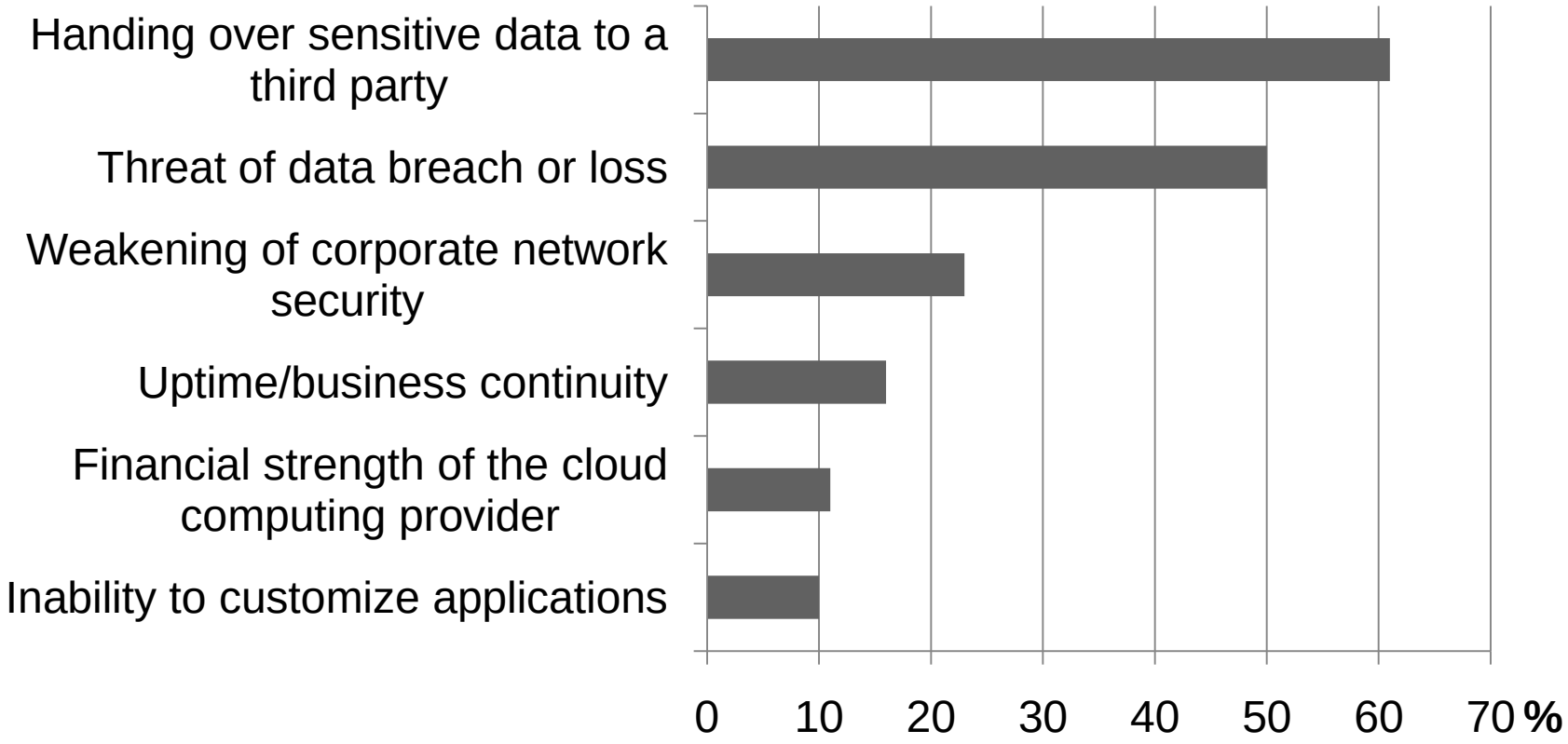
4. “We see organizations placing a lot more scrutiny on cloud providers as to their controls and security processes; and they are more likely to defer adoption because of security inadequacies than to go ahead despite them."

5. Opportunities in the cloud for vendors are data security, identity and access management, cloud governance, application security, and operational security.

FORRESTER® Forrester Research
MAKING LEADERS SUCCESSFUL EVERY DAY

http://www.eweek.com/c/a/Security/Forrester-Cloud-Computing-to-Fuel-Security-Market-170677/

Risks associated with cloud computing



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

The Changing Threat Landscape (Aug, 2010)

Some issues have stayed constant:

1. Threat landscape continues to gain sophistication
2. Attackers will always be a step ahead of the defenders

Different motivation, methods and tools today:

- We're fighting highly organized, well-funded crime syndicates and nations

Move from detective to preventative controls needed:

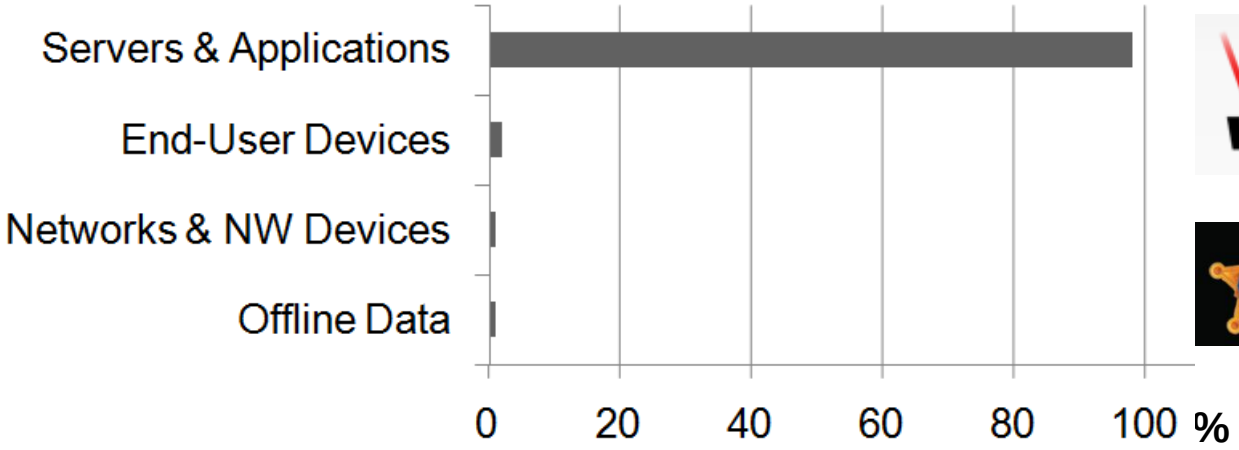
- Several layers of security to address more significant areas of risks

Source: http://www.csoonline.com/article/602313/the-changing-threat-landscape?page=2

2010 Data Breach Investigations Report

- Six years, 900+ breaches, and over 900 million compromised records
- The majority of cases have not yet been disclosed and may never be
- Over half of the breaches occurred outside of the U.S.

Online Data is Compromised Most Frequently:

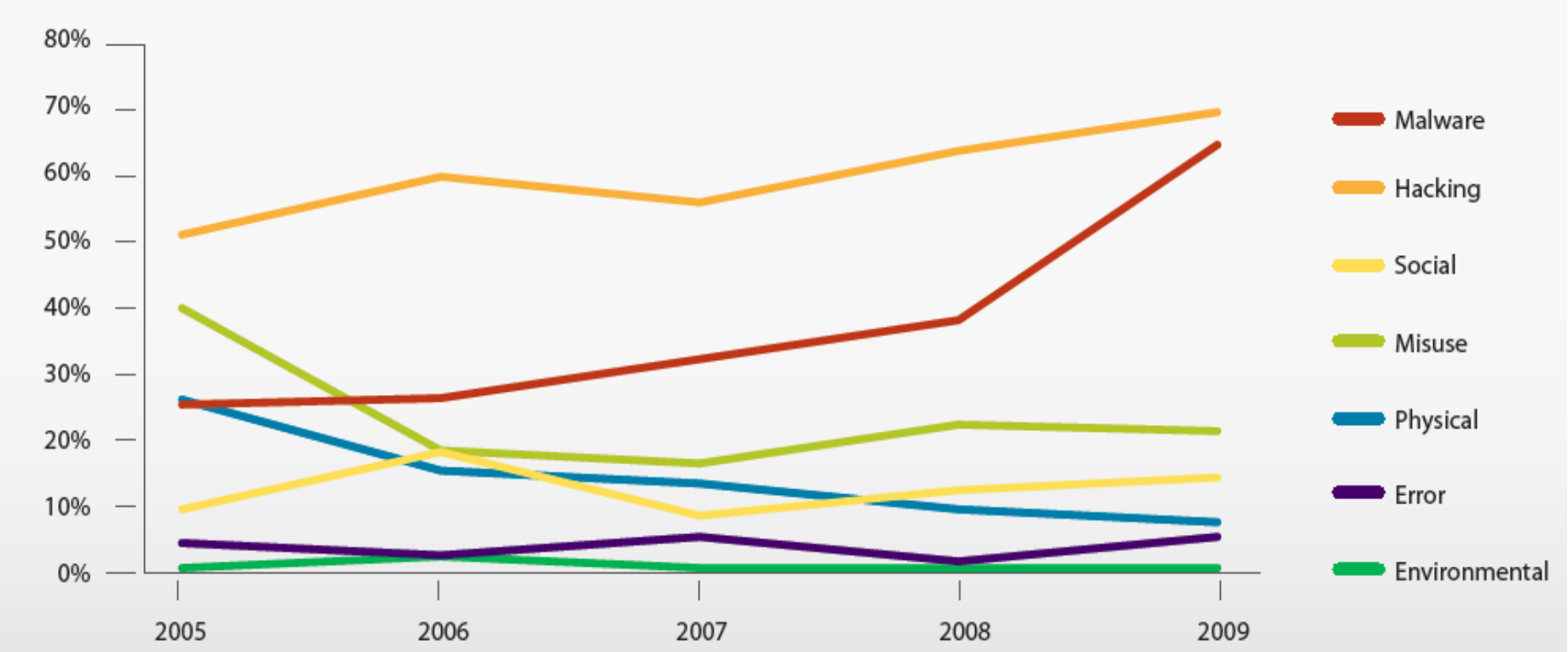


Source: 2010 Data Breach Investigations Report, Verizon Business RISK team and USSS

