New York Oracle Users Group, Inc.

NYOUG

Understanding New Options in Data Protection for the Data Warehouse Environment

Ulf Mattsson, CTO, Protegrity Corporation

Special Joint BI/DW & Web SIG Meeting

February 3, 2010

Agenda

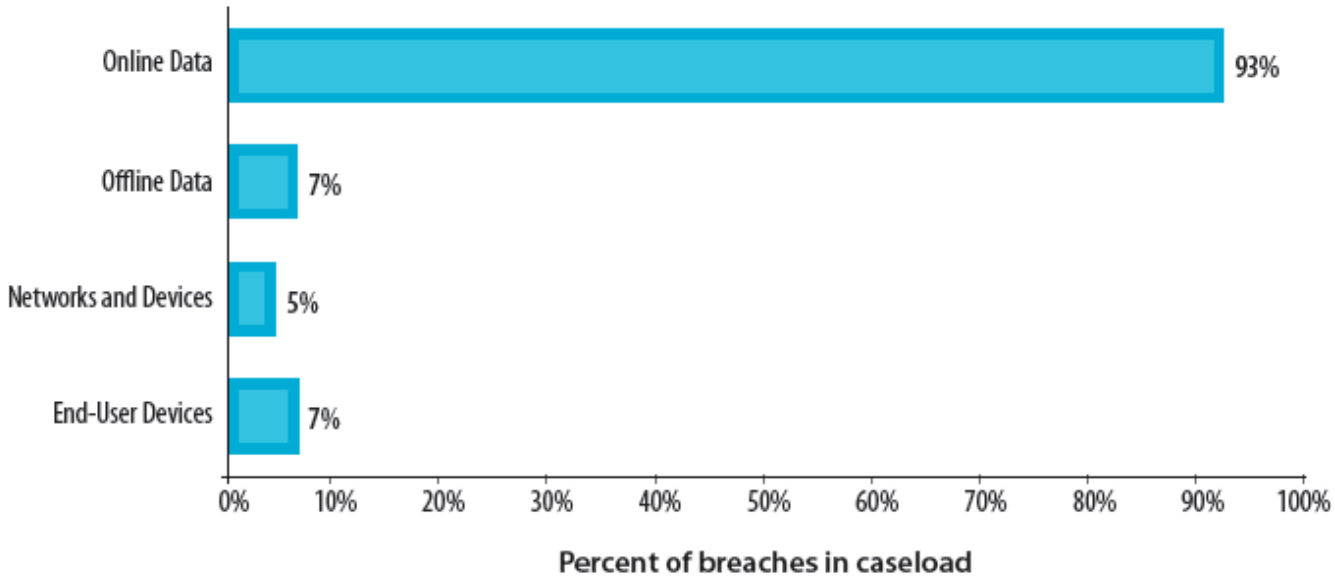
- Attacks on databases
- Different data protection technologies being marketed today
  - Do they offer the same levels of protection?
  - What risks to data exist in the different schemes?
  - How can a company decide between competing encryption technologies?
- Review the latest methodologies and technologies, such as
  - Type Preserving Encryption, Data Masking, Tokenization and Database Activity Monitoring
- Focused on answering the question
  - "How can IT security professionals provide data protection in the most cost effective manner in an Oracle environment?"

Data
Under Attacked

Online Data Under Attack – Not Laptops or Backup

Breaches attributed to insiders are much larger than those caused by outsiders

The type of asset compromised most frequently is online data:



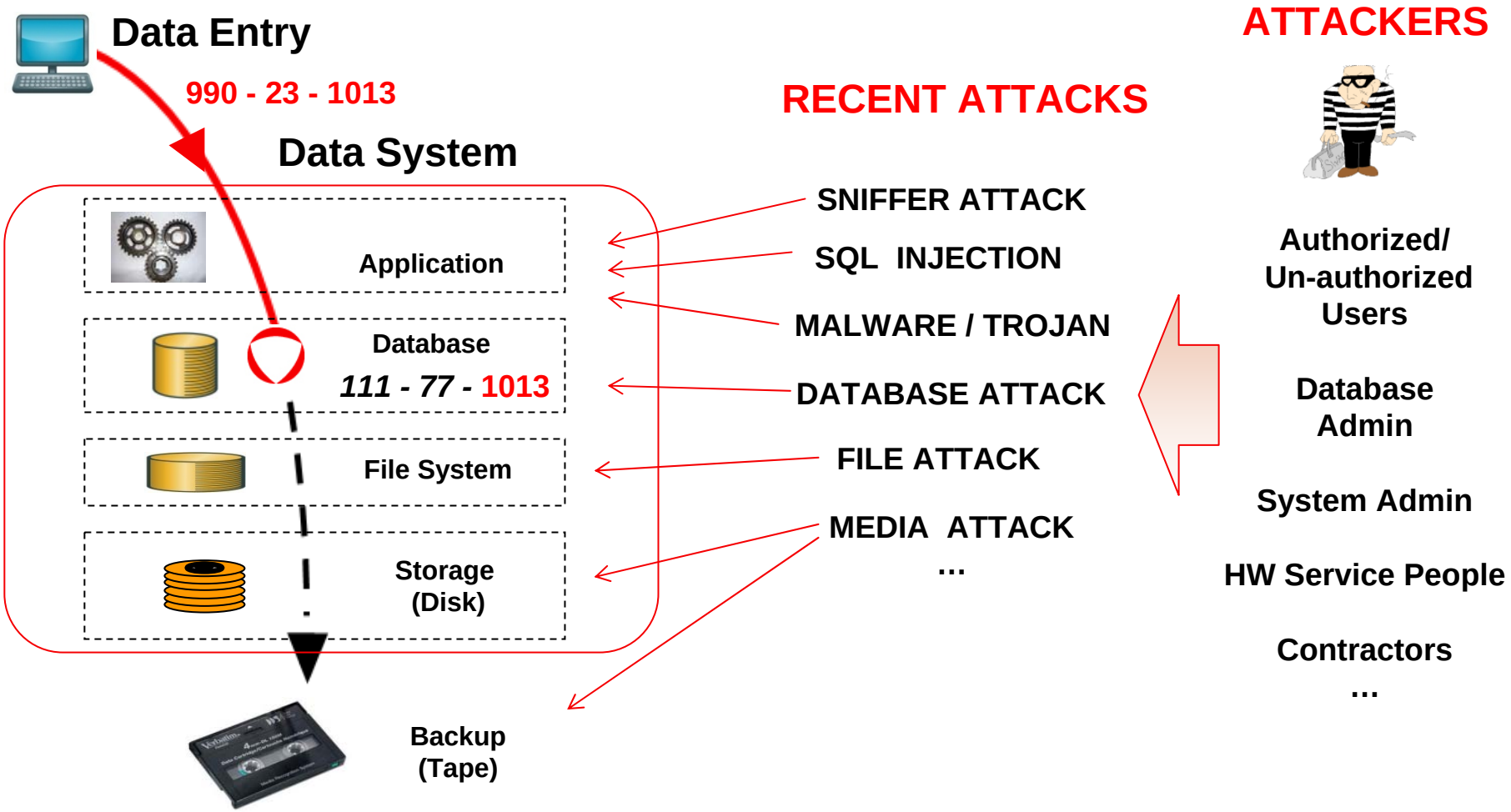
87% of breaches could have been avoided through reasonable controls

Slide source: Verizon Business 2008 Data Breach Investigations Report

protegrity

Choose Your Defenses

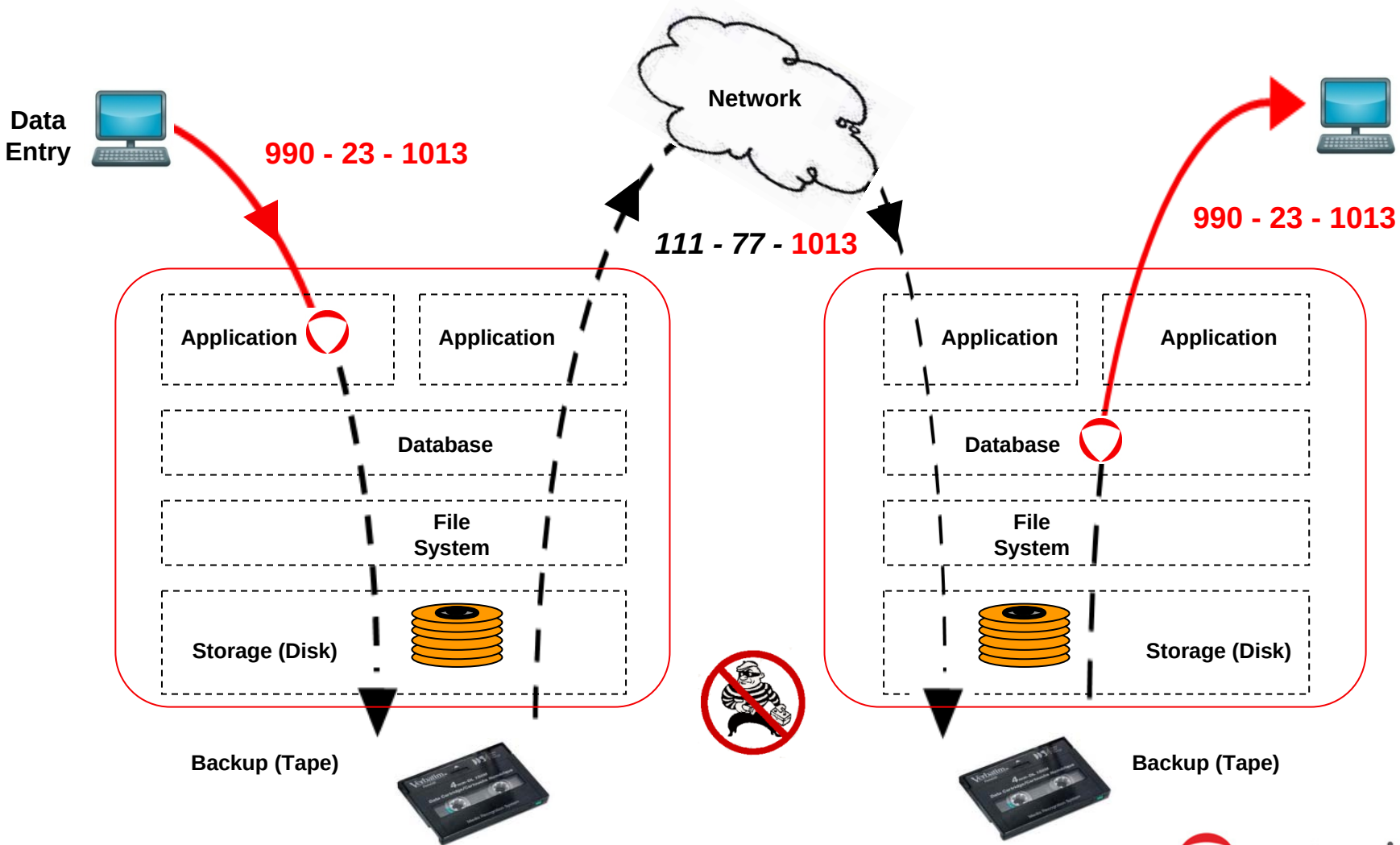
Where is data exposed to attacks?



