ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

National Capital Chapter

News Events Store Sponsors

PCI DSS Compliance

Ulf Mattsson, CTO

Bio

- **20 years with IBM Development & Services**
  - IBM Software Development & IBM Research consulting resource
  - IBM Certified IT Architect in IT Architecture & IT Security
- **Created Protegrity's Data Security Technology**
  - Protegrity Policy driven Data Encryption (1994)
- **Inventor of 20+ Patents**
  - In the areas of Encryption Key Management, Separation of Duties, Policy Driven Data Encryption, Tokenization, Internal Threat Protection, Data Usage Control, Dynamic Access Control, Intrusion Prevention and Cross System Layer Security.
- **Master's degree in Physics and degrees in Finance and Electrical engineering**
  - Research member of the International Federation for Information Processing (IFIP) WG 11.3 Data and Application Security.
  - Member of IEEE, OASIS, Computer Security Institute (CSI), Object Management Group (OMG) CORBA Security Service, Open Web Application Security Project (OWASP), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA),, The International Association of Science and Technology for Development (IAST), The Medical Records Institute (MRI), and The World Scientific and Engineering Academy and Society for Computer Security (WSEAS).

Agenda

- Data Protection Options for PCI and Beyond
- PCI Case Studies
- Advanced Attacks on Data Flow
- Determining Risks
- Cost Effective Approach

ISSA™
Information Systems Security Association

New York Metro Chapter

Information | My Registration

Summary | Invitation | Agenda | Presenter Bios | Who should attend?

March 18, 2009: The Reality of PCI-DSS Compliance

ISSA New York Metro Chapter - Educational Program

Summary

The 2007 Computer Security Institute (CSI) Report indicates that more than one fifth of those surveyed have been victimized by a targeted attack. The study also concluded that financial fraud overtook virus attacks for the first time in seven years as the number one cause of financial losses from an IT security breach. Finally, customer and proprietary information was the second worst cause of financial loss. These trends show that the payment card industry faces more data security threats than ever before. The Payment Card Industry Data Security Standard (PCI-DSS) was created to mitigate these threats.

This session examines the challenges faced by organizations as they address their PCI DSS compliance requirements.

Presenter Bios

Ulf Mattsson, Protegrity Corporation

Ulf T. Mattsson, Chief Technology Officer, Protegrity Corporation, created the initial architecture of Protegrity's database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization. He specializes in the areas of IT Architecture and IT Security. Ulf is the inventor of a number of European patents and US Patents in the areas of Encryption Key Management, Separation of Duties, Policy Driven Data Encryption, Internal Threat Protection, Data Usage Control, Dynamic Access Control, Intrusion Prevention and Cross System Layer Security. He holds a master's degree in physics, a degree in finance and a degree in electrical engineering.

MasterCard
Academy of Risk Management

Payment System Integrity

MasterCard Worldwide

How to Evaluate Encryption Technologies

Ulf Mattsson, CTO

Protegrity

PCI Security Standards Council™

Participating Organization

http://www.knowpci.com

Discussion of Data Protection for PCI DSS

Build and maintain a secure network.	***1. Install and maintain a firewall configuration to protect data*** ***2. Do not use vendor-supplied defaults for system passwords and other security parameters***
Protect cardholder data. ⇨	**3. Protect stored data** ***4. Encrypt transmission of cardholder data and sensitive information across public networks***
Maintain a vulnerability management program.	***5. Use and regularly update anti-virus software*** **6. Develop and maintain secure systems and applications**
Implement strong access control measures.	**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***
Regularly monitor and test networks.	**10. Track and monitor all access to network resources and cardholder data** ***11. Regularly test security systems and processes***
Maintain an information security policy.	**12. Maintain a policy that addresses information security**

PCI DSS Applicability Information & PII Aspects

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

1 *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.*

2 *Sensitive authentication data must not be stored after authorization (even if encrypted).*

3 *Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.*

Requirement 3: Protect stored cardholder data

Section 3.4

- Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:
  - One-way hashes based on strong cryptography
  - Truncation
  - Index tokens and pads (pads must be securely stored)
  - Strong cryptography with associated key-management processes and procedures
- The MINIMUM account information that must be rendered unreadable is the PAN.
- *Notes:*
  - *If for some reason, a company is unable render the PAN unreadable, refer to Appendix B:* Compensating Controls.
  - *"Strong cryptography" is defined in the PCI DSS Glossary of* Terms, Abbreviations, and Acronyms

Requirement 3: Protect stored cardholder data

Section 3.5

- *"Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.*
  - *3.5.1 Restrict access to keys to the fewest number of custodians necessary*
  - *3.5.2 Store keys securely in the fewest possible locations and forms."*

Section 3.6

- *"Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:*
  - *3.6.1 Generation of strong keys*
  - *3.6.2 Secure key distribution*
  - *3.6.3 Secure key storage*
  - *3.6.4 Periodic changing of keys*
  - *• As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically. At least annually.*
  - *3.6.5 Destruction of old keys*
  - *3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)*
  - *3.6.7 Prevention of unauthorized substitution of keys*
  - *3.6.8 Replacement of known or suspected compromised keys*
  - *3.6.9 Revocation of old or invalid keys*

Requirement 3.6.6: Split knowledge and dual control

- *Split knowledge and dual control of keys requires two or three people, each knowing only their part of the key, to reconstruct the whole key*
- *The principle behind dual control and split knowledge is required to access the clear text key.*
  - *Only a single master key will be needed under this control.*
  - *The determination of any part of the key must require the collusion between at least two trusted individuals.*
- *Any feasible method to violate this axiom means that the principles of dual control and split knowledge are not being upheld.*
  - *At least two people are required to 'reconstruct' the key, and they each must have a physical thing and they each must have some information that is required.*
- *The use of a key in memory to encipher or decipher data, or access to a key that is enciphered under another key does not require such control by PCI DSS.*
  - *Keys appearing in the clear in memory, the principles of dual control and split knowledge are difficult but not impossible to enforce.*
- *Please review http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1126002 for additional discussion.*

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1051481

PCI – Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

   Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

PCI Security Standards Council about Data in Transit

- The PCI Security Standards Council (https://www.pcisecuritystandards.org/) manages the PCI DSS standards
  - End-to-end encryption is likely to be a central focus as the council seeks input on how this might best be achieved in the payment-card environment through different technologies.
  - If that is accomplished, it might result in a decidedly new PCI standard in the future for card-data protection, PCI Security Standards Council says in http://www.networkworld.com/news/2008/100108-pci-credit-card.html?page=2 .
  - "Today we say if you're going outside the network, you need to be encrypted, but it doesn't need to be encrypted internally," PCI Security Standards Council says.
- "But as an example, if you add end-to-end encryption, it might negate some requirements we have today, such as protecting data with monitoring and logging.
  - Maybe you wouldn't have to do that. So we'll be looking at that in 2009."

Data Protection Approaches

- Data Access Control
  - How the data is presented to the end user and/or application
- Data Protection
  - How sensitive data is rendered unreadable

Data Protection Options

- Data Stored As
  - Clear – actual value is readable
  - Hash – unreadable, not reversible
  - Encrypted – unreadable, reversible
  - Replacement value (tokens) – unreadable, reversible
  - Partial encryption/replacement – unreadable, reversible

Data Protection Options

- Data in the Clear
  - Audit only
  - Masking
  - Access Control Limits
- Advantages
  - Low impact on existing applications
  - Performance
  - Time to deploy
- Considerations
  - Underlying data exposed
  - Discover breach after the fact
  - PCI aspects

Data Protection Options

- Hash
  - Non – reversible
  - Strong protection
    - Keyed hash (HMAC)
    - Unique value if salt is used
- Advantages
  - None really
- Considerations
  - Key rotation for keyed hash
  - Size and type
  - Transparency

Data Protection Options

- Strong Encryption
  - Industry standard (NIST modes - AES CBC …)
  - Highest security level
- Advantages
  - Widely deployed
  - Compatibility
  - Performance
- Considerations
  - Storage and type
  - Transparency to applications
  - Key rotation

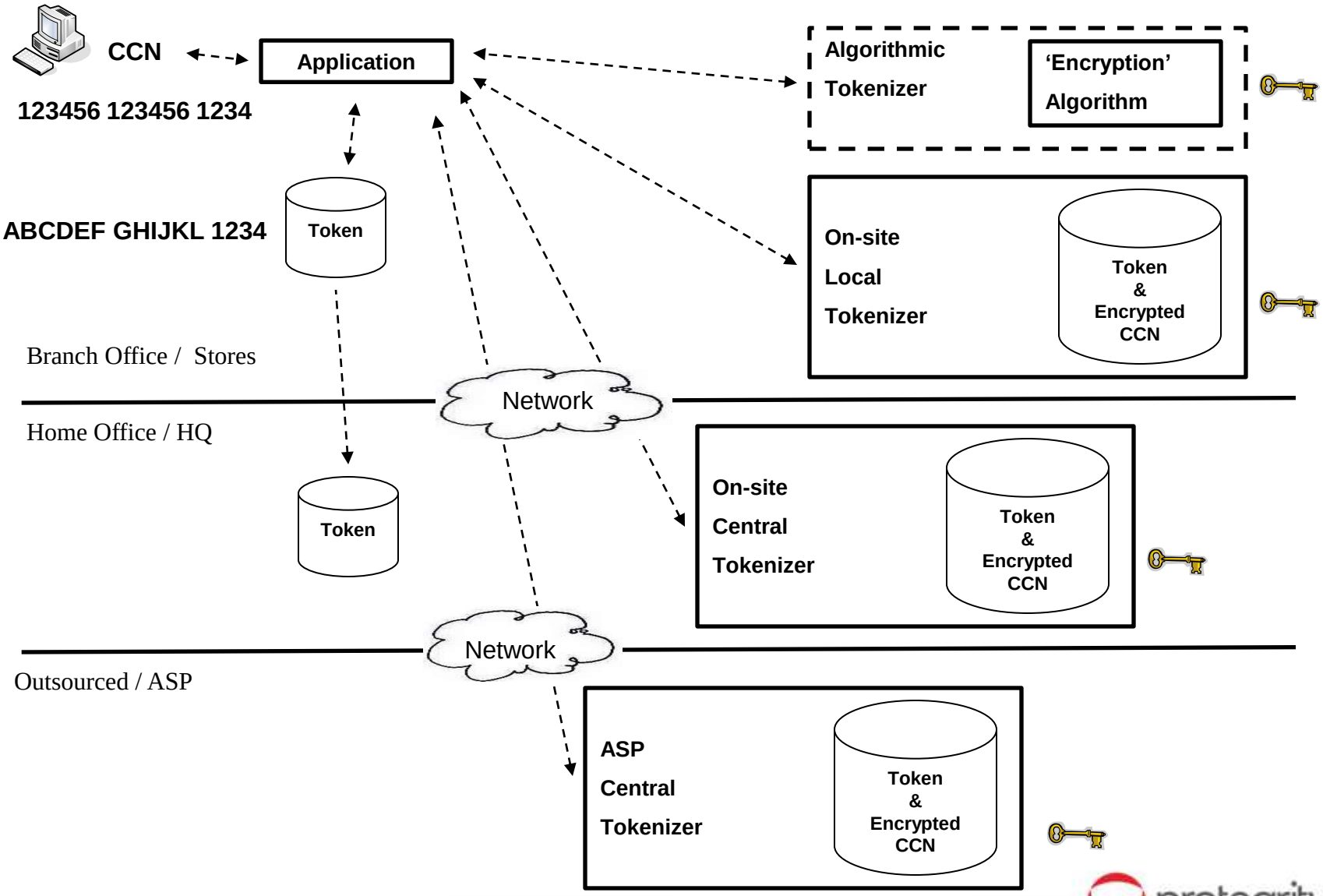
Data Protection Options

- Format Controlling Encryption
  - Maintains data type, length
- Advantages
  - Reduces changes to downstream systems
  - Storage
  - Partial encryption
- Considerations
  - Performance
  - Security and compliance
  - Key rotation
  - Transparency to applications

Data Protection Options

- Replacement Value (i.e. tokens, alias)
  - Proxy value created to replace original data
  - Centrally managed, protected
- Advantages
  - No changes to most downstream systems
  - Out of scope for compliance
  - No local key rotation
  - Partial replacement
- Considerations
  - Transparency for applications needing original data
  - Availability and performance for applications needing original data

Different ‘Tokenizing’ Approaches & Topologies



protegrity

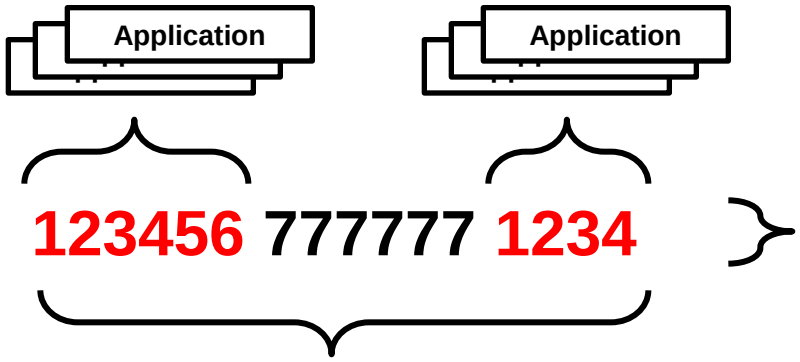
Limit Exposure across the Data Flow - Partial Encryption/Tokenizing

A policy driven approach

- Decide what sensitive bytes to protect
- A high level of transparency to applications

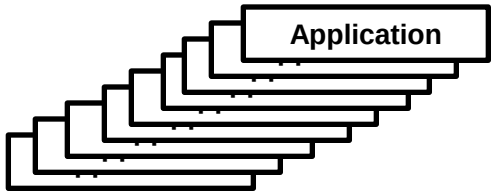
Some applications

• Partial clear data



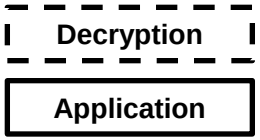
Many applications/tools

• Moving data around



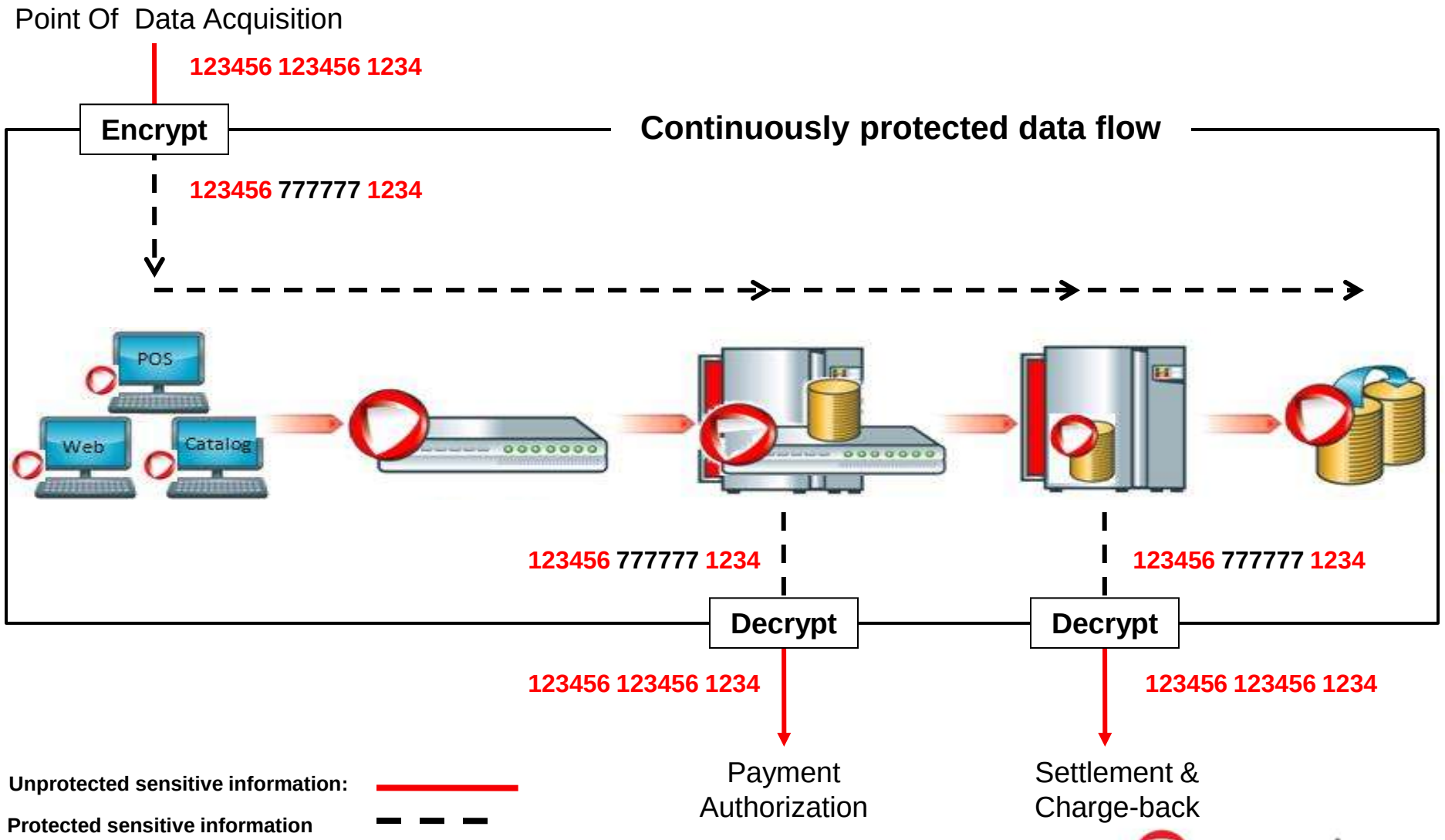
Few applications

• Full clear data

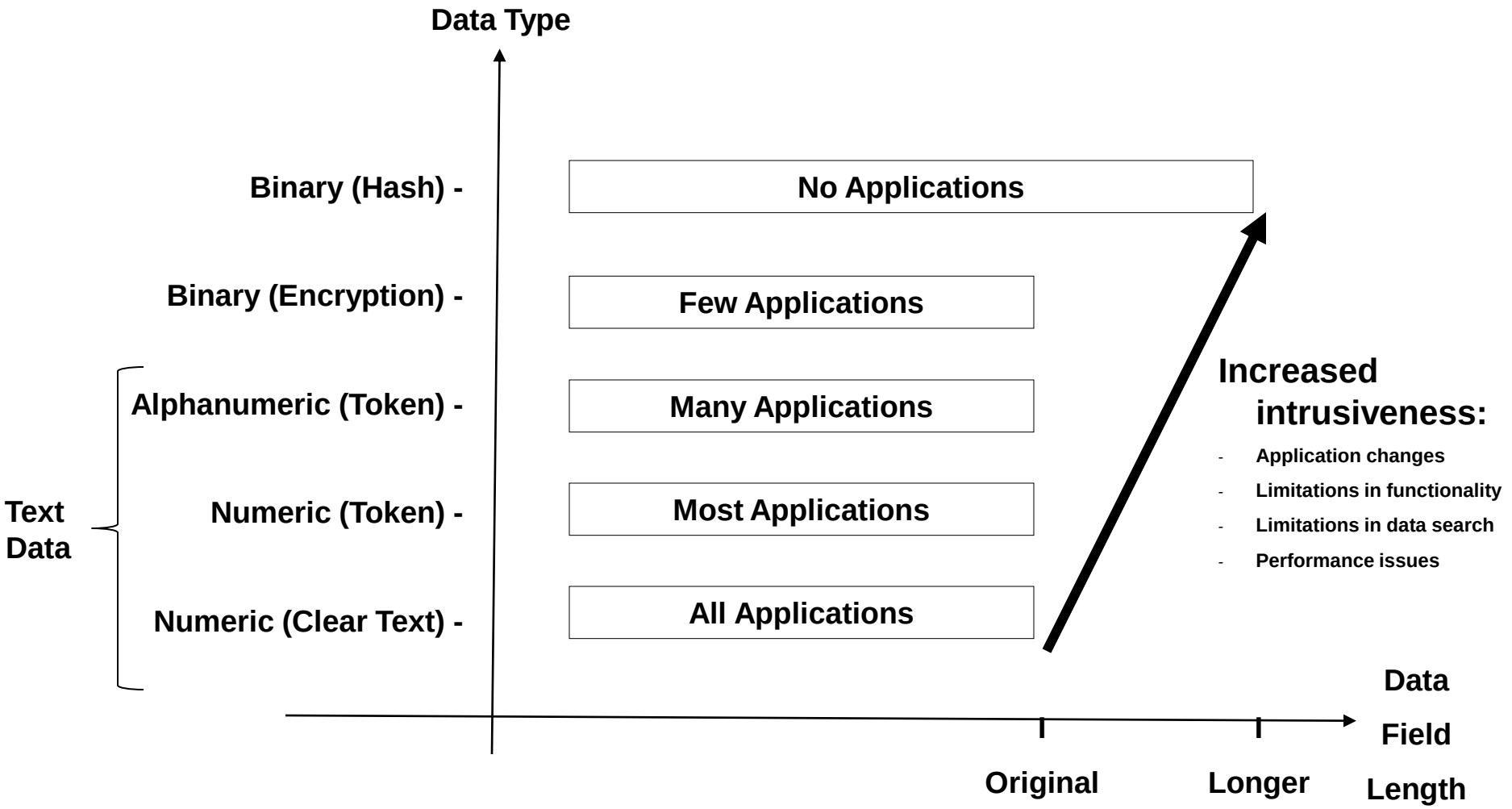


protegrity

How to Protect the Data Flow Against Advanced Attacks



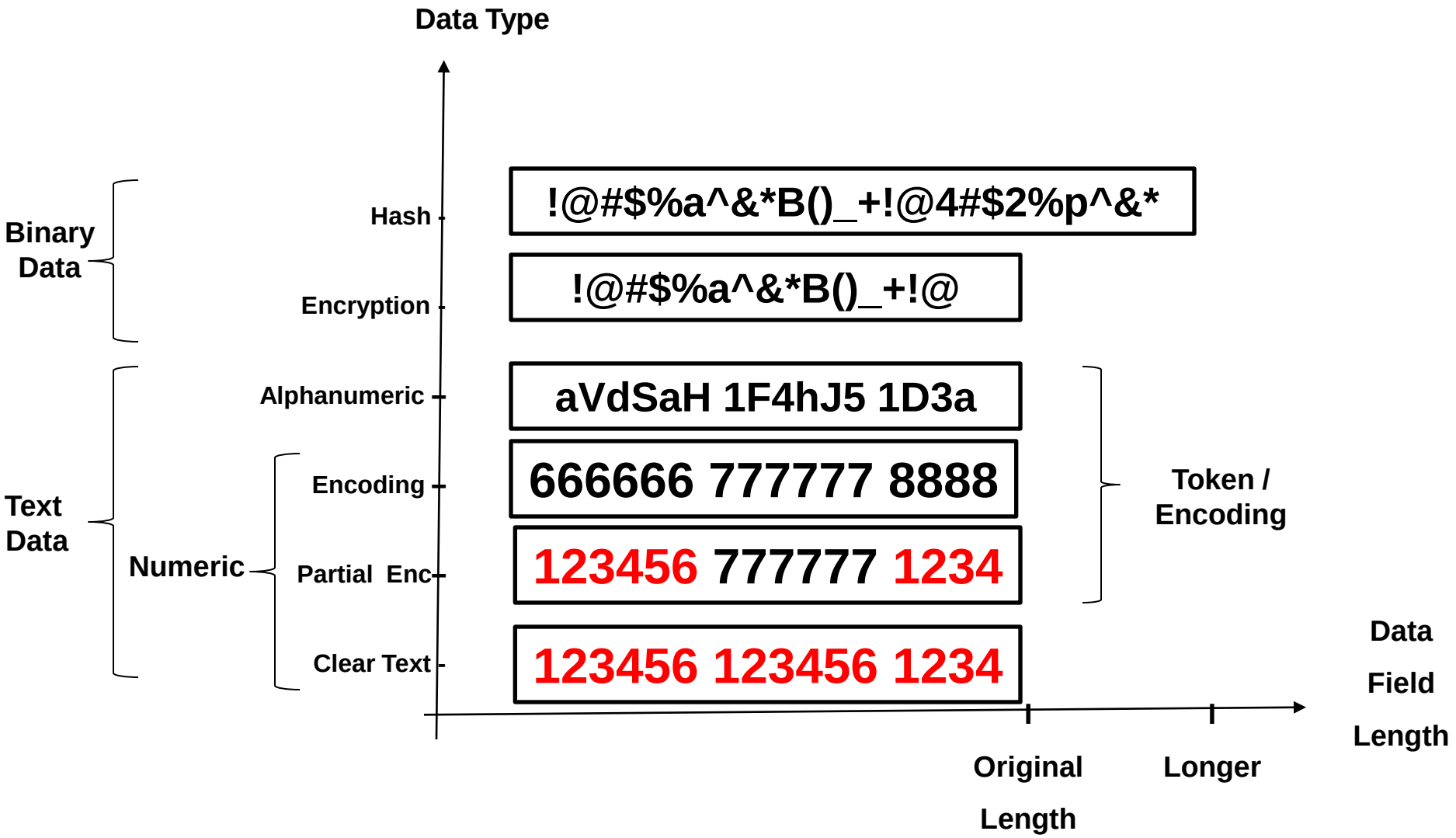
Applications are Sensitive to the Data Format