Threat Action Categories

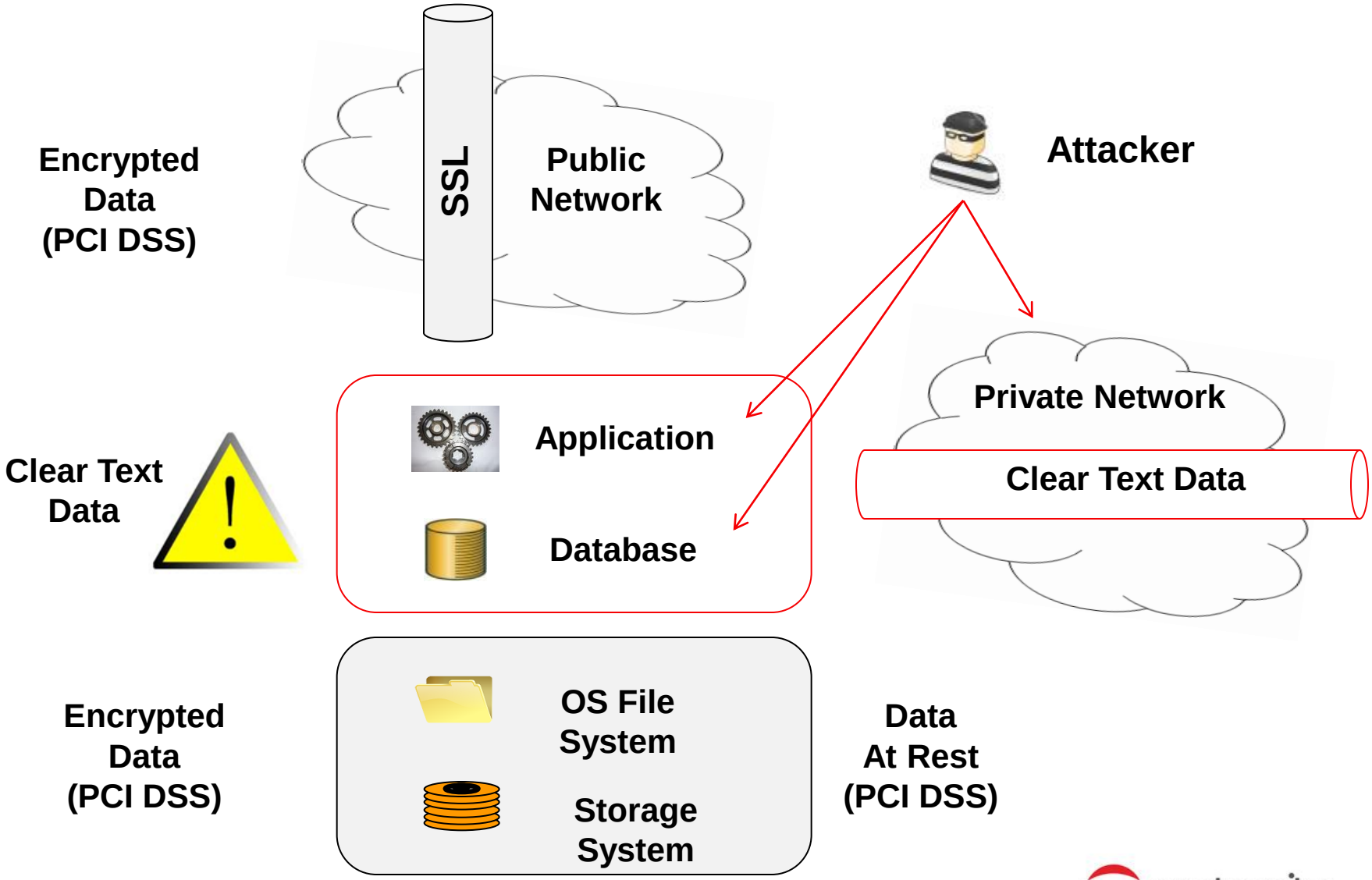
Compromised records

1. 90 % lost in highly sophisticated attacks
2. Hacking and Malware are more dominant

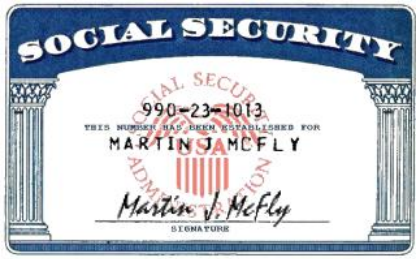


Source: 2010 Data Breach Investigations Report, Verizon Business RISK team and USSS

Not Enough to Encrypt the Pipe & Files!



New Methods for Hiding Data in Plain Sight



990-23-1013

4000 0012 3456 7899

123-45 -1013

40 *12 3456 7890* 7899

Application Databases

Cloud Environment

: Data Transformer

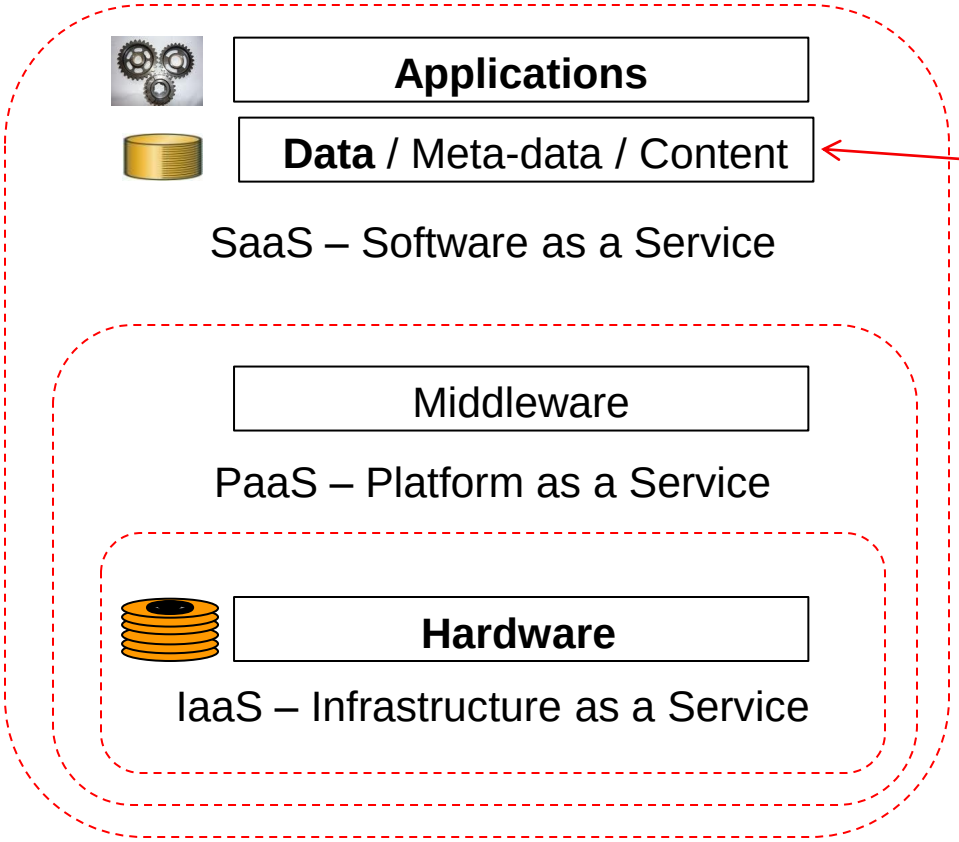
Unprotected sensitive information: ————————

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

protegrity

Mapping the Cloud to Compliance – PCI DSS

Cloud Service Models

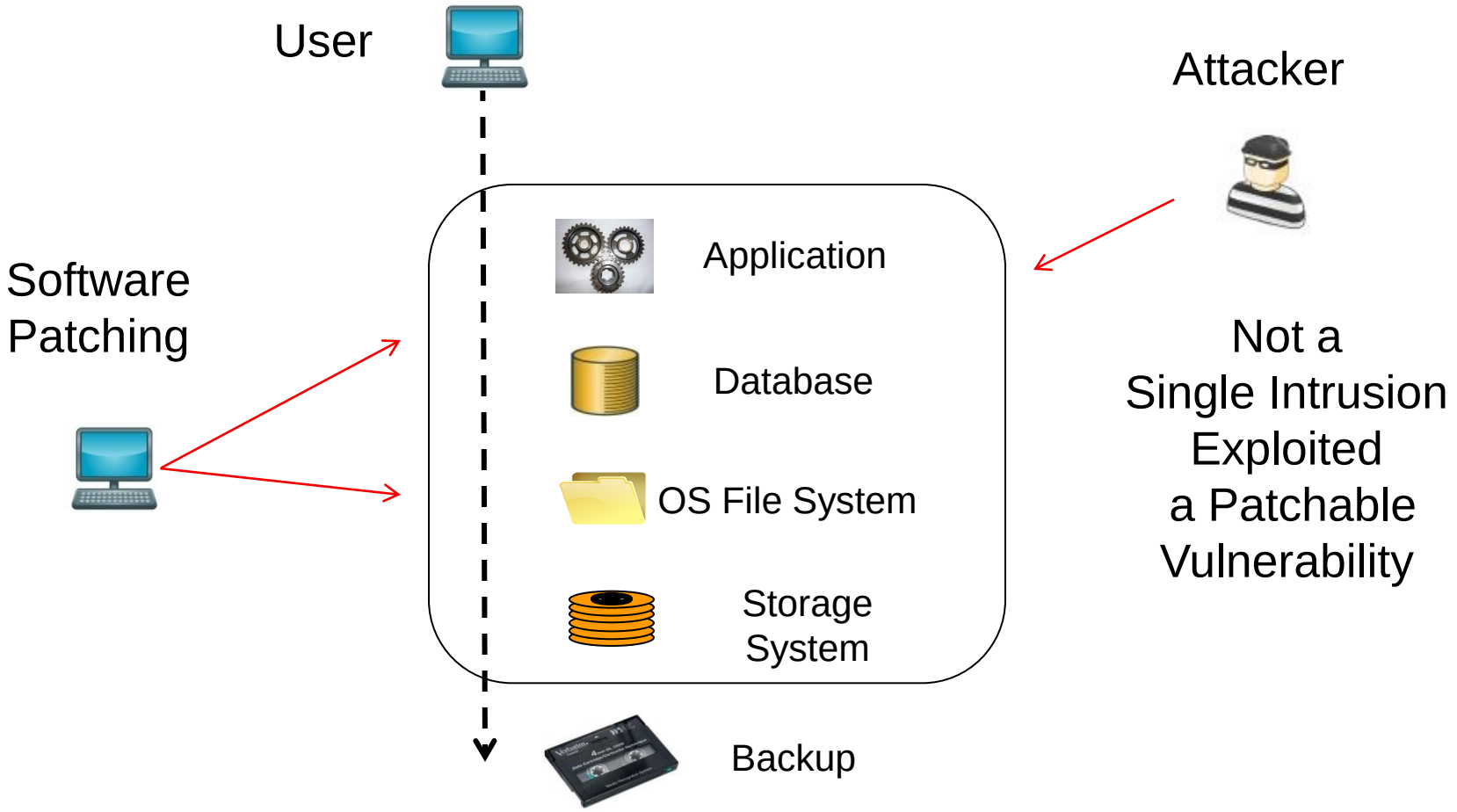


Compliance Model – PCI DSS

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/

Patching Software vs. Locking Down Data



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

protegrity

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

Case Studies – Retail Environments

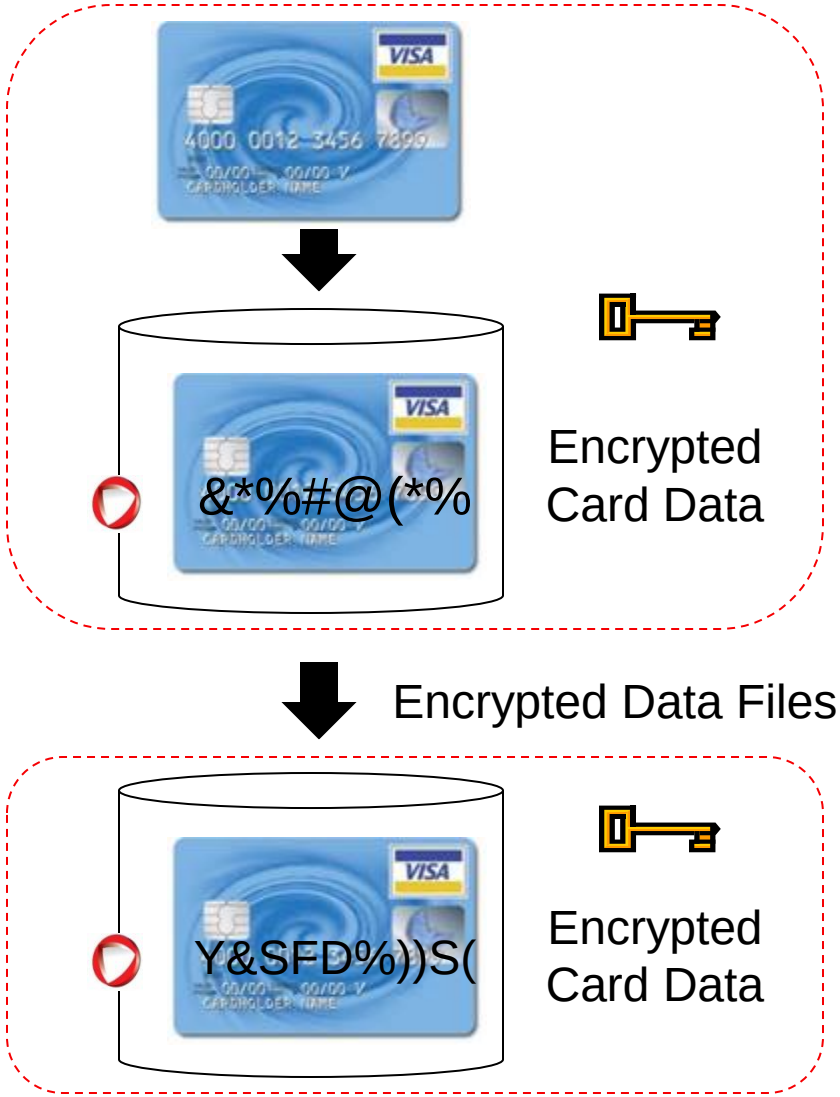
Study #1 – Major US Retailer – PCI / PII / PHI Data