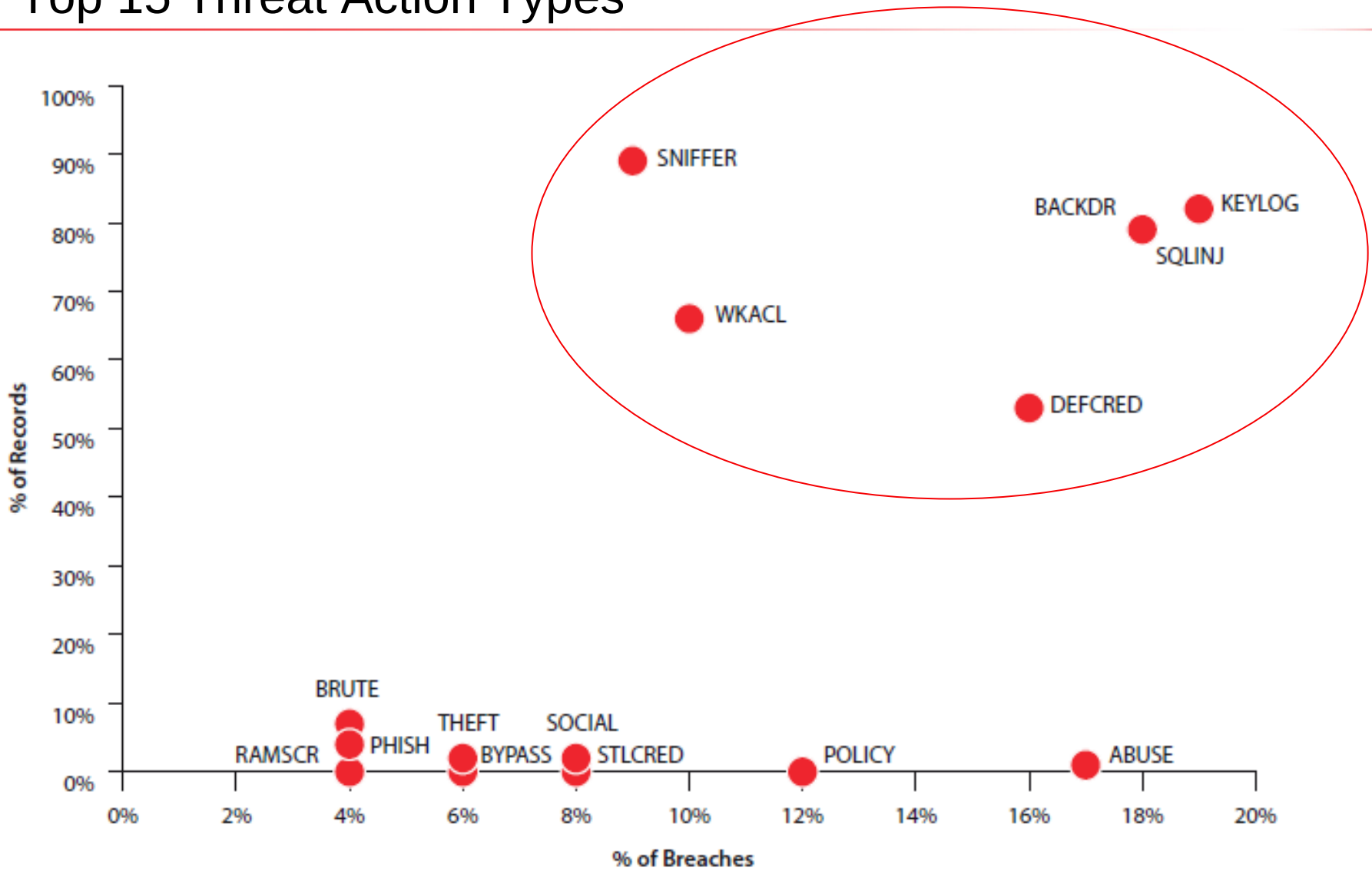
protegrity

Choose Your Defenses – Protect the Data Flow

Mitigation at the Right System Layer



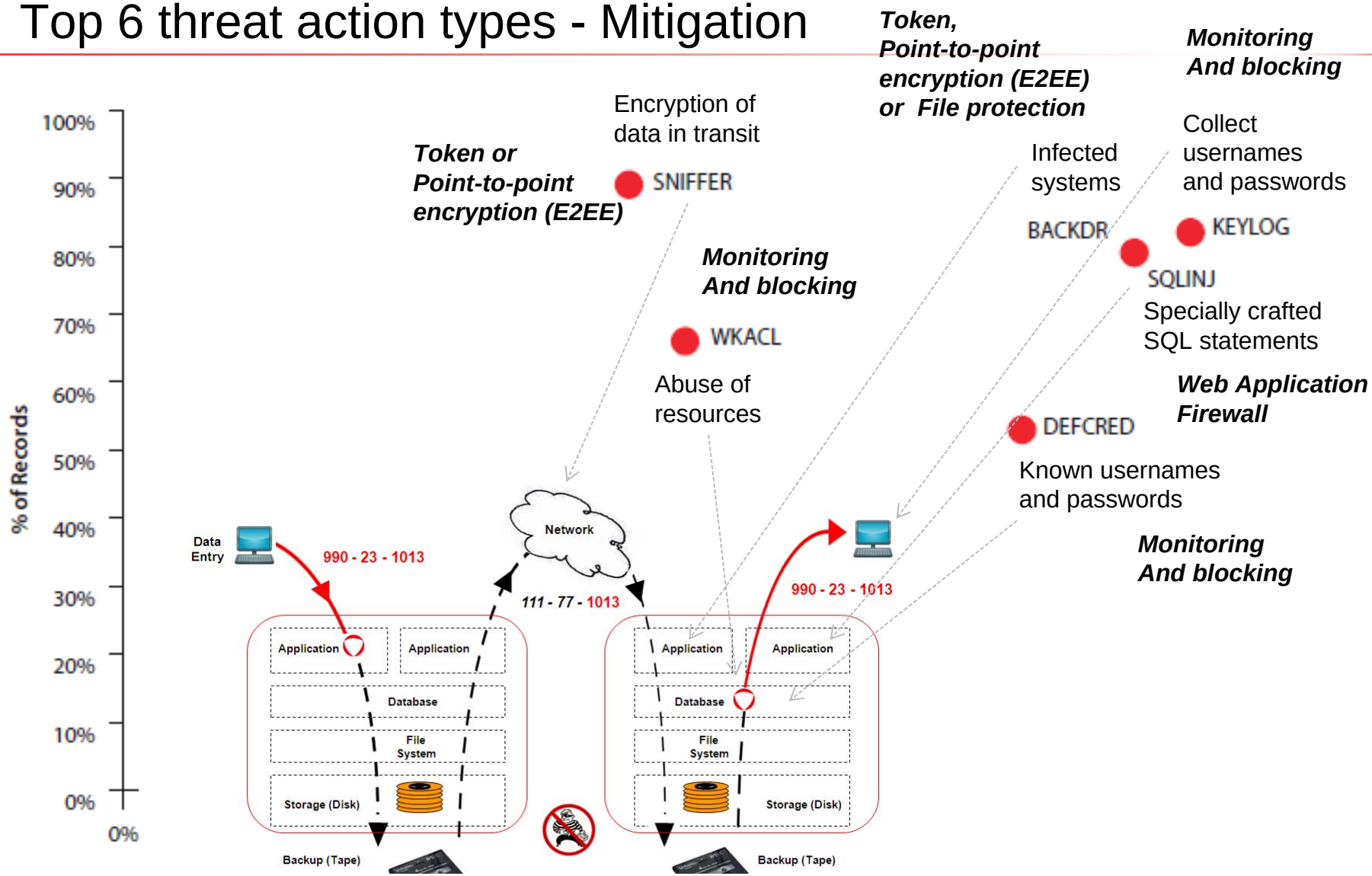
Top 15 Threat Action Types



Source: 2009 Data Breach Investigations Supplemental Report, Verizon Business RISK team

protegrity

Top 6 threat action types - Mitigation



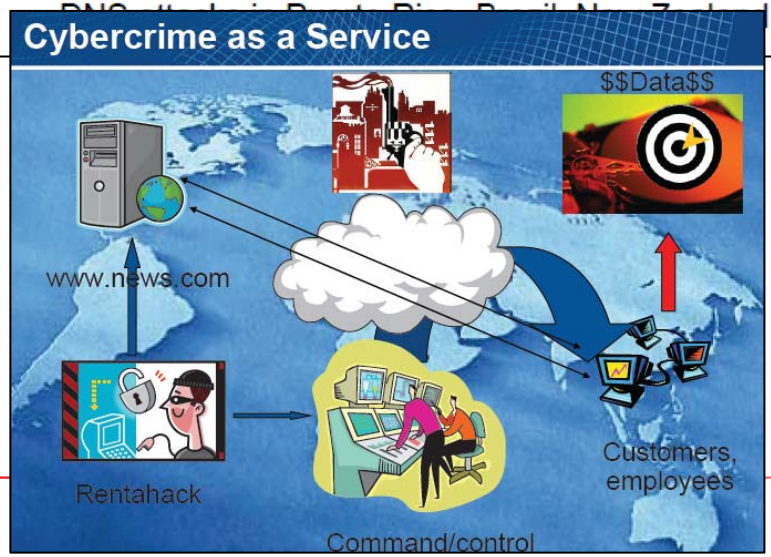
Source: 2009 Data Breach Investigations Supplemental Report, Verizon Business RISK team

protegrity

The Gartner 2010 CyberThreat Landscape

- Latest "largest ever" — Heartland Payment Systems
- DoD Bans USB after trojan on thumb drive
- Security incidents rise 24.7% at educational institutes
- Conficker hits medical machinery
- Worms hit Twitter, Facebook, LinkedIn, MySpace
- "Chinese attackers" steal jet fighter data

, U.S.

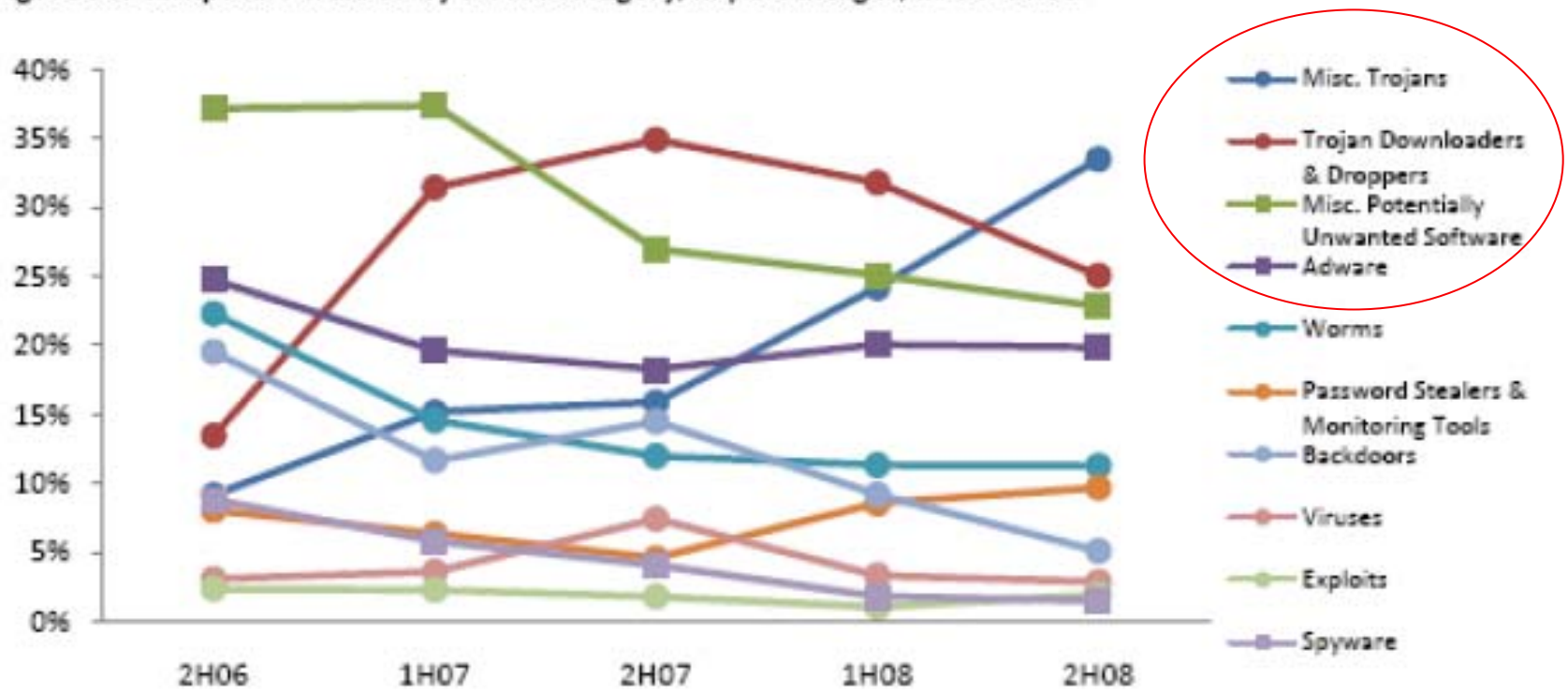


The Aha Slide

- We have met the threat and they are us.
  - New processes
  - New technologies
  - Complacency
- You need very different armor to survive a sniper's rifle shot than you do for a hailstorm.
- Threats will always change faster than user behavior

Targeted Threat Growth

Figure 16. Computers cleaned by threat category, in percentages, 2H06–2H08

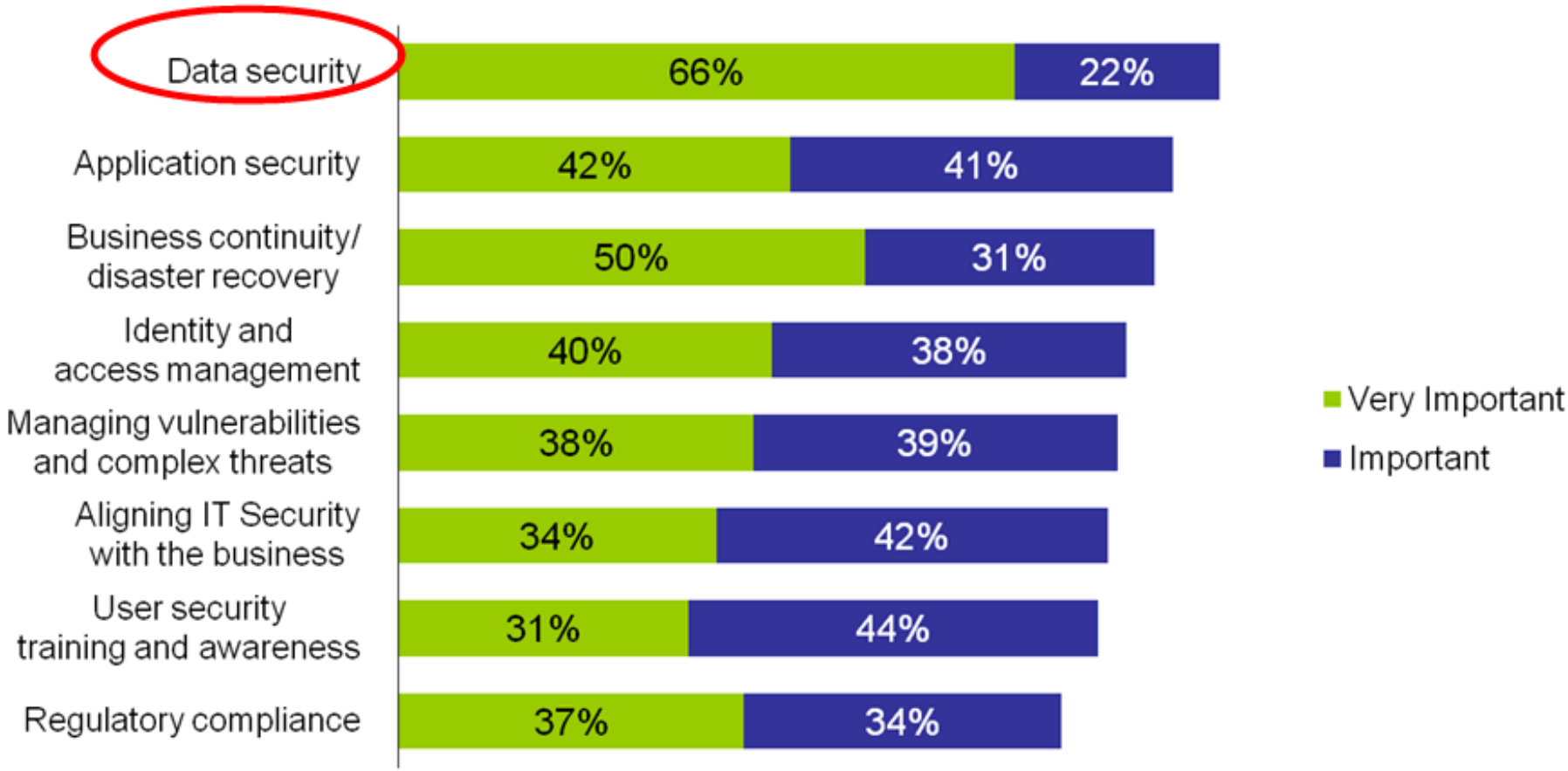


Source: Microsoft Malicious Software Removal Tool disinfections by category, 2H06–2H08'

Gartner.

Data security remains important for most

"How important to your IT security organization will each of the following issues be in the next 12 months?"