This is a generalized example

protegrity

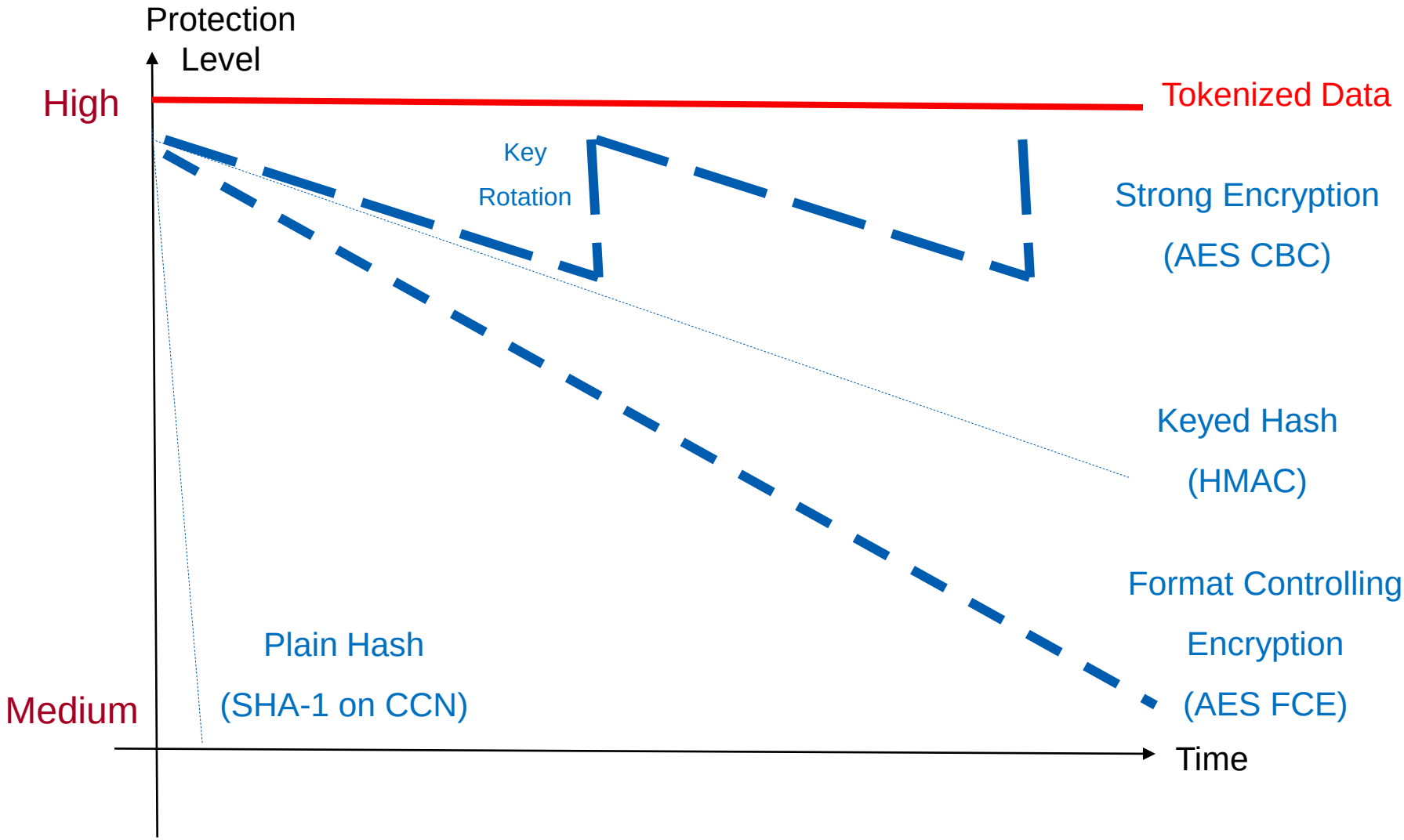
Preserving the Data Format



This is a generalized example

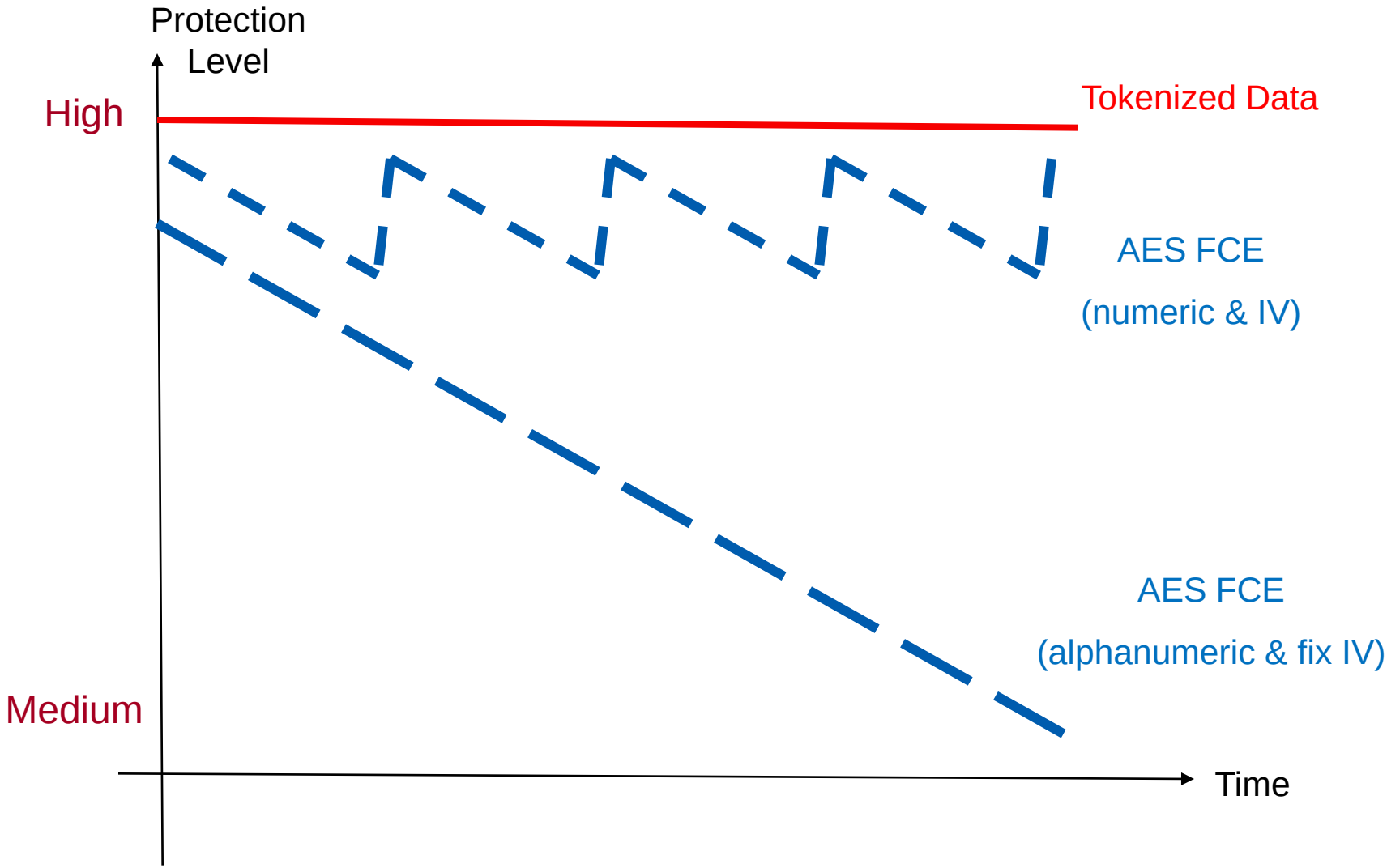
protegrity

Field Level Data Protection Methods vs. Time

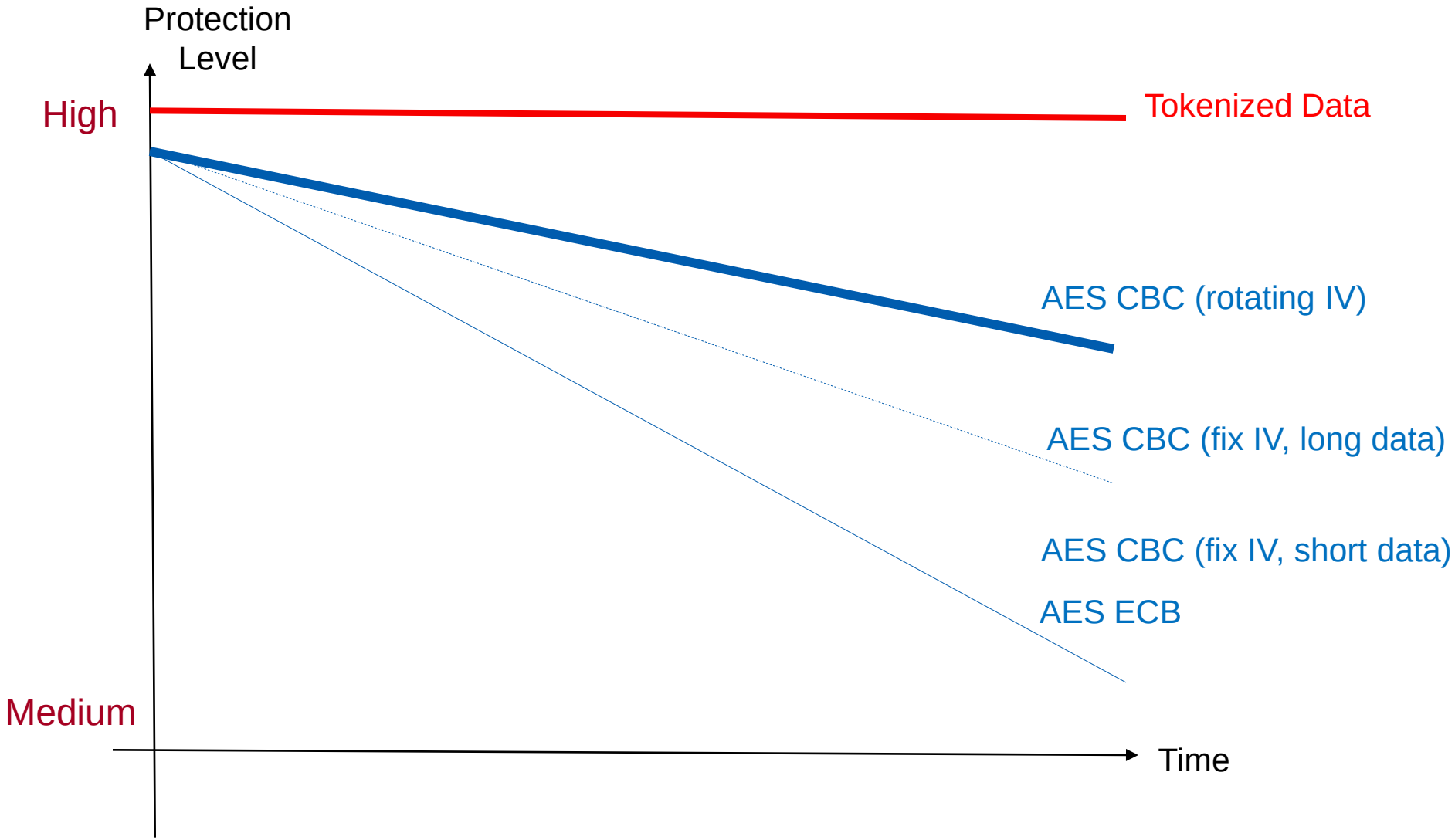


protegrity

Format Controlling Encryption vs. Time



Field Level Data Protection Methods vs. Time



http://ssrn.com/abstract=1126002

Data Protection Options & Cost Factors

Storage	Performance	Storage	Security	Transparency
Clear				
Strong Encryption				
Format Control Encryption				
Token (reversible)				
Hash				

protegrity

Data Protection Capabilities

Storage	Performance	Storage	Security	Transparency
Clear	●	●	○	●
Strong Encryption	◔	◔	●	◒
Format Controlling Encryption	◒	●	◒	◔
Token	◕	●	●	◔
Hash	●	◕	●	○

Highest ● ◔ ◒ ◕ ○ Lowest

Data Protection Implementation Choices

- Data Protection Options are not mutually exclusive
- Data Protection Layers
  - Application
  - Database
  - File System
- Data Protection Topologies
  - Remote services
  - Local service
- Data Security Management
  - Central management of keys, policy and reporting

http://www.net-security.org/dl/insecure/INSECURE-Mag-2.pdf

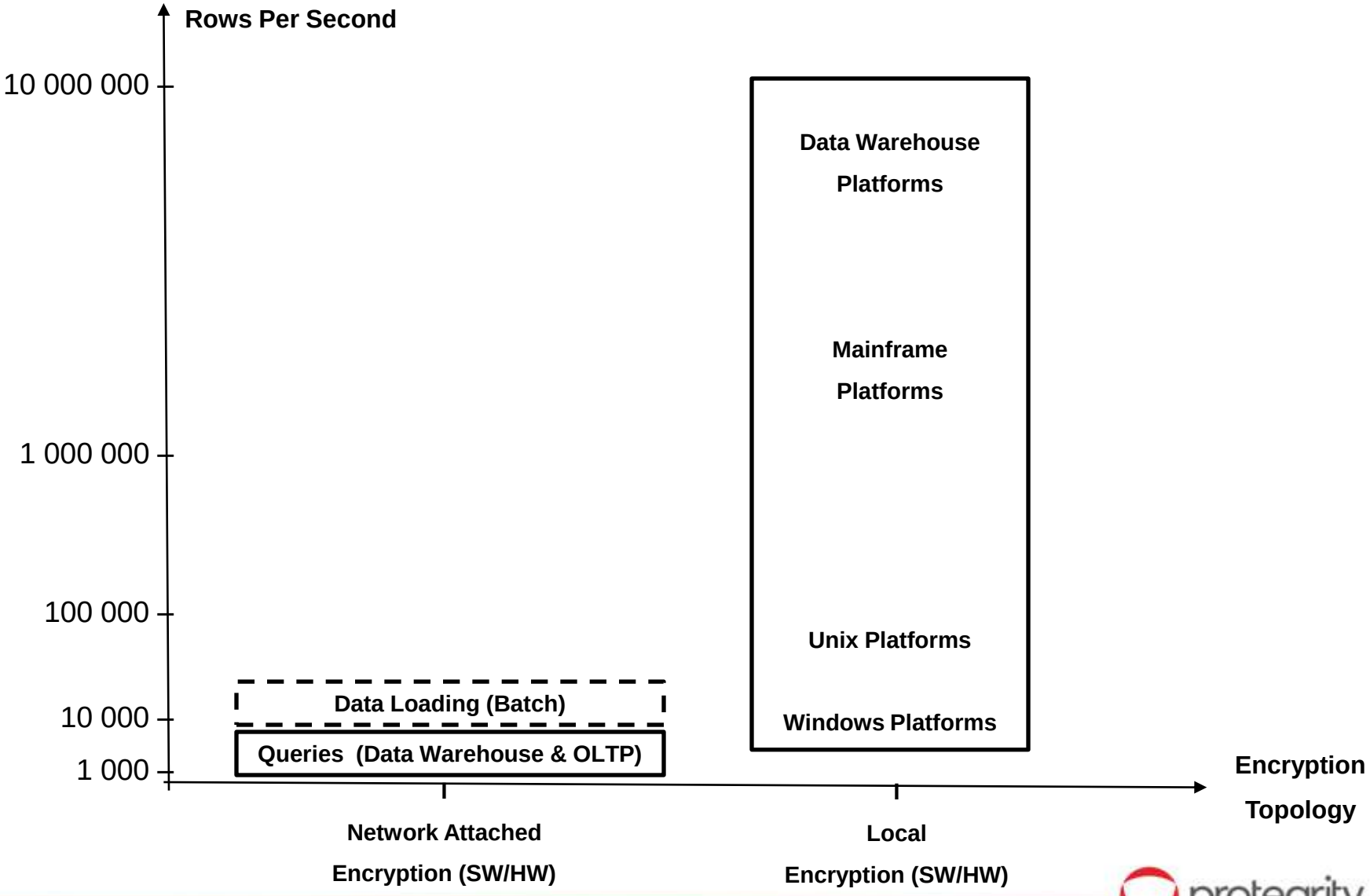
Data Protection Implementation Choices

System Layer	Performance	Transparency	Security
Application	●	○	●
Database	◒	◔	◔
File System	◔	●	◒

Topology	Performance	Scalability	Security
Local Service	●	●	◔
Remote Service	○	○	●