1. Transparency to exiting applications
2. Central key management
3. Ensuring performance on the mainframe
4. Protect the flow of sensitive information
   - From thousands of stores, Back office systems and Data warehouse

Study #2 – Major US Retailer – PCI Data

1. Reduced cost – TCO
2. Reduced attack surface
3. Transparency to exiting applications
4. Central key management
5. Protect the flow of sensitive credit card information
   - From thousands of stores, Back office systems and Data warehouse

Case Study – PCI & Application Transparency



File Encryption:

Windows, UNIX, Linux, Mainframe z/OS

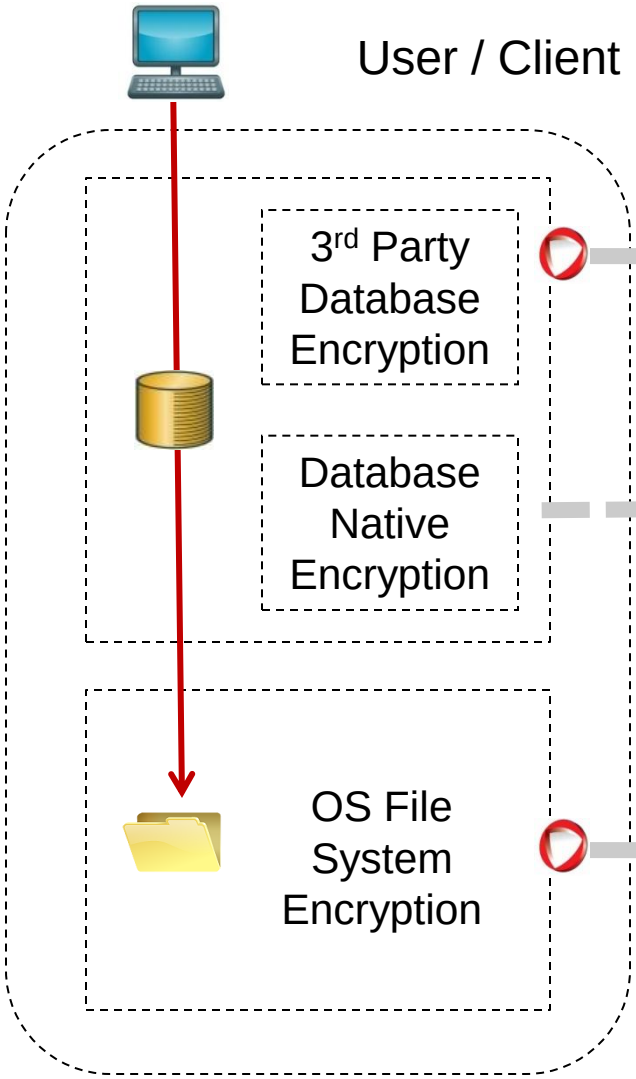
Database Encryption:

DB2 (zOS, iSeries), Oracle, SQL Server

: Encryption service

protegrity

Case Study: Granularity of Reporting and Separation of Duties



User	Access	Patient	Health Record
x	Read	a	xxx
DBA	Read	b	xxx
z	Write	c	xxx

Complete Log

Possible DBA manipulation

User	Access	Patient	Health Record
z	Write	c	xxx

No Read Log

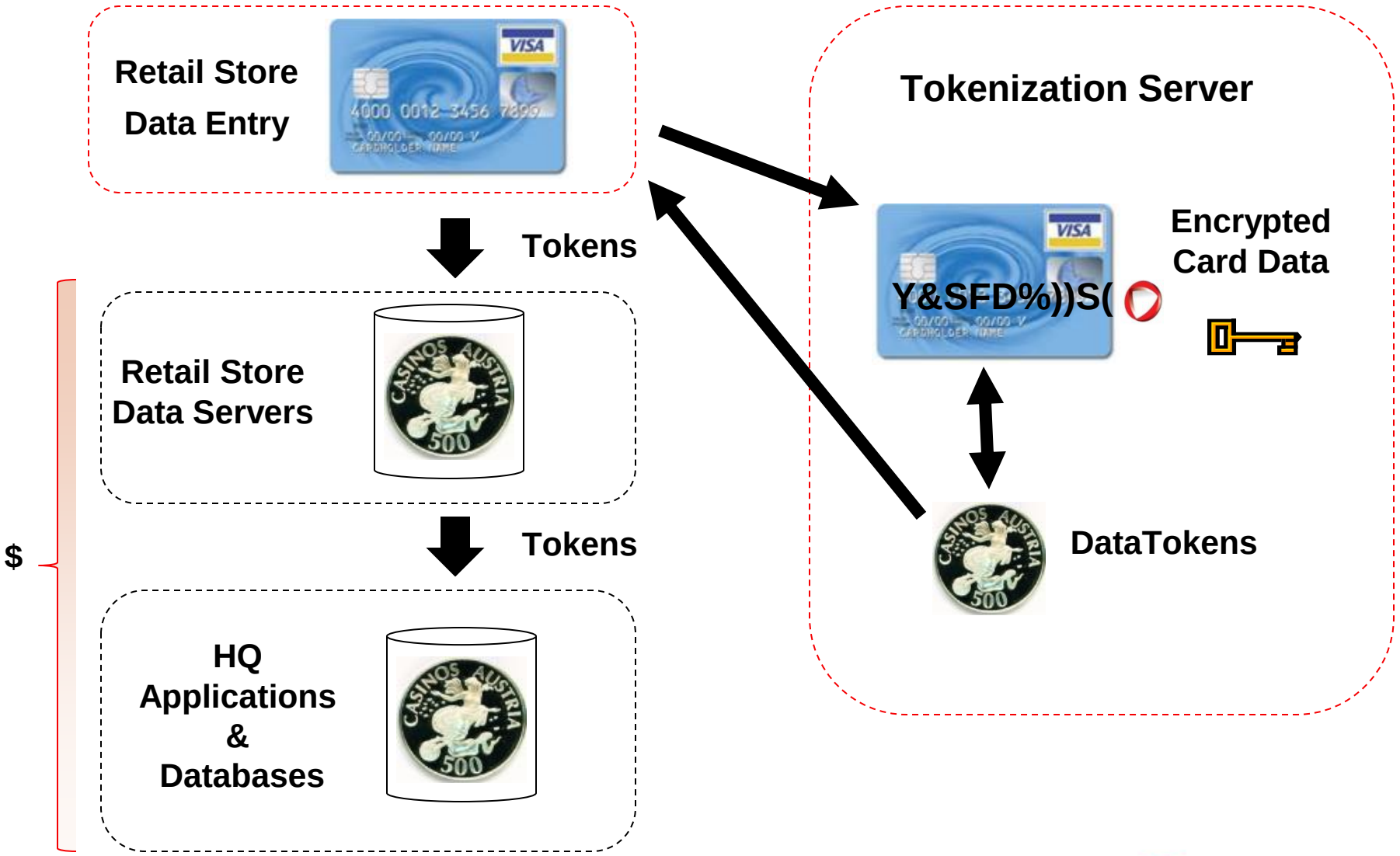
Possible DBA manipulation

User	Access	Patient	Health Data Record	Health Data File
Database Process 0001	Read	?	?	PHI002
Database Process 0001	Read	?	?	PHI002
Database Process 0001	Write	?	?	PHI002