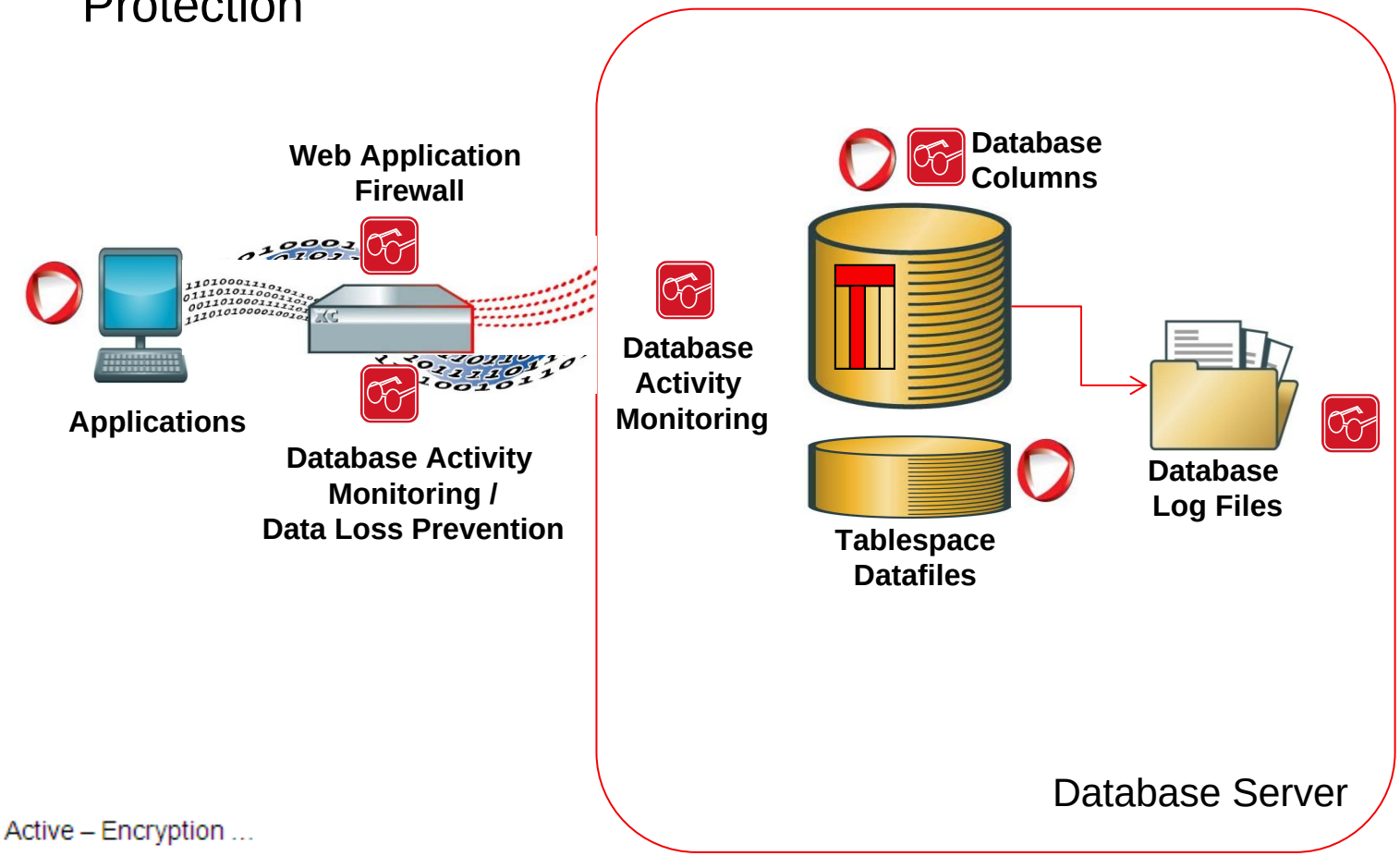
Base: 1,782 North American and European enterprise and SMB decision-makers responsible for IT security

Different Data Protection Approaches - High Level

protegrity

Protecting Data in the Enterprise Data Flow

Passive Approaches and Active Approaches = End-To-End Protection



Active – Encryption …

Passive – Monitoring …

protegrity

Data Protection Options – Passive Methods

Monitoring, Blocking & Masking

Application

Application Database or File

Server

Log Files

Blocking/ Masking

Example of Masked user output:

XXXX XXXX XXXX **4560**

protegrity

Monitoring

- Monitor Access without Encryption
  - Reporting and alerting
  - Can Block or Mask based on Policy
- Advantages
  - Low impact on existing applications
  - Performance
  - Time to deploy
- Considerations
  - Underlying data exposed
  - PCI aspects

Is DAM, DLP and WAF Cost Effective for PCI?

Technologies in ascending order by average cost effectiveness rating	Pct%*
Firewalls	82%
Anti-virus & anti-malware solutions	74%
Encryption for data at rest	74%
Encryption for data in motion	71%
Access governance systems	64%
Identity & access management systems	63%
Web application firewalls (WAF)	55%
Correlation or event management systems	55%
Endpoint encryption solution	46%
Data loss prevention systems	43%
Code review	36%
Traffic intelligence systems	32%
Virtual privacy network (VPN)	26%
Intrusion detection or prevention systems	22%
Database scanning and monitoring	18%
ID & credentialing system	11%
Website sniffer or crawlers	7%
Perimeter or location surveillance systems	3%
Average	43%

*Pct% defines the average percentage of respondents rating the technology as highly cost effective.

Encryption 74%

WAF 55%

DLP 43%

DAM 18%

Source: 2009 PCI DSS Compliance Survey, Ponemon Institute

protegrity

Passive Database Protection Approaches

Operational Impact Profile

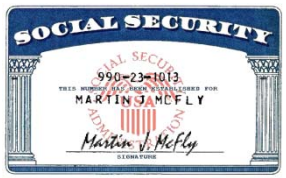
Database Protection Approach	Performance	Storage	Security	Transparency	Separation of Duties
Web Application Firewall	●	●	◔	●	○
Data Loss Prevention	●	●	◔	●	○
Database Activity Monitoring	●	●	◔	●	○
Database Log Mining	◔	●	○	●	○

Best ● ◕ ◔ ◒ ◔ ◔ ○ Worst

protegrity

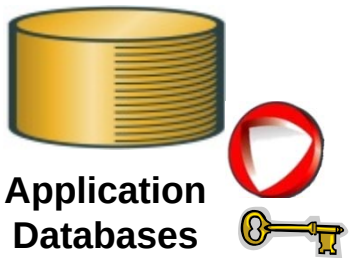
Data Protection Options – Newer Methods

Format Controlling Encryption



Example of Encrypted format:

*111-22-**1013***

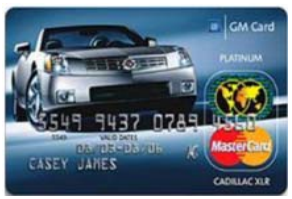


Application Databases

Example of clear text user output:

990-23-1013

Data Tokenization



Example of Token format:

*1234 1234 1234 **4560***

Application Databases

Example of clear text user output:

5549 9437 0789 4560

Token Server

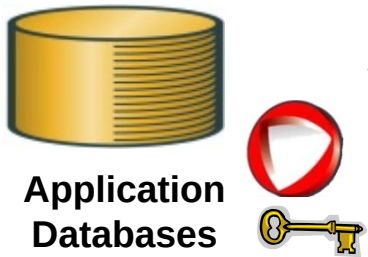
protegrity

Data Protection Options – Traditional Methods

Strong Encryption

Example of Encrypted format:

x%$#..=…….(*)& …



Application Databases

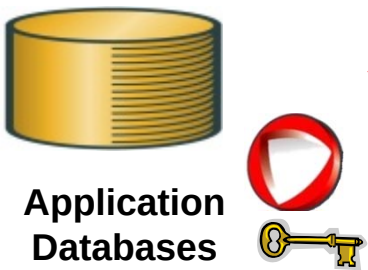
Example of clear text user output:

5549 9437 0789 4560

Hashing (key'd – HMAC – SHA-1)

Example of hashed format (SHA-1 = 20 bytes):

(#@…&&..x…..%$#..=…….(*)& …)*



Application Databases

Example of Hashed user output:

(#@…&&..x…..%$#..=…….(*)& …)*

protegrity

Active Database Protection Approaches

A High Level View

Operational Impact Profile

Database Protection Approach	Performance	Storage	Security	Transparency	Separation of Duties
Application Protection - API					
Column Level Encryption; FCE, AES, 3DES					
Column Level Replacement; Tokens					
Tablespace - Datafile Protection					

Best  Worst

protegrity

Choose Your Defense Methods – Strengths/Weaknesses

Data Protection Options	Performance	Storage	Security	Transparency
Clear	●	●	○	●
Monitoring + Blocking + Masking	●	●	◔	●
Format Controlling Encryption	◒	●	◒	◔
Strong Encryption *	◔	◔	●	◒
Tokens *	◔	●	●	◔
Hash *	●	◔	●	○

Best ● ◔ ◒ ◔ ○ Worst

*: Compliant to PCI DSS 1.2 for making PAN unreadable

protegrity

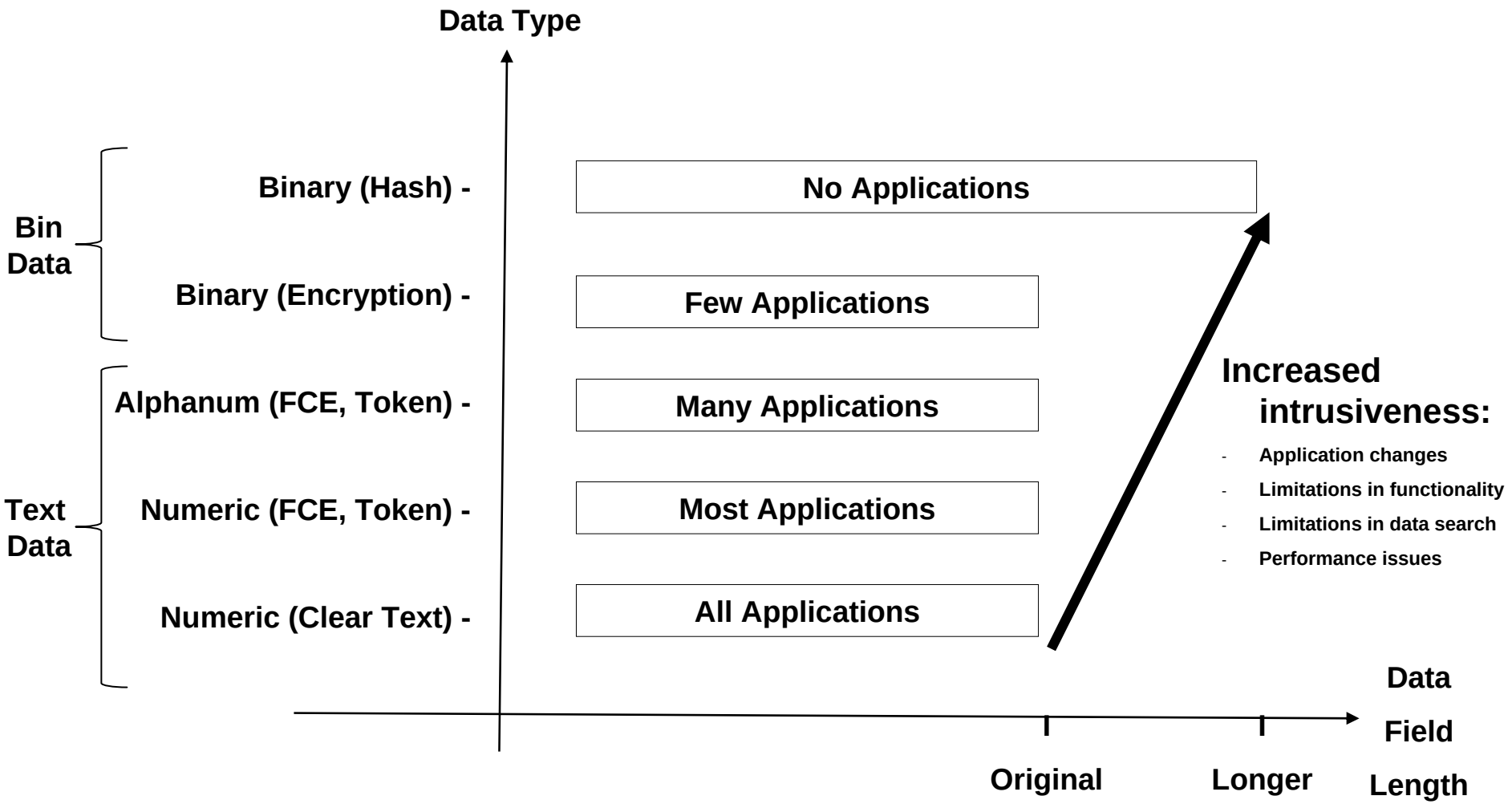
Strong Encryption

- Industry Standard
  - Algorithms & modes - AES CBC, 3DES CBC …
  - Approved by NIST (National Institute of Standards and Technology)
  - Can Block or Mask based on Policy
- Advantages
  - Widely deployed
  - Compatibility
  - Performance
  - PCI
- Considerations
  - Database Transparency
  - Key rotation

Hash

- Non – Reversible
  - Strong protection if the original value is not required
  - Key'd hash (HMAC) or salt
- Advantages
  - No advantages for PCI and PII data
  - Can Block or Mask based on Policy
- Considerations
  - Size and type
  - Transparency
  - Key rotation for key'd hash

Applications are Sensitive to the Data Format



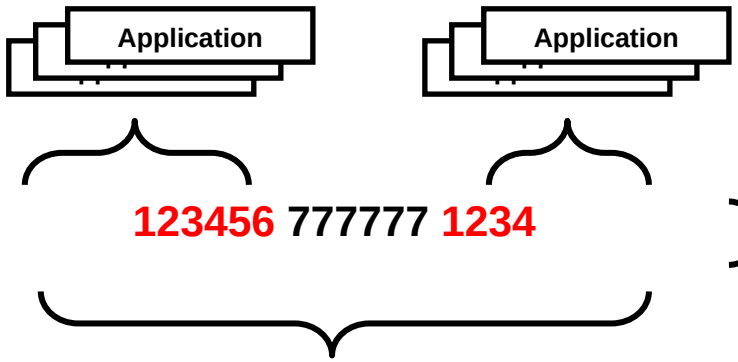
This is a generalized example

protegrity

Partial Encryption/Tokenizing - Example

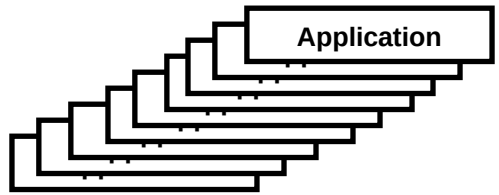
Some applications

- Partial clear data



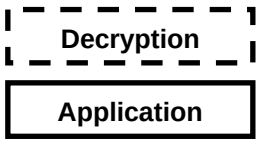
Many applications/tools

- Moving data around



Few applications

- Full clear data



protegrity

Tokenization

-

Details

Data Protection in the Enterprise – Implementation Example

Need partial Information in clear:

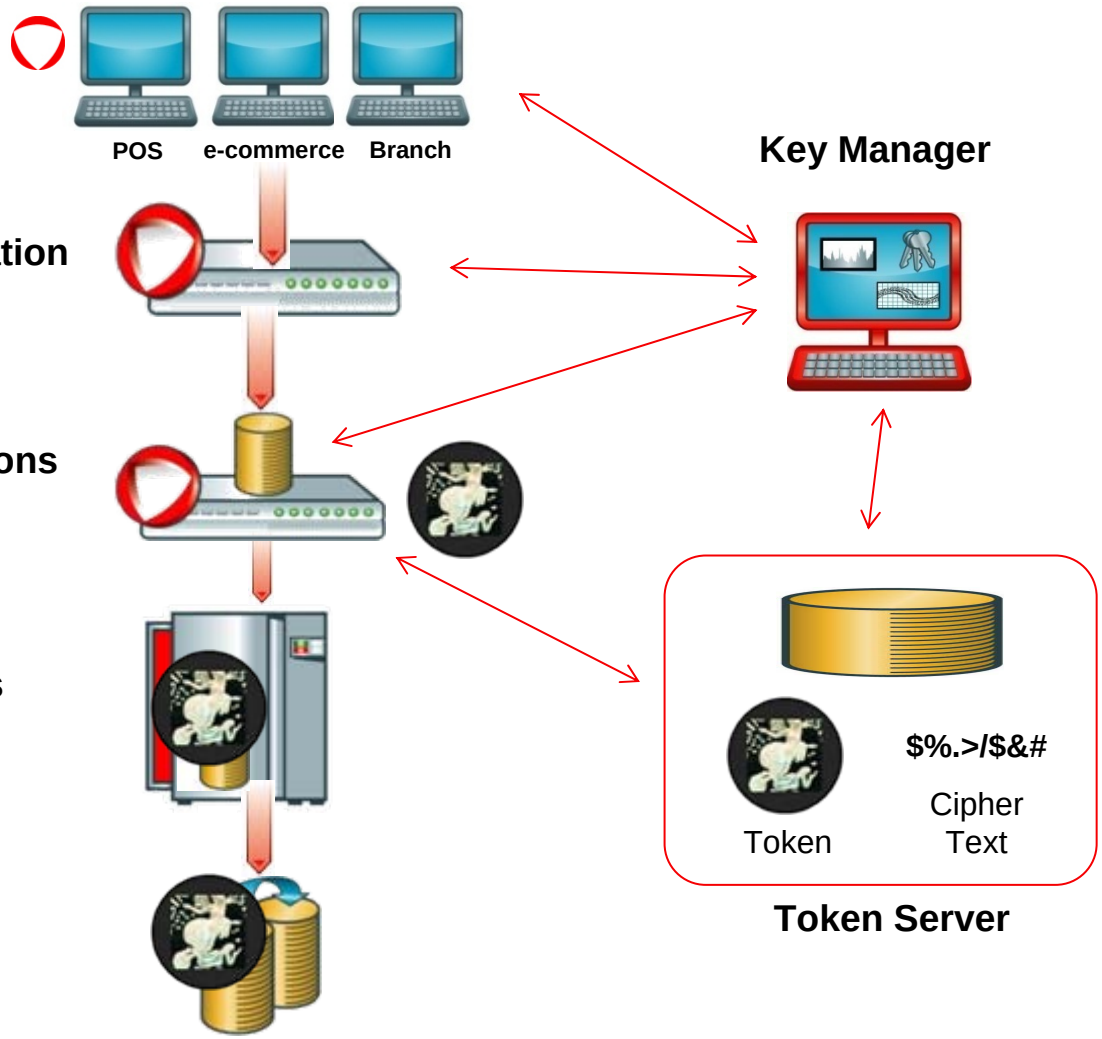
1234 1234 1234 **4560**

Need full Information in clear:

55 49 9437 0789 4560

Can use stored protected value:

1234 1234 1234 **4560**



Token Cipher

What is Tokenization?

- Tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information without compromising its security
- Tokenization is reversible, aka de-tokenization, which is the process of translating a token back to the sensitive data in its original form.
- Tokenization can theoretically be used with sensitive data of all kinds (e.g. bank transactions, medical, license, voter records, etc…)

What is a Token?

- A token is retrievable from a look-up table
- A token is a stream of textual/numeric characters that represent sensitive data
- The same data is always tokenized to the same token and vice versa
- A token for a credit card number typically contains some of the card digits in clear

Examples:

Sensitive data (clear):	458082736473329
Token (alpha-numeric):	4580axdczgs3329
Token (numeric only):	458082734833329

Tokenization

Function	Vendor A	Vendor B	Vendor C
Software Solution			
Central Key Management			
Database Integration			
FIPS 140 Certified			
HSM Support / Interface			

Best  Worst

protegrity

Use Case Comparison for Protection Options

Use Cases	Clear	Strong Encryption	Tokens
High risk data	○	●	●
Long life-cycle data	●	◔	●
Frequently queried/reconstructed data	●	◔	○
Key rollover needed	●	◒	◔
Distributed environments	●	●	◔
Support all data size, type, etc.	●	●	◔

Best ● ◔ ◒ ◔ ○ Worst

Evaluating Data Protection Options

	Performance	Storage	Security	Transparency
Clear	●	●	○	●
Strong Encryption	◔	◔	●	◒
Token	◶	●	●	◔

protegrity

Data Tokenization

Tokenization & PCI DSS

- Tokenization in PCI guidelines in 2010
  - This version is almost certain to include **guidance about how the council wants retailers to deal with encryption and tokenization.**
  - Will the **PCI Council consider a token to be within the scope of PCI?**
  - Is it payment card data that is merely masked?
  - But the software has a way of matching each token to the actual card number, for chargeback and other purposes.
- Vendors will argue that tokens “should be” out of scope
  - But that’s **not likely to be an argument that the card brands or the PCI Council will find persuasive.**

Tokenizing Targets – Market Feedback

- Selling tokenization outside the payment processing industry
  - You are going to have a **tough sell and pricing will be an issue**
  - You need to consider that you will run headlong into masking/ETL providers
- Payment processors
  - Volumes of traffic are enormous
  - **Pricing model is low** – a per transaction fee can offset
- Tier the pricing to address the markets you are going after
  - Some verticals will **not tolerate per-transaction pricing**
  - Others will demand **a decreasing costs with a rise in volume**

Tokenization Pricing Models - PCI

New service, the providers are **still assessing their cost models**

- Someone will **drop pricing dramatically to grab market share** and scare off competition

Pricing Models

- Merchants:
  - **Outsource** transaction processing
  - Addition to their **cost per transaction**, so they can build it into their retail pricing model.
- Processors, acquirers, and data ware-housers,
  - An outsourced model - yearly fee - **operation expense**
  - An on-premises model - **capital expense**

Tokenization PCI Benefits – Hosted Model

- It's **potentially a huge market** but it has not shaken out yet
  - The annual PCI DSS audit costs for such a large merchant can range from $20,000 to hundreds of thousands of dollars,
- With tokenization, some of these applications are removed from the scope of PCI DSS compliance
  - One large merchant reported **$2 million annual savings by moving to an outsourced tokenization solution** after it had already become PCI DSS compliant.
- The **reduction in scope of the audit** and the security-**monitoring** posture taken by the merchant are welcome improvement and the results are **worthwhile**

Tokenization Use Cases

Data Protection Options – 3 Use Cases

Can use stored protected value:

1234 1234 1234 **4560**
Or
Kjh3409)(&@$%^&*

Application 1

Need partial Information in clear:

1234 1234 1234 **4560**

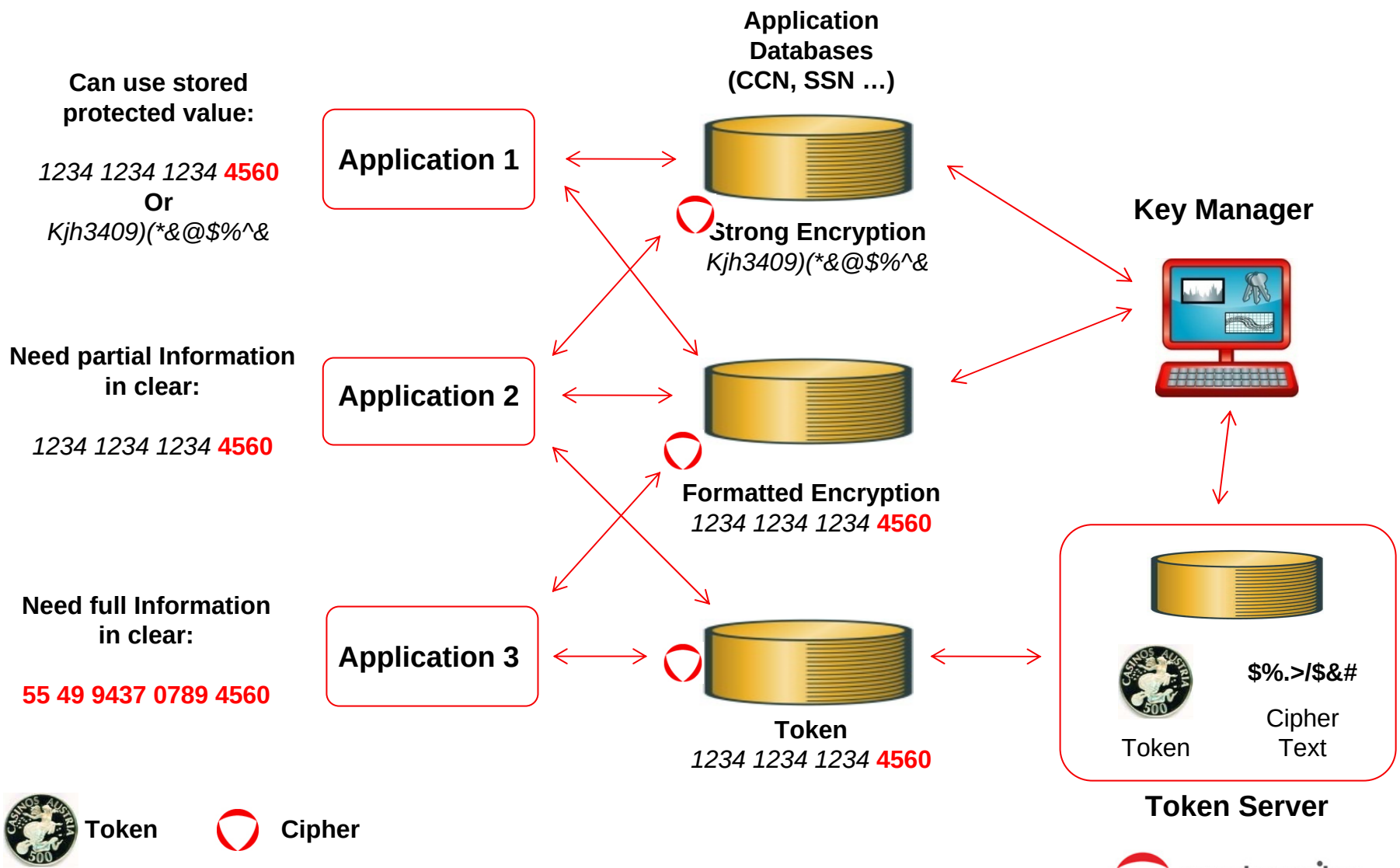
Application 2

Need full Information in clear:

55 49 9437 0789 4560

Application 3

How will different Protection Options Impact Applications?



Application Impact with Different Protection Options

Transparency

Type of Application	Strong Encryption	Formatted Encryption	Token
Can operate on the stored protected value (few)	●	●	●
Need partial information in clear (many)	○	●	●
Need full clear text information (few)	●	○	○

Security

Type of Application	Strong Encryption	Formatted Encryption	Token
Can operate on the stored protected value (few)	●	◒	●
Need partial information in clear (many)	◔	◒	●
Need full clear text information (few)	◔	◔	◔

Application Impact with Different Protection Options

Performance and scalability

Type of Application	Strong Encryption	Formatted Encryption	Token
Can operate on the stored protected value (few)	●	●	●
Need partial information in clear (many)	◔	●	●
Need full clear text information (few)	◔	◒	○

Availability

Type of Application	Strong Encryption	Formatted Encryption	Token
Can operate on the stored protected value (few)	●	●	●
Need partial information in clear (many)	◔	●	●
Need full clear text information (few)	◔	◔	○

Tokenization Considerations

- Transparency – not transparent to downstream systems that require the original data
- Performance & availability – imposes significant overhead from the initial tokenization operation and from subsequent lookups
- Performance & availability – imposes significant overhead if token server is remote or outsourced
- Security vulnerabilities of the tokens themselves – randomness and possibility of collisions
- Security vulnerabilities typical in in-house developed systems – exposing patterns and attack surfaces

Tokenization Use Cases

- Suitable for high risk data – payment card data
- When compliance to NIST standard needed
- Long life-cycle data
- Key rollover – easy to manage
- Centralized environments
- Suitable data size, type, etc.
- Support for “big iron” mixed with Unix or Windows
- Possible to modify the few applications that need full clear text – or database plug-in available

Formatted Encryption

Format Controlling Encryption (FCE)

- Maintains Data Type & Length of Encrypted data
  - Used for character identifiers (CCN, SSN)
- Advantages
  - Slightly improves Transparency to databases
  - Can Block or Mask based on Policy
- Considerations
  - Size of data (between 9 and 16 characters)
  - Poor performance
  - Not supported by NIST
  - Not applicable to PCI
  - Key Rotation

FCE Considerations

- Unproven level of security – makes significant alterations to the standard AES algorithm
- Encryption overhead – significant CPU consumption is required to execute the cipher
- Key management – is not able to attach a key ID, making key rotation more complex - SSN
- Some implementations only support certain data (based on data size, type, etc.)
- Support for “big iron” systems – is not portable across encodings (ASCII, EBCDIC)
- Transparency – some applications need full clear text

FCE Use Cases

- Suitable for lower risk data
- Compliance to NIST standard not needed
- Distributed environments
- Protection of the data flow
- Added performance overhead can be accepted
- Key rollover not needed – transient data
- Support available for data size, type, etc.
- Point to point protection if “big iron” mixed with Unix or Windows
- Possible to modify applications that need full clear text – or database plug-in available