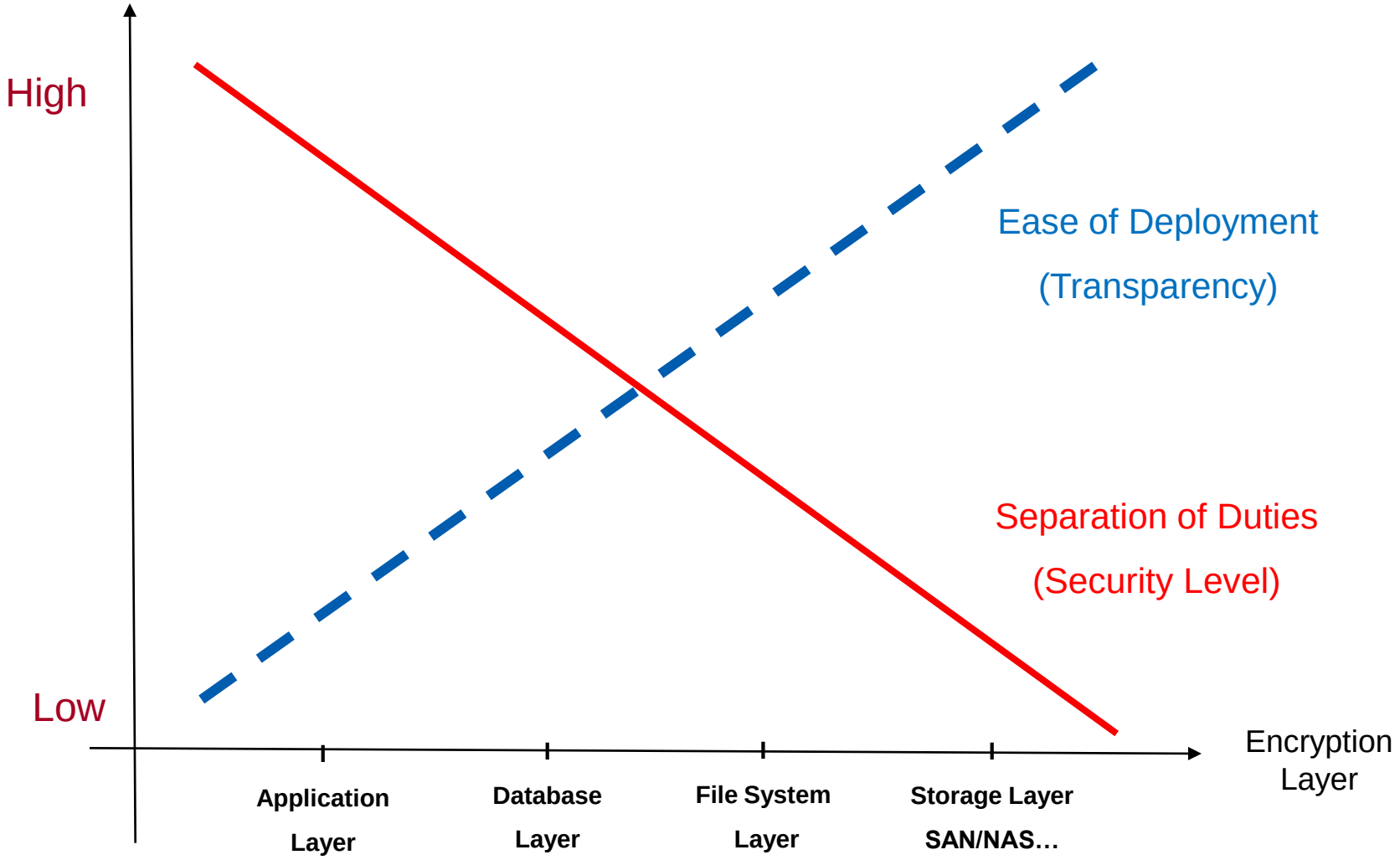
Highest ● ◔ ◒ ◔ ○ Lowest

Column Encryption Performance - Different Topologies



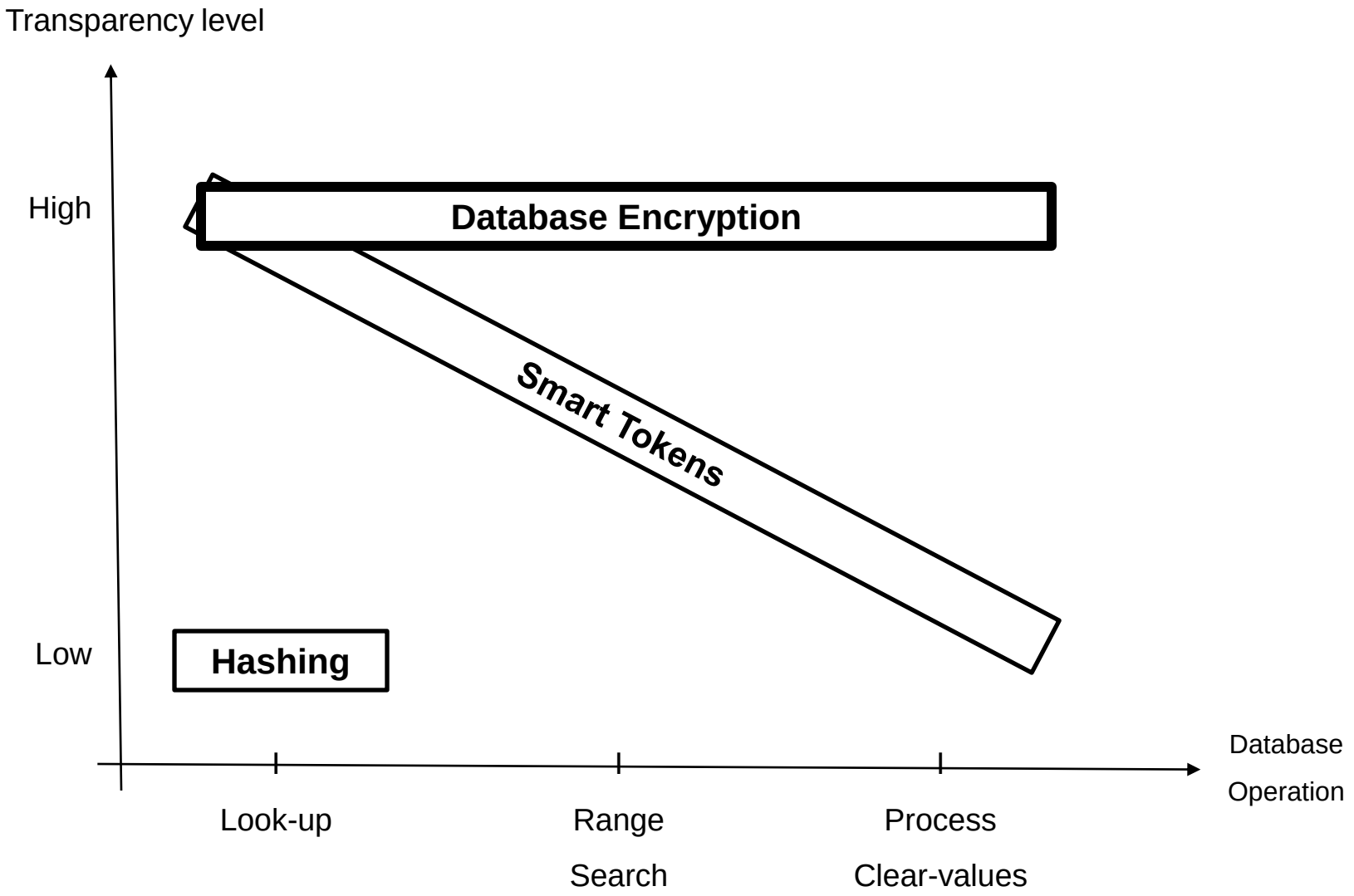
protegrity

Generalization: Encryption at Different System Layers



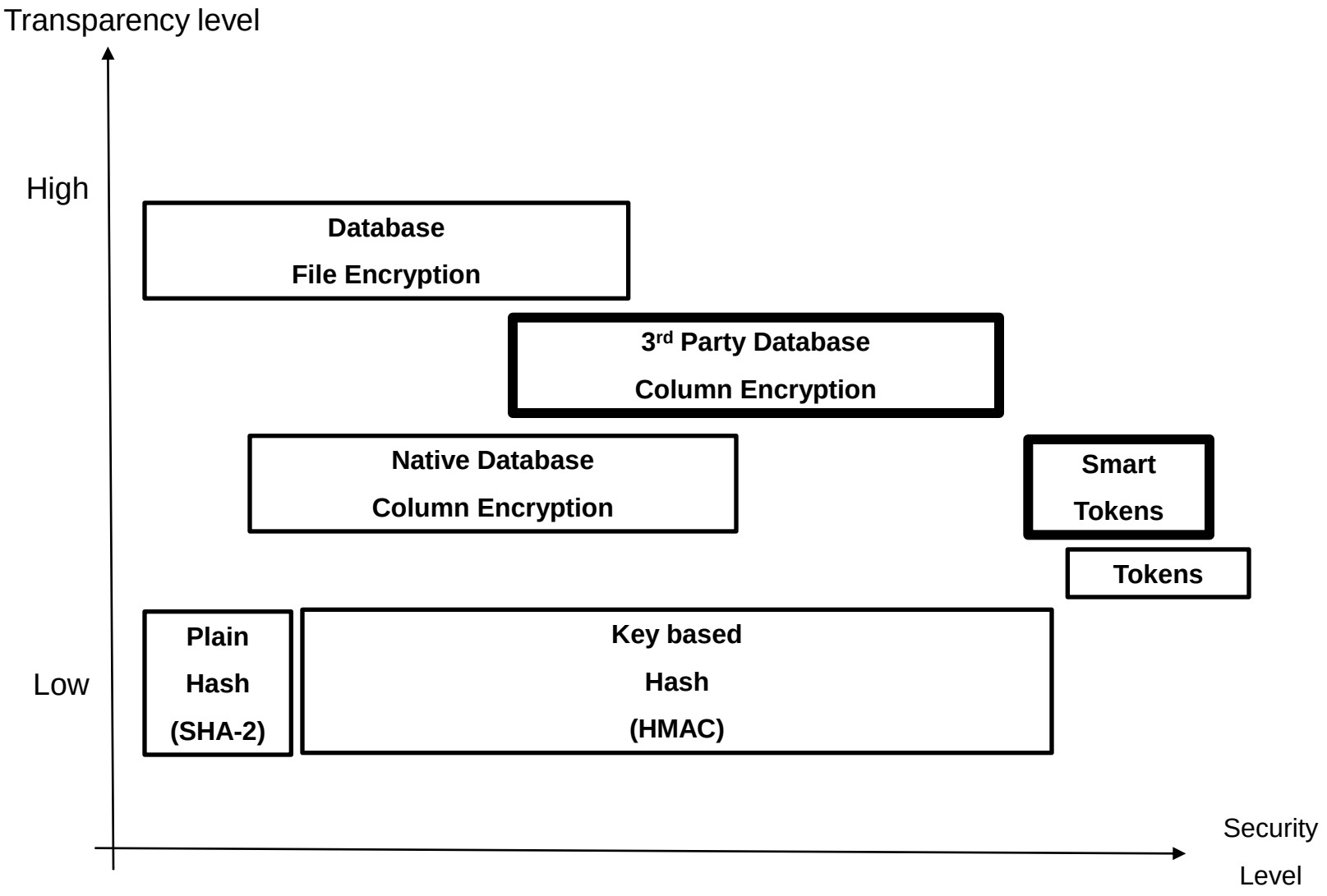
protegrity

Application Transparency – Encryption, Tokens & Hashing

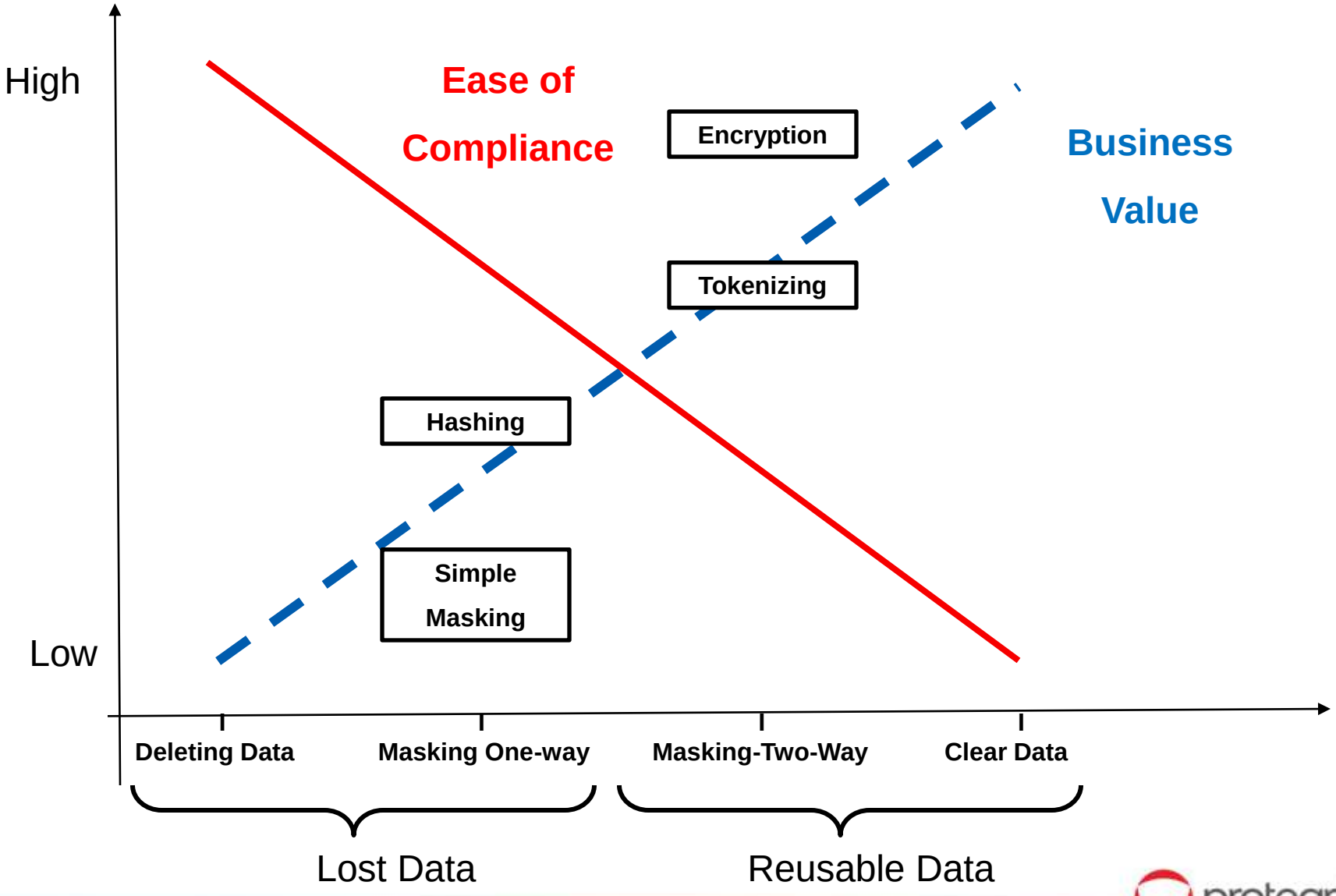


protegrity

Application Transparency



Business Value vs. Ease of Compliance

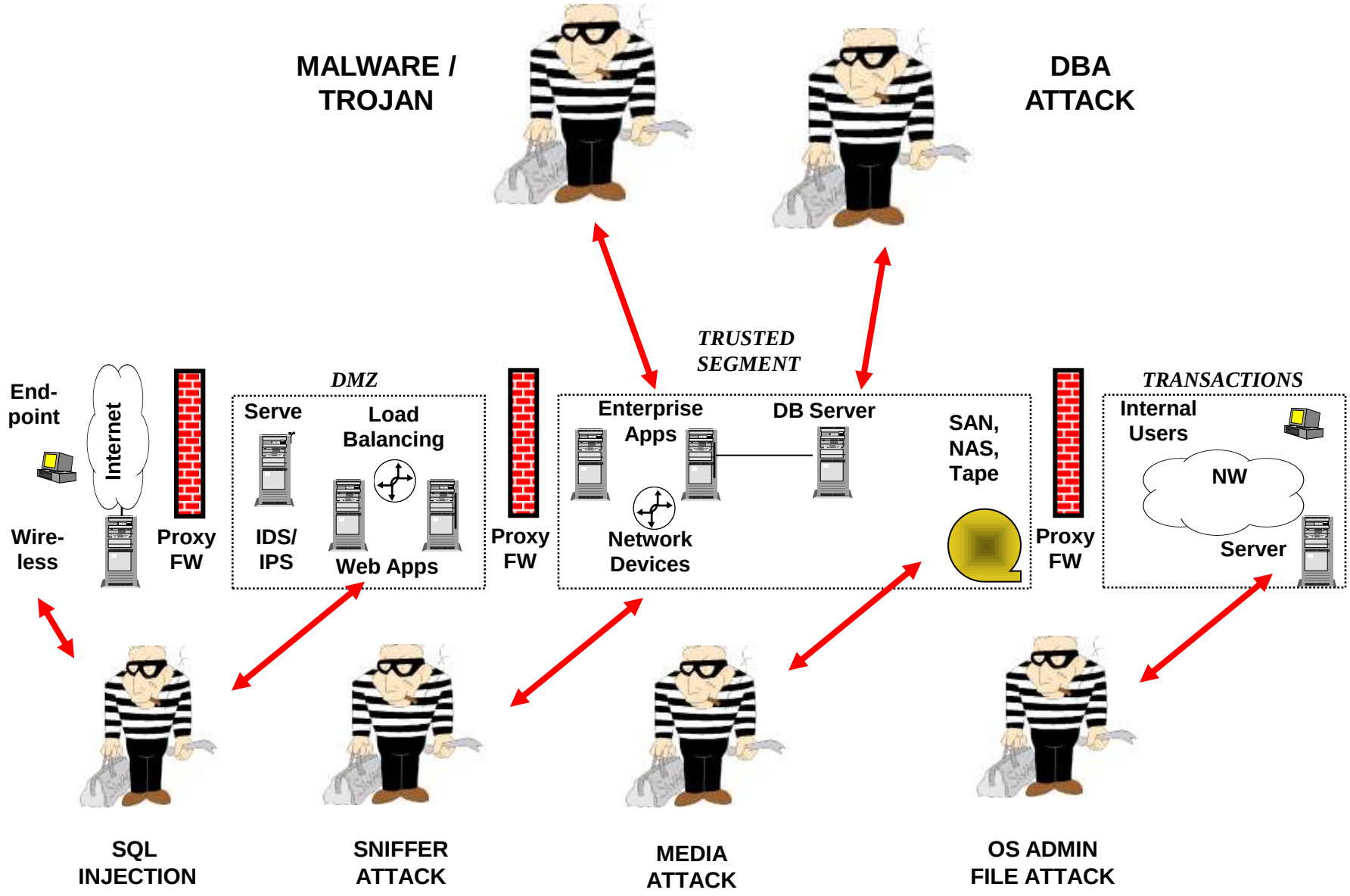


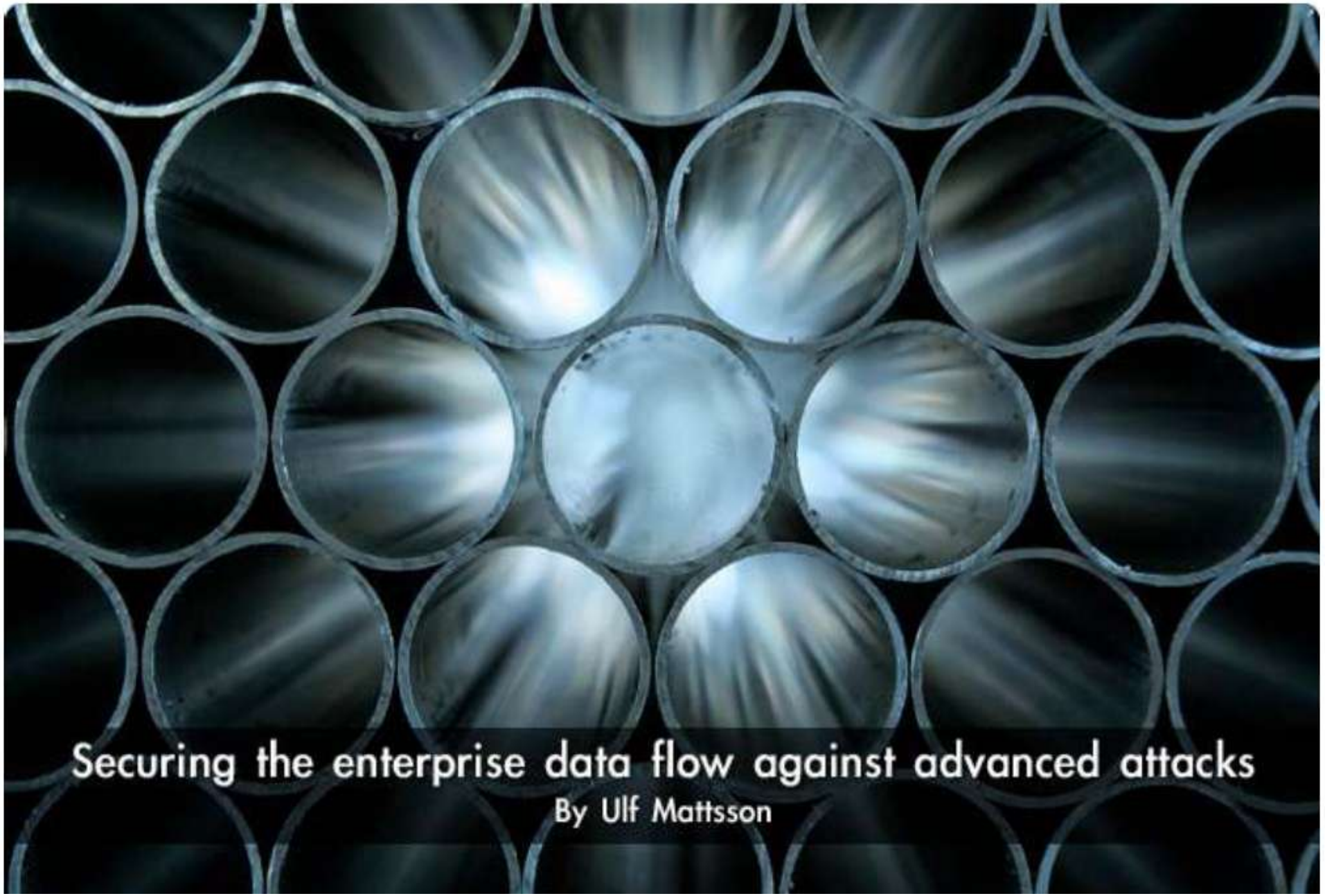
protegrity

Protecting the Data Flow:

Case Studies

Data Level Attacks



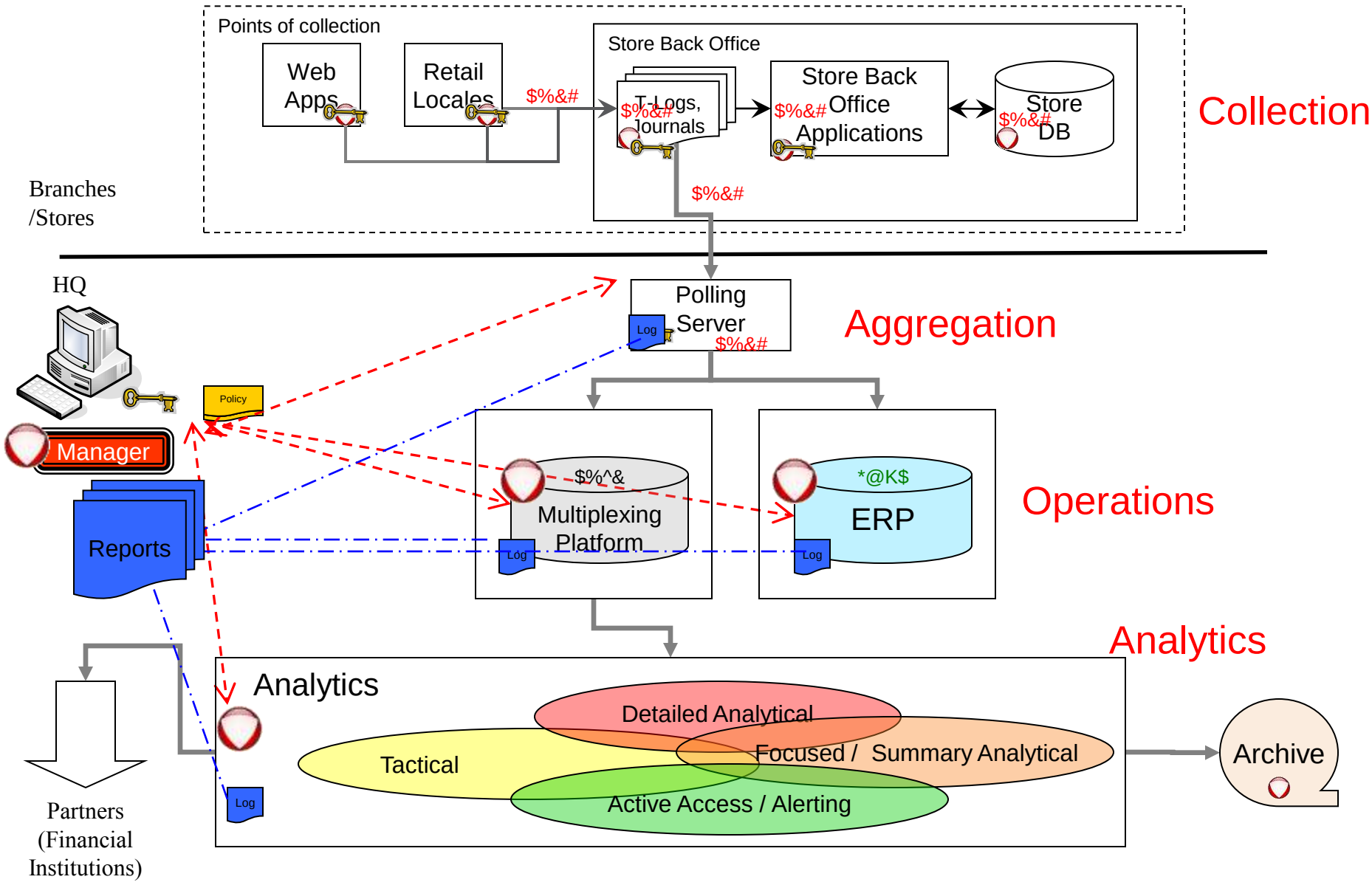


http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1144290

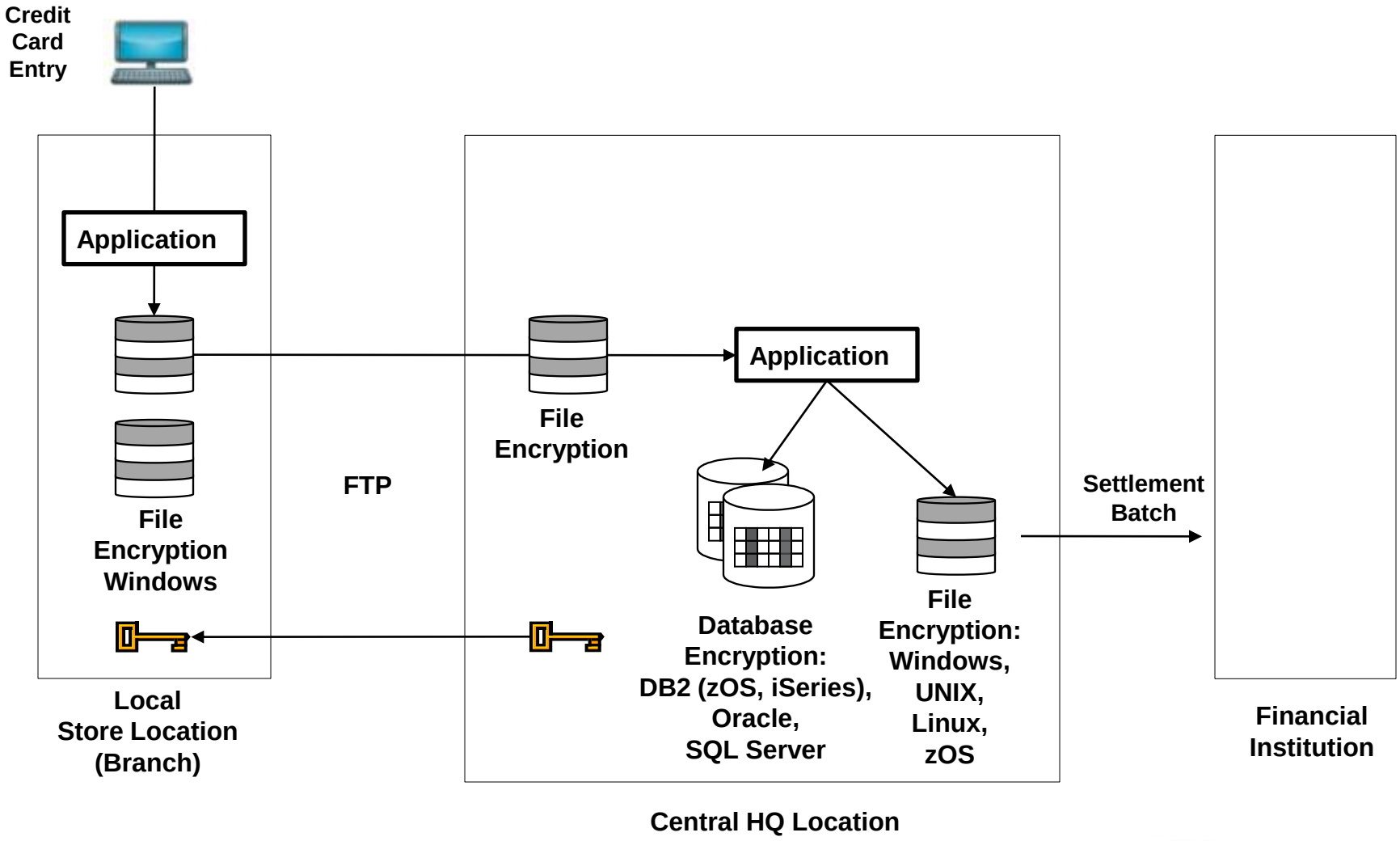
Case Studies

- **One of the most widely recognized credit and debit card brands in the world**
  - Their volume of data is in the multiple billions of rows and needed a solution that would not degrade performance.
- **Major financial institution**
  - Protecting high-worth clients financial information.
  - Central key management and separation of duties were of the utmost importance.
- **One of the world largest retailers**
  - Protecting the flow of sensitive credit card information from the store, through to back office systems and into the data warehouse and storage.
  - The central key management and ability to support thousands of stores was critical for this success.
  - Transparent to exiting applications.
  - Protect sensitive information in their Teradata data warehouse. iSeries (AS/400), zSeries (mainframe), Oracle and MS SQL Server, and to protect files that reside across platforms including Unix and z/Series.

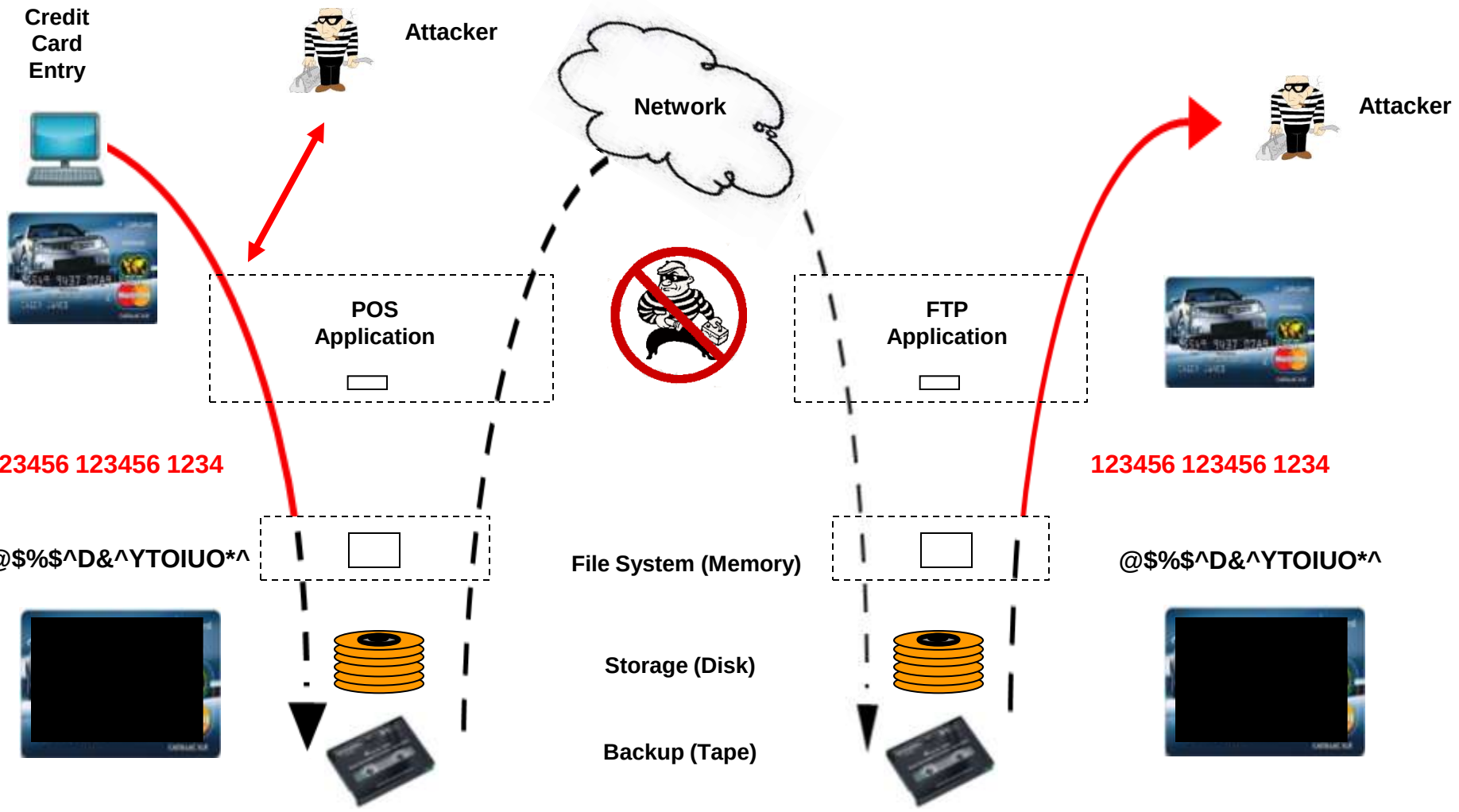
Security for the Sensitive Data Flow



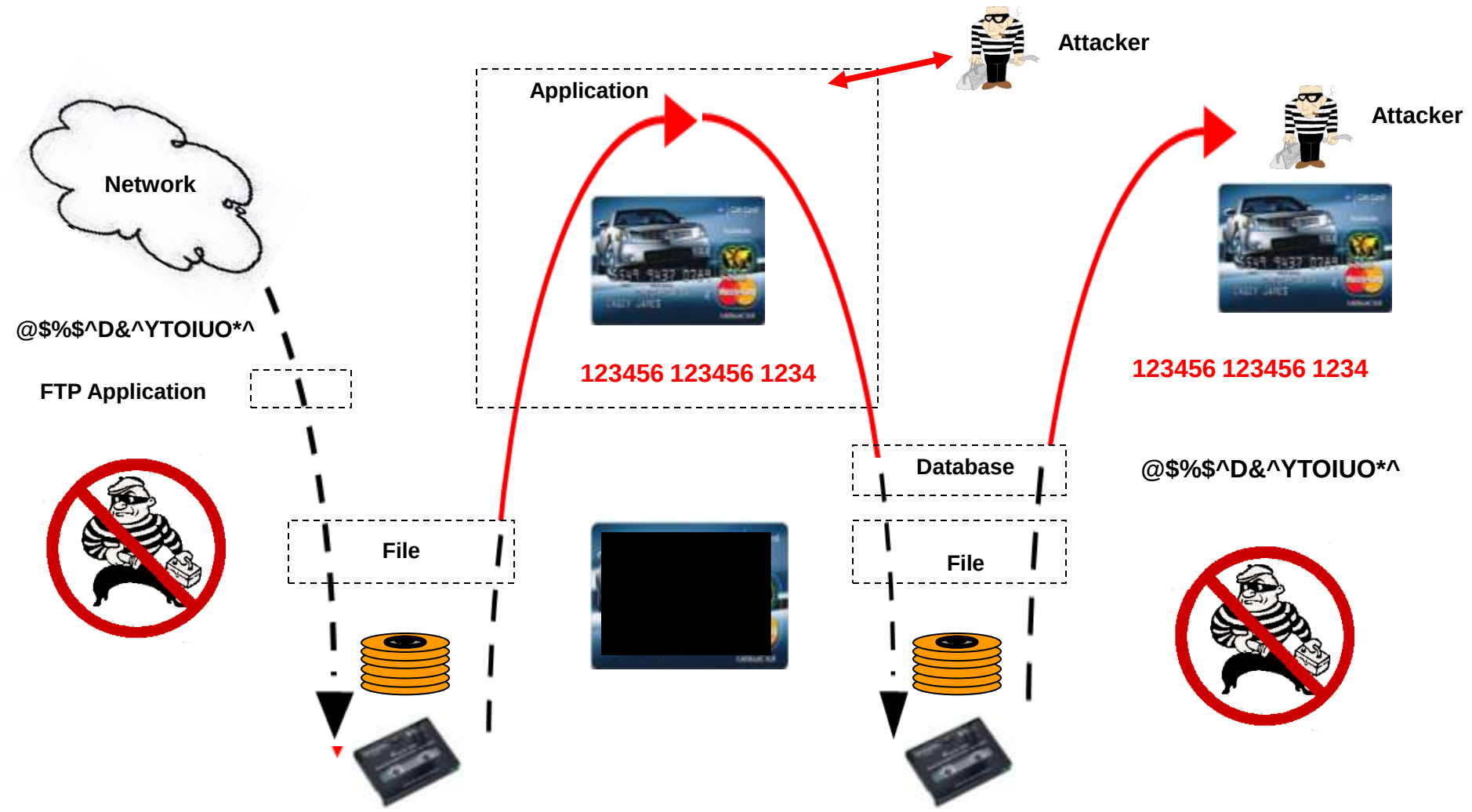
Case 1: Goal – PCI Compliance & Application Transparency