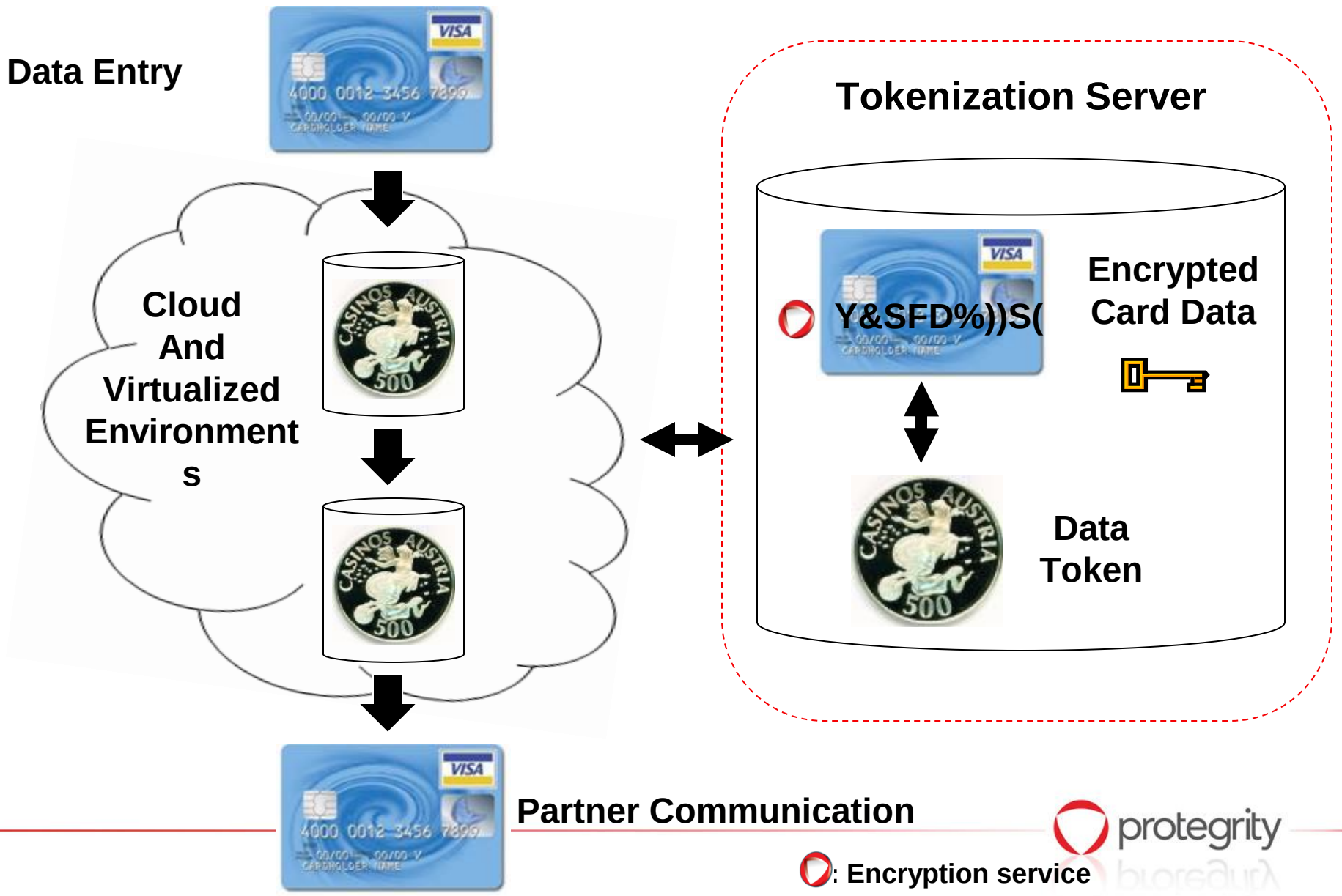
No Information On User or Record

: Encryption service

Case Study – PCI, Reduce Cost and Attack Surface



Tokenization in a Cloud Environment



Best Practices from Visa

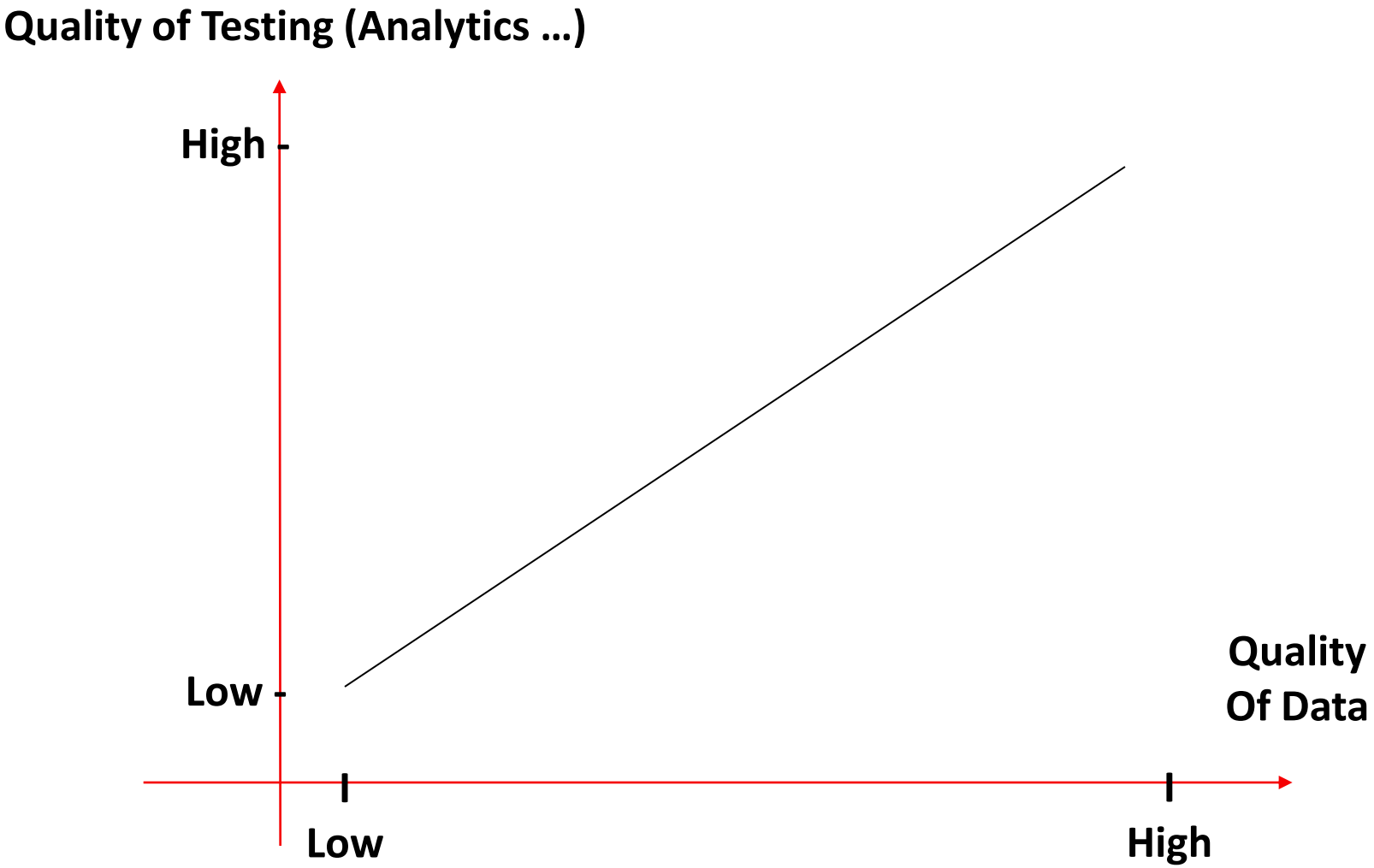
Best Practices for Token Generation		Token type	
		Single-Use	**Multi-Use**
Algorithm and key	Known strong algorithm	ANSI or ISO approved algorithm	
One way irreversible function	Unique sequence number	**OK**	**OK**
	Hashing	Secret per transaction	Secret per merchant
	Randomly generated value	**OK**	**OK**

VISA

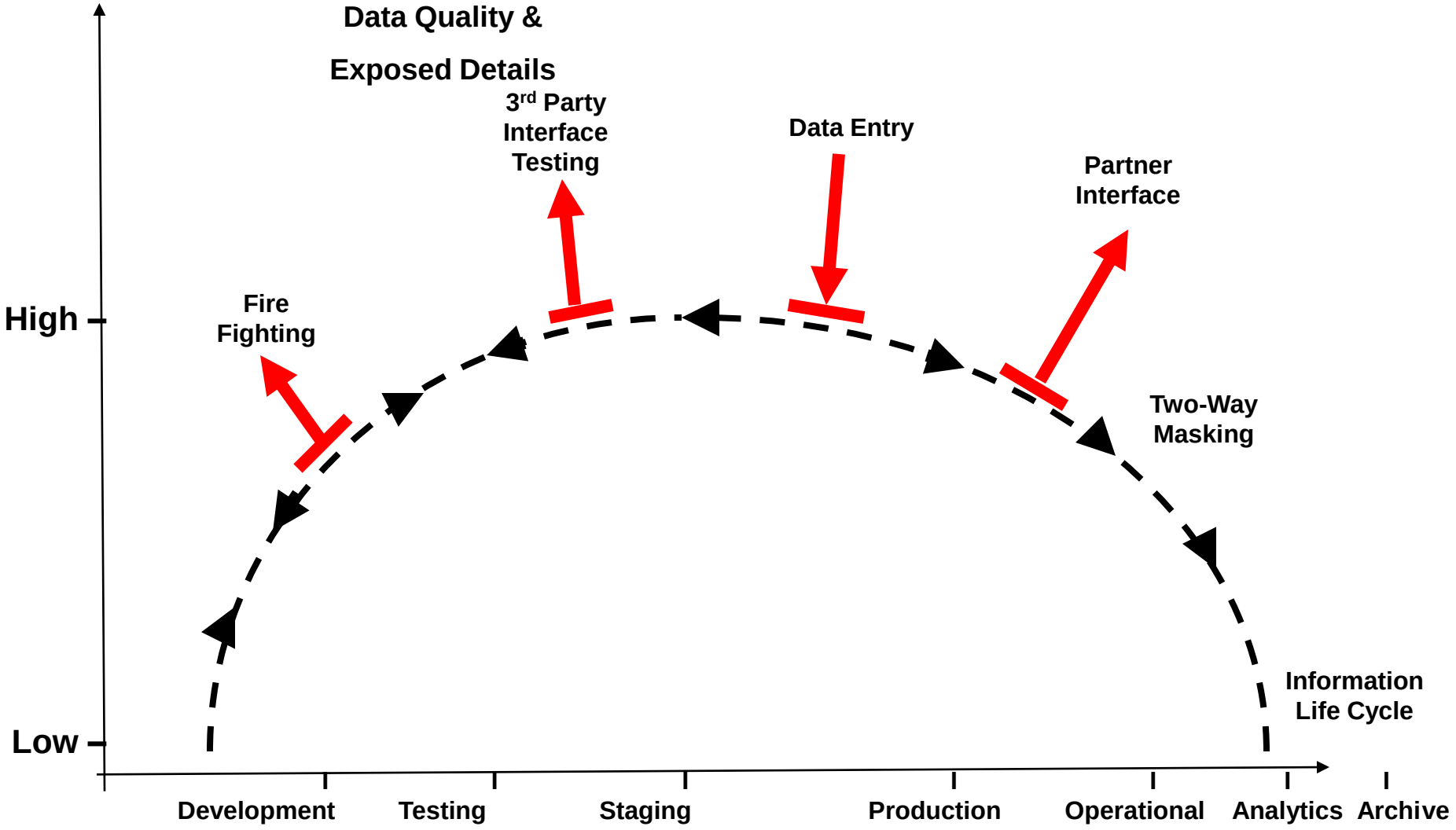
protegrity

Data Protection Strategies and Methods

Quality of Systems Testing vs. Data Exposure



Data Security Life Cycle – Reversible Protection

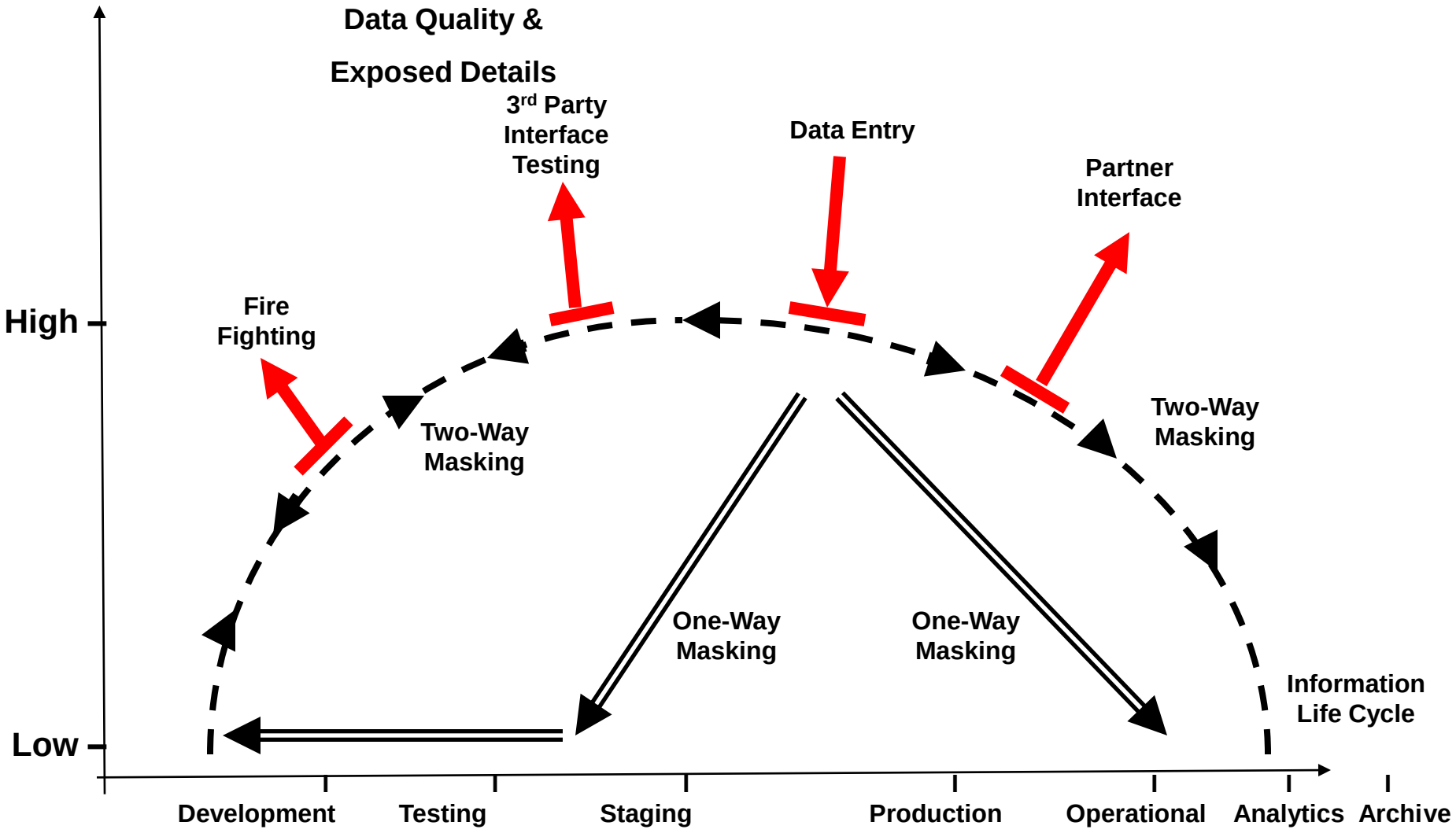


Unprotected sensitive information:

Protected sensitive information

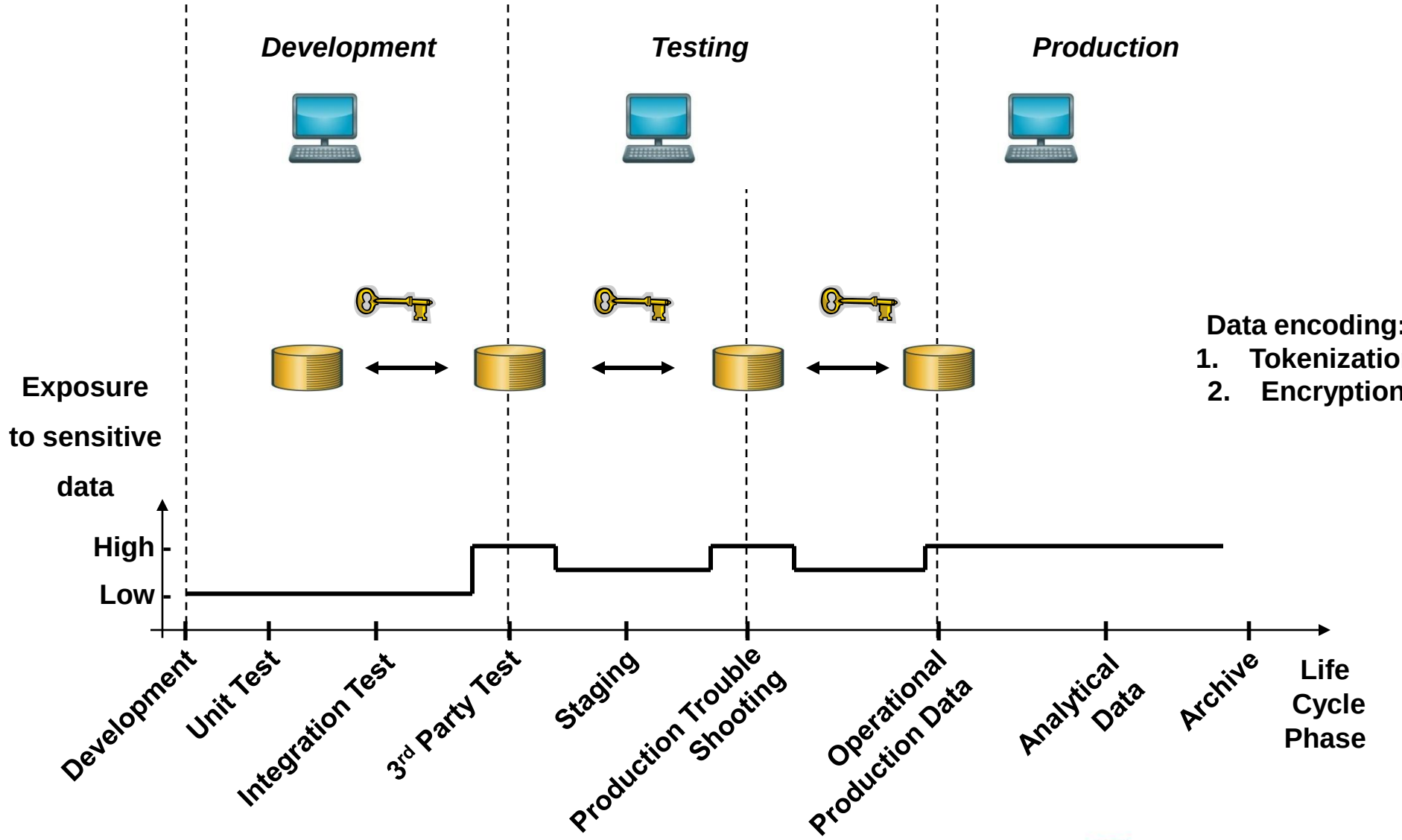
protegrity

Data Protection – Reversible or Not



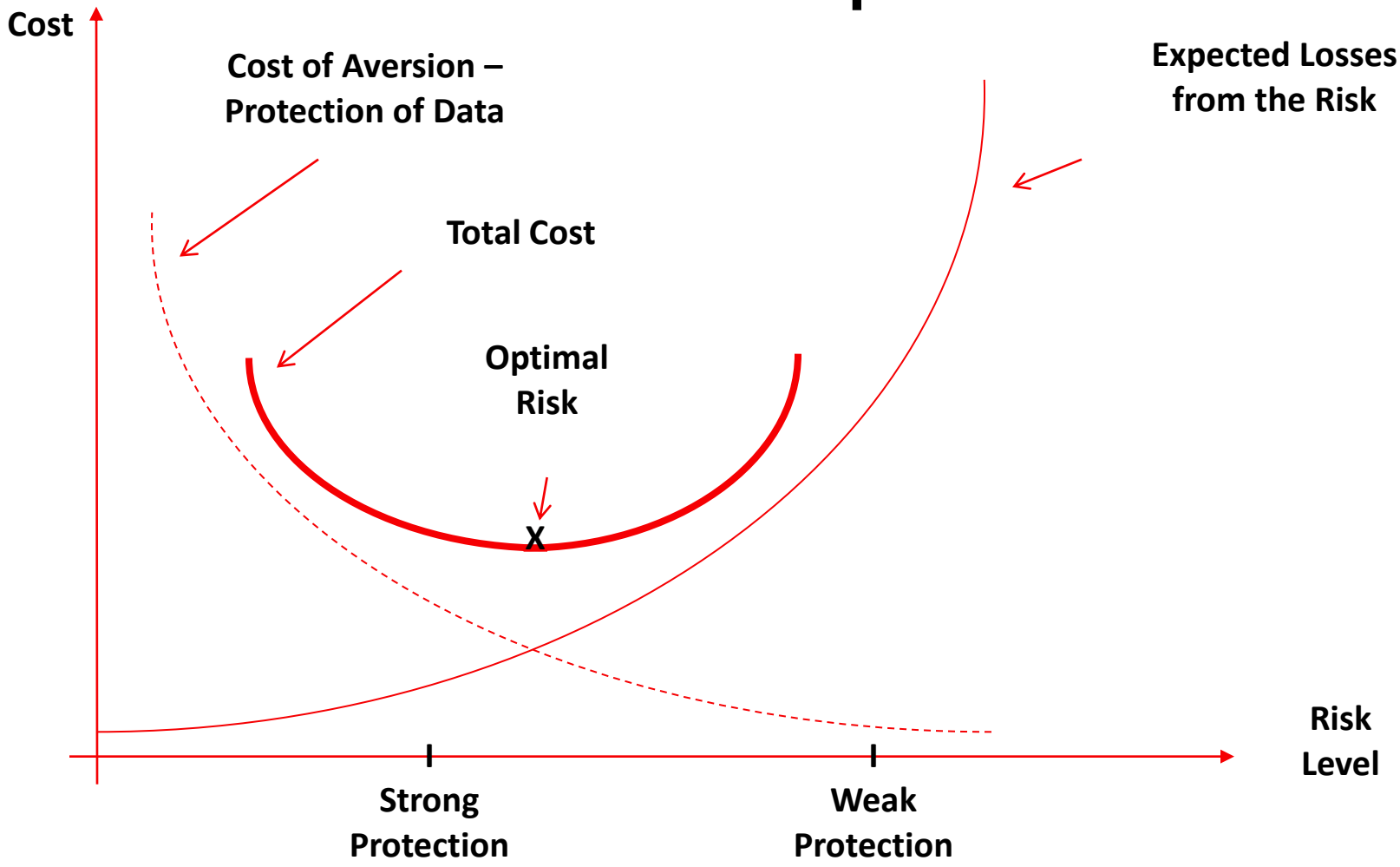
protegrity

Limit Exposure to Sensitive Data

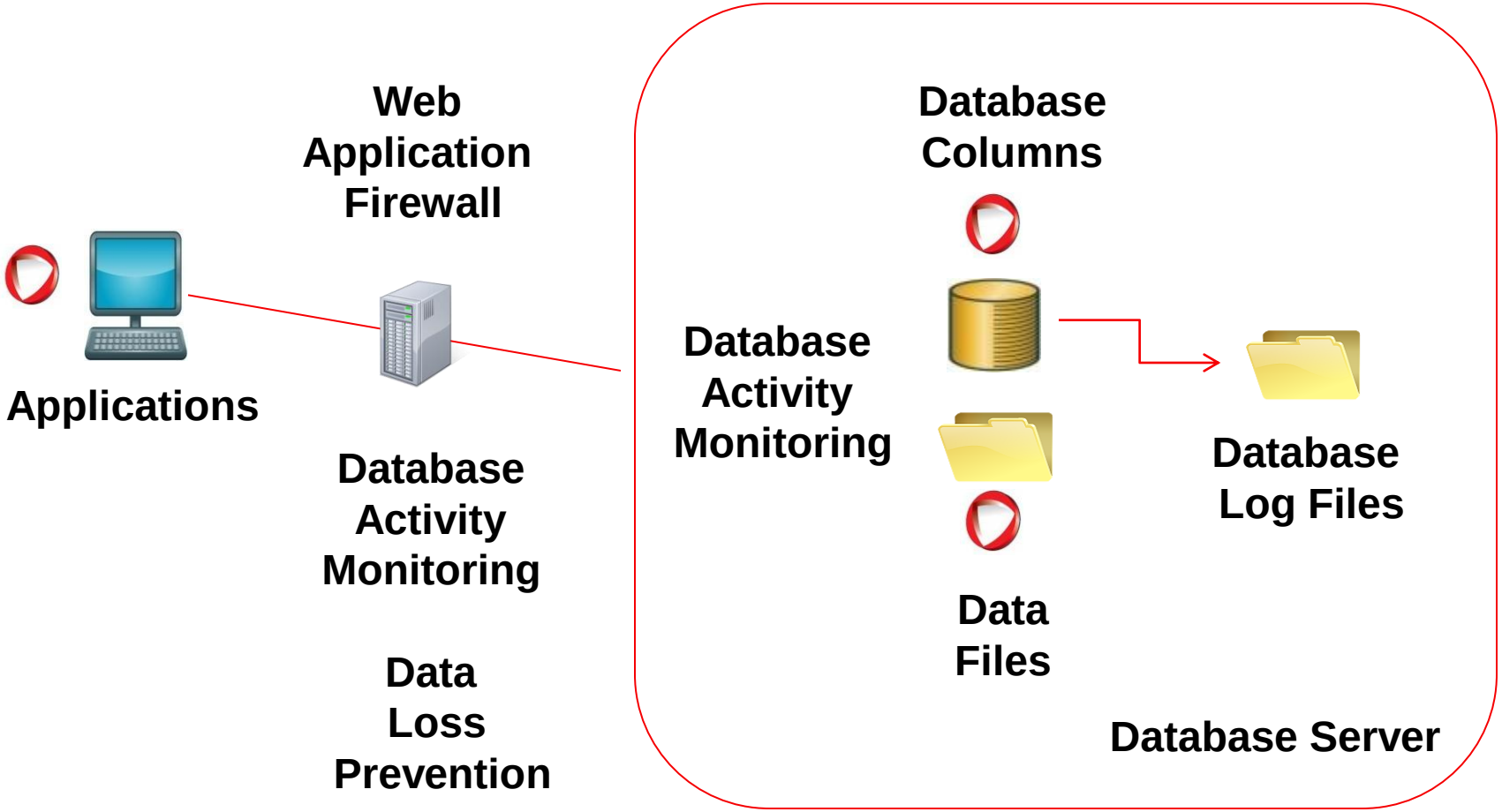


protegrity

Choose Your Defenses – Total Cost of Ownership



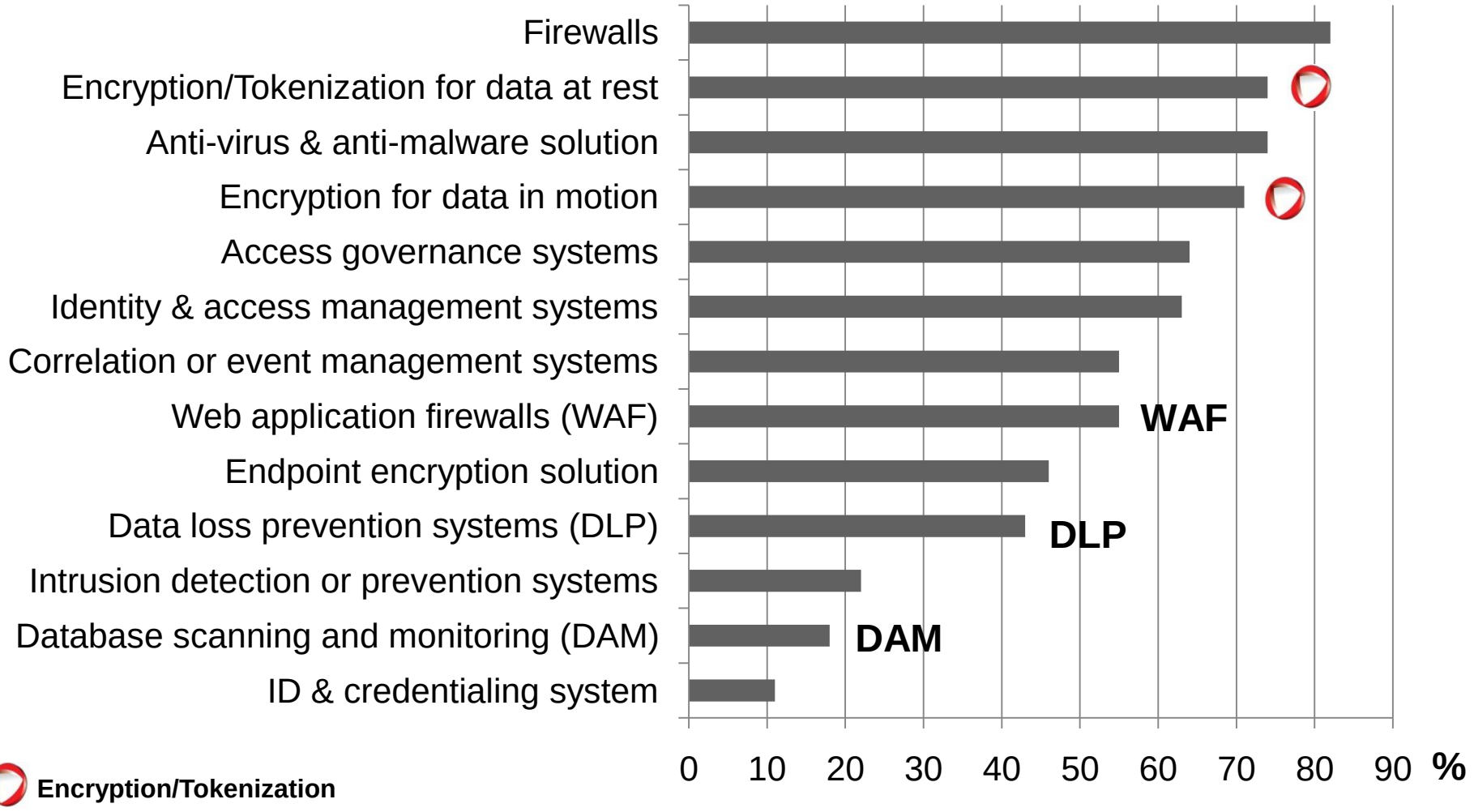
Choose Your Defenses – Different Approaches



Encryption/Tokenization

protegrity

Choose Your Defenses – Cost Effective PCI DSS



Encryption/Tokenization

Source: 2009 PCI DSS Compliance Survey, Ponemon Institute

protegrity

Know Your Data – Identify High Risk Data