Column Level Encryption - Oracle

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

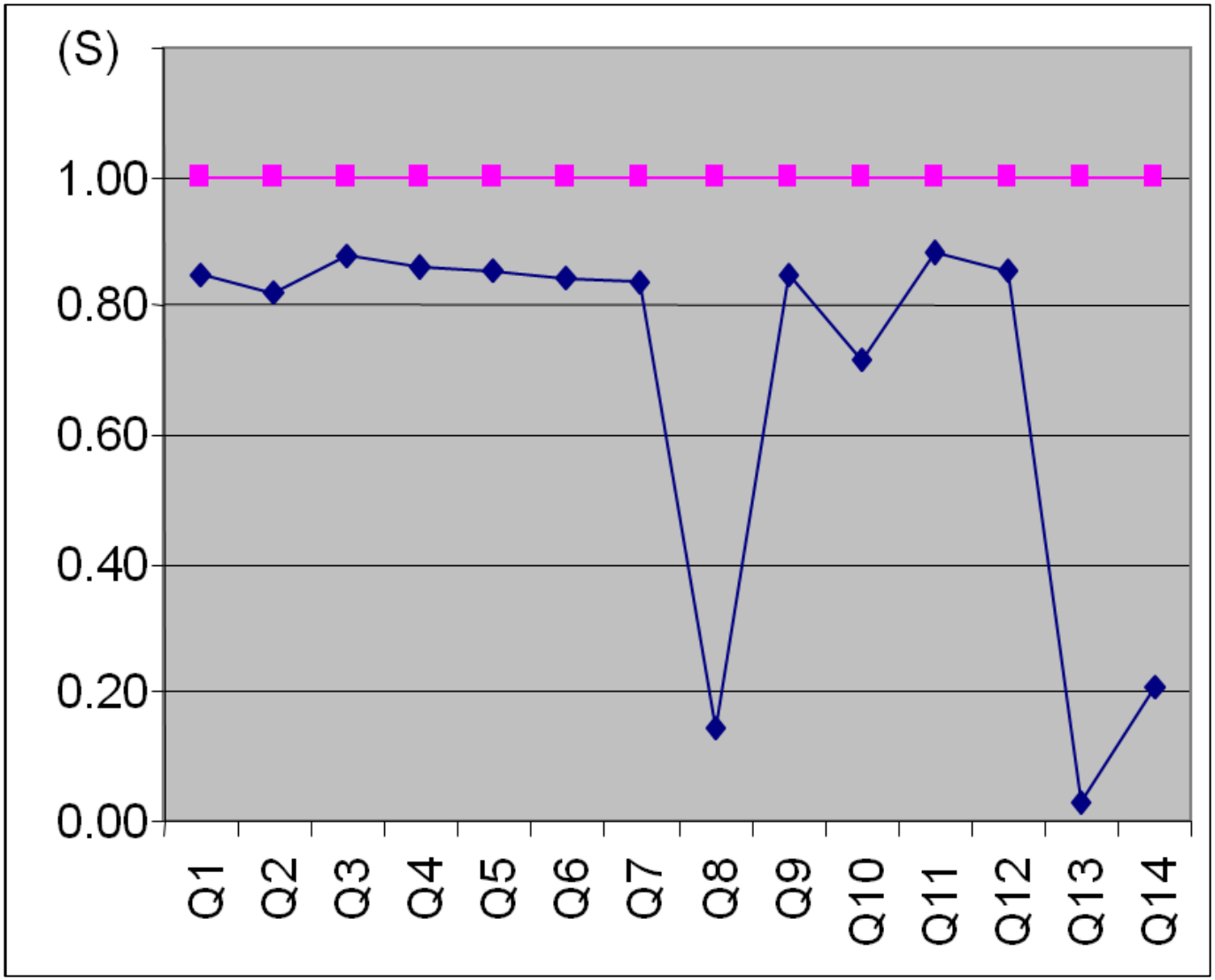
Column Encryption Solutions – Some Considerations

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	●	○	○

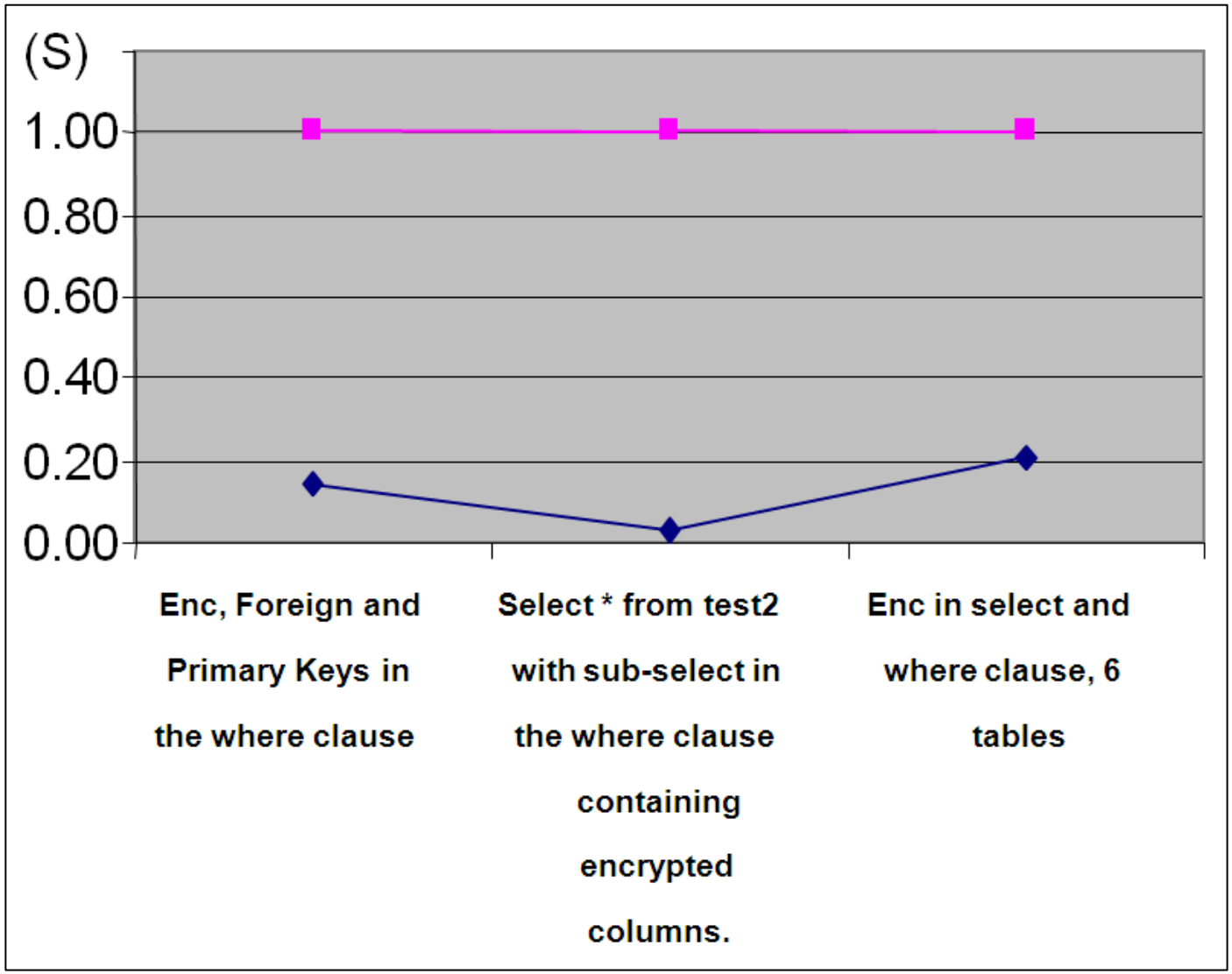
Best ● ◔ ◒ ◕ ○ Worst

protegrity

Oracle Domain Index



Oracle Domain Index



protegrity

Oracle Domain Index

Query	Test Description	Number rows returned	ENC with DI (secs)	ENC w/o DI (secs)	Comments	Total decrypts (est.)	Avg cost per decrypt (msecs)
Q1	Straight select from sample2 table. 3 encrypted columns in the select.	10069	6.000	7.08	Overhead due to decryption of 3 fields * the number of rows returned.Explain plans identical.	30207	0.04
Q2	Straight select from test2 table. 3 encrypted columns in the select.	21999	11.500	14.08	Overhead due to decryption of 3 fields * the number of rows returned.Explain plans identical.	65997	0.04
Q3	Straight select from result2 table. 4 encrypted columns in the select.	19998	14.070	16.09	Overhead due to decryption of 4 fields * the number of rows returned.Explain plans identical.	79992	0.03
Q4	Join of Sample2, Test2 and Results2 Table. No encrypted columns in where clause. 5 encryped columns in the select clause.	5037	6.010	7.00	Overhead due to decryption of 5 fields * the number of rows returned.Explain plans similar.	25185	0.04
Q5	Select 3 encrypted columns from sample2 table. No joins, 1 encrypted column, S62_ENC, in the where clause (=).	400	2.600	3.05	Overhead includes full table access and decrypting s62_enc * 10770 rows even though only 400 rows are returned.	11570	0.04

Oracle Domain Index

Query	Test Description	Number rows returned	ENC with DI (secs)	ENC w/o DI (secs)	Comments	Total decrypts (est.)	Avg cost per decrypt (msecs)
Q6	Select from test2 table. No joins, 1 encrypted column (T2_ENC) in the where clause (< > range	3090	5.900	7.02	Overhead includes decrypting t2_enc * 22,000 rows even though only 3090 rows are returned. T10_enc was decrypted for each returned row.	25090	0.04
Q7	Select from sample2 table. No joins, 2 encrypted column (S62_ENC = , S26_ENC >) in the where clause.	1000	5.070	6.07	Overhead includes a full table scan and decrypting s62_enc for every row in the table (25000 times). S35_enc and s26_enc were decrypted for each row returned.	27000	0.04
Q8	Select from sample2 & boted2 table. 2 encrypted column in the select clause. Encrypted columns, Foreign and Primary Keys in the where clause (sample2.S62_ENC = boted2.B_PK1_ENC).	899	0.010	0.07	Overhead includes decryption of 2 fields for every row returned (2 fields in sample2 and 1 field in boted2 during the join). Explain plans are identical.	2697	0.02
Q9	Select from test2 & analysis2 table. 1 encrypted column in the select clause. Encrypted columns, Primary and Foreign Keys in the where clause (test2.T2_ENC = analysis2.A_PK1_ENC) .	620	8.500	10.03	Overhead includes decryption of t2_enc field for every row in test2 and decryption of a_pk1_enc for every row in analysis2. Explain plan includes full table scan of analysis2 VS index range scan.	44913	0.03

Oracle Domain Index

Query	Test Description	Number rows returned	ENC with DI (secs)	ENC w/o DI (secs)	Comments	Total decrypts (est.)	Avg cost per decrypt (msecs)
Q10	Select from result2 & component2 table.5 encrypted column in the select clause. Encrypted columns, Foreign and Primary Keys in the where clause (result2.R_PK2_ENC = componet2.C_PK1_ENC).	920	10.000	14.01	Overhead includes decryption of r_pk2_enc field for every row in result2 and decryption of c_pk1_enc for every row in result2. Explain plans are similar.	68105	0.06
Q11	Select from Sample2 and Boted2 table. Outer join on encryted columns. (sample2.S62_ENC = boted2.B_PK1_ENC(+))	5599	2.700	3.06	Overhead includes decryption of s62_enc and b_pk1_enc field for every row returned due since the join is on the encrypted column. Explain plans are similar.	11198	0.03
Q12	Select from result2 table. 5 encrypted columns in the select clause. 5 Encrypted columns in the where clause.	600	12.000	14.01	Overhead includes decryption of s62_enc and b_pk1_enc field for every row returned due since the join is on the encrypted column. Explain plans are similar.	64065	0.03
Q13	Select * from test2 with sub-select in the where clause containing encrypted columns.	1300	0.030	1.05	Overhead includes decryption of 3 fields in test2 for every row returned and decryption of 1 field in for each row in analysis2 to satisfy the subquery. Explain plans are similar.	6034	0.17
Q14	Encrypted columns in select and where clause, 6 tables: Sample2, boted2, Test2, Analysis2, Results2 & Components2 joined in the from clause.	1197	1.050	5.04	Overhead includes decryption of seven fields for every row returned. Additional overhead decrypting fields during table joins but exact number of decryptions not known. Explain plans are similar.	18379	0.22

Oracle 11 - Native Features

Feature	3rd party	Oracle 11
Prevents highly privileged users from accessing credit card information and helps reduce the risk of insider threats with separation of duty, multi-factor authorization and command rules.	Y	Database Vault
Provide encryption of credit card number columns and other columns	Y	Advanced Security Transparent Data Encryption (TDE)
Consolidates and protects database audit data from across the enterprise	Y	Audit Vault
Provides secure configuration scanning to insure your databases stay configured securely.	Open Source	Enterprise Manager

Oracle

Vendor	Product	Hub ($k)		Agent ($k)		
		Per Processor	Per Server	Per Processor	Per Core	Per Server
Oracle	Audit Vault	58		4		
	Masking	12				
	Advanced Security			12		
	Label Security			12		
	Database Vault			23		
	DB Enterprise Edition			48		

Oracle Master Key Management

EXTERNAL SECURITY MODULE SUPPORT BY DATABASE VERSION			
DATABASE VERSION	**MASTER KEY FOR ...**	**... IN ORACLE WALLET**	**... IN HSM**
Oracle Database 10gR2	Column Encryption	Yes	No
Oracle Database 11gR1 (11.1.0.6)	Column Encryption	Yes	Yes
	Tablespace Encryption	Yes	No
Oracle Database 11gR1 (11.1.0.7)	Column Encryption	Yes	Yes
	Tablespace Encryption	Yes	Yes (no re-key)

RE-KEY SUPPORT				
	TDE COLUMN ENCRYPTION		**TDE TABLESPACE ENCRYPTION**	
	MASTER KEY	**TABLE KEYS**	**MASTER KEY**	**TABLESPACE KEYS**
Re-key support	Yes	Yes	No	No

protegrity

TDE Tablespace or TDE Column Encryption?