Case 1: File Encryption & FTP



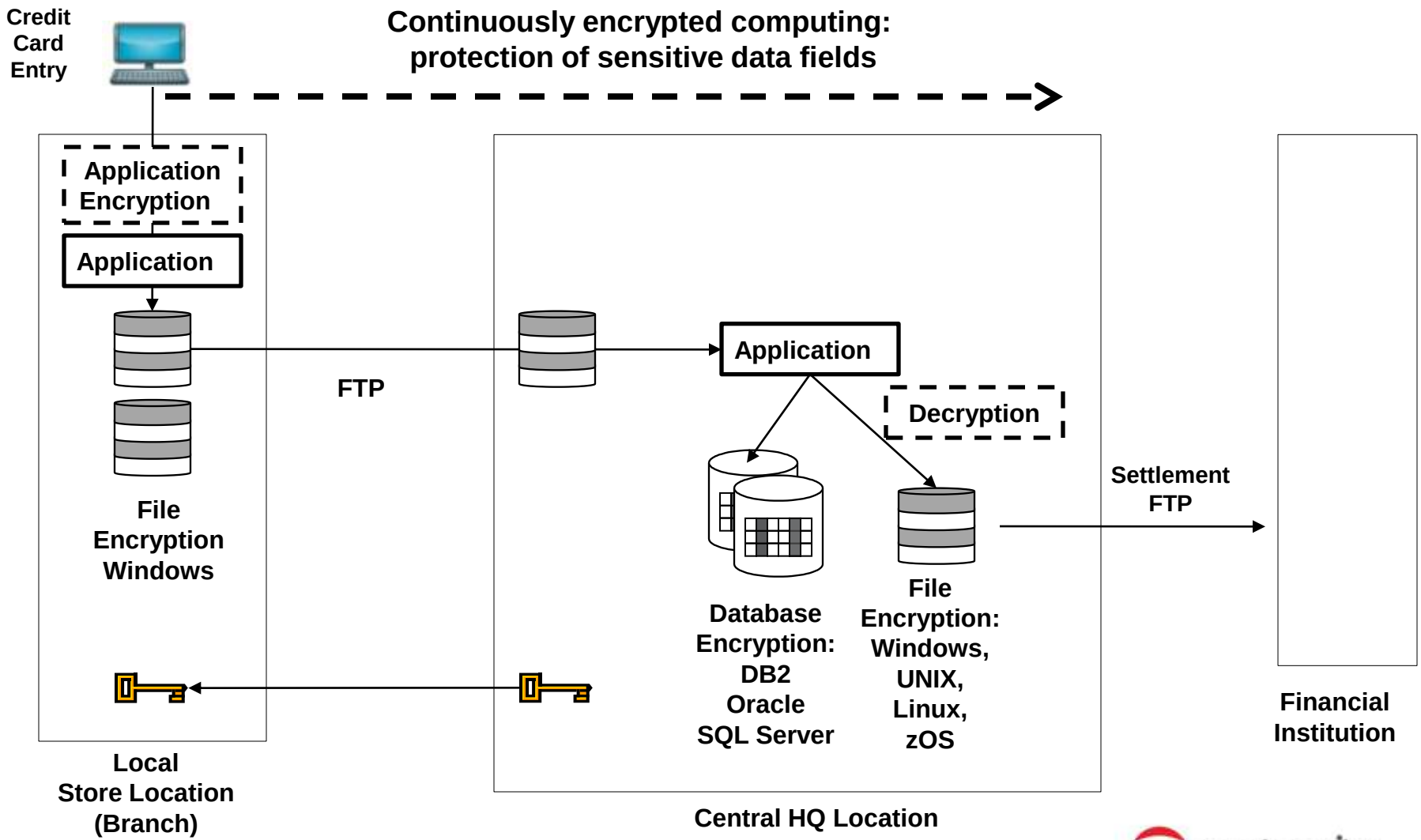
Case 1: From Encrypted File to Encrypted Database



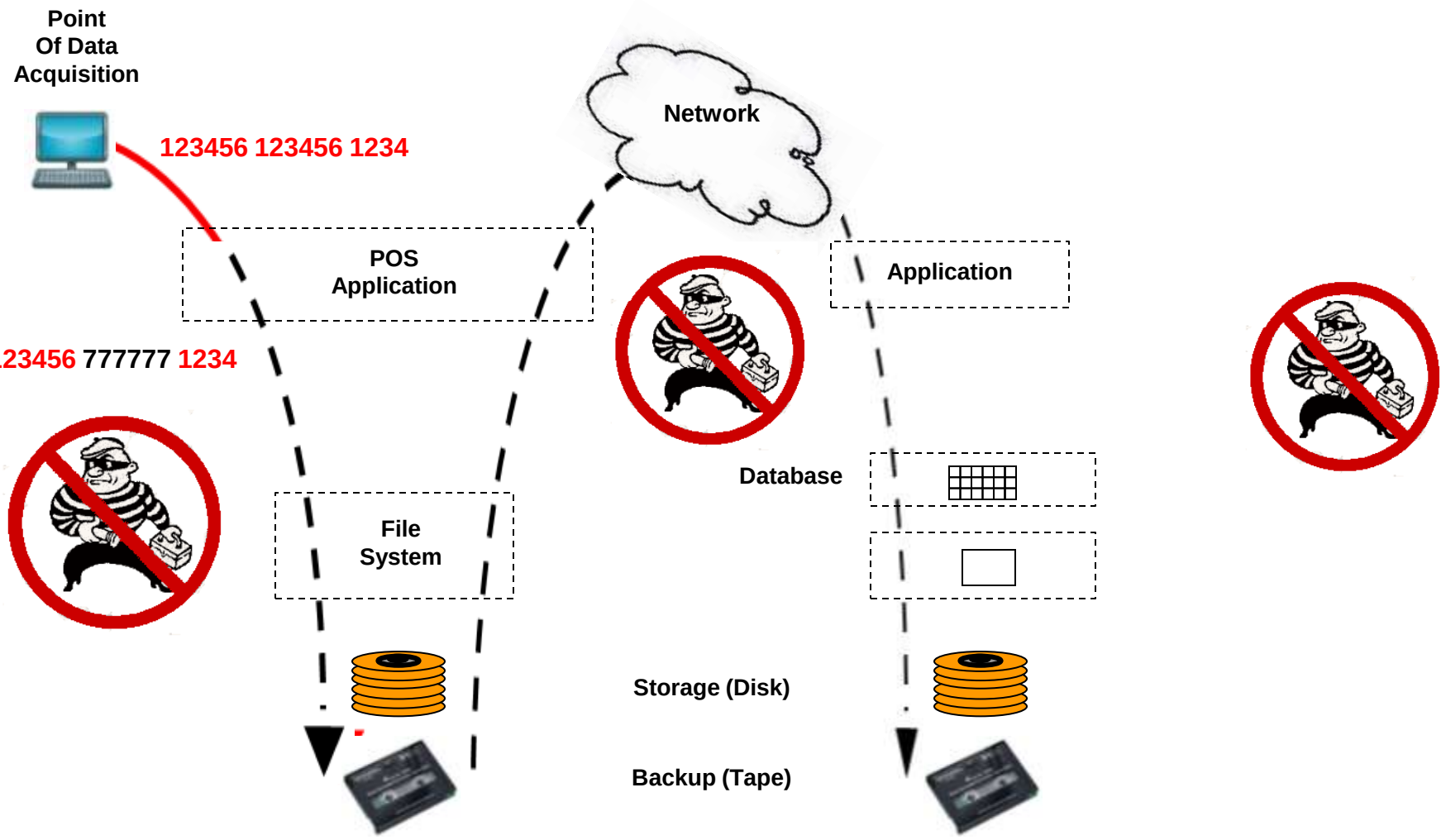
Unprotected sensitive information:

Protected sensitive information

Case 2a: Goal – Addressing Advanced Attacks & PCI



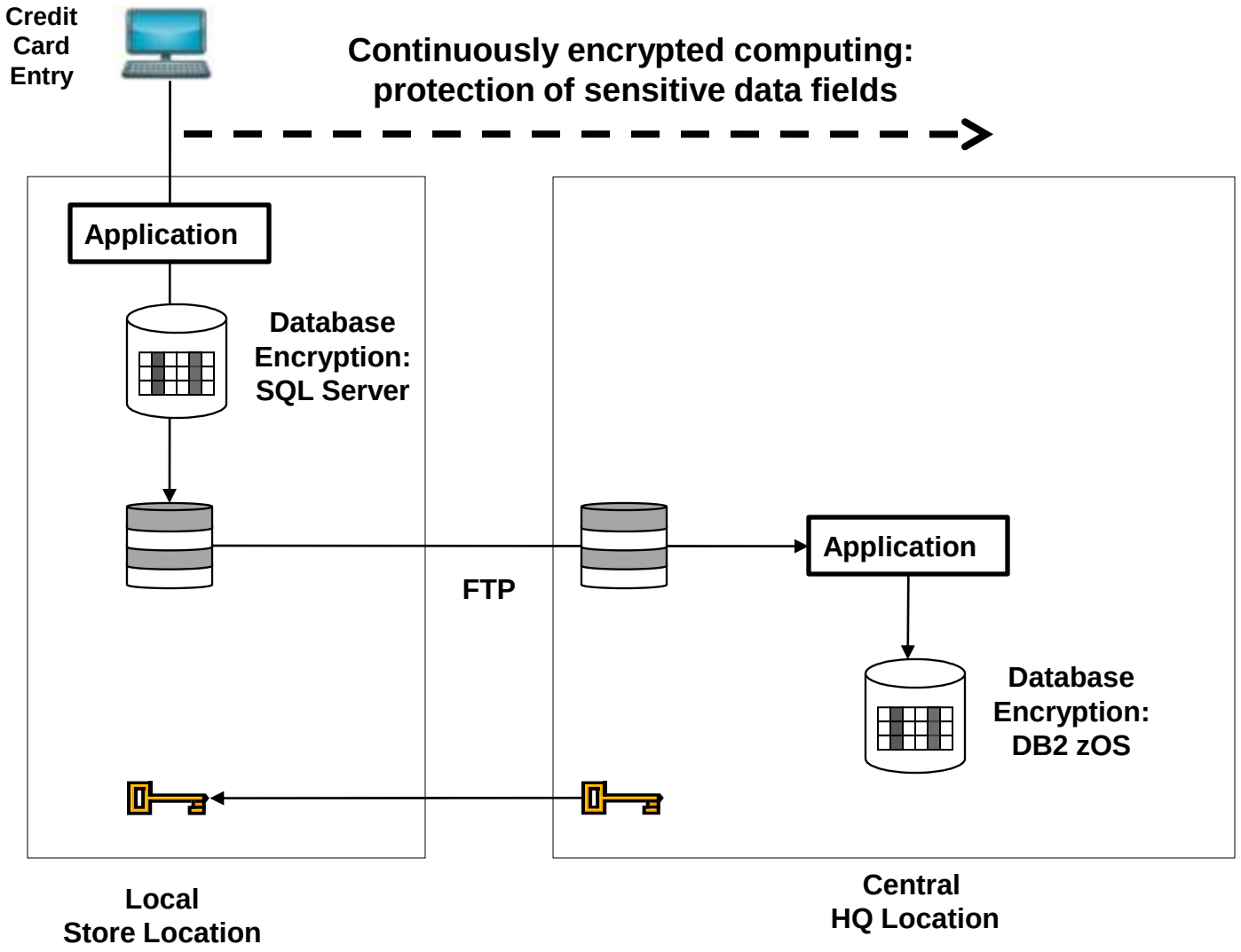
Case 2a: Application Encryption to Encrypted Database



Unprotected sensitive information:

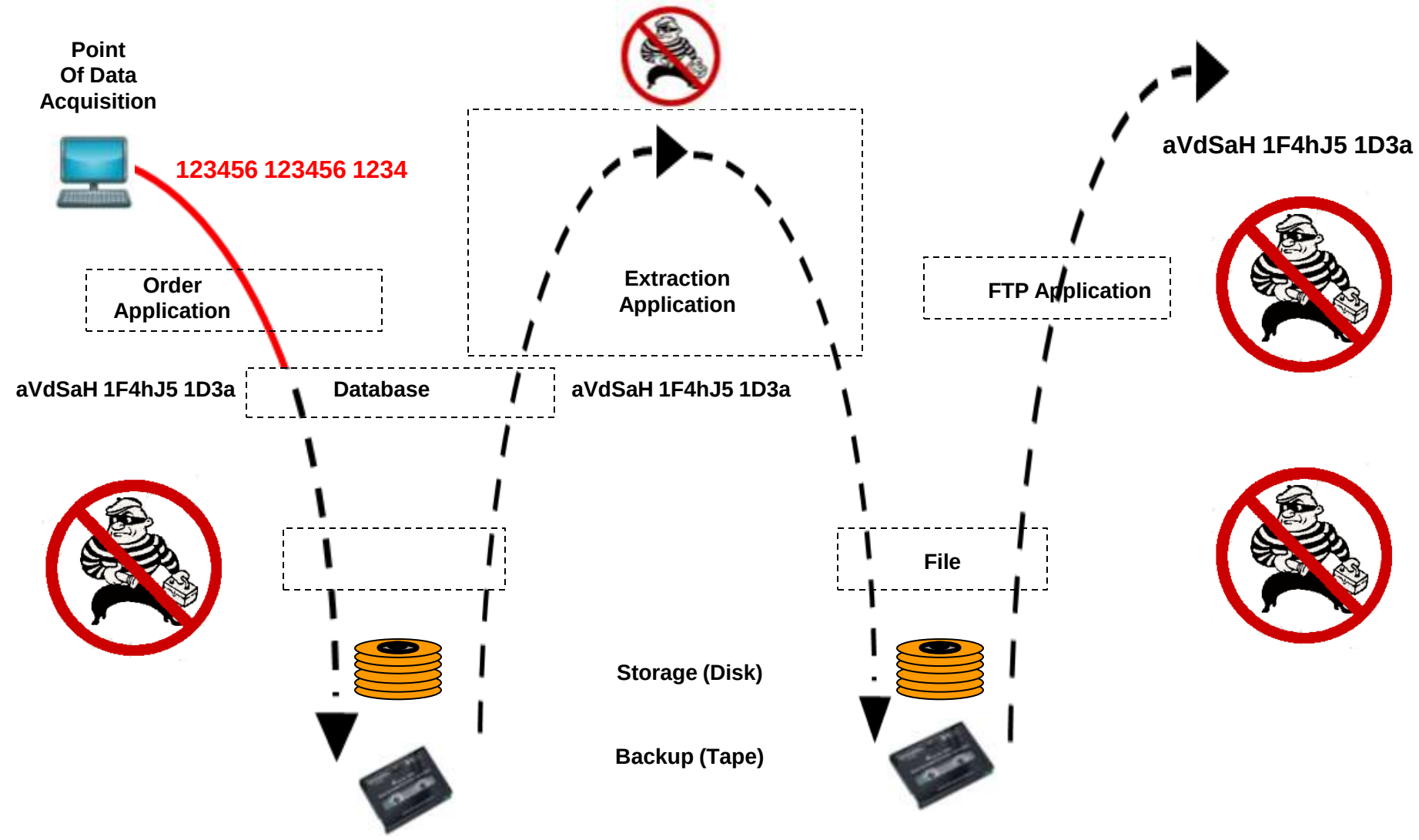
Protected sensitive information

Case 2b: Goal – Addressing Advanced Attacks & PCI

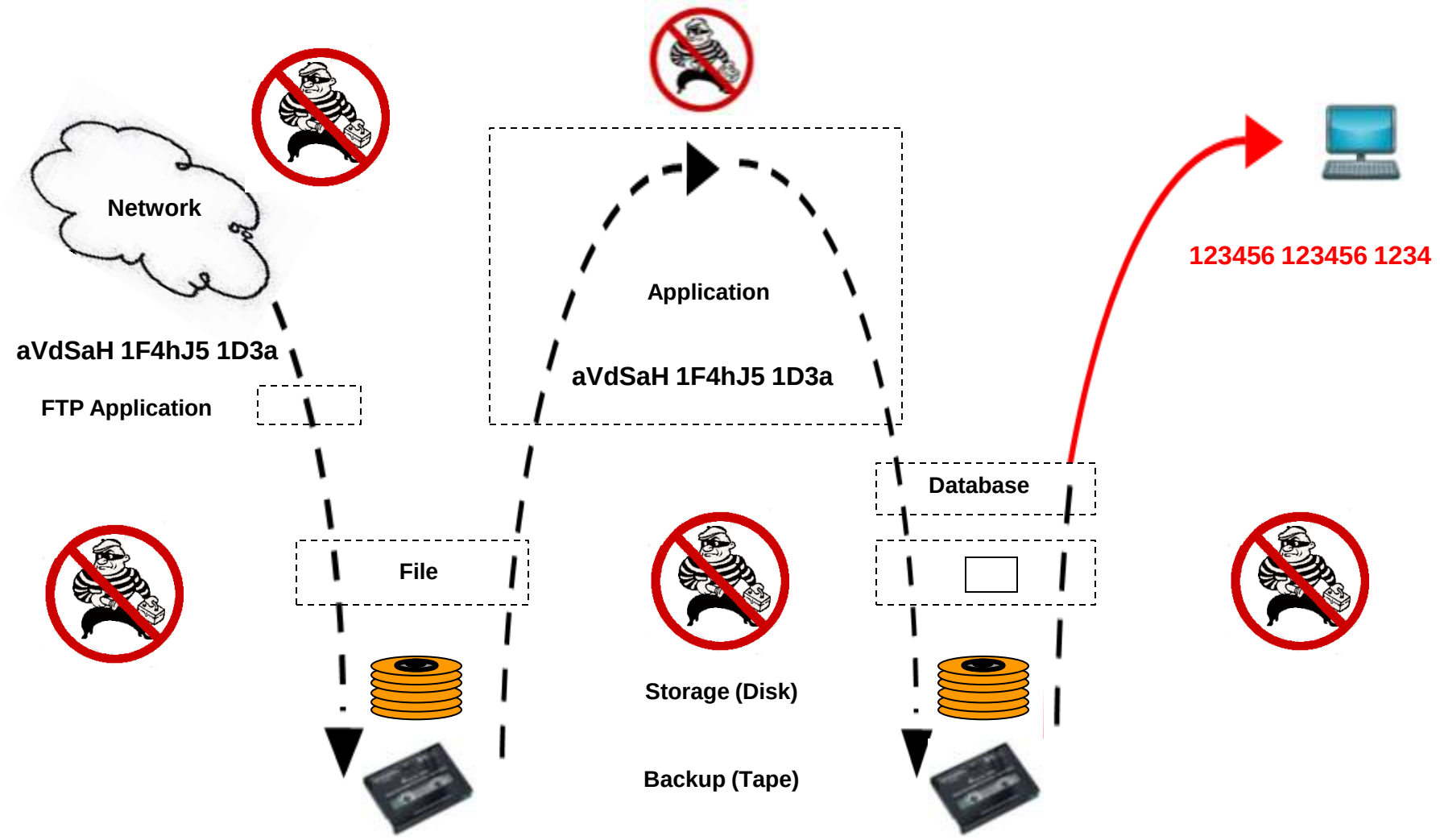


protegrity

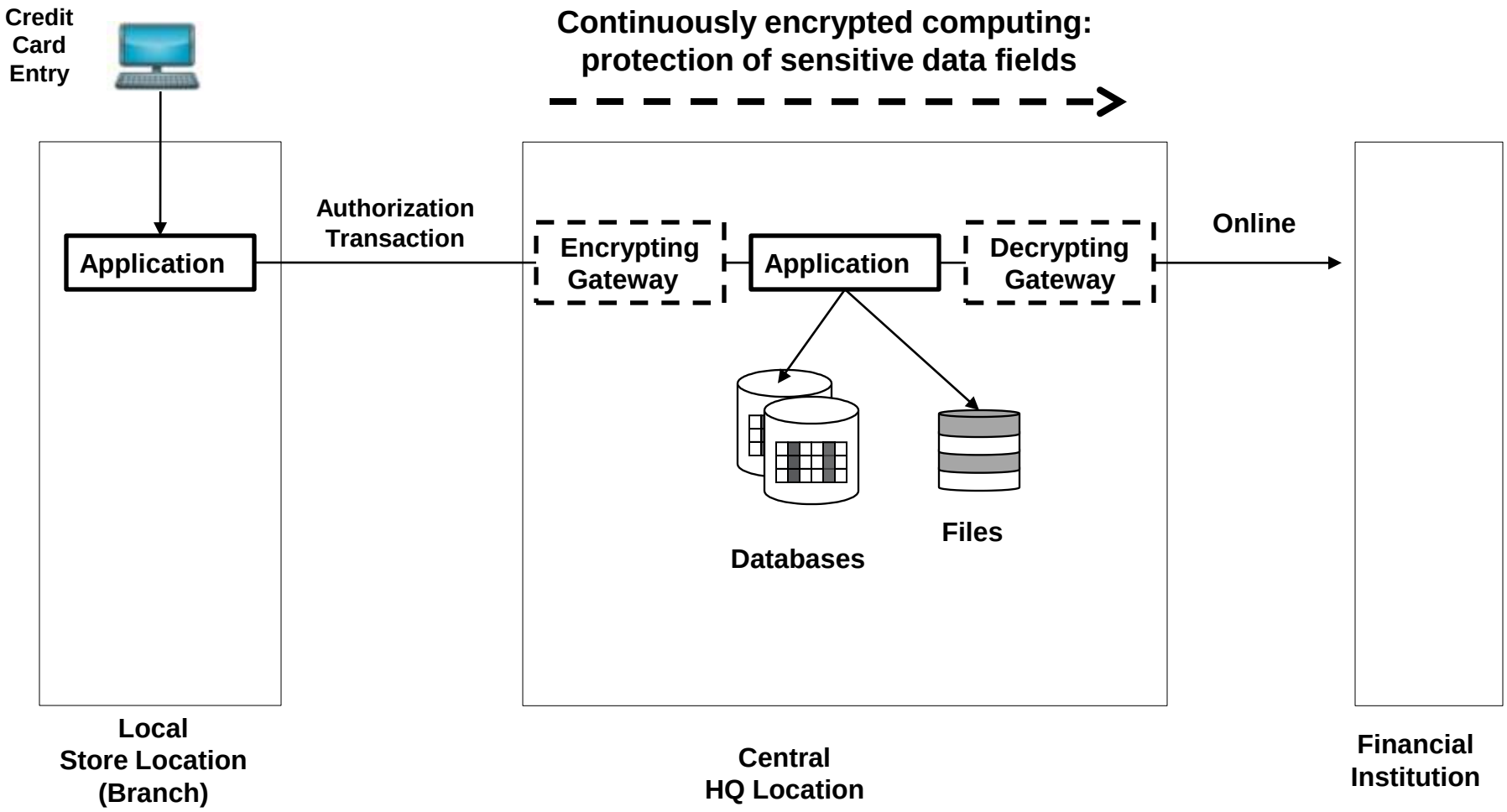
Case 2b: From Encrypted Database to File & FTP



Case 2b: From Selectively Encrypted File to Encrypted Database

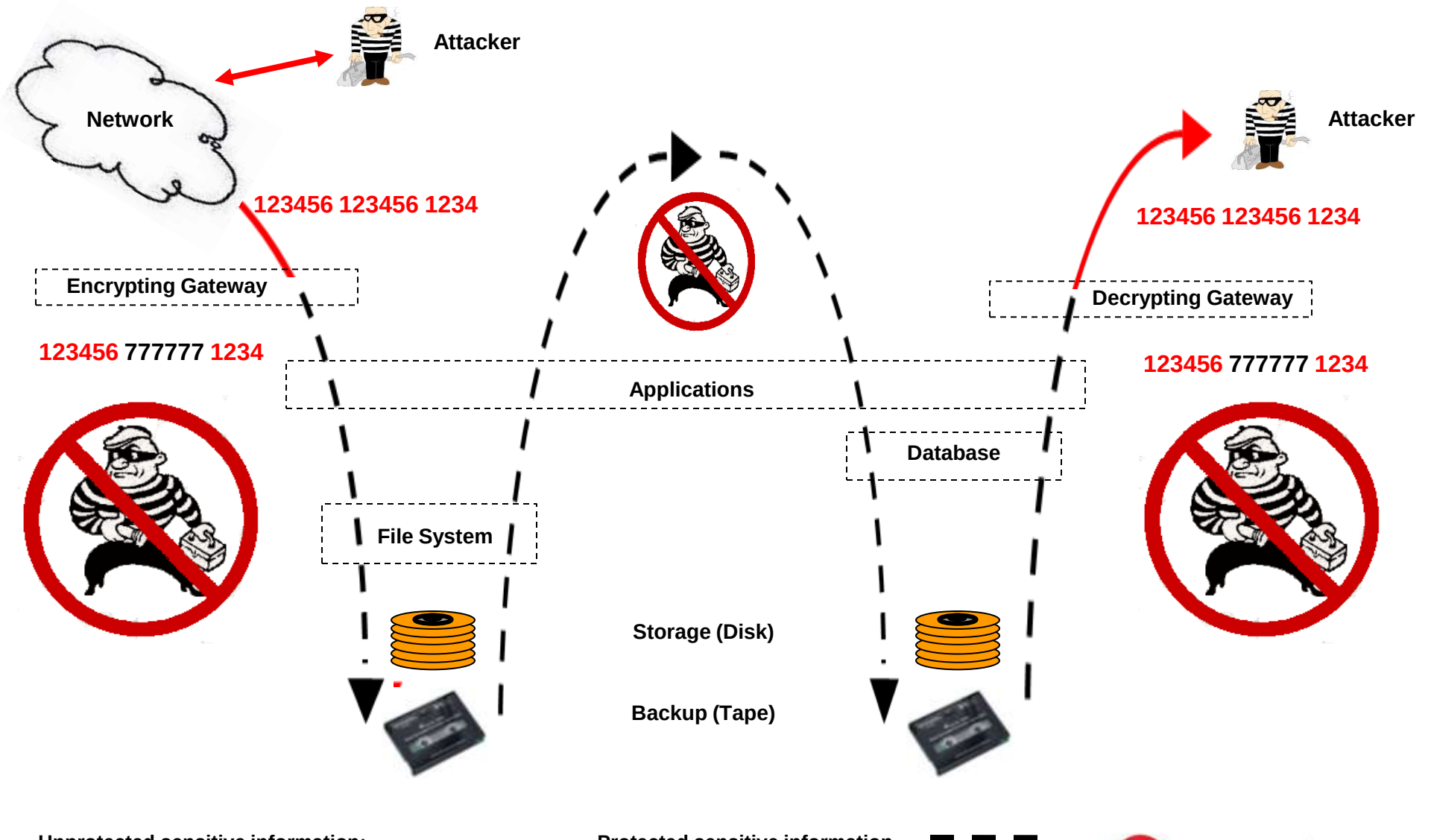


Case 3: Goal – Addressing Advanced Attacks & PCI



protegrity

Case 3: Gateway Encryption



Unprotected sensitive information: ——— Protected sensitive information - - -

How to keep sensitive data locked down across applications, databases, and files, including ETL data loading tools, FTP processes and EDI data transfers.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=940287

protegrity

Determine Risk

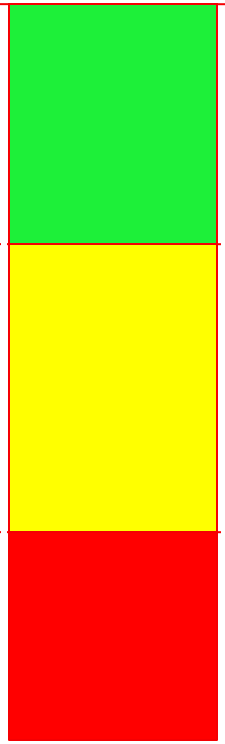
- Data Security Risk=Data Value * Exposure