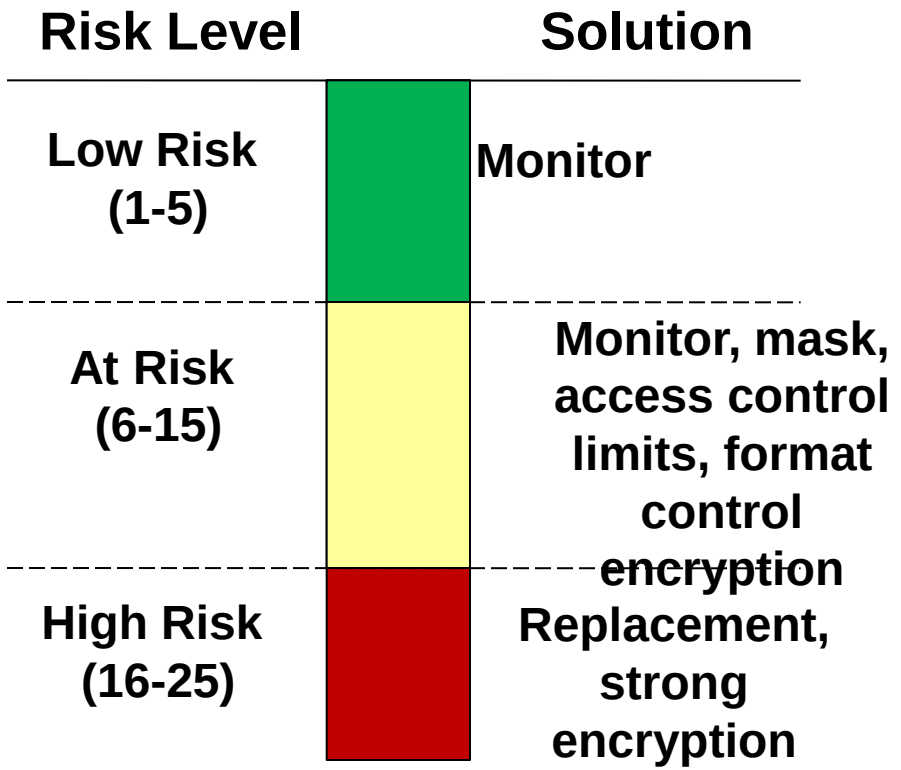
- Begin by determining the risk profile of all relevant data collected and stored
  - Data that is resalable for a profit
  - Value of the information to your organization
  - Anticipated cost of its exposure

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

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

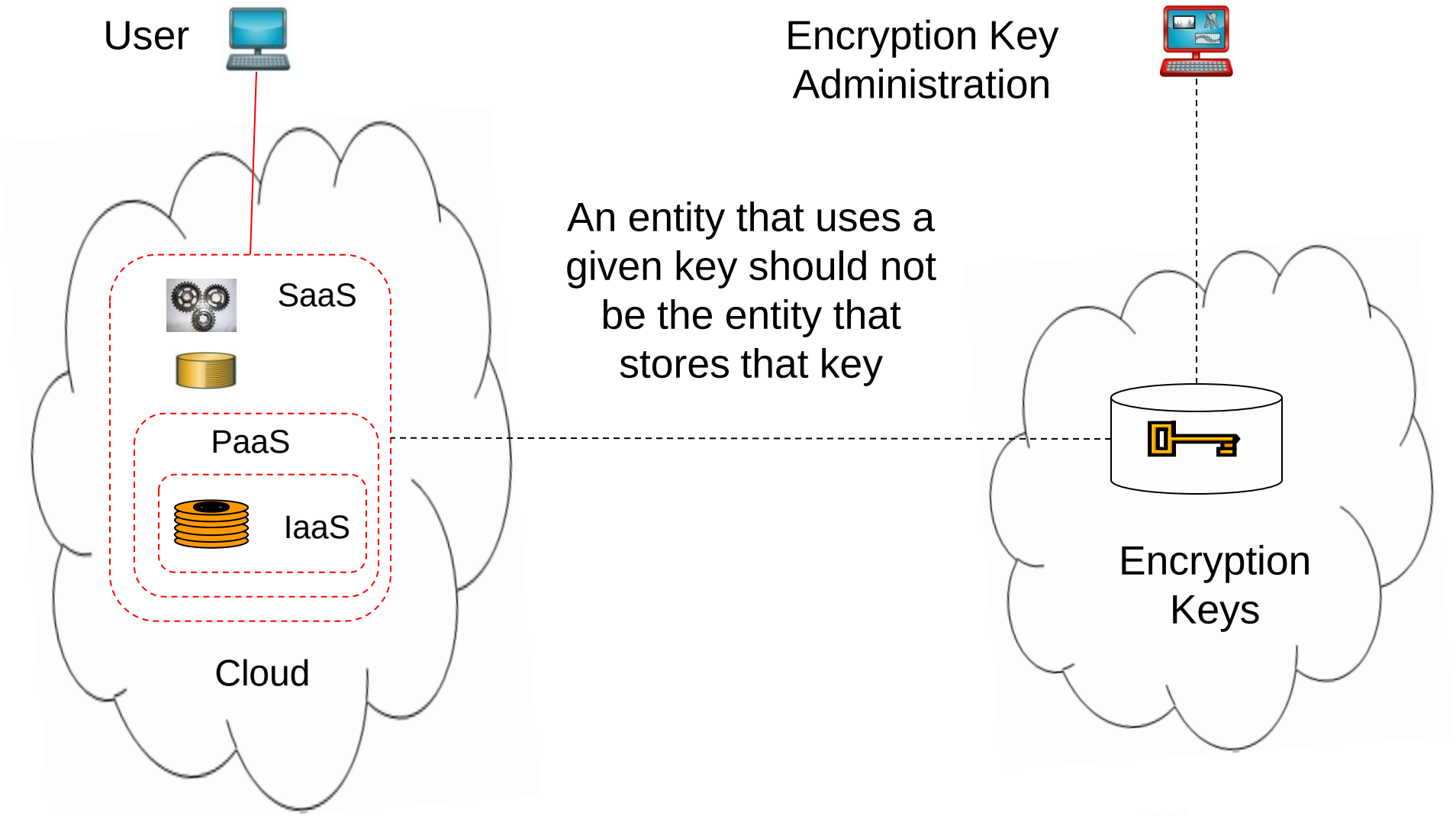


protegrity

Developing a Risk-adjusted Data Protection Plan

1. **Know Your Data**
2. **Find Your Data**
3. **Understand Your Enemy**
4. **Understand the New Options in Data Protection**
5. **Deploy Defenses**
6. **Crunch the Numbers**