CHOOSE TDE COLUMN ENCRYPTION IF ...:	CHOOSE TDE TABLESPACE ENCRYPTION IF ...:
Keys need to be rotated on a semi frequent basis	Key rotation is not required
Location of sensitive information is known	Location of sensitive information is unknown
Less than 5% of all application columns are encryption candidates.	Most of the application data is deemed sensitive, or **multiple** national and international security and privacy mandates apply to your industry
Data type and length is supported by TDE column encryption	Not all data types that hold sensitive information are supported by TDE column encryption
Encryption candidates are not foreign-key columns	Encryption candidates are foreign key columns
Indexes over encryption candidates are normal B-tree indexes	Indexes of encryption candidates are functional indexes
Application does not perform range scans over encrypted data	Application searches for ranges of sensitive data
Increase in storage by 1 to 52 bytes per encrypted value	No storage increase acceptable
Performance impact depends on percentage of encrypted columns; how often the encrypted values are selected or updated, the size of encrypted data, and other variables.	Constant performance impact below 10%

Evaluation Criteria – Real Key Rotation

Criteria & Steps	Vendor A	Vendor B
Create a new key.		
Re-encrypt the entire table.		
Record the lapsed time (CPU) for benchmarking.		
Capture the downtime needed for Key Rotation.		
What are the ways that downtime can be minimized?		
How are multiple keys per column enabled?		
How is the Key Rotation process kicked-off?		
Demonstrate that the reporting tools can access clear text from the encrypted data.		
Demonstrate that sensitive data can be accessed from Oracle's Admin. Tools (Oracle SQL*Plus).		
Demonstrate database encryption as an available and more transparent alternative.		
Demonstrate access to the sensitive data by common 3rd Party tools.		
Provide a list of all data security Patents owned by the Vendor.		

Native Database Encryption - Considerations

Functionality	3rd Party	Oracle 9	Oracle 10	Oracle 11	DB2 UDB	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 (table space)	●	○	○	○	○	○
Separation of duties	●	◔	◒	◔	◒	◔

Best ● ◔ ◒ ◔ ○ Worst

Enterprise View of Different Protection Options

Evaluation Criteria	Strong Encryption	Formatted Encryption	Token
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	●	○	●

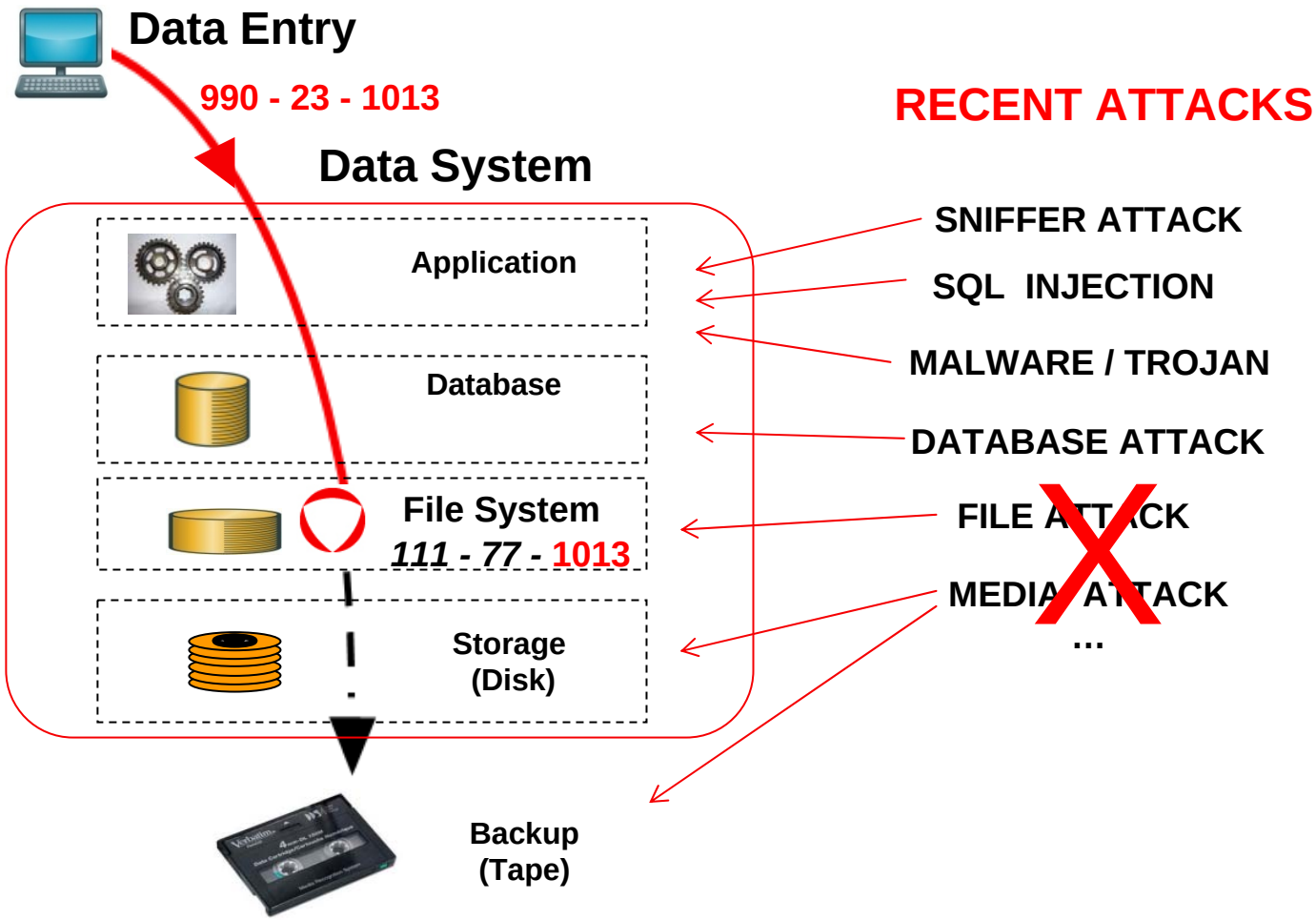
Best  Worst

protegrity

Enforcement at Different System Layers

Choose your Defenses – File Encryption

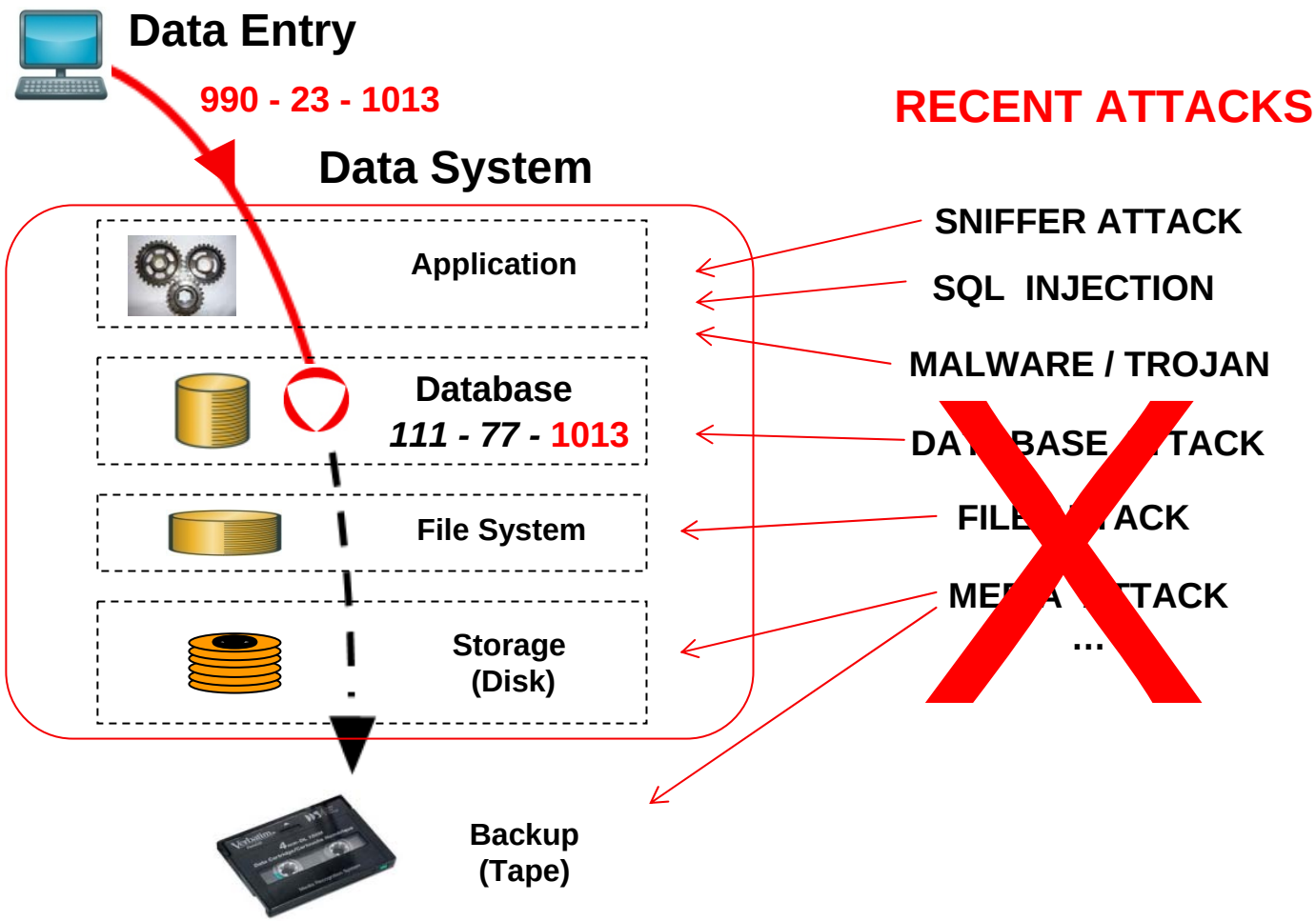
Where is data exposed to attacks?



protegrity

Choose your Defenses – Option #1

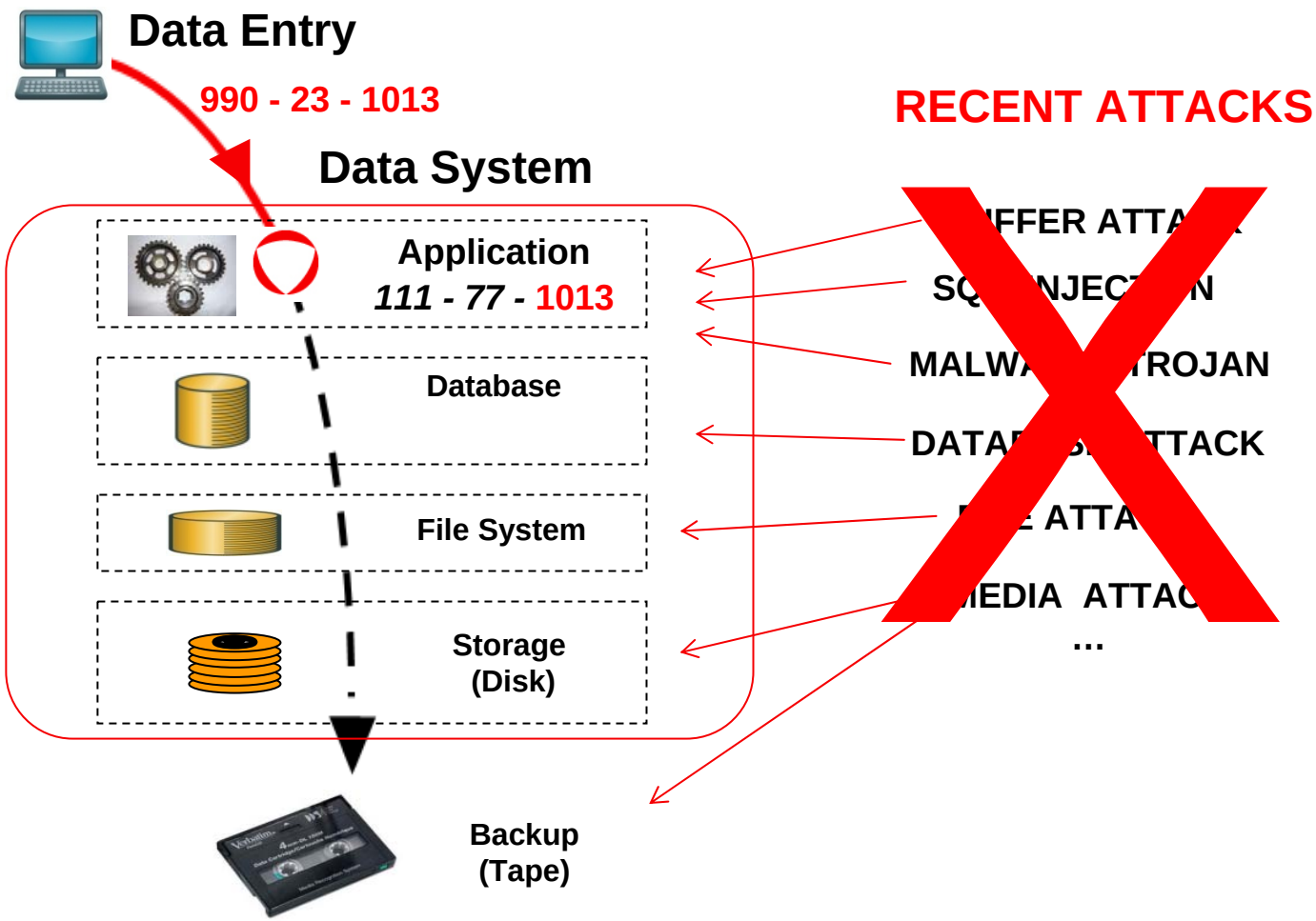
Where is data exposed to attacks?



protegrity

Choose your Defenses –Option #2

Where is data exposed to attacks?



protegrity

Data Protection Implementation – System Layers

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

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

Best  Worst

Database Protection at Different System Layers

Transparency Impact Profile

Protection at different system layers	Application code	SQL code	Database schema	Database version	OS version	File system type
Application API	○	●	◔	●	●	●
Database column	◔	◔	○	◔	●	●
Database table space	●	●	◒	○	●	●
OS database file	●	●	●	●	○	◒

Best ● ◕ ◔ ◒ ◔ ○ Worst

protegrity

Database Protection - Encryption at Different Layers

Transparency Impact Profile

Protection at different System Layers	Application Code	SQL Code	Database Schema	OS Version	File System Type
Application API	○	●	◔	●	●
Database Column	◔	◔	○	●	●
Database Table Space	●	●	◒	●	●
OS Database File	●	●	●	○	◒
Volume/Disk Level	●	●	●	●	●