Data Field	Value	Exposure	Risk Level
Credit Card Number	5	5	25
Social Security Number	5	4	20
CVV	5	4	20
Customer Name	3	4	12
Secret Formula	5	2	10
Employee Name	3	3	9
Employee Health Record	3	2	6
Zip Code	1	3	3

Enables prioritization
Groups data for potential solutions

Matching Data Protection Solutions with Risk Level

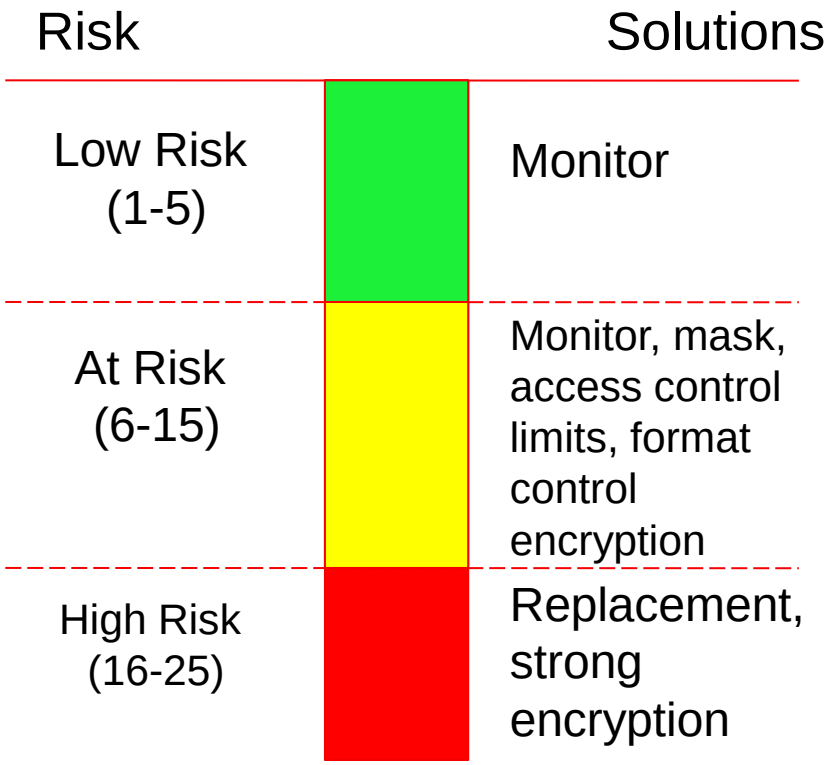
Risk	Solutions
Low Risk (1-5)	Monitor
At Risk (6-15)	Monitor, mask, access control limits, format control encryption
High Risk (16-25)	Replacement, strong encryption



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

Select risk-adjusted solutions for costing



protegrity

Estimate Costs

Cost = Solution Cost + Operations Cost

- Solution Cost = cost to license or develop, install and maintain
- Operations Cost = cost to change applications, impact on downstream systems, meeting SLAs, user experience

Operation Cost Factors

- Performance
  - Impact on operations - end users, data processing windows
- Storage
  - Impact on data storage requirements
- Security
  - How secure Is the data at rest
  - Impact on data access – separation of duties
- Transparency
  - Changes to application(s)
  - Impact on supporting utilities and processes

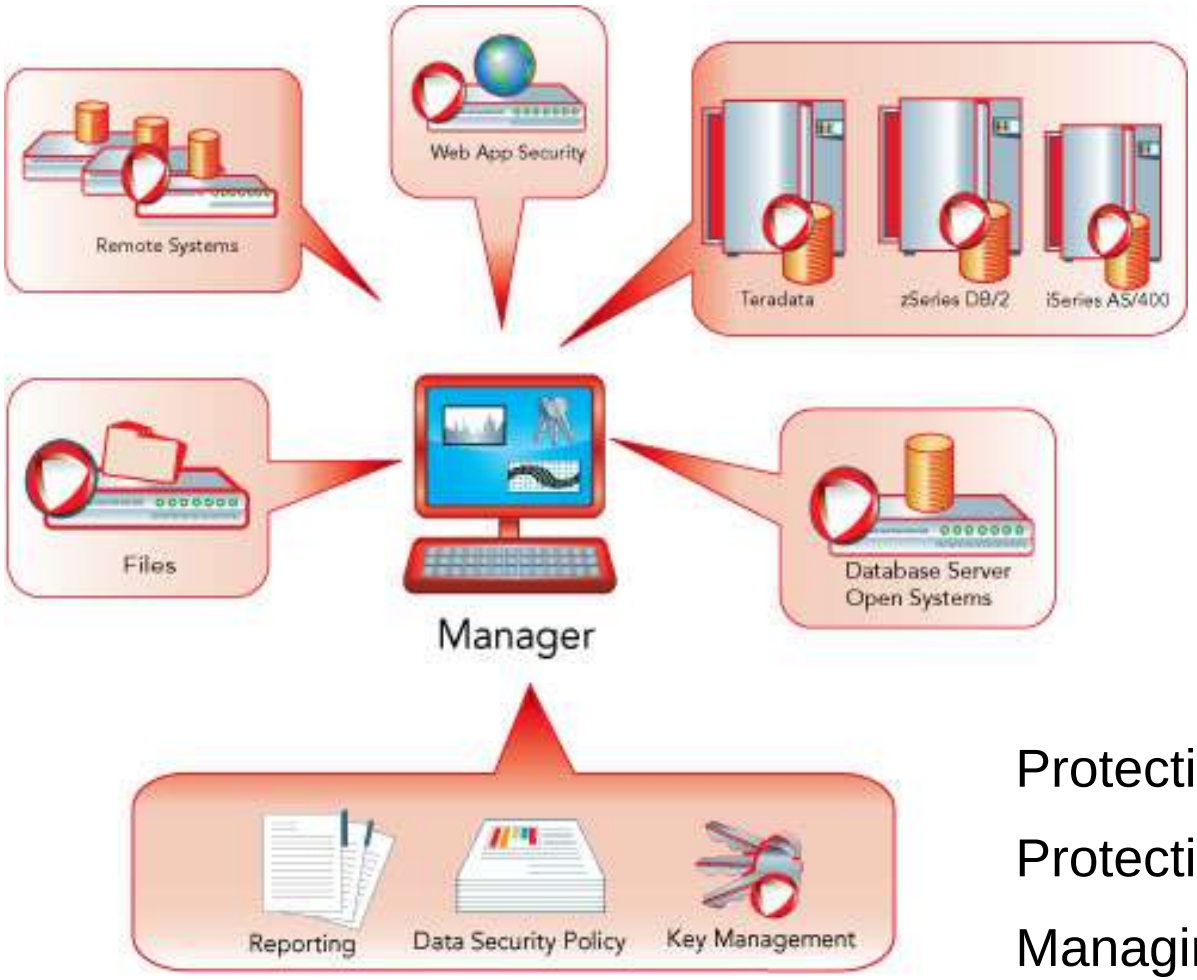
Operation Cost Factors

- Solution should be able to change with the environment
  - Progress from less to more secure solution, or the reverse
  - Add new defenses for future threats
  - Plug into existing infrastructure, integrate with other systems

The Protegrity Defiance© Suite

- Data Protection System (DPS)
  - Encryption, monitoring, masking
  - Database, file and application level
- Threat Management System (TMS)
  - Web application firewall
- Enterprise Security Administrator
  - Security policy
  - Key management
  - Alerting, reporting, and auditing

Protegrity Solutions



Protecting data

Protecting web applications

Managing data security

protegrity

Protegrity and PCI

Build and maintain a secure network.	**1. Install and maintain a firewall configuration to protect data** **2. Do not use vendor-supplied defaults for system passwords and other security parameters**
Protect cardholder data.	**3. Protect stored data** **4. Encrypt transmission of cardholder data and sensitive information across public networks**
Maintain a vulnerability management program.	**5. Use and regularly update anti-virus software** **6. Develop and maintain secure systems and applications**
Implement strong access control measures.	**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**
Regularly monitor and test networks.	**10. Track and monitor all access to network resources and cardholder data** **11. Regularly test security systems and processes**
Maintain an information security policy.	**12. Maintain a policy that addresses information security**

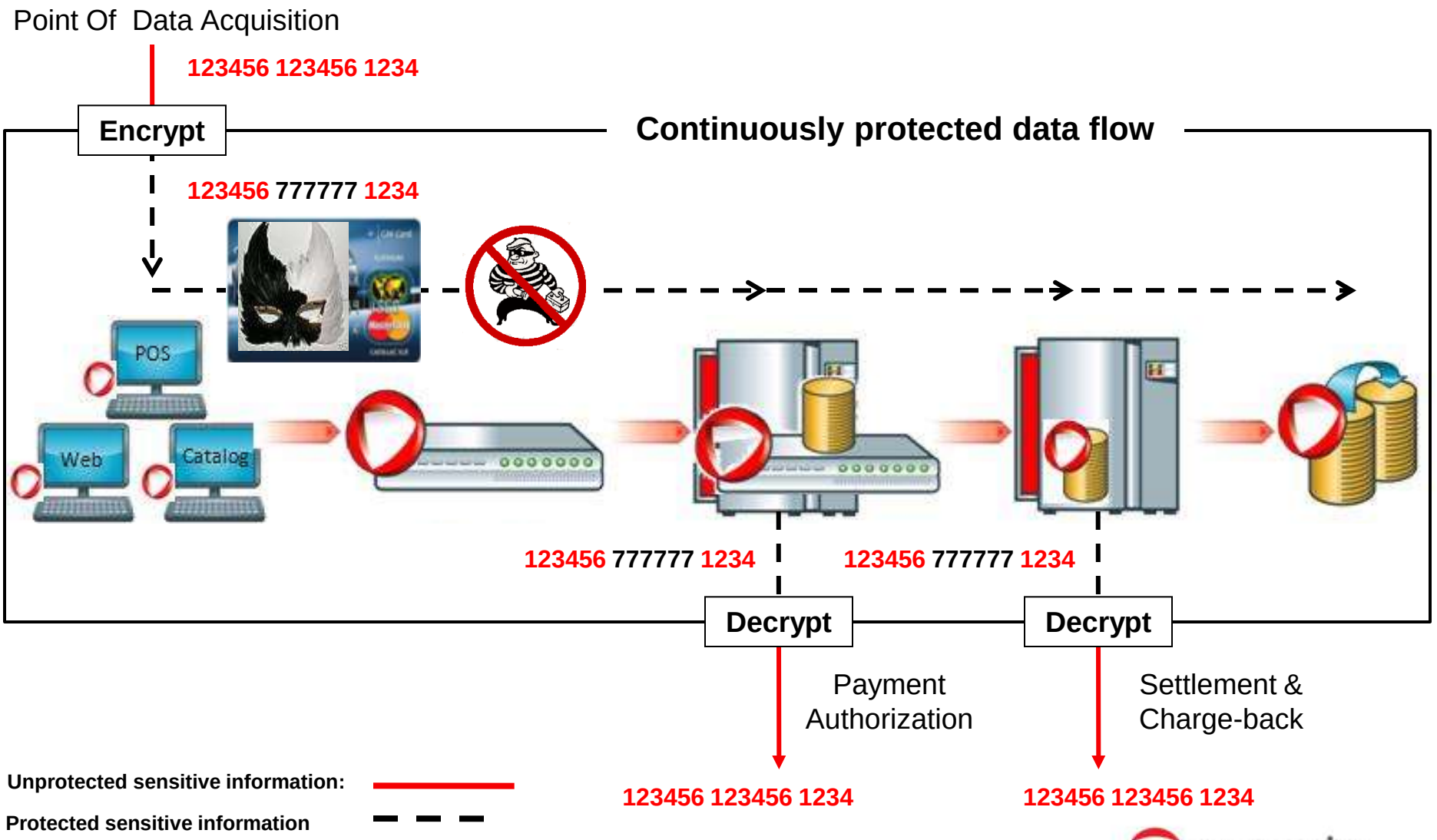
Data Security Management

- An integral part of technical and business process
- Security Policy
  - Centralized control of security policy
  - Consistent enforcement of protection
  - Separation of duties
- Reporting and Auditing
  - Compliance reports
  - Organization wide security event reporting
  - Alerting
  - Integration with SIM/SEM
- Key Management

Cost Effective Data Protection

- Uses Risk as an adjusting factor for determining a Data Protection strategy
- Risk=Data Value*Exposure
- Determines solutions that fit the risk level, then determines cost
- Cost=Solution Cost + Operational Cost
- Prepare for the future

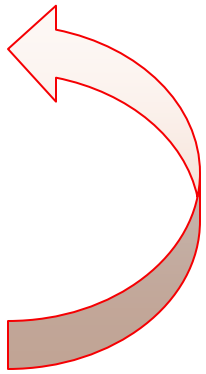
How to Protect the Data Flow Against Advanced Attacks



How to Protect the Weak Links in your Data Flow

Review Risk & Determine Protection Approach

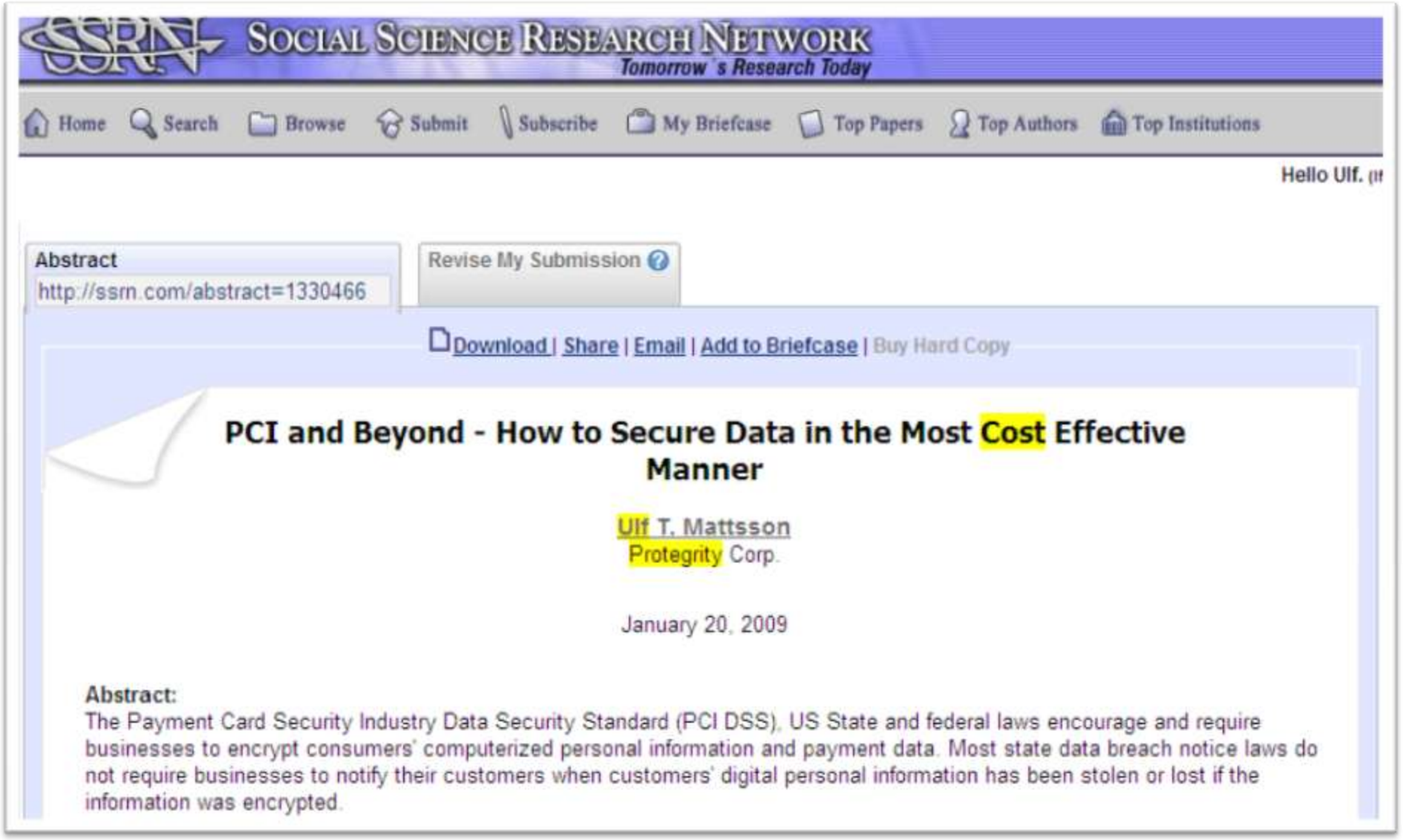
- Analyze the Data Flow
- Identify Assets and Assign Business Value to each
- Identify Vulnerabilities for each Asset
- Identify potential Attack Vectors & Attackers
- Assess the Risk
- Compliance Aspects
- Select Data Protection Points & Protection Methods



Adjust

Assess Total Impact

- Functionality Limitations
- Performance & Scalability
- Application Transparency
- Platform Support & Development Life Cycle Support
- Key Management, Administration & Reporting
- Deployment Cost, Time & Risk



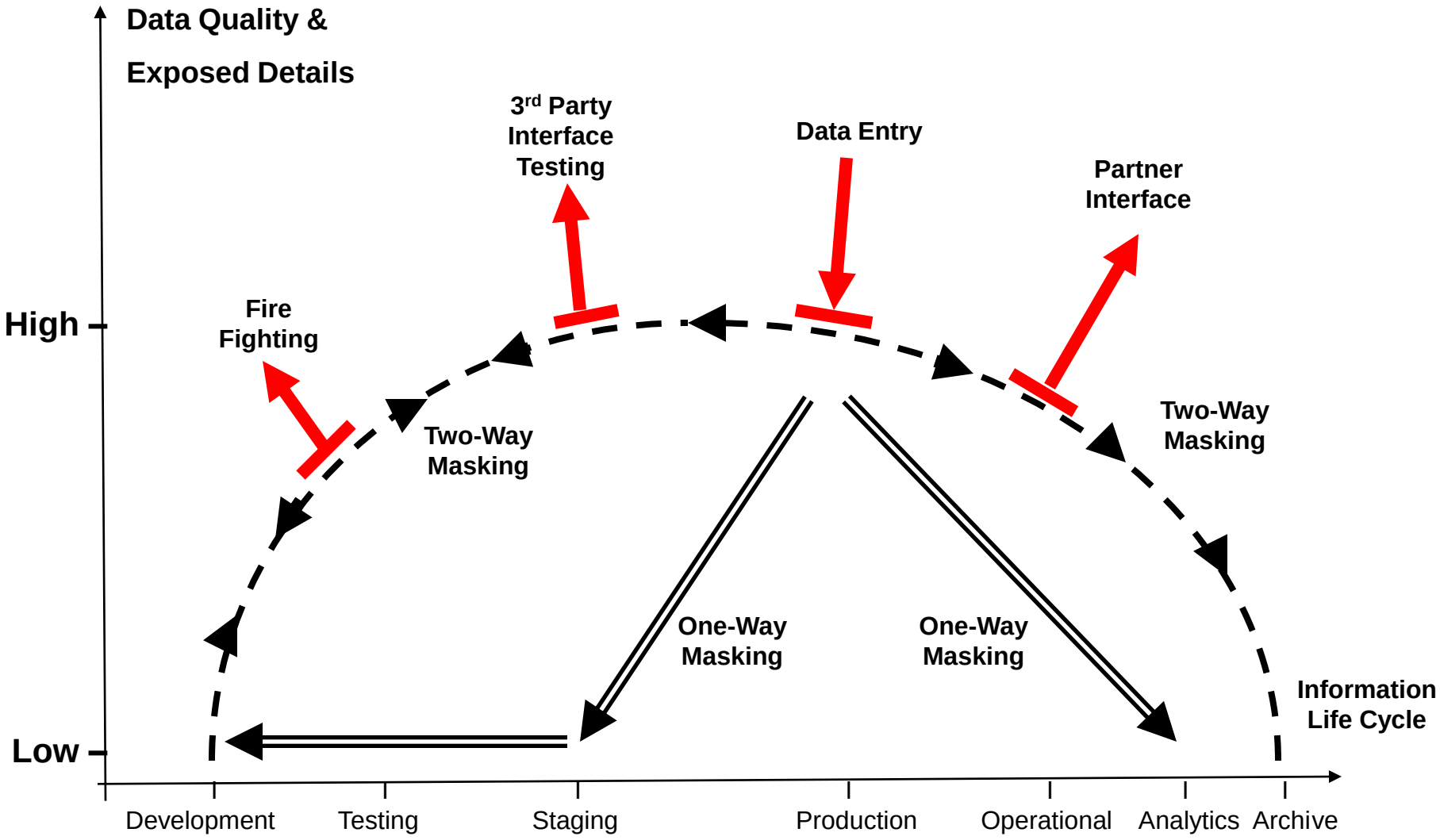
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1330466

Organizations are now required to protect sensitive data, or face the wrath of public consequences - be that public disclosure to your customers or regulatory non-compliance. With growing incidents of intrusions across industries and strong regulatory requirements to secure private data, enterprises need to make DBMS security a top priority.

protegrity

http://www.quest-pipelines.com/newsletter-v7/0706_C.htm

Data Masking – One-way vs. Two-way



Unprotected sensitive information:

Protected sensitive information

protegrity

ITSECURITY

RESOURCE CENTERS

IT Security Home
Access Control NEW!
Email Security
Firewalls
Intrusion Detection Systems
Malware
Network Access Control
Vulnerability Scanning NEW!
Security Audit
Spyware
VPN

STAY CURRENT

Blog
Features

Stay Current

Meet the Experts

Ulf Mattsson

(106 Comments)

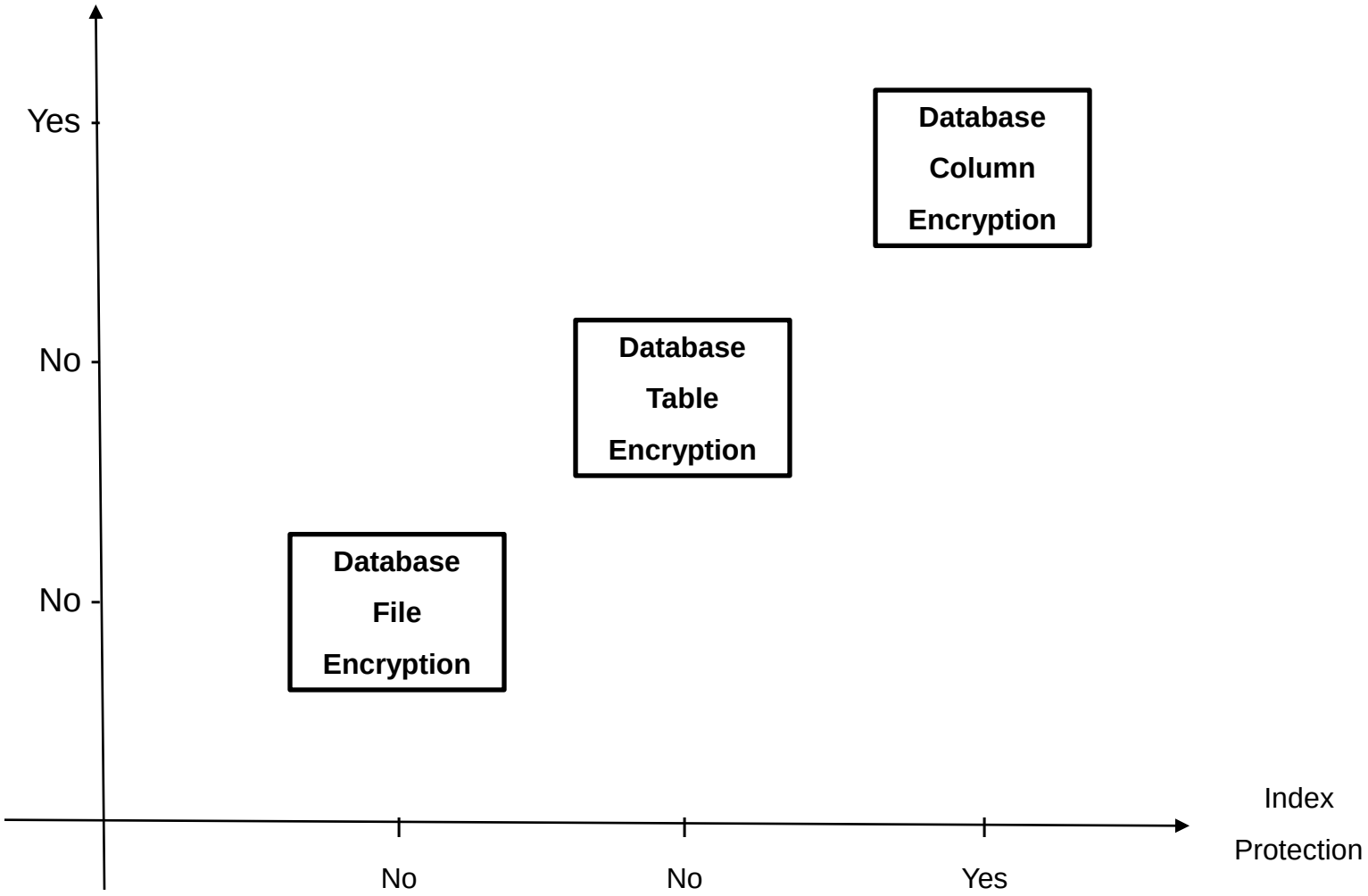
I created the initial architecture of Protegrity's database security technology, for which the company owns several patents.

Chief Technology Officer
Protegrity Corp.