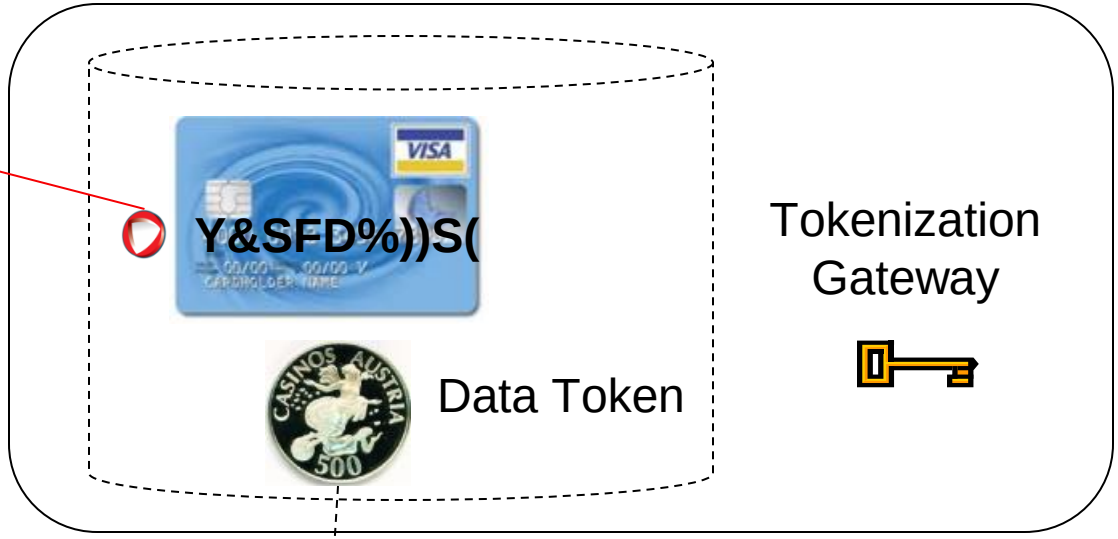
Securing Encryption Keys



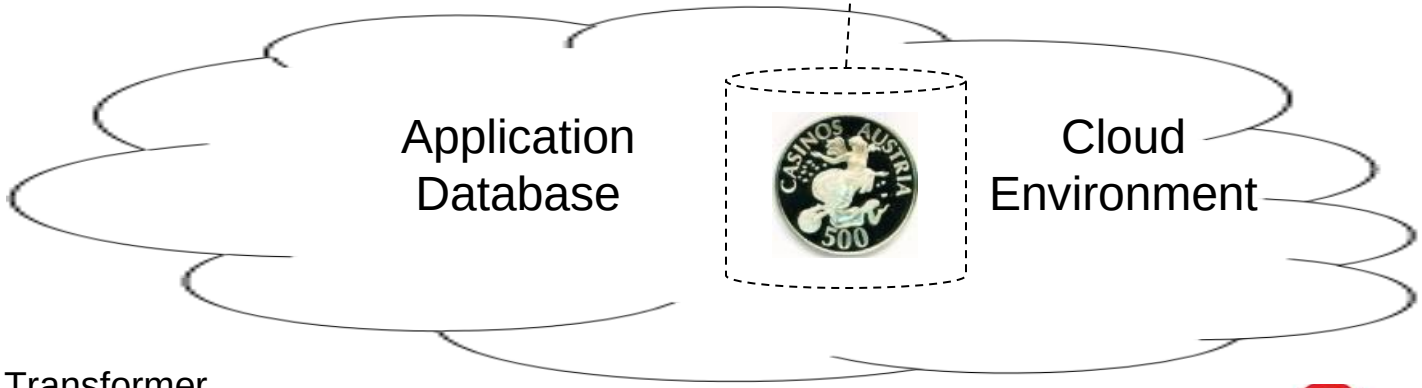
Source: http://csrc.nist.gov/groups/SNS/cloud-computing/

Hiding Data in Plain Sight – Data Tokenization

4000 0012 3456 7899



40 *12 3456 7890* 7899

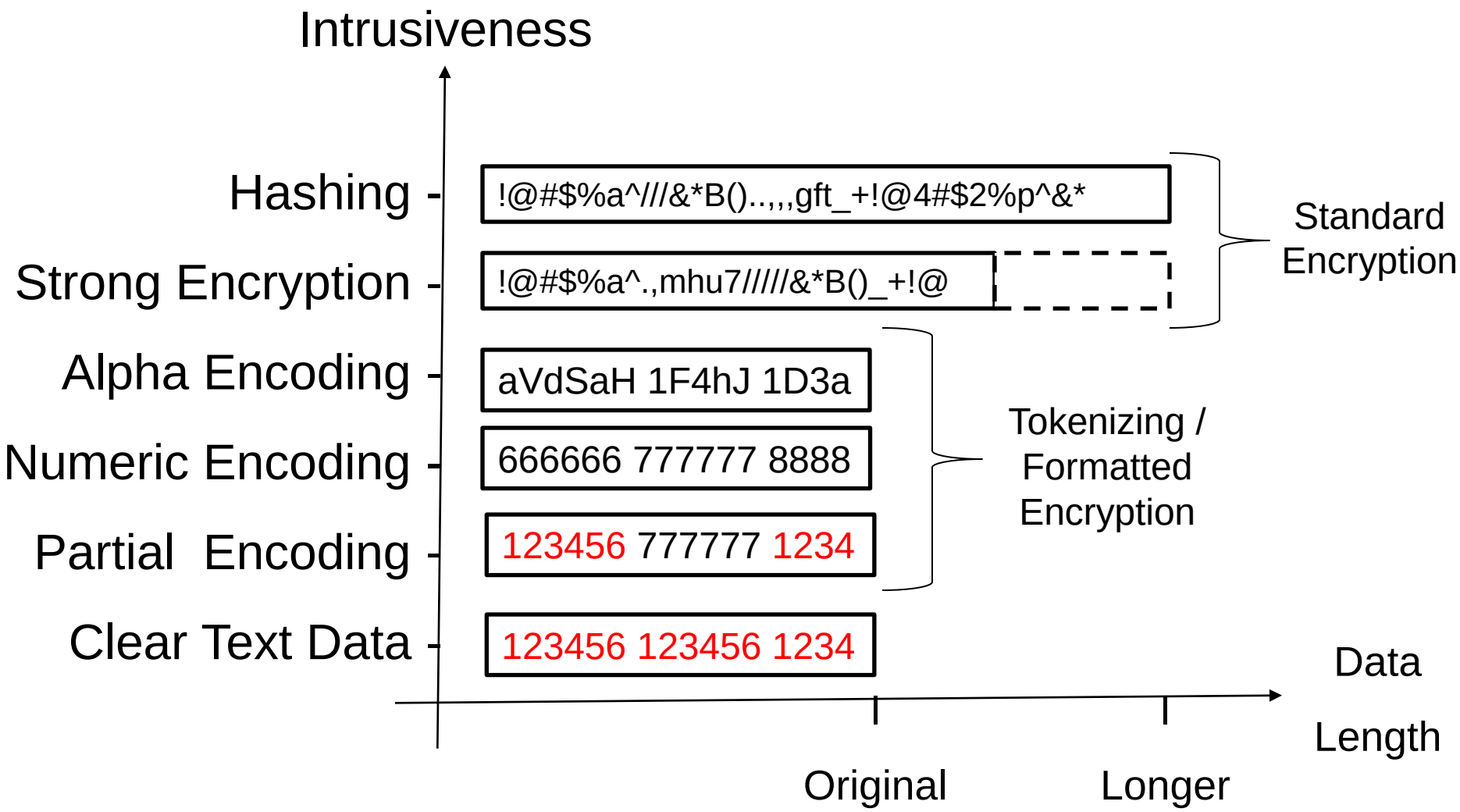


: Data Transformer

Unprotected sensitive information: ——————

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

Transparency to Applications and Databases



Unprotected sensitive information:

Protected sensitive information

Column Level Encryption - Oracle

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

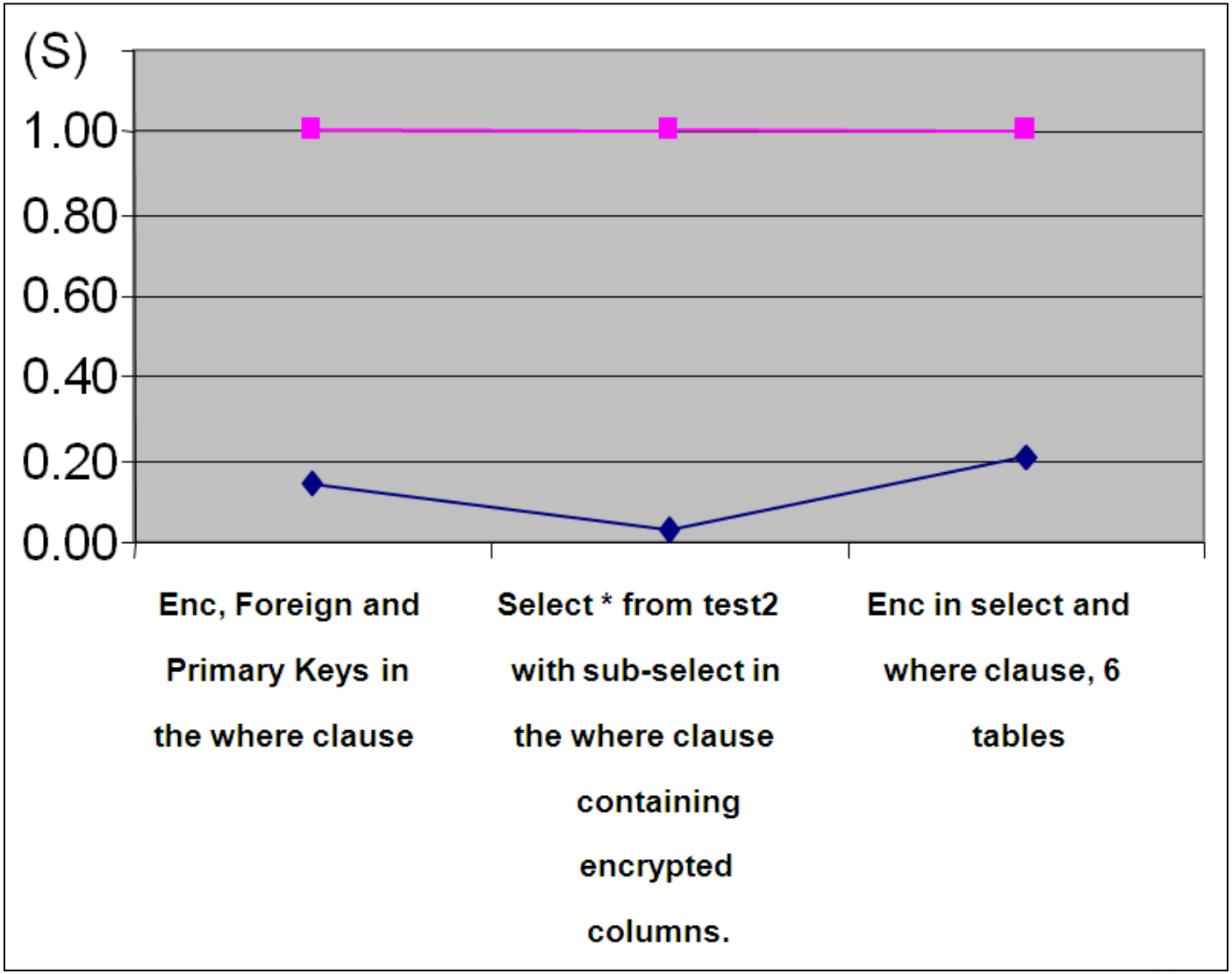
Column Encryption Solutions – Some Considerations

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



Evaluating Encryption & Tokenization

Evaluation Criteria		Encryption		Tokenization	
Area	**Impact**	**Database File Encryption**	**Database Column Encryption**	**Centralized Tokenization (old)**	**Distributed Tokenization (new)**
Scalability	Availability				
	Latency				
	CPU Consumption				
Security	Data Flow Protection				
	Compliance Scoping				
	Key Management				
	Randomness				
	Separation of Duties				