Best ● ◕ ◔ ◒ ◔ ◔ ○ Worst

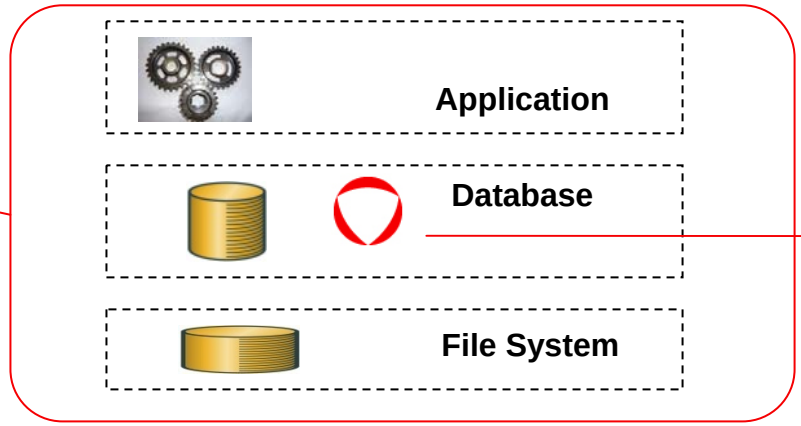
protegrity

Reporting

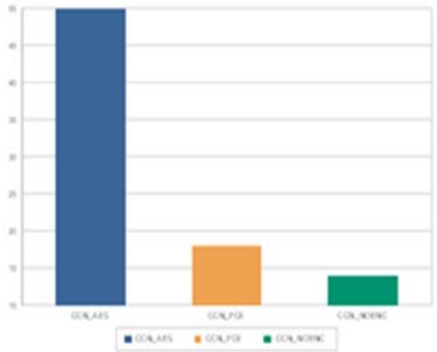
Protegrity

Security Admin

Application / Database Server



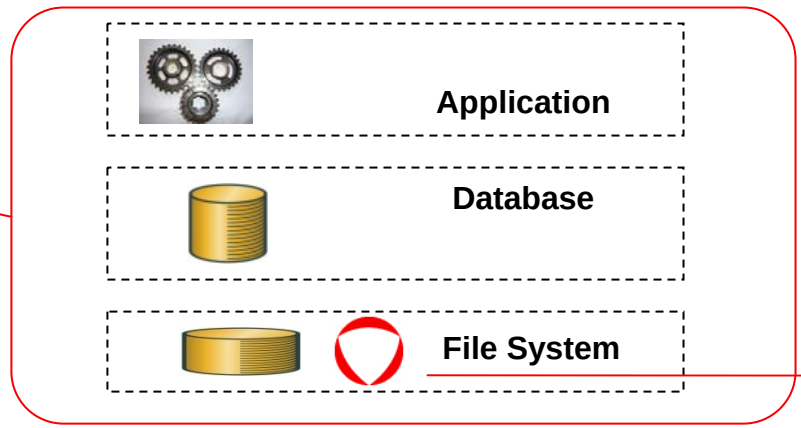
Monitoring of Column and User



Vormetric

Security Admin

Application / Database Server

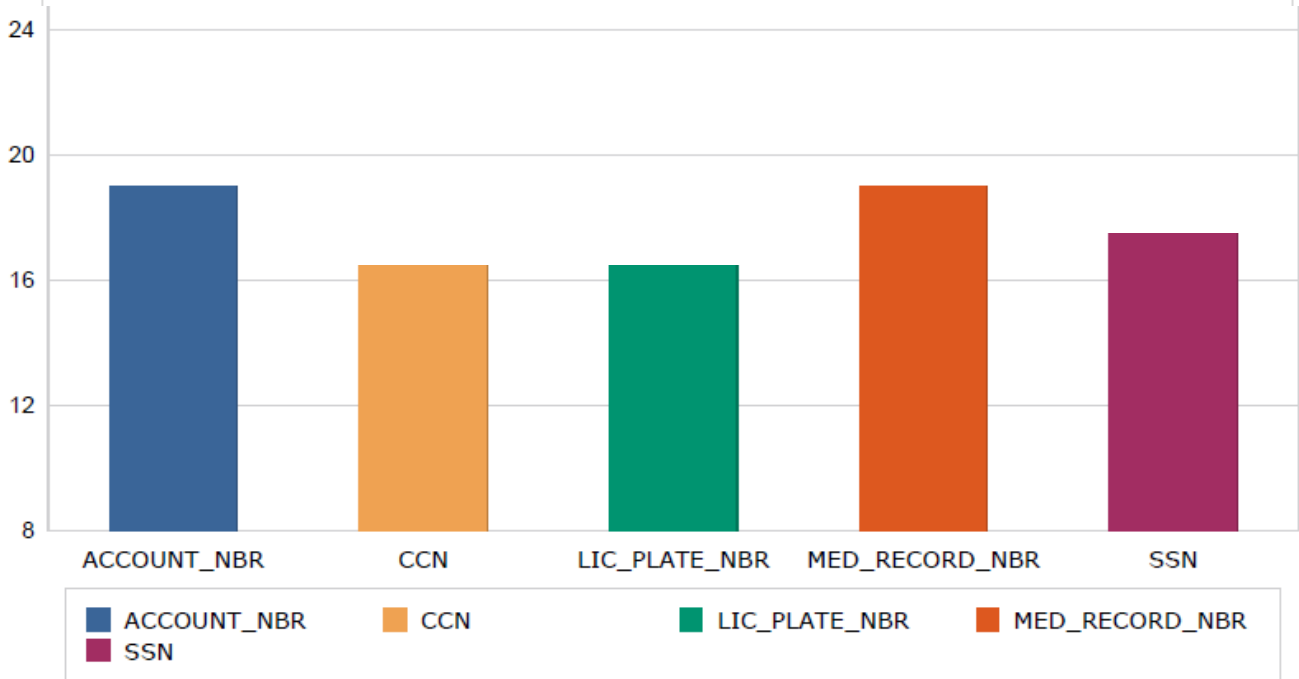


NO Monitoring of Column and User

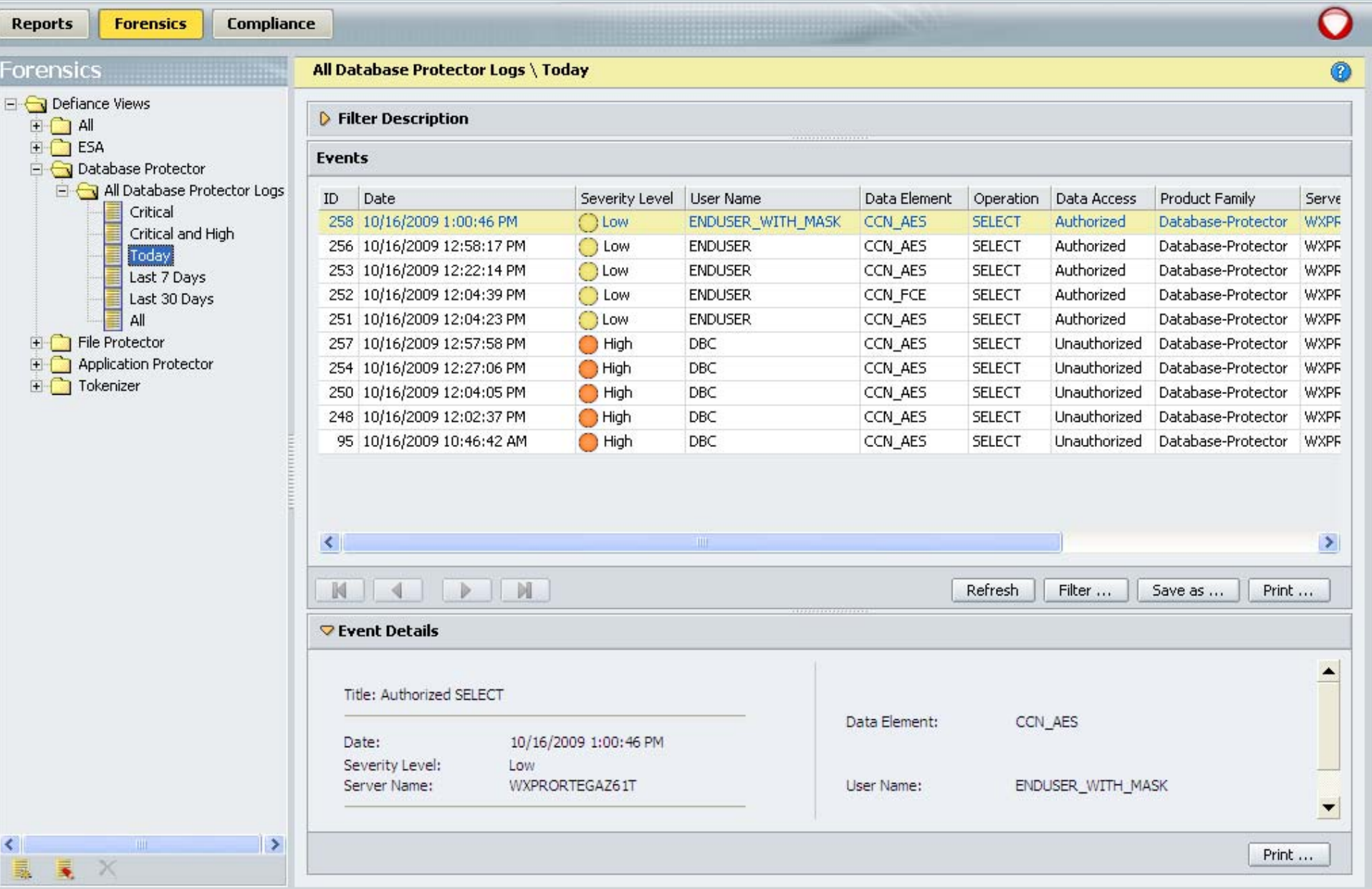
protegrity

Report Criteria

Severity Level:	Critical, High, Medium, Low, Lowest		
From Date:	1/28/2010	To Date:	1/28/2010
Server:	(Any)	Event Type:	(Any)
Data Access:	(Any)	Operation:	(Any)
Data Element:	(Any)	User Name:	(Any)
Last Event On:	1/28/2010	Total Number of Events:	95