I created the initial architecture of Protegrity's database security technology, for which the company owns several patents. My IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organisation, in the areas of IT architecture and IT security.

Separation of Duties (DBA)

Separation of Duties (DBA)



protegrity

The Goal: Good, Cost Effective Security

The goal is to deliver a solution that is a balance between security, cost, and impact on the current business processes and user community

- Security plan - short term, long term, ongoing
- How much is ‘good enough’
- Security versus compliance
  - Good Security = Compliance
  - Compliance ≠ Good Security

Risk Adjusted Data Protection

- Assign value to your data
- Assess exposure
- Determine risk
- Understand which Data Protection solutions are available to you
- Estimate costs
- Choose most cost effective method

Assign Value to Your Data

- Identify sensitive data
  - If available, utilize data classification project
  - Rank what is sensitive on its own (think PCI)
  - Consider what is sensitive in combination (think Privacy)
- How valuable is the data to (1) your company and (2) to a thief
  - Corporate IP, Credit Card numbers, Personally Identifiable Information
- Assign a numeric value: high=5, low=1

Assess Exposure

- Locate the sensitive data
  - Applications, databases, files, data transfers across internal and external networks
- Location on network
  - Segmented
  - External or partner facing application
- Access
  - How many users have access to the sensitive data?
  - Who is accessing sensitive data?
  - How much and how frequently data is being accessed?
- Assign a numeric value: high=5, low=1

Determine Risk

- Data Security Risk=Data Value * Exposure

Data Field	Value	Exposure	Risk Level
Credit Card Number	5	5	25
Social Security Number	5	4	20
CVV	5	4	20
Customer Name	3	4	12
Secret Formula	5	2	10
Employee Name	3	3	9
Employee Health Record	3	2	6
Zip Code	1	3	3

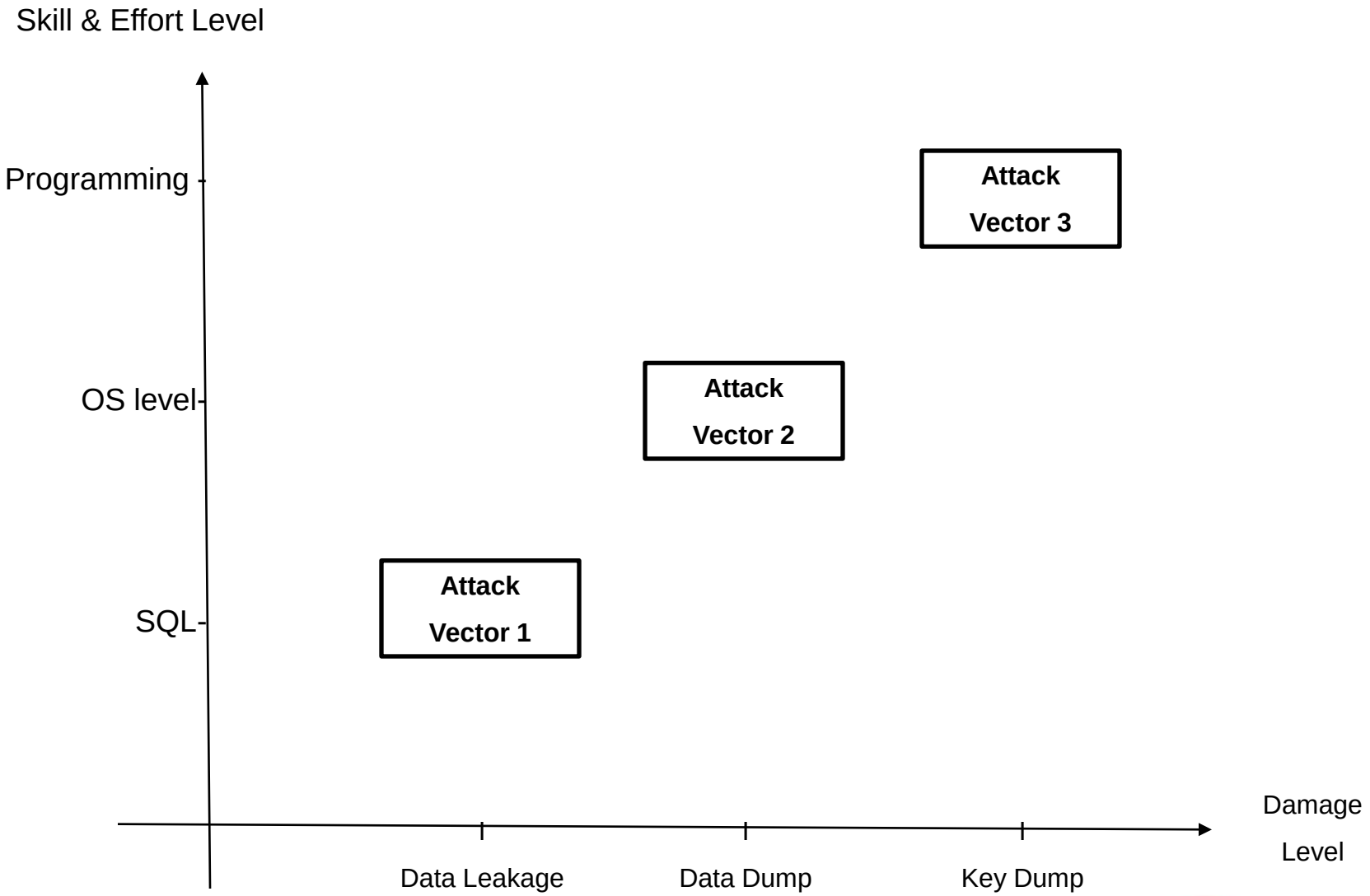
Enables prioritization
Groups data for potential solutions

Example – Software Application

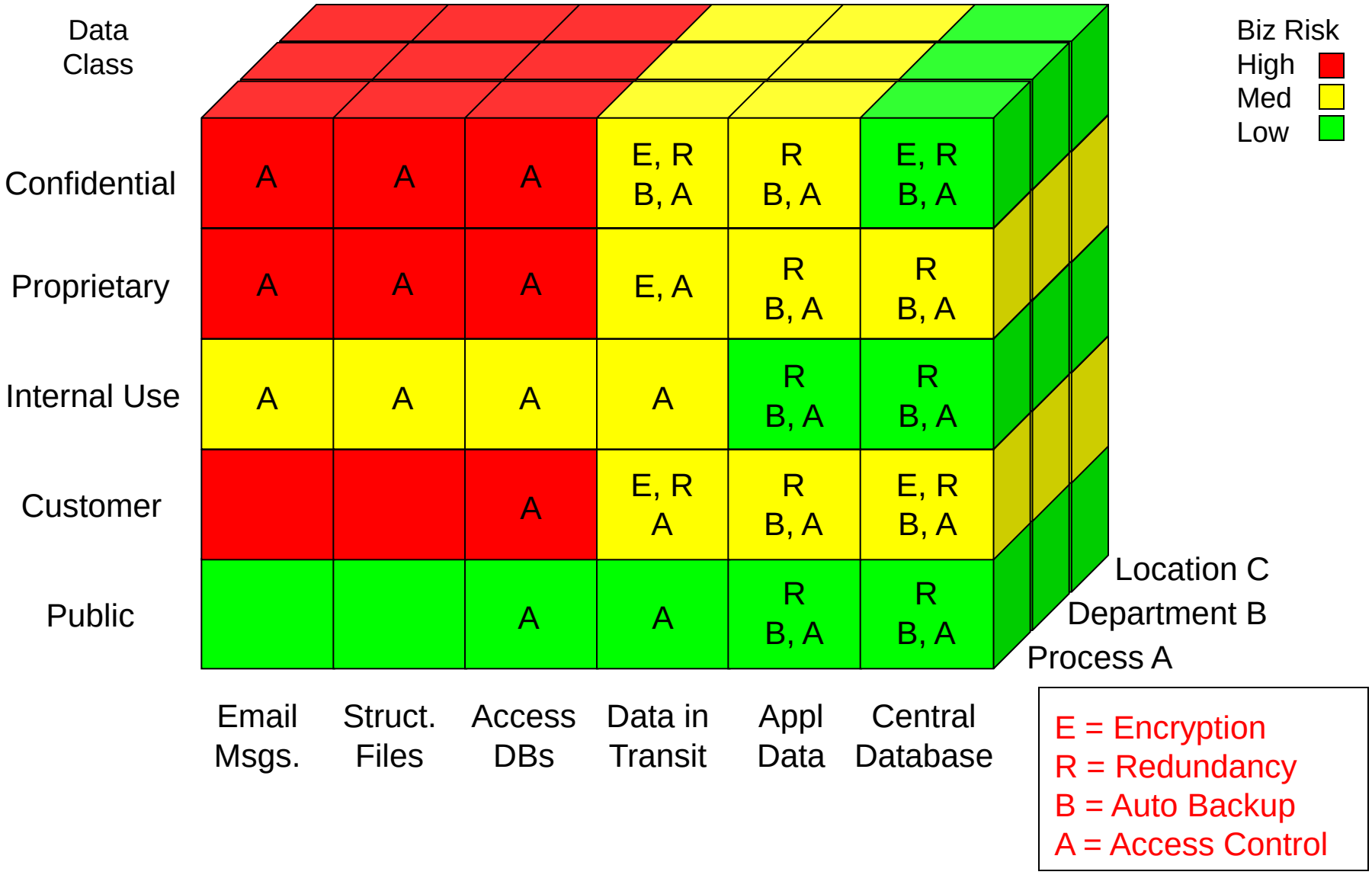
Priority	Threat ID	Attack Vector	Requirements IDs	Attacker	Time 1 - Very Long 10 - Very Fast	Skill 1 - Very Profesional	HW Investmnet 1 - Very Large 10 - No	Money 1 - Very Expensive 10 - Free	Human Resources 1 - > 3 3 - >= 2	Customer Exposure 1 - Very Low 10 - Very High	Vendor Exposure 1 - Very Low 10 - Very High	BFI Requirment
E	1.0	Using xxx an attacker can yyy the data knowing aaa and bbb	1.0, 42.0, 43.0, 44.0	xxx Administrator, User with yyy rights	10	10	10	10	5	2	1	
A	2.0	Using xxx an attacker can yyy the data knowing aaa and bbb	2.0	xxx Administrator, User with yyy rights	10	5	10	10	5	10	10	
B	3.0	Using xxx an attacker can yyy the data knowing aaa and bbb	2.0, 3.0, 19.0, 32.0	xxx Administrator, User with yyy rights	8	5	8	8	5	10	10	
A	4.0	Using xxx an attacker can yyy the data knowing aaa and bbb	4.0 1.0	xxx Administrator, User with yyy rights	10	10	10	10	5	10	10	
C	5.0	Using xxx an attacker can yyy the data knowing aaa and bbb	4.0 1.0	xxx Administrator, User with yyy rights	8	8	10	10	5	10	10	
C	6.0	Using xxx an attacker can yyy the data knowing aaa and bbb	4.0, 1.0, 41.0, 42.0	xxx Administrator, User with yyy rights	8	8	8	8	5	10	10	
E	7.0	Using xxx an attacker can yyy the data knowing aaa and bbb	5.0 1.0	xxx Administrator, User with yyy rights	10	10	10	10	5	2	1	
E	8.0	Using xxx an attacker can yyy the data knowing aaa and bbb	5.0 1.0	xxx Administrator, User with yyy rights	8	8	10	10	5	2	1	
B	9.0	Using xxx an attacker can yyy the data knowing aaa and bbb	6.0	xxx Administrator, User with yyy rights	8	5	8	8	5	10	10	

protegrity

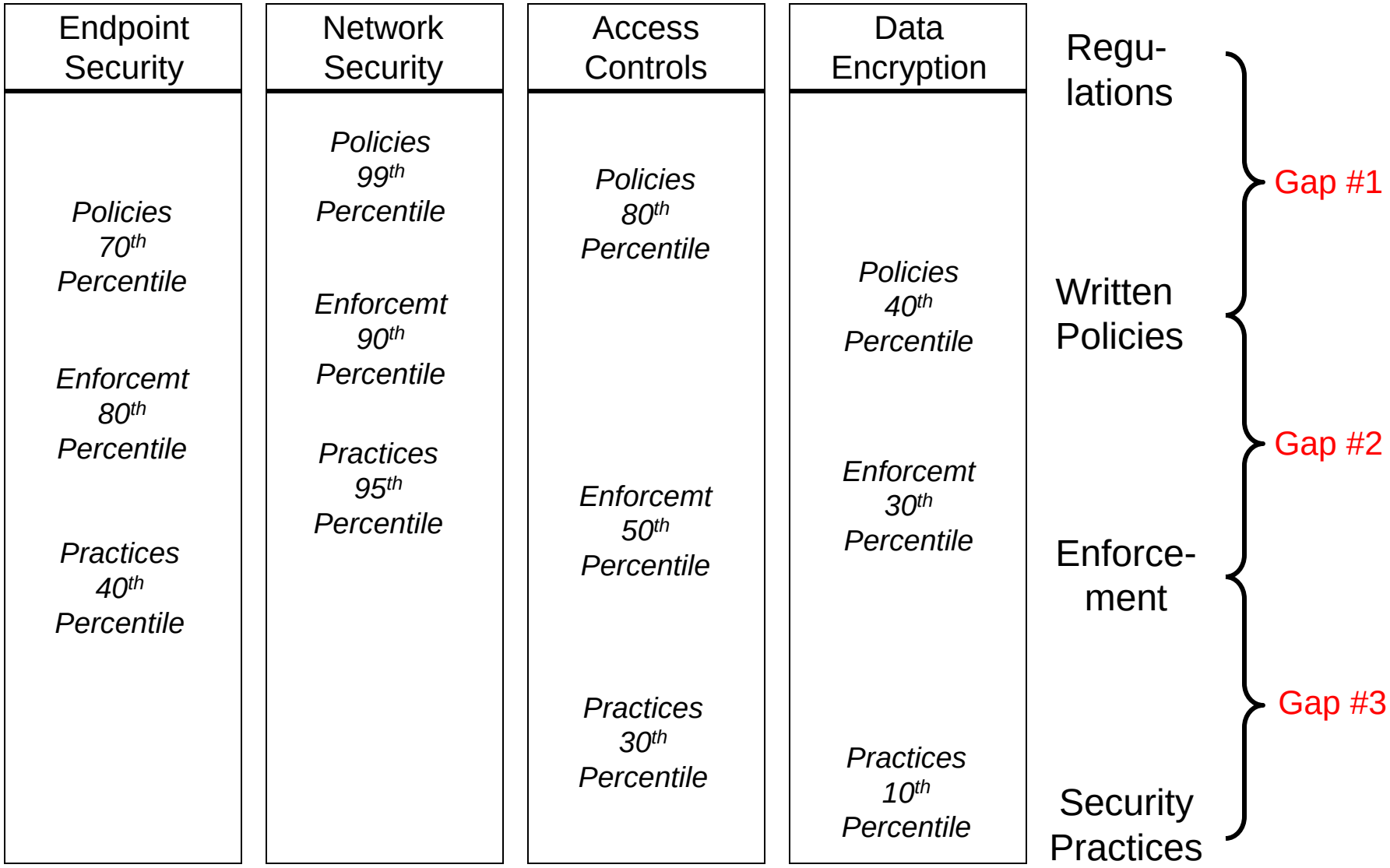
Example - Attack by DBA



Data Classification by Level of Protection

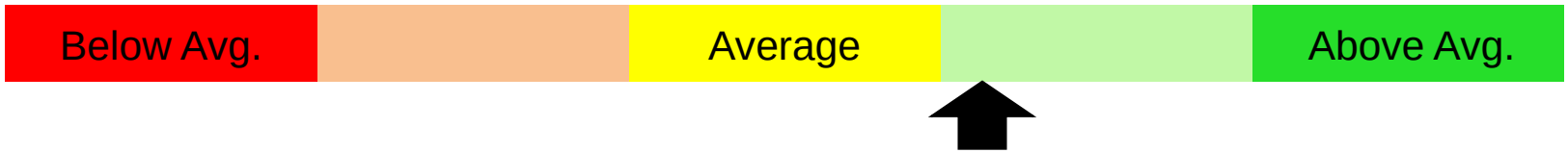


Gap Analysis: Regulations - Policies - Enforcement - Practice



Security Documentation Overall

Security Documentation Review / Analysis



Policy Completeness		Organization issues
Policy Enforceability		Punishment specs
Policy Awareness		Very good in IT
Security Architecture		Security architect?
Network Security		Excellent
Storage Security		Not in most docs
Application Security		Reviewed few apps
Database Security		Being upgraded

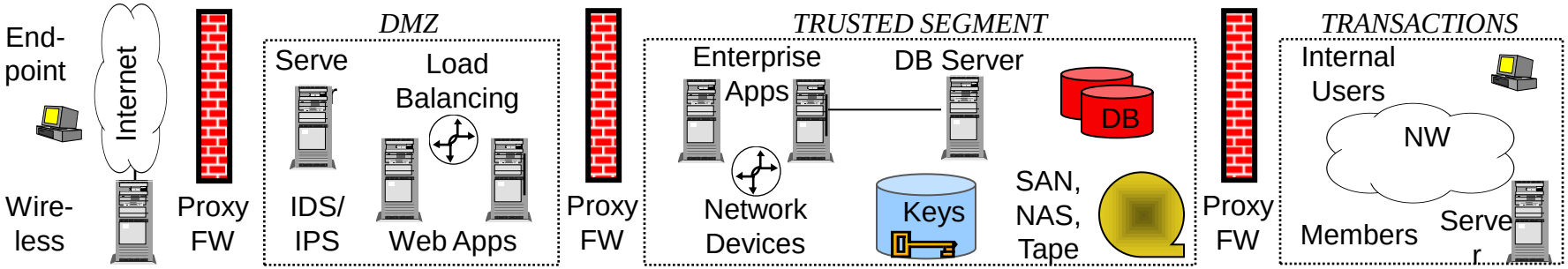
Control Effectiveness Rating

Effectiveness Strong Mixed Weak	**Control**	**Pervasiveness**		**In Practice Usage**	
	DB access control	Externally facing	Internally facing	Awareness of control	Compliance with control
Effectiveness ratings cover the use of the control across multiple organizations and applications in the enterprise					
Corporate data center	🟢	🟡	🔴	🔴	🔴
Division data centers	🟢	🟡	🟡	🔴	🔴
Regional offices	🟢	🟡	🟡	🔴	🔴
Home offices	🟡	🟡	🔴	🟡	🟡
Remote users	🟡	🟢	🟡	🔴	🔴
Effectiveness ratings are also applied to service providers who handle sensitive data on behalf of the enterprise					
Service providers	🟡	🟡	🔴	🟡	🟡
Resellers	🟡	🔴	🔴	🔴	🔴

Data Security Case Study - Interview

DATA SECURITY BEST PRACTICES STUDY -- RESTRICTED ACCESS -- DO NOT DISTRIBUTE			
This interview is being conducted as part of a study of data security best practices. The study is being conducted for the organization Information Security organization by Protegrity. EVERTHING YOU SAY IS COVERED BY A VERY STRICT NON-DISCLOSURE AGREEMENT. We want your detailed feedback about the handling of sensitive data within your organization at organization. This feedback will be used to help organization improve its data protection policies and procedures. Please feel free to share your experiences and feelings. YOU WILL NEVER BE IDENTIFIED TO ANYONE ELSE WITHIN organization AT ANY TIME.			
OVERVIEW		**Comments**	
1	What types of confidential business data do you handle as part of your job?		
2	What are the procedures you have to follow when you handle confidential information?		
3	What security policies affect how you handle this information?		
4	How do you keep track of changes to the security policies and procedures?		
5	Who is responsible for monitoring and enforcing these policies and procedures?		
FILL IN THE FOLLOWING BEFORE THE INTERVIEW			
a	Date of the interview:		
b	Name of the enterprise:	organization International	
c	Name of the interviewee:	First Name	Last Name
d	Phone # of the Interviewee:		
e	Email address of the Interviewee:		
f	Name of Interviewer		

Case Study - Data Security Vulnerability Points



Organization data security vulnerability points under study:

1. Endpoint security / desktop security / wireless security
2. Customer access to Organization via Web Applications
3. Web application development and access controls
4. Global bulk file transfer to/from member institutions
5. Corporate network infrastructure, including firewalls, IDS/IPS
6. XxxNet/YyyNet global infrastructure
7. Application-to-database access controls
8. Database management controls, including separation of duties
9. Key management systems
10. Customer premises HW/SW data protection (the XXX)
11. Protection of stored data in SAN, NAS and backup tapes

Questions?

If you would like a copy of the slides,
please email
ulf.mattsson@protegrity.com

protegrity

protecting your data.
protecting your business.

Organizations are now required to protect sensitive data, or face the wrath of public consequences - be that public disclosure to your customers or regulatory non-compliance. With growing incidents of intrusions across industries and strong regulatory requirements to secure private data, enterprises need to make DBMS security a top priority.

protegrity

http://www.quest-pipelines.com/newsletter-v7/0706_C.htm

Article Information

A practical implementation of transparent encryption and separation of duties in enterprise databases: protection against external and internal attacks on databases

Mattsson, U.T.

E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on
Volume , Issue , 19-22 July 2005 Page(s): 559 - 565
Digital Object Identifier 10.1109/ICECT.2005.9

Summary: Security is becoming one of the most urgent challenges in database research and industry, and there has also been increasing interest in the problem of building accurate data mining models over aggregate data, while protecting privacy at the level of individual records. Instead of building walls around servers or hard drives, a protective layer of encryption is provided around specific sensitive data items or objects. This prevents outside attacks as well as infiltration from within the server itself. This also allows the security administrator to define which data stored in databases are sensitive and thereby focusing the protection only on the sensitive data, which in turn minimizes the delays or burdens on the system that may occur from other bulk encryption methods. Encryption can provide strong security for data at rest, but developing a database encryption strategy must take many factors into consideration. We present column-level database encryption as the only solution that is capable of protecting against external and internal threats, and at the same time meeting all regulatory requirements. We use the key concepts of security dictionary, type transparent cryptography and propose solutions on how to transparently store and search encrypted database fields. Different stored data encryption strategies are outlined, so you can decide the best practice for each situation, and each individual field in your database, to handle different security and operating requirements. Application code and database schemas are sensitive to changes in the data type and data length, the paper presents a policy driven solution that allows transparent data level encryption that does not change the data field type or length.

PCI 3.1 Keep cardholder data storage to a minimum.

PCI DSS Requirements	Testing Procedures
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	**3.1** Obtain and examine the company policies and procedures for data retention and disposal, and perform the following ▪ Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) ▪ Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data ▪ Verify that policies and procedures include coverage for all storage of cardholder data ▪ Verify that policies and procedures include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for a review, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements

PCI 3.2 Do not store sensitive authentication data

PCI DSS Requirements	Testing Procedures
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	**3.2** If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable. For each item of sensitive authentication data below, perform the following steps:
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* ▪ *The cardholder's name,* ▪ *Primary account number (PAN),* ▪ *Expiration date, and* ▪ *Service code* *To minimize risk, store only these data elements as needed for business.* *Note: See* PCI DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*	**3.2.1** For a sample of system components, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents

PCI 3.3 Mask PAN when displayed

PCI DSS Requirements	Testing Procedures
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. *Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.*	**3.2.2** For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: ▪ Incoming transaction data ▪ All logs (for example, transaction, history, debugging, error) ▪ History files ▪ Trace files ▪ Several database schemas ▪ Database contents
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Notes:* ▪ *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*	**3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.

PCI 3.4 Render PAN unreadable anywhere it is stored

PCI DSS Requirements	Testing Procedures
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN. *Notes:* ▪ *If for some reason, a company is unable render the PAN unreadable, refer to* Appendix B: Compensating Controls. ▪ *"Strong cryptography" is defined in* the PCI DSS Glossary of Terms, Abbreviations, and Acronyms.	**3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads, with the pads being securely stored ▪ Strong cryptography, with associated key-management processes and procedures
	3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).
	3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.
	3.4.d Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases).
	3.4.1.b Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).

PCI 3.5 Protect cryptographic keys

PCI DSS Requirements	Testing Procedures
not be tied to user accounts.	**3.4.1.c** Verify that cardholder data on removable media is encrypted wherever stored. *Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately.*
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:	**3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following:
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**3.5.1** Examine user access lists to verify that access to keys is restricted to very few custodians.
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	**3.5.2** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	**3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data. *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*
	3.6.b For service providers only: If the service provider shares keys with their customers for transmission of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely store and change customer's keys (used to transmit data between customer and service provider).
	3.6.c Examine the key-management procedures and perform the following:
3.6.1 Generation of strong cryptographic keys	**3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys.
3.6.2 Secure cryptographic key distribution	**3.6.2** Verify that key-management procedures are implemented to require secure key distribution.
3.6.3 Secure cryptographic key storage	**3.6.3** Verify that key-management procedures are implemented to require secure key storage.

PCI 3.6 Fully document and implement all key-management processes and procedures

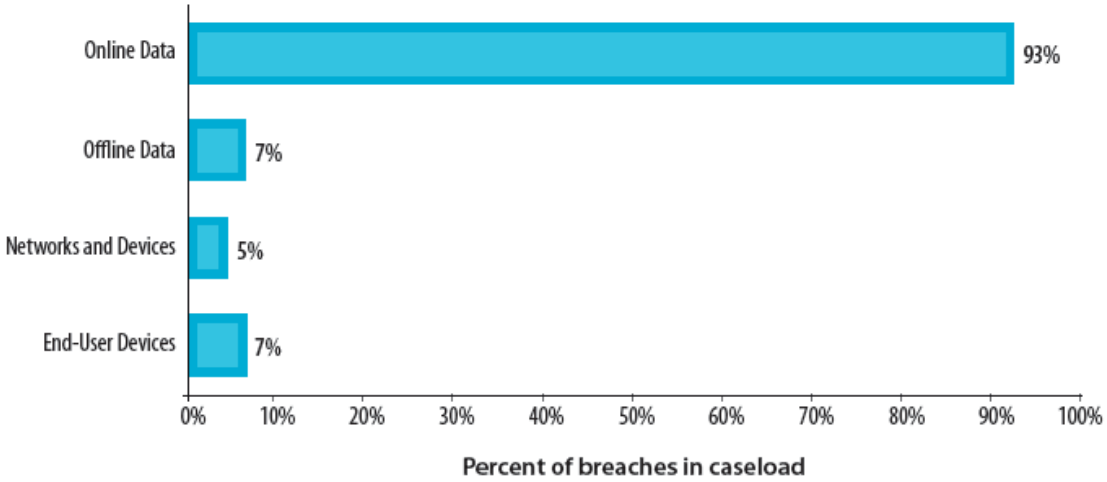
PCI DSS Requirements	Testing Procedures
3.6.4 Periodic cryptographic key changes ▪ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically ▪ At least annually	**3.6.4** Verify that key-management procedures are implemented to require periodic key changes at least annually.
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys	**3.6.5.a** Verify that key-management procedures are implemented to require the retirement of old keys (for example: archiving, destruction, and revocation as applicable).
	3.6.5.b Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys.
3.6.6 Split knowledge and establishment of dual control of cryptographic keys	**3.6.6** Verify that key-management procedures are implemented to require split knowledge and dual control of keys (for example, requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key).
3.6.7 Prevention of unauthorized substitution of cryptographic keys	**3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.
3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	**3.6.8** Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.