Best  Worst

protegrity

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

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

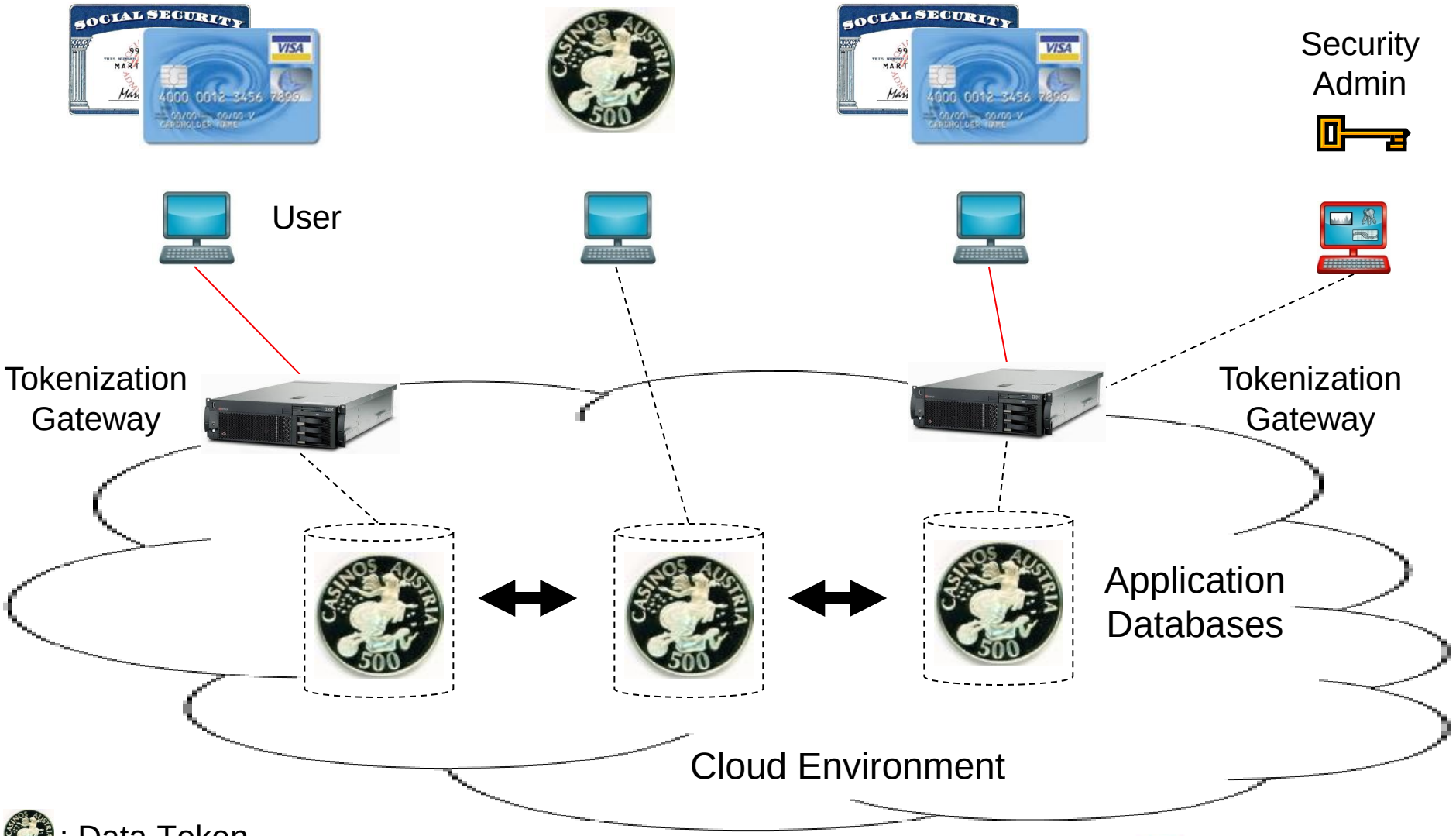
: Data Token

protegrity

Unprotected sensitive information: ——————

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

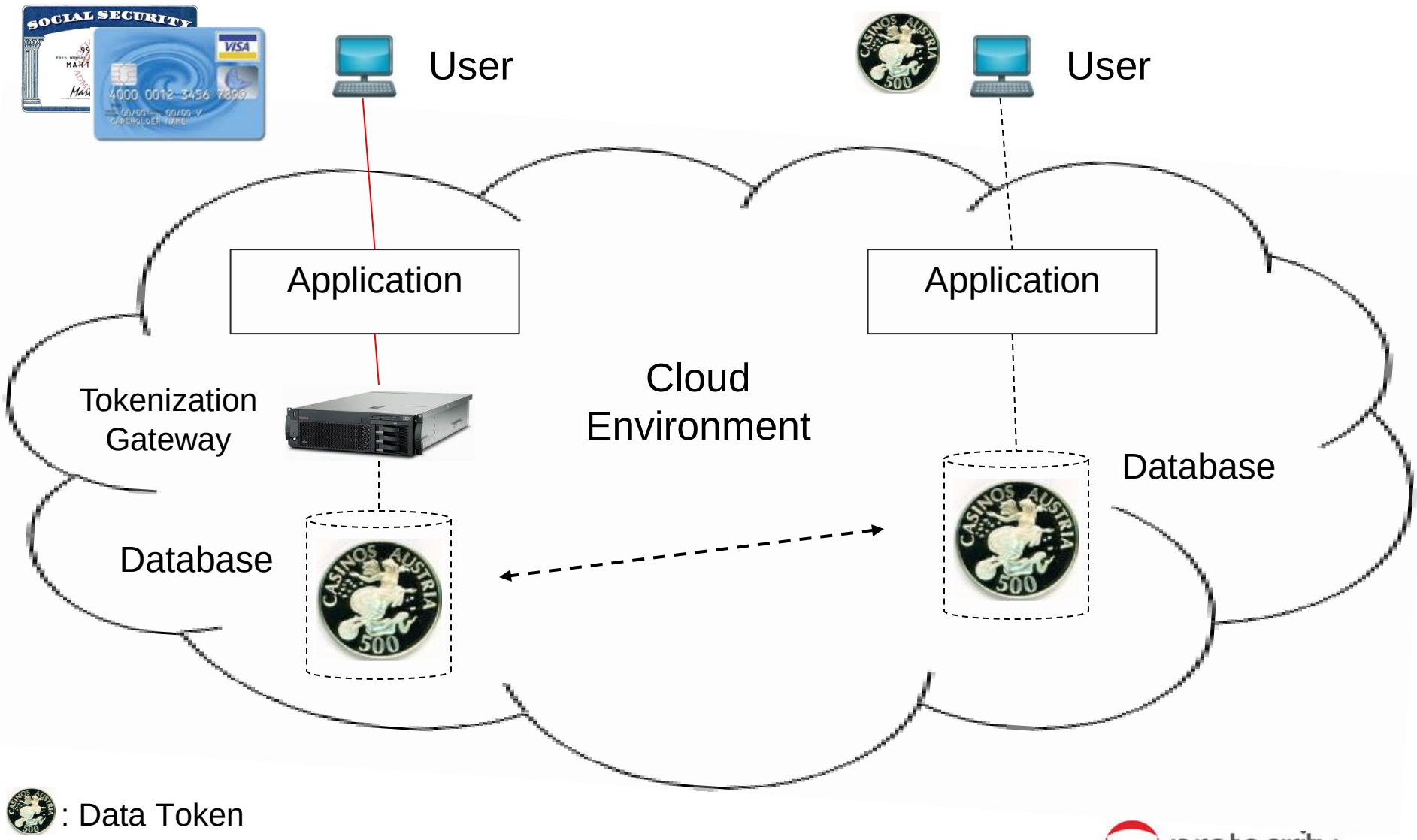
Data Tokens in a Cloud Environment – Integration Example



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

protegrity

Unprotected sensitive information:

Protected sensitive information

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

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

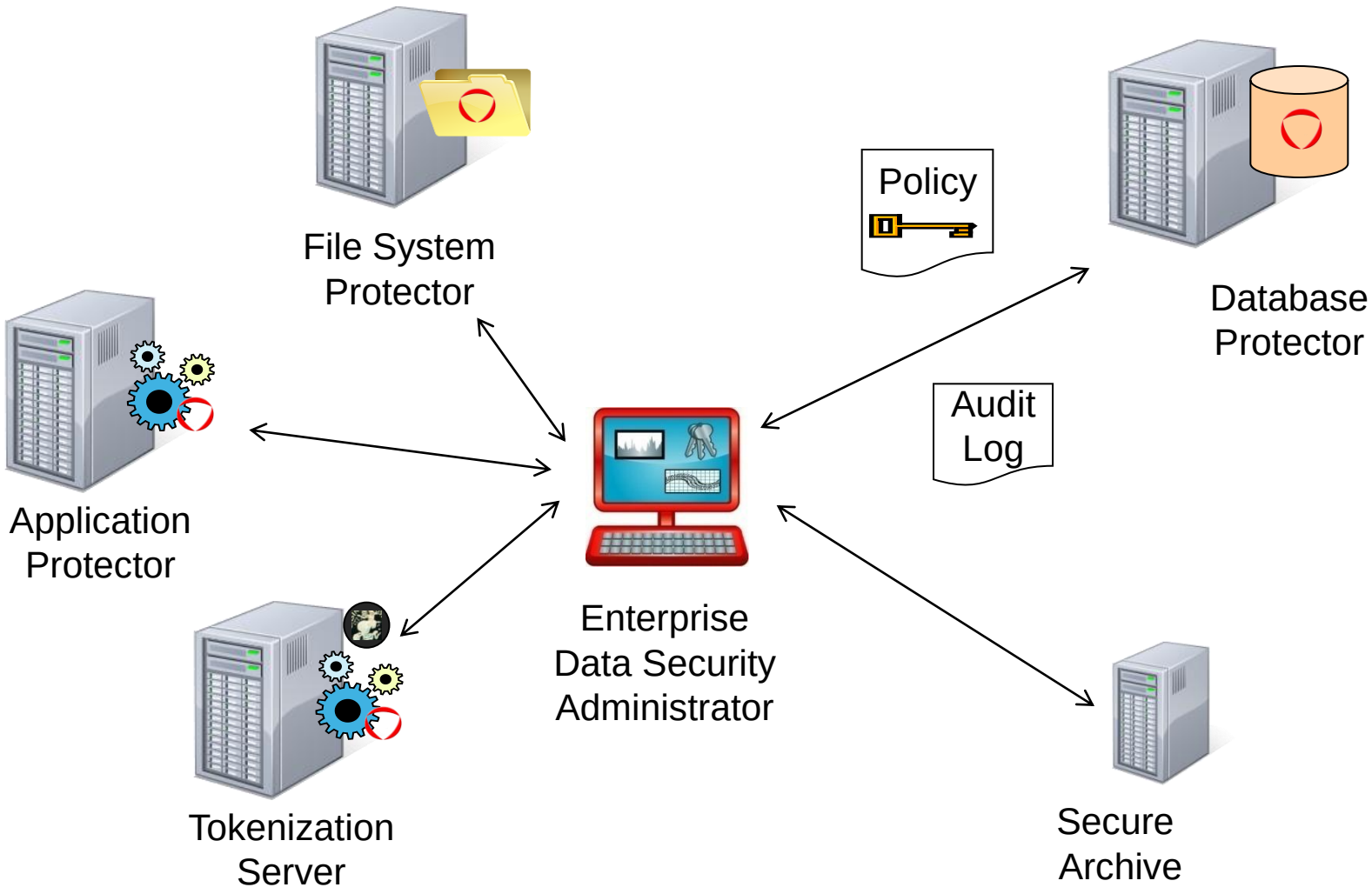
Best Practices from NIST on PII Data - SP800-122

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/)

Best Practices - Data Security Management



: Encryption service

Please contact me for more information

Ulf Mattsson

Ulf . Mattsson AT protegrity . com

protegrity

protecting your data.
protecting your business.