Online Exposure[2]

•Insider incidences were much larger in terms of the amount of data compromised.

•Hacking and malcode proved to be the attack method of choice among cybercriminals, targeting the application layer and data more than the operating system.

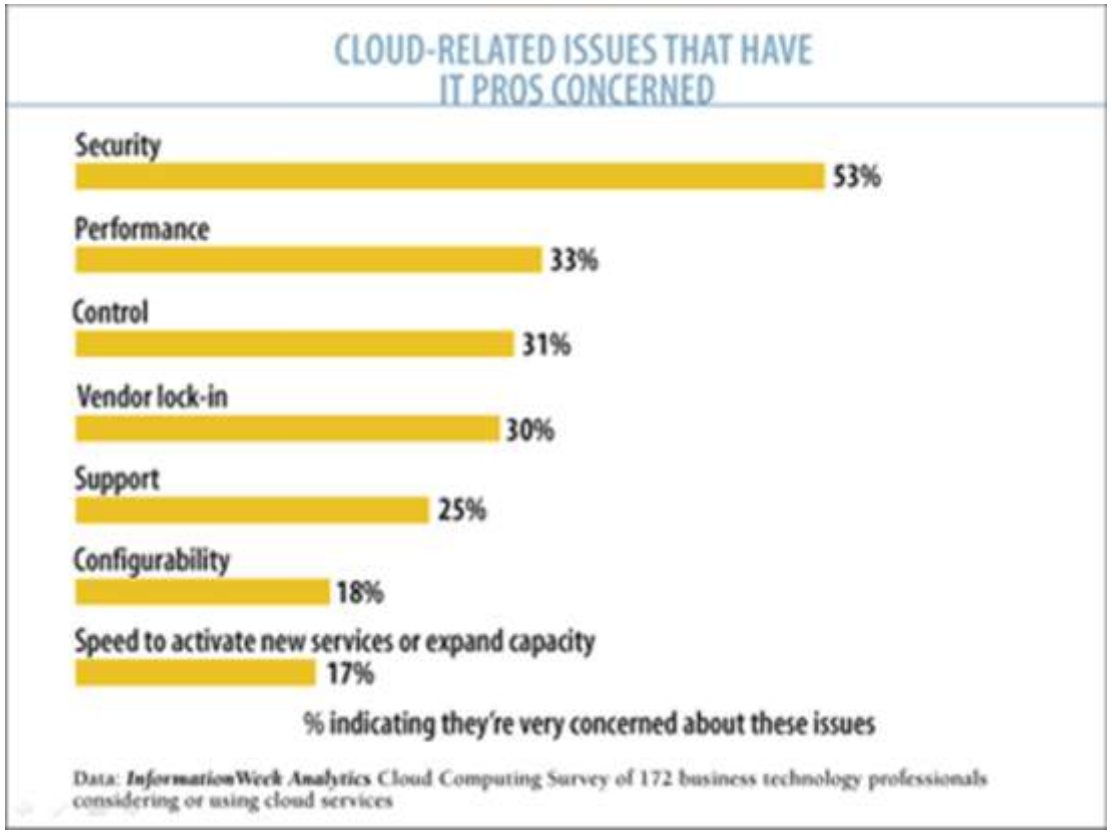
•The type of asset compromised most frequently (82%) is without doubt online data.
- •Compromises to online data repositories were seen in more cases than all other asset classes combined by a ratio of nearly five to one.
- •Offline data, networks, and end-user devices were all closely grouped.



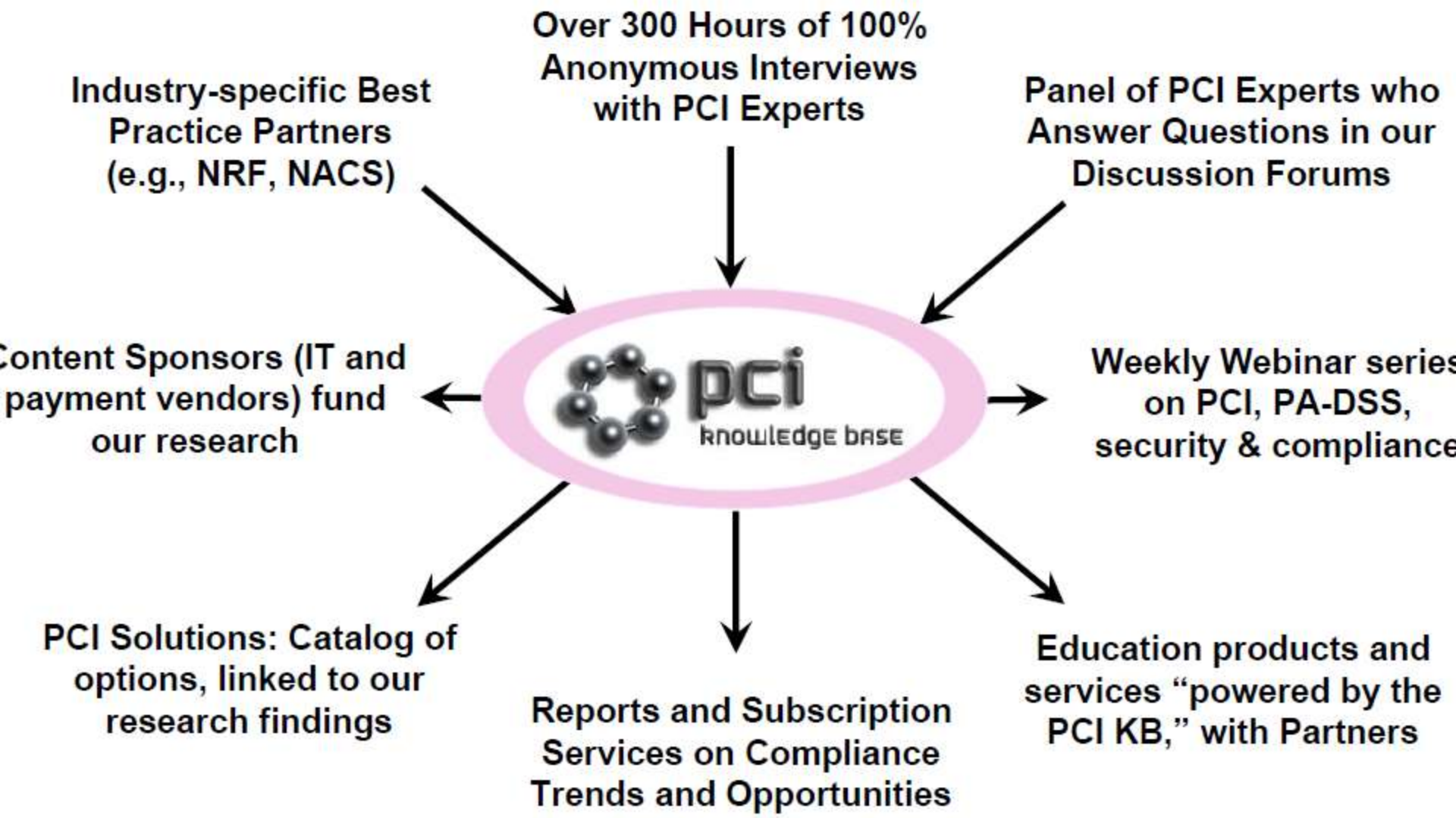
[2]*Slide source: Verizon Business 2008 Data Breach Investigations Report*

Cloud Services

Why aren't enterprises falling all over themselves to buy and use cloud services? Is it risk aversion? Is it a lack of confidence in the service providers? Is it just another version of the insource/outsource debate? Or is it something else more fundamental as discussed at http://www.internetevolution.com/document.asp?doc_id=170782&image_number=1

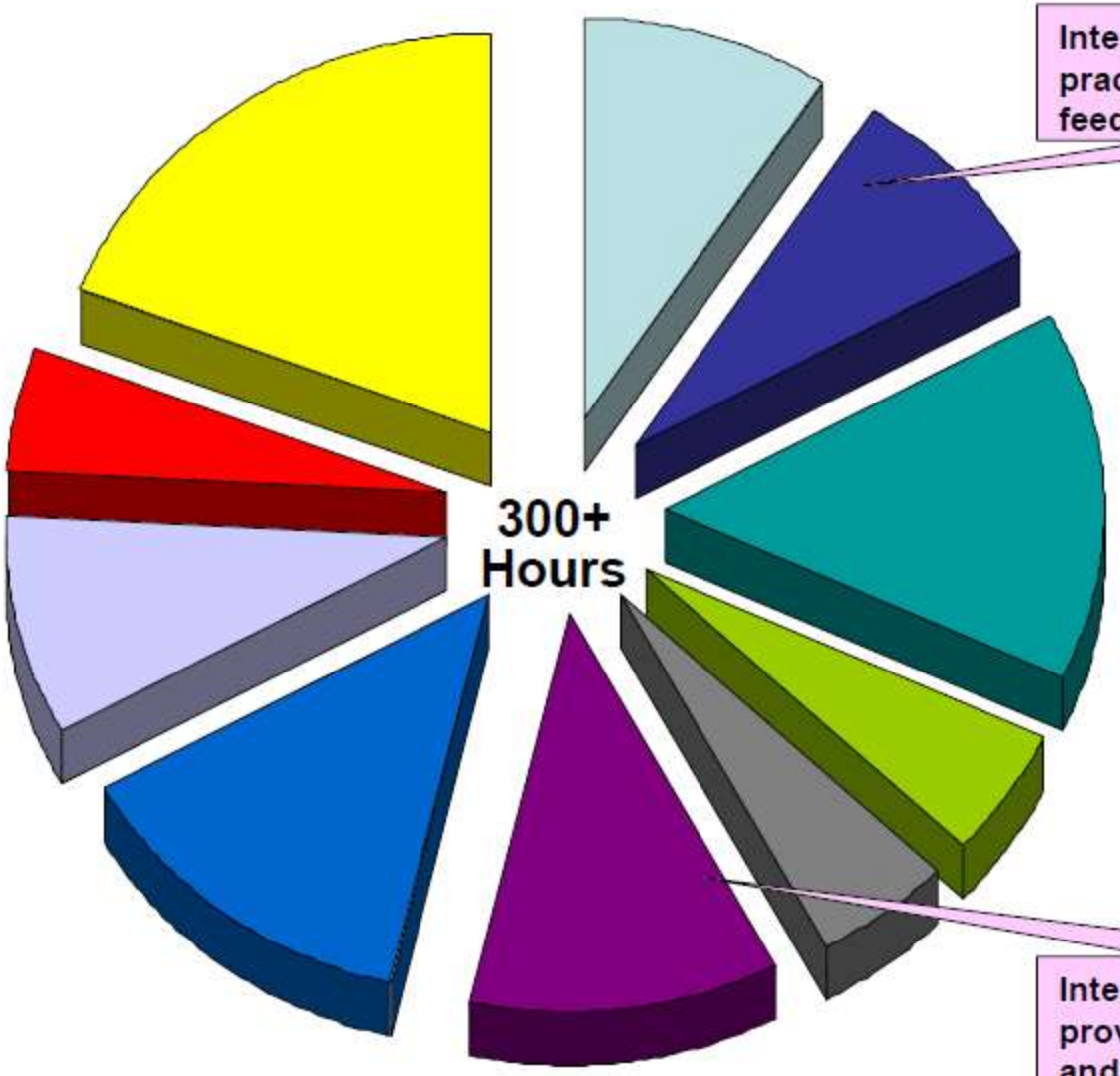


What is The PCI Knowledge Base?



Source: PCI Knowledge Base, March 2009

Based on Over 300 Hours of 100% Anonymous Interviews – Not a Sur



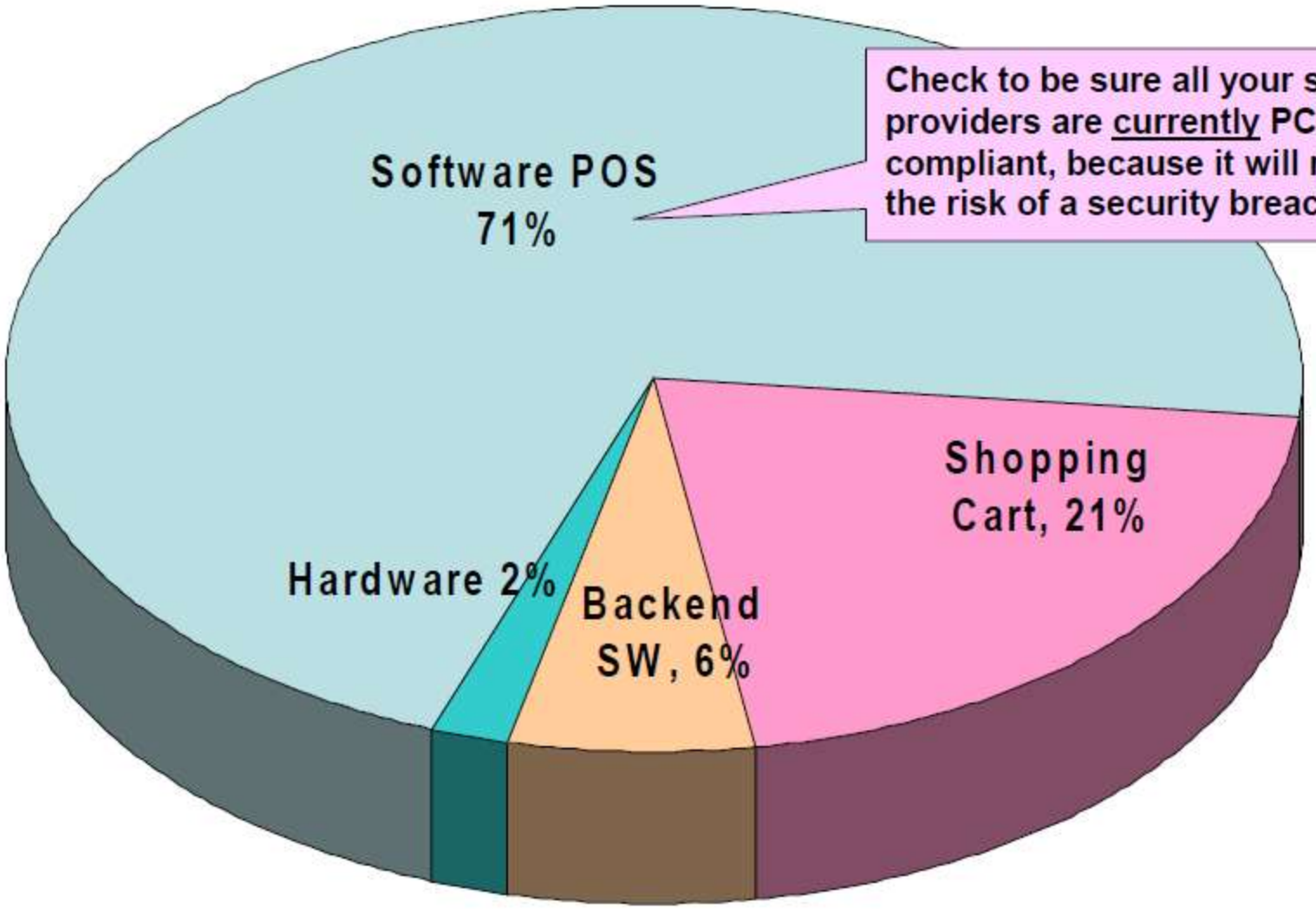
Interviews with merchants focus on bes
practices, experiences, QSA and vendo
feedback, budgets and priorities.

- F1000 Retailers
- SME Retailers
- QSAs
- Payment Processors
- Banks
- Retail Consultants
- IT Providers
- E-Comm Retailers
- Hospitality
- Other Merchants

Interviews with QSAs, consultants and
providers focused on vulnerabilities, ris
and technology adoption trends.

Source: PCI Knowledge Base, January 2

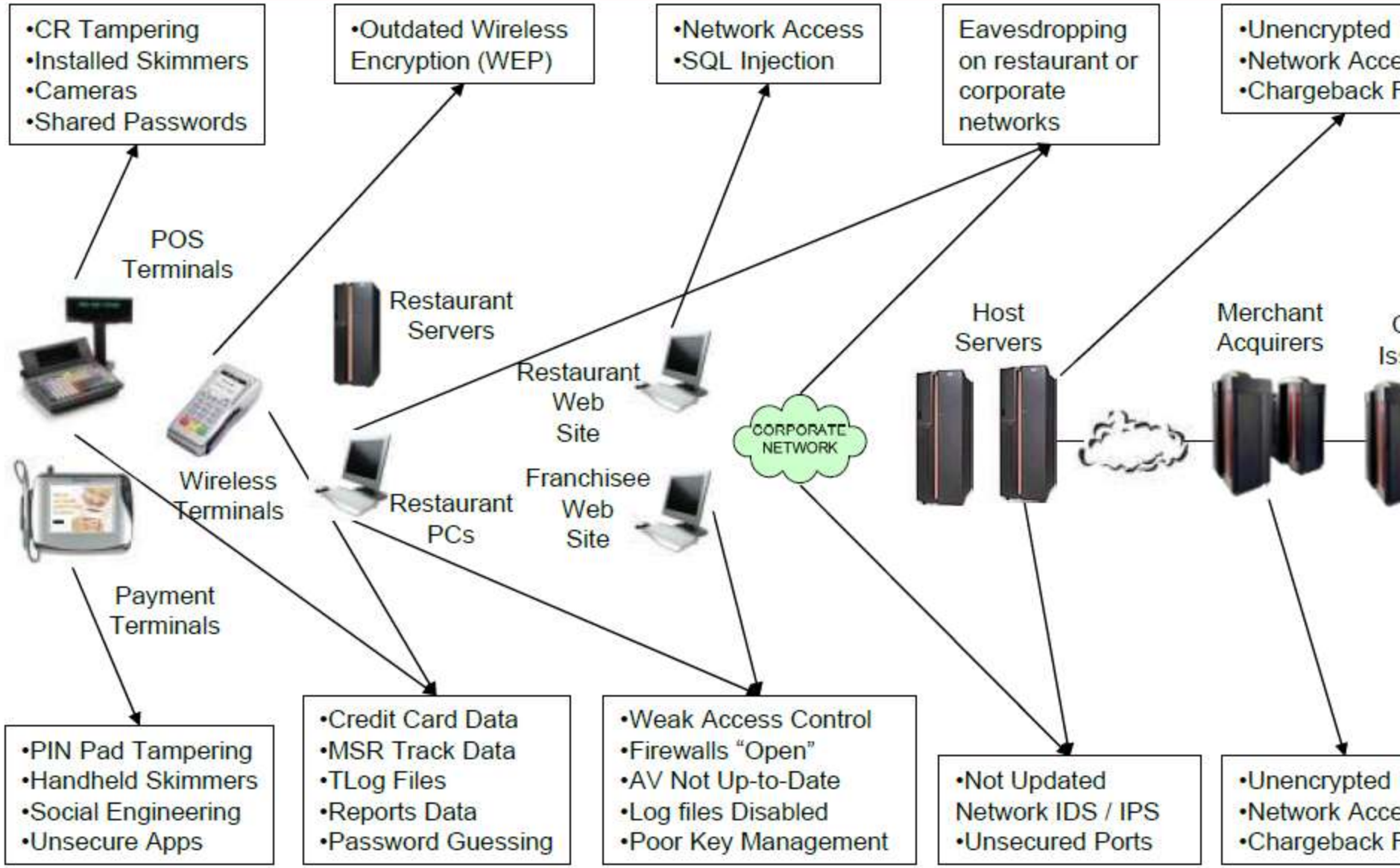
Over 90% of Retail Security Breaches Due to SW POS or Shopping C



Check to be sure all your service providers are currently PCI compliant, because it will reduce the risk of a security breach.

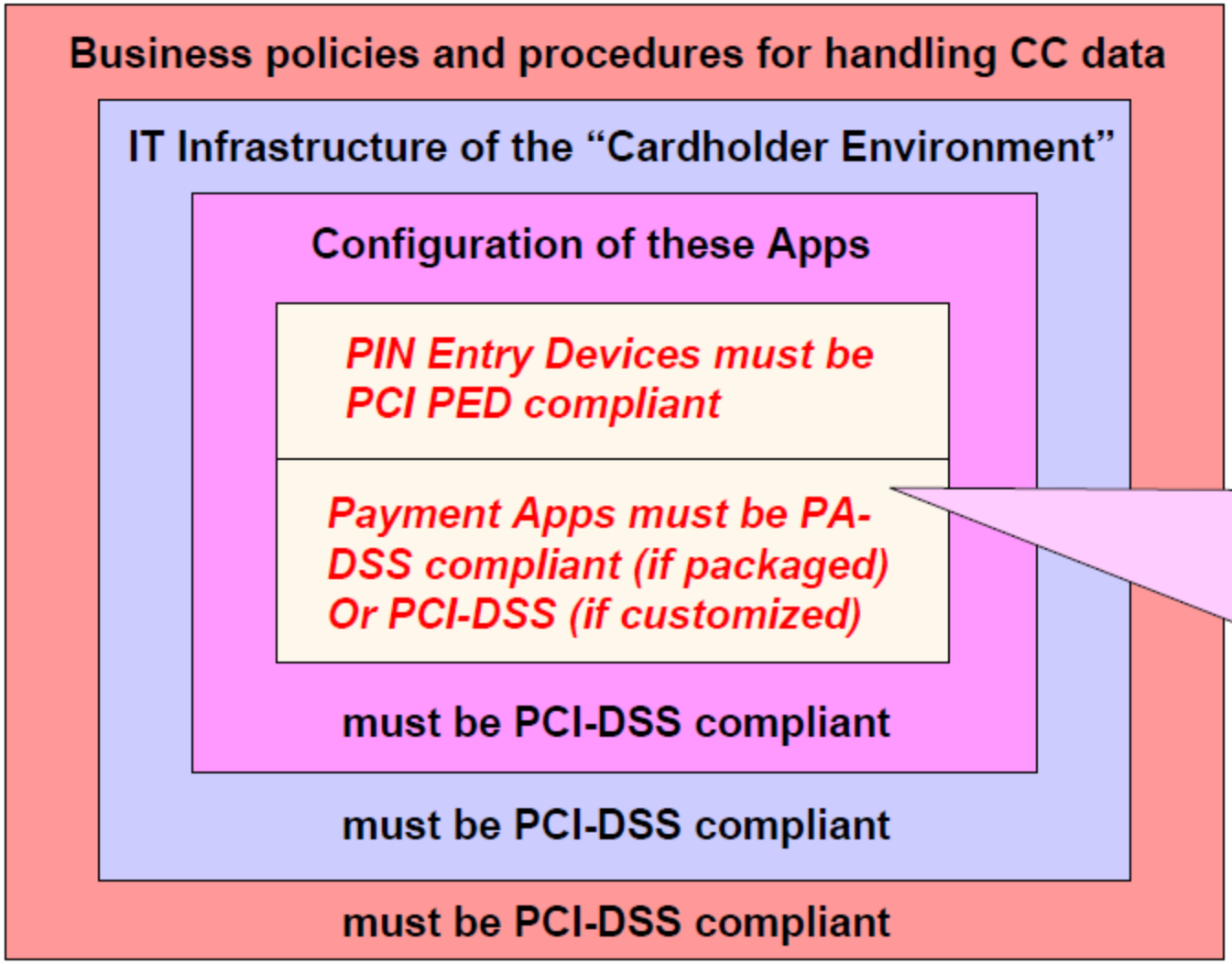
Source: Verifone, 2008

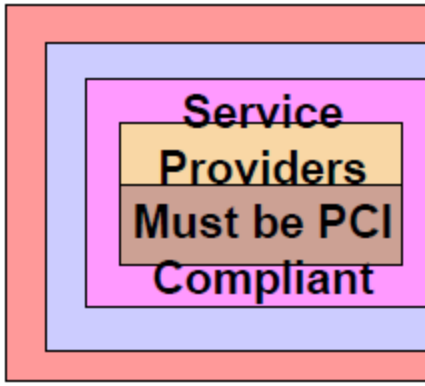
Show Common Brick & Mortar and E-Commerce Security Vulnerabilit



Source: Adapted from Verifone, 2008

PCI is Not Just About POS – It's Affects the Entire Company, and Mo





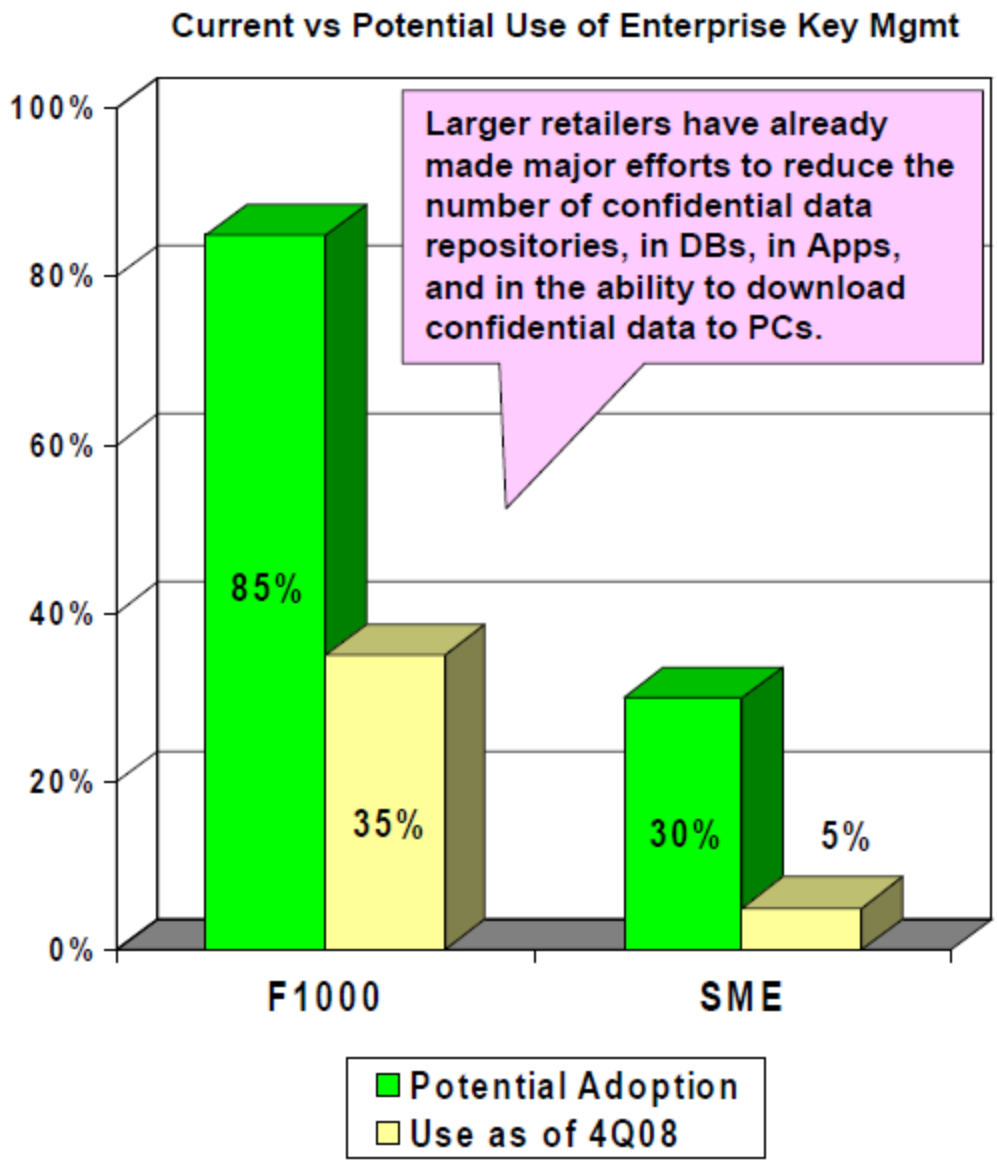
Running fully compliant apps does not make the whole company compli

The "new standards" a PA-DSS and PCI PED. Most firms do not yet comply with them.

The "multi-level" proce makes "outsourcing PC complex proposition.

Source: PCI Knowledge Base, March 2

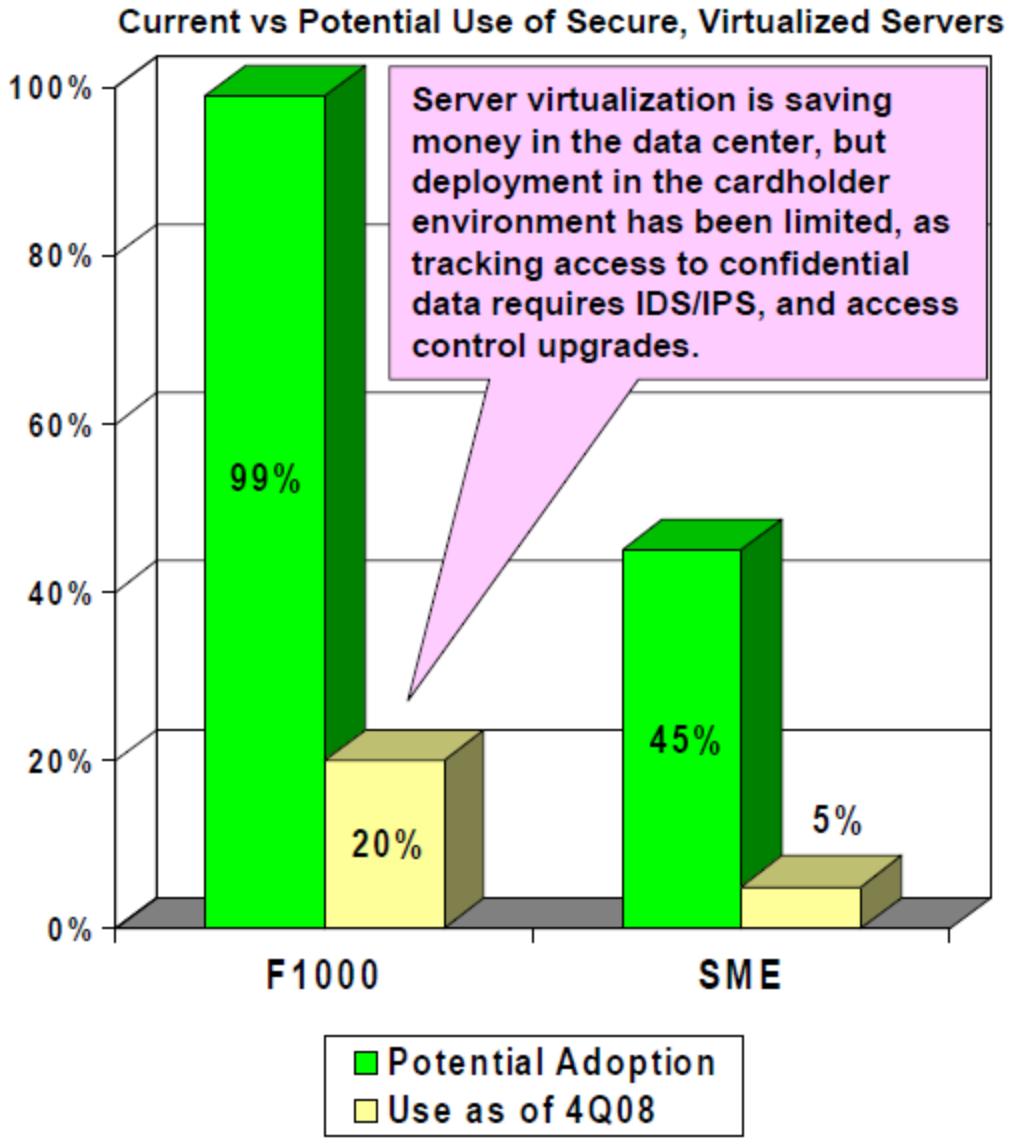
Implement Enterprise Key Management for Needed Confidential Dat



Best Practice Description	Implement a centralized, automated management process for encryption keys, particularly if the encryption ke are native to each application, OS, o DB. This is the best way to effectivel meet the split knowledge and key rotation requirements of PCI without major outages.
Level of Investment	$25,000 – 125,000, or more, fo enterprise key management.
Potential Savings	$50,000 – 200,000 if implement after a QSA finds a problem an recommends a different tool.
Best for	F1000 retailers who have data t encrypt across multiple systems where the data is handed off.
Primary Dept Owner	IT Infrastructure
PCI Reqmts Met	3.6

Source: PCI Knowledge Base, January 2

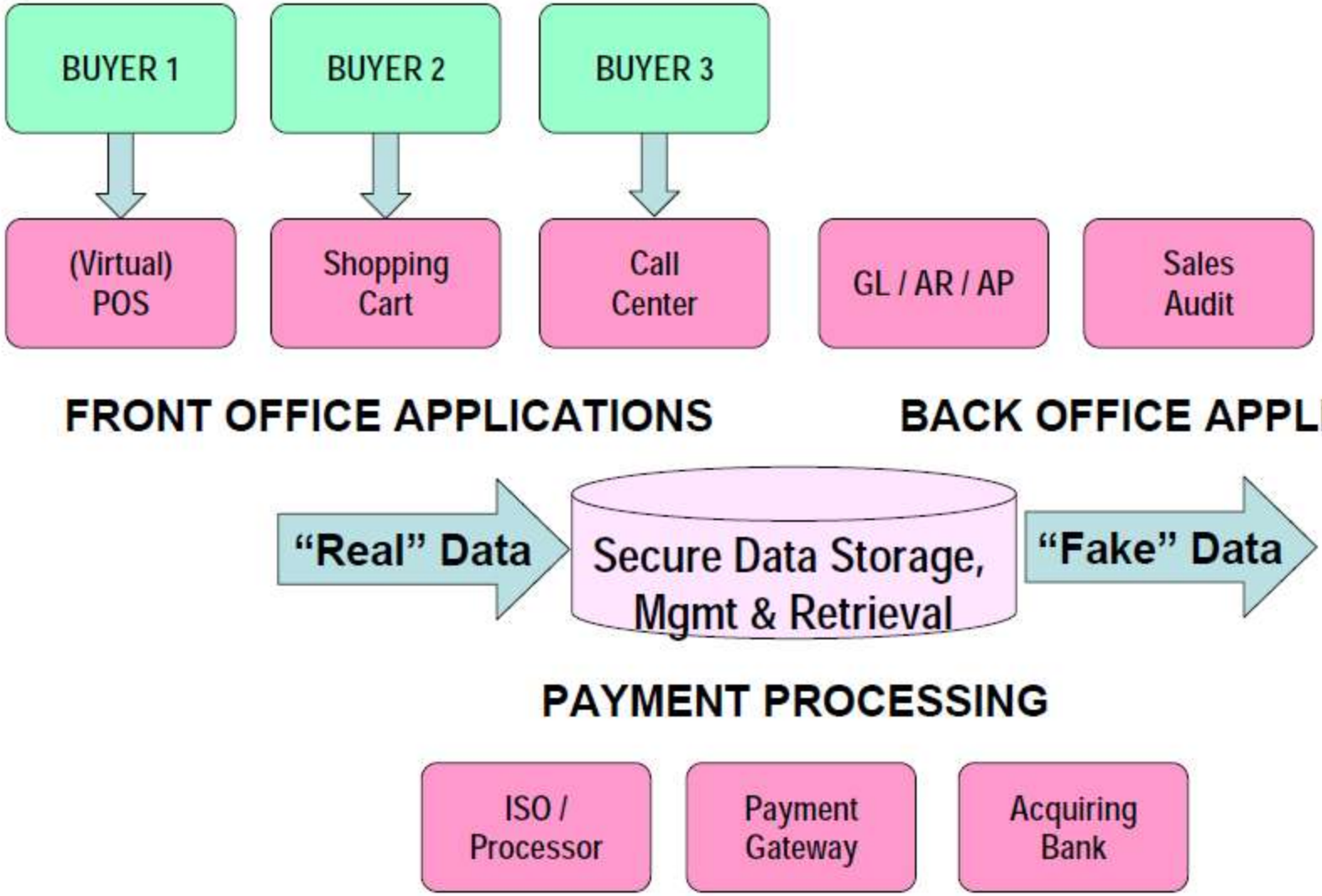
Upgrade Access Controls To Secure Virtualized Servers



Best Practice Description	Ensure that as you implement server desktop virtualization in the cardholde environment and for other servers wit confidential data that intrusion and access controls have been upgraded enable tracking of individual access t confidential data.
Level of Investment	$10K – 40K, for security control upgrades, but this increases as servers protected increases.
Potential Savings	$10K – 50K, primarily on manua tracking, monitoring, but some savings on PCI audit, through better reporting tools.
Best for	Larger companies.
Primary Dept Owner	IT Infrastructure and application
PCI Reqmts Met	2.2.1

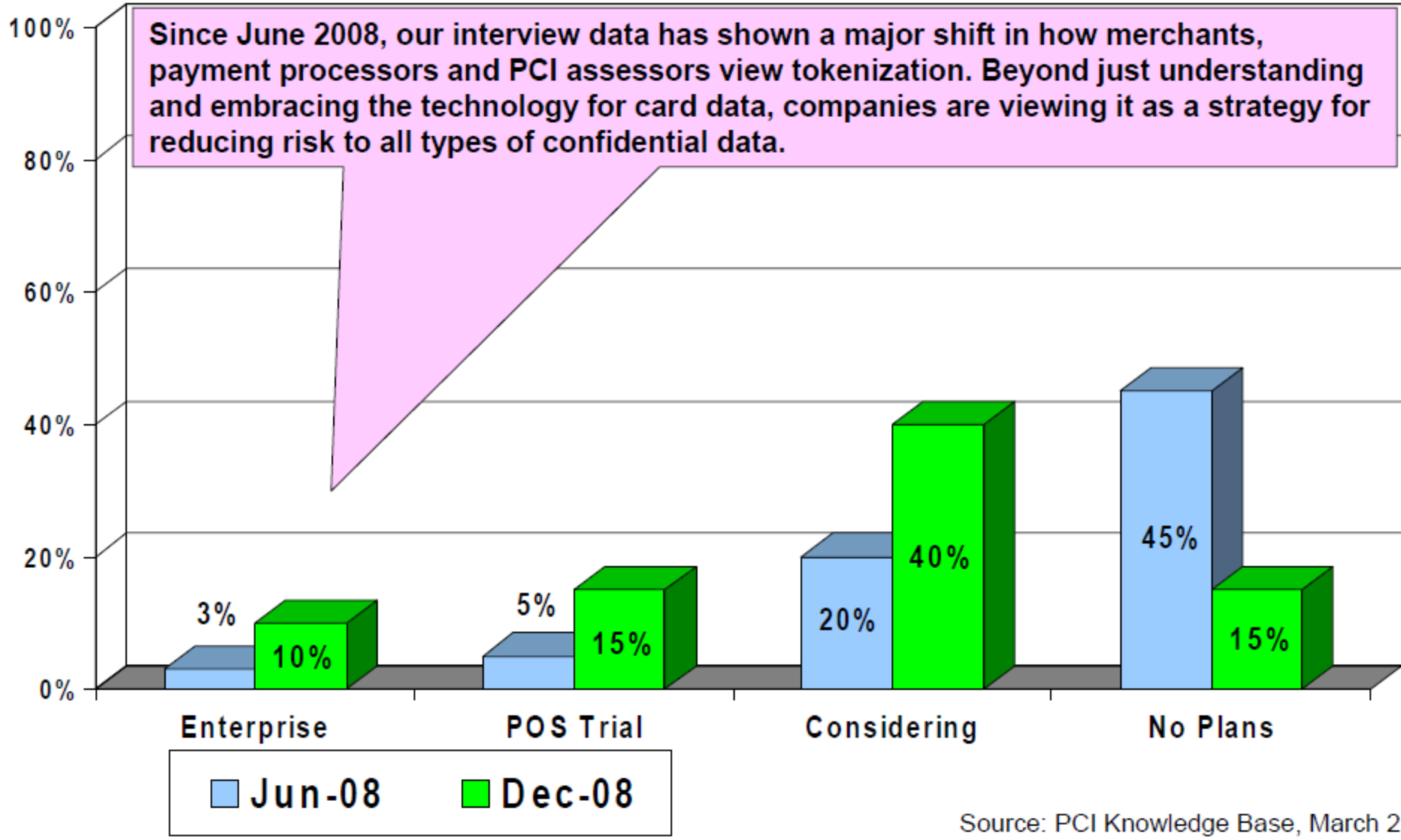
Source: PCI Knowledge Base, March 2

Tokenization: Reduce Scope via Data Centralization & Outsourcing



Source: PCI Knowledge Base, March

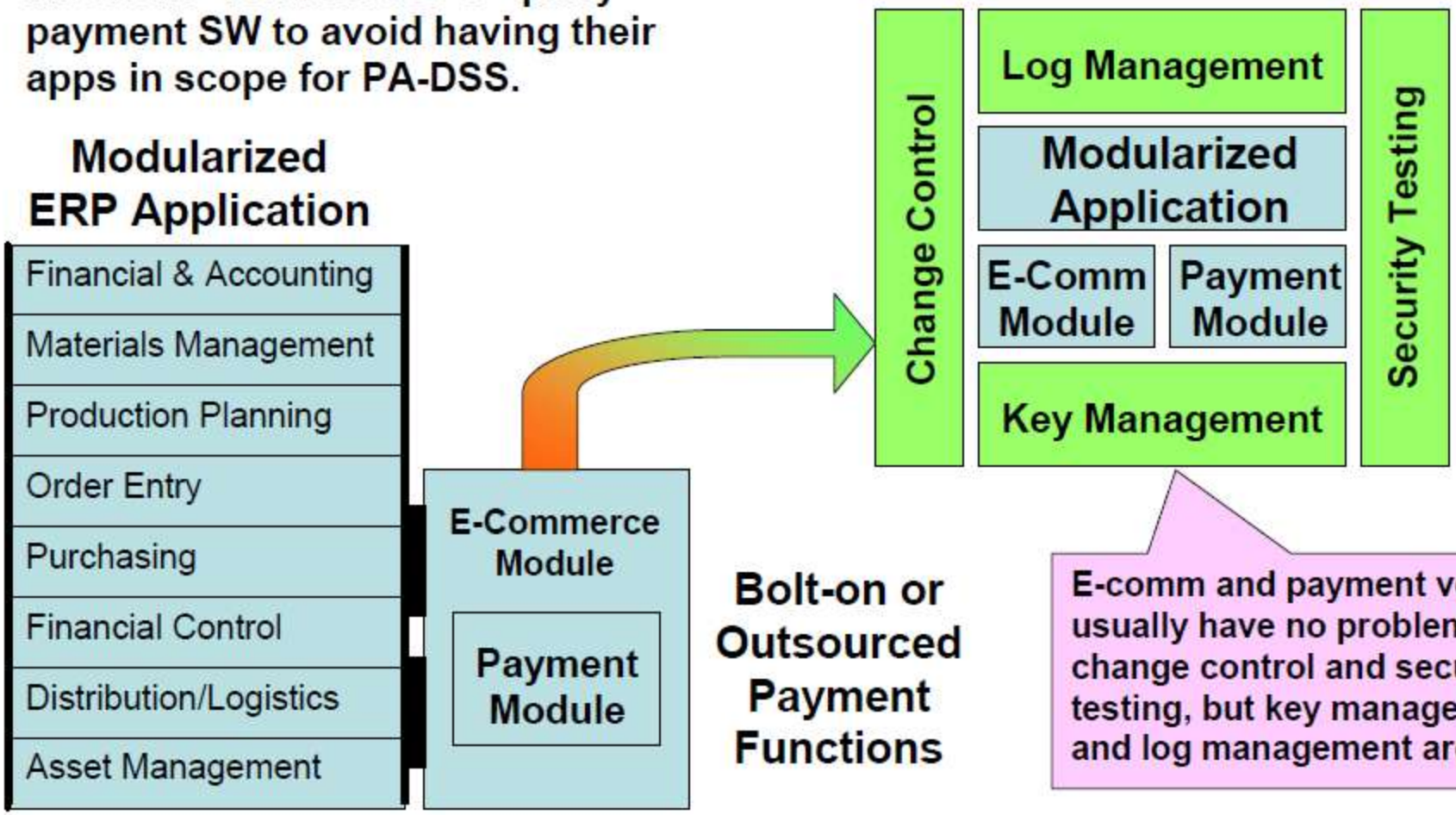
Trend: Major Shift in Favor of Tokenization as Enterprise Strategy



Source: PCI Knowledge Base, March 2

Manage the Impact of PCI & PA-DSS on POS, ERP, CRM and SaaS Ap

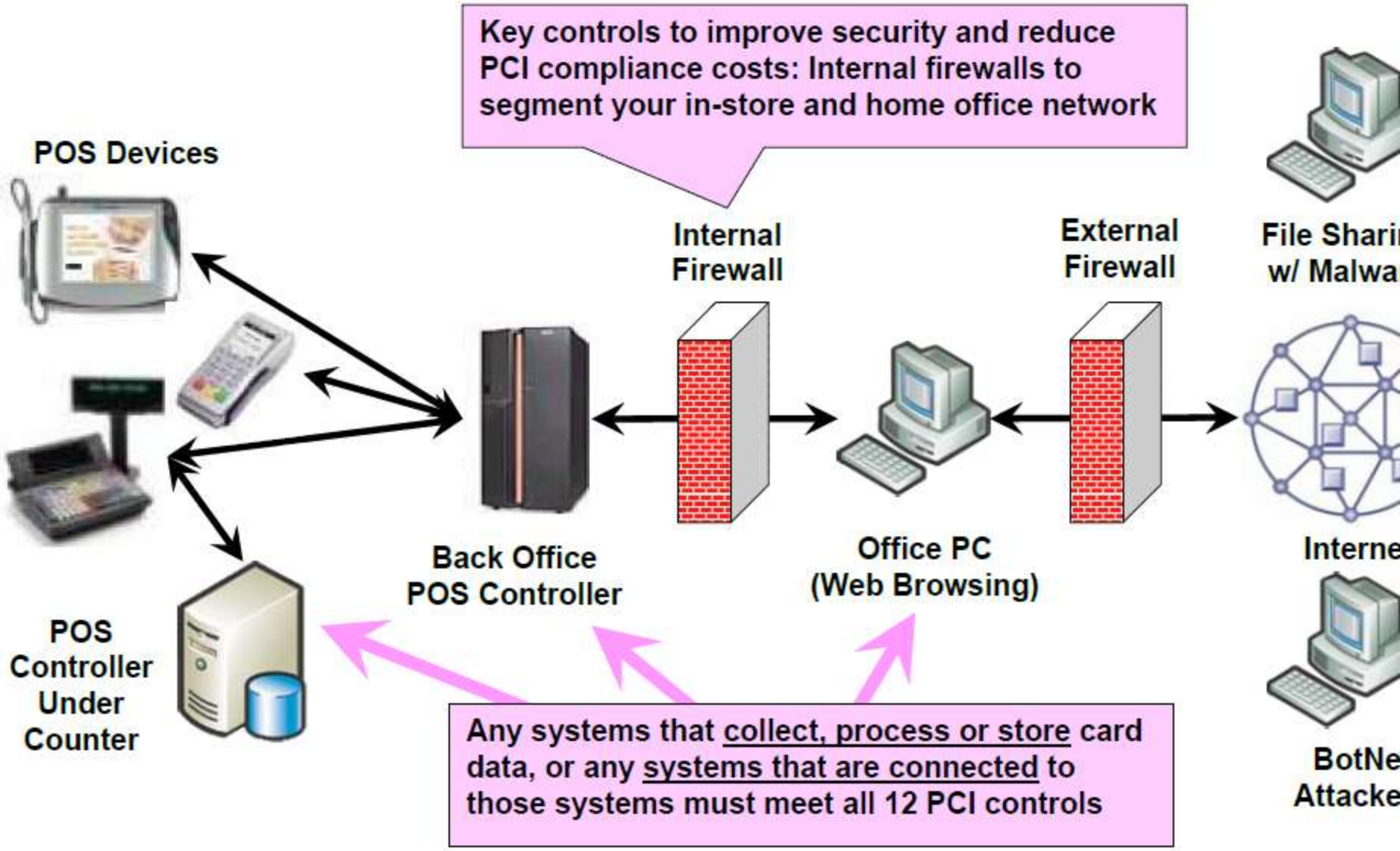
Most ERP vendors use 3rd party payment SW to avoid having their apps in scope for PA-DSS.



Vendors affected: Payment providers to SAP, Oracle Apps, Infor Global, Sage, Microsoft Dynamics, Lawson, Epicor, QAD

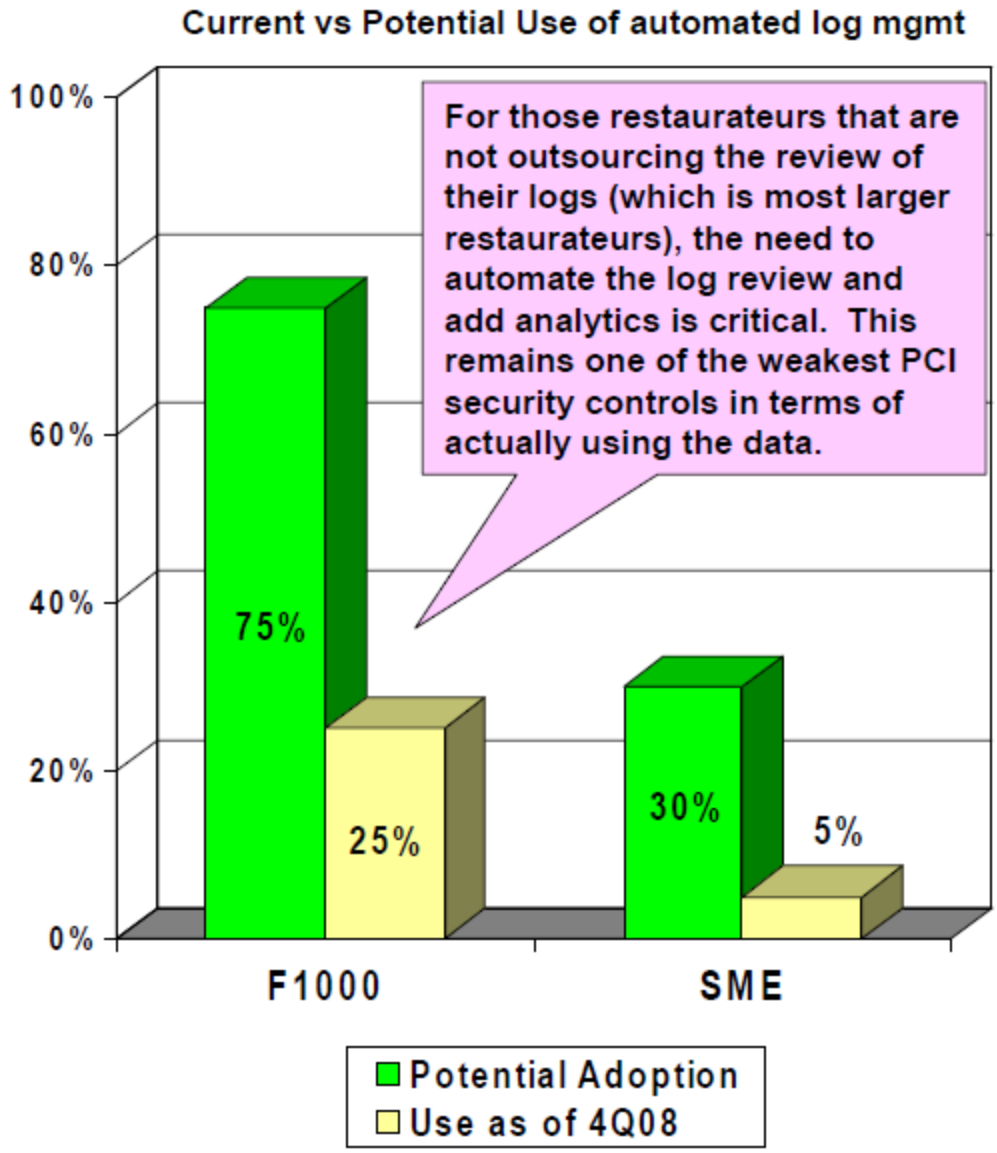
Source: PCI Knowledge Base, November 2

Best Practice: Segment Network Against Downloaded Malware



Source: PCI Knowledge Base, November 2008

Automate Log Management and Integrate with SIM Analytics



Best Practice Description	Develop a centralized log manageme and analysis process. Replace manu log reviews with automated tools. SI tools can be justified based on improved visibility and responsivenes to potential security breaches. Inclu logs from both the wired and the wireless environments.
Level of Investment	$10,000 – 25,000 for projects, depending on size & complexity
Potential Savings	$20,000 – 200,000 in reduced assessment costs and security control cost avoidance costs.
Best for	F1000 restaurateurs who canno segment networks and have ca data throughout the enterprise.
Primary Dept Owner	Network management, with support from IT Infrastructure.
PCI Reqmts Met	1, 10, 11

Source: PCI Knowledge Base, March 2

Where is the PCI Knowledge Base (www.KnowPCI.com)?