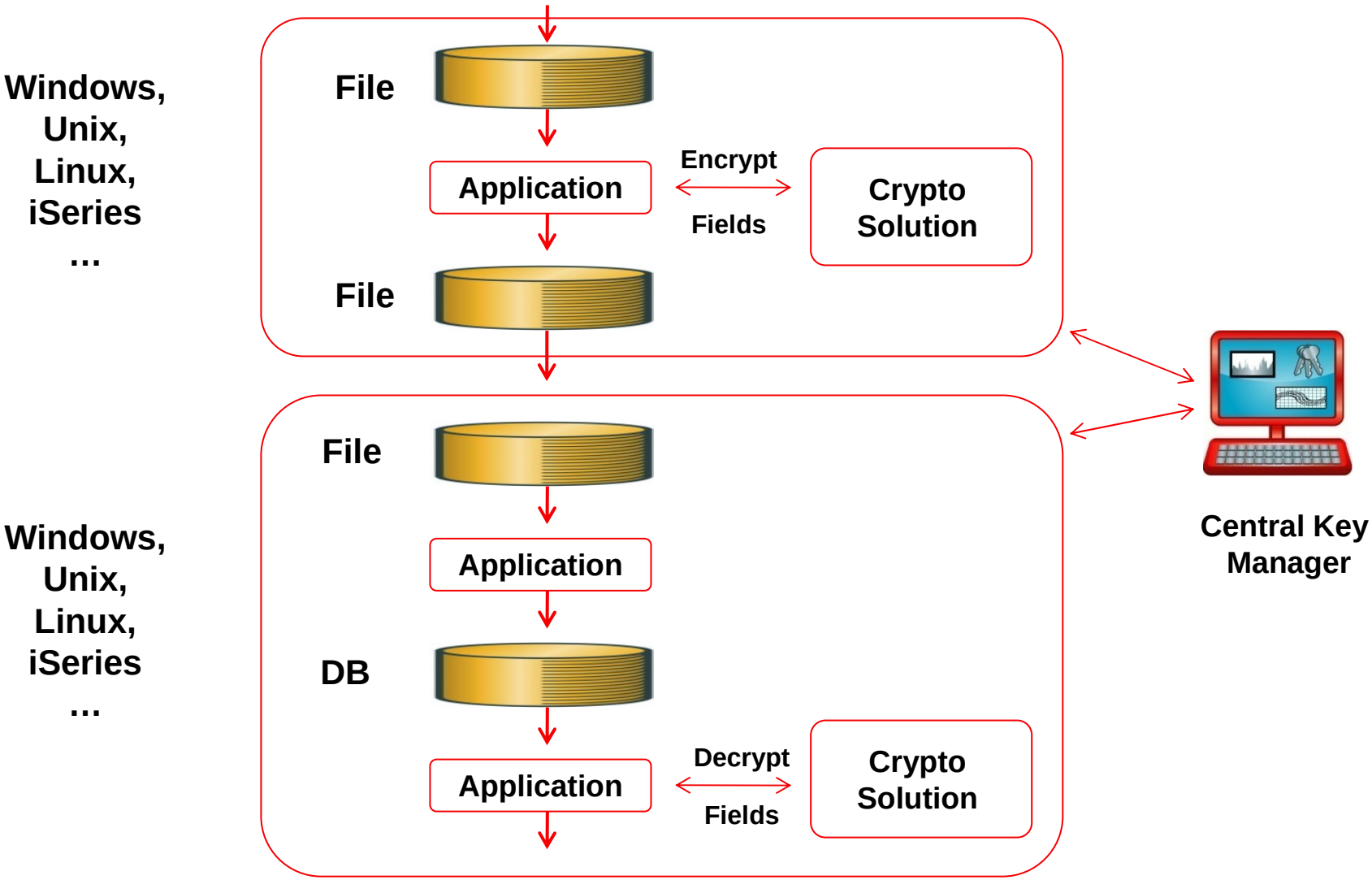


protegrity

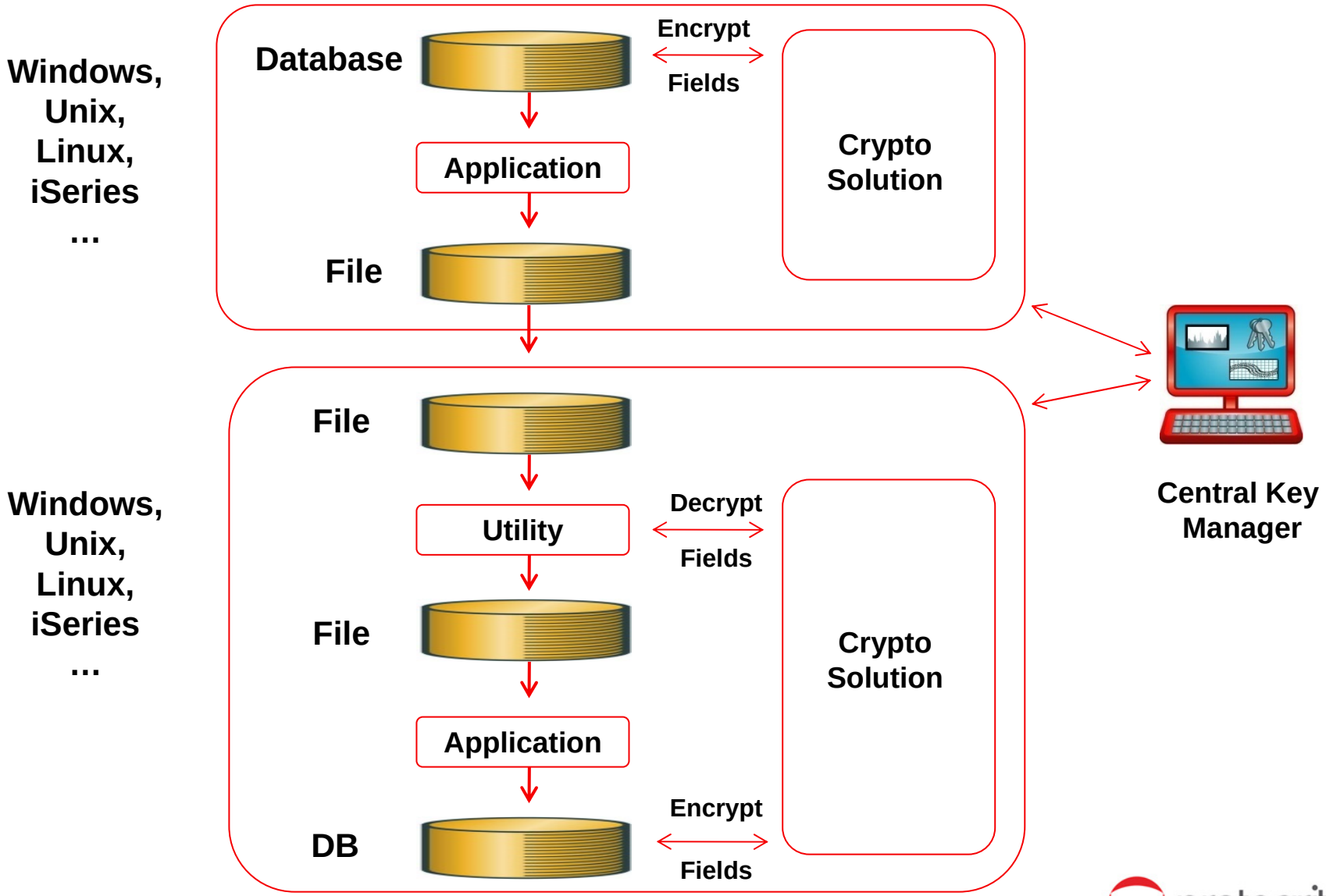

Reports
Forensics
Compliance
Forensics
Defiance Views
All
ESA
Database Protector
All Database Protector Logs
Critical
Critical and High
Today
Last 7 Days
Last 30 Days
All
File Protector
Application Protector
Tokenizer
All Database Protector Logs \ Today
Filter Description
Events
ID Date Severity Level User Name Data Element Operation Data Access Product Family Serve
258 10/16/2009 1:00:46 PM Low ENDUSER_WITH_MASK CCN_AES SELECT Authorized Database-Protector WXPF
256 10/16/2009 12:58:17 PM Low ENDUSER CCN_AES SELECT Authorized Database-Protector WXPF
253 10/16/2009 12:22:14 PM Low ENDUSER CCN_AES SELECT Authorized Database-Protector WXPF
252 10/16/2009 12:04:39 PM Low ENDUSER CCN_FCE SELECT Authorized Database-Protector WXPF
251 10/16/2009 12:04:23 PM Low ENDUSER CCN_AES SELECT Authorized Database-Protector WXPF
257 10/16/2009 12:57:58 PM High DBC CCN_AES SELECT Unauthorized Database-Protector WXPF
254 10/16/2009 12:27:06 PM High DBC CCN_AES SELECT Unauthorized Database-Protector WXPF
250 10/16/2009 12:04:05 PM High DBC CCN_AES SELECT Unauthorized Database-Protector WXPF
248 10/16/2009 12:02:37 PM High DBC CCN_AES SELECT Unauthorized Database-Protector WXPF
95 10/16/2009 10:46:42 AM High DBC CCN_AES SELECT Unauthorized Database-Protector WXPF
Refresh
Filter ...
Save as ...
Print ...
Event Details
Title: Authorized SELECT
Date: 10/16/2009 1:00:46 PM
Severity Level: Low
Server Name: WXPRORTEGAZ61T
Data Element: CCN_AES
User Name: ENDUSER_WITH_MASK
Print ...

Data Flow
–
Use Cases

Field Encryption – Protecting the Data Flow

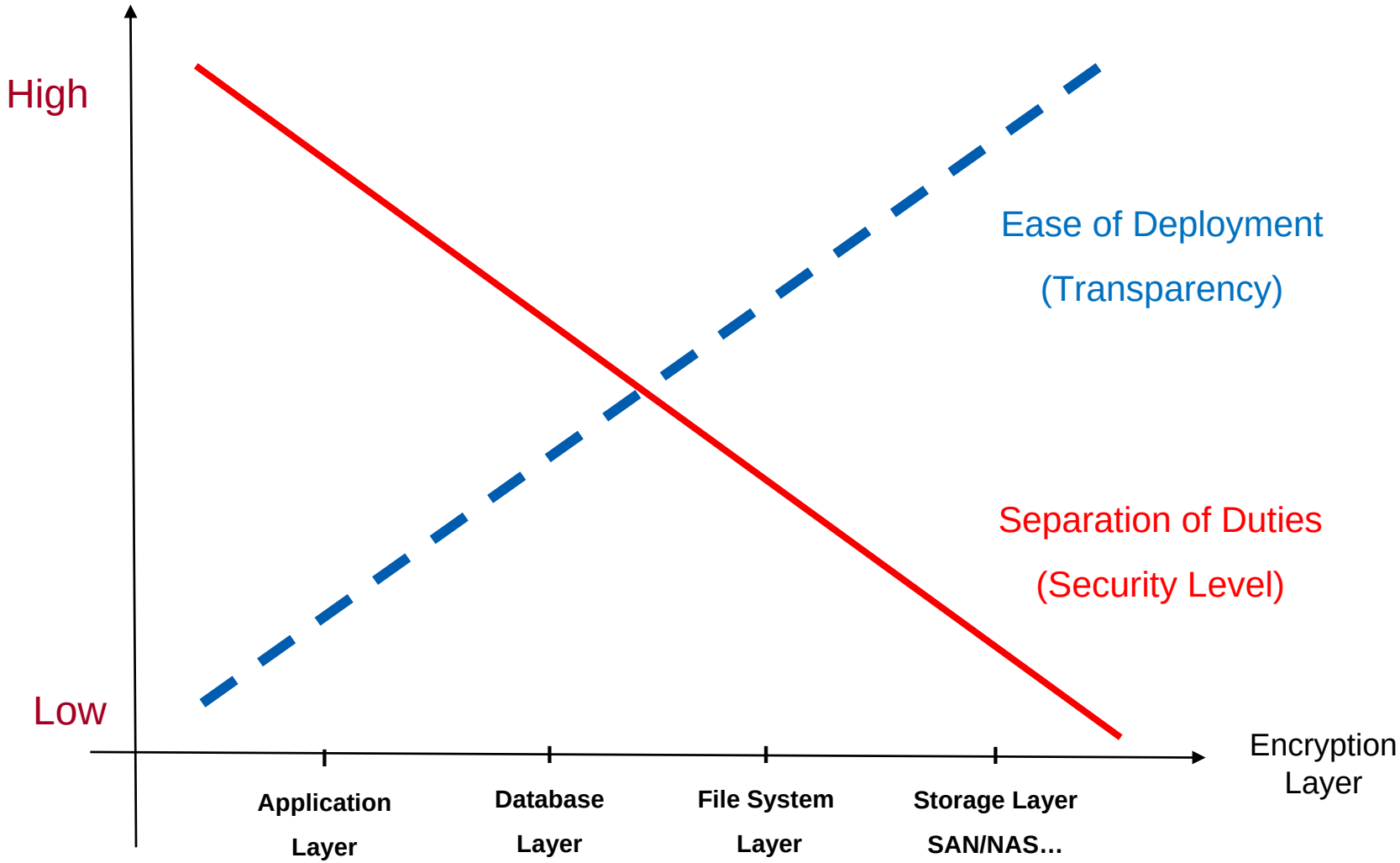


Transparent Encryption – No Application Changes



protegrity

Generalization: Encryption at Different System Layers



protegrity

Managing Risk to Data

Find Your Data – Understand the Data Flow

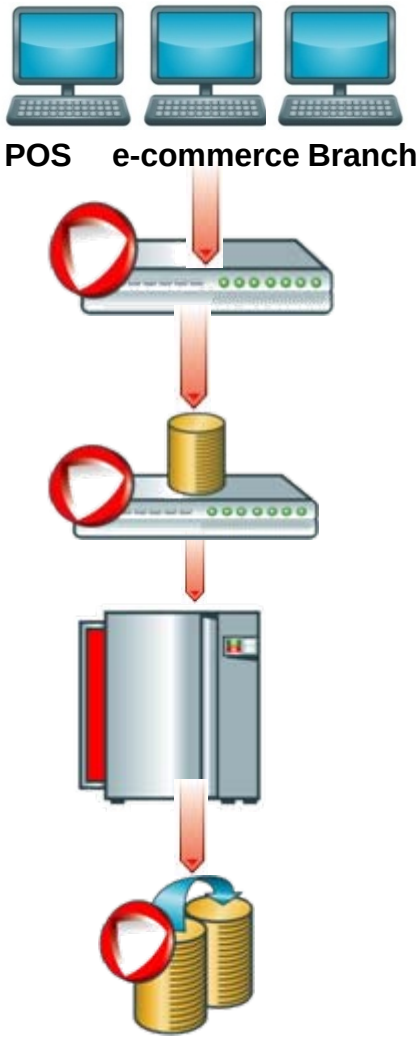
Collection

Aggregation

Operations

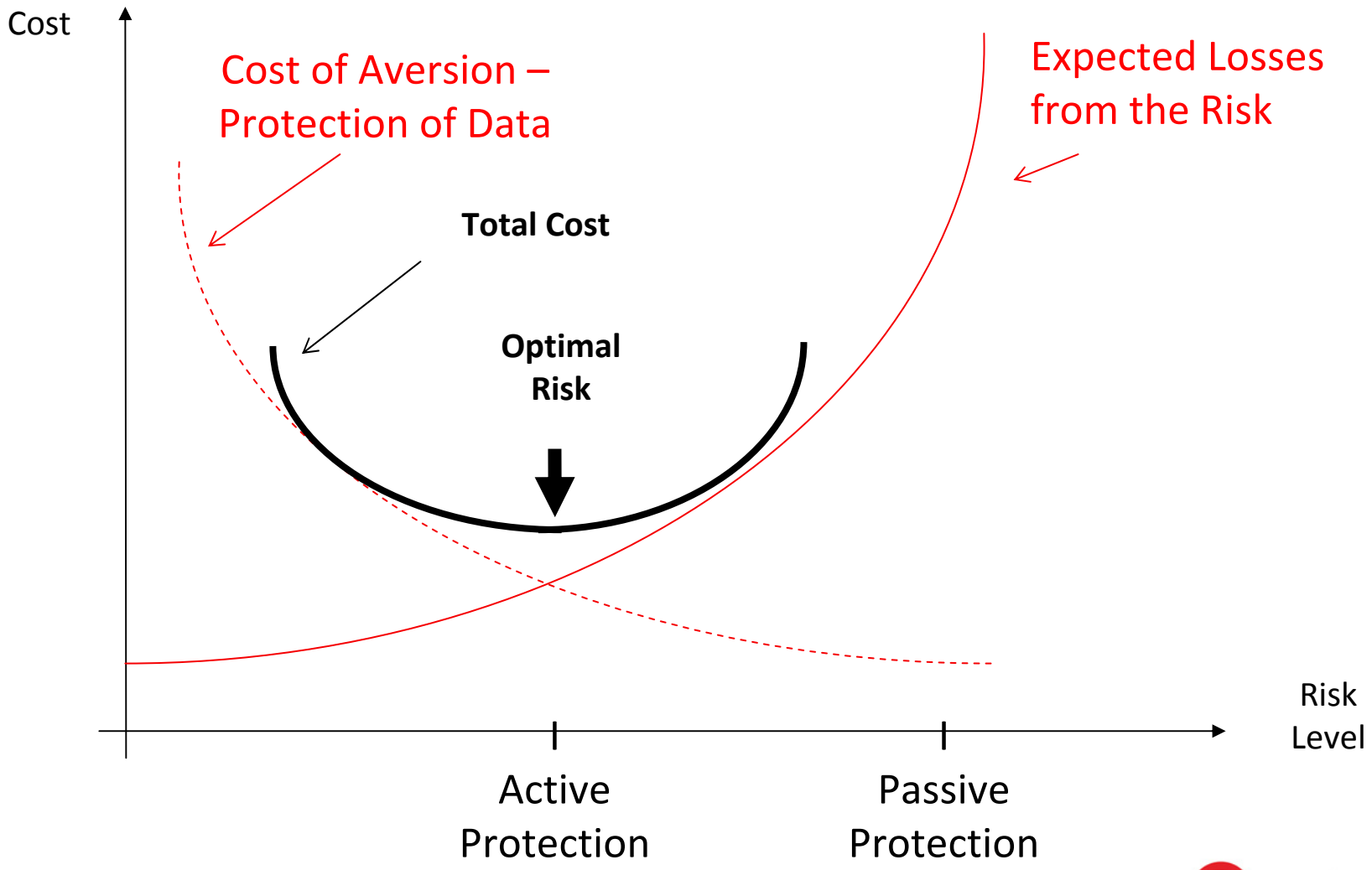
Analysis

Archive



- ‘Information in the wild’
  - Short lifecycle / High risk
- Temporary information
  - Short lifecycle / High risk
- Operating information
  - Typically 1 or more year lifecycle
  - Broad and diverse computing and database environment
- Decision making information
  - Typically multi-year lifecycle
  - Homogeneous computing environment
  - High volume database analysis
- Archive
  - Typically multi-year lifecycle
  - Preserving the ability to retrieve the data in the future is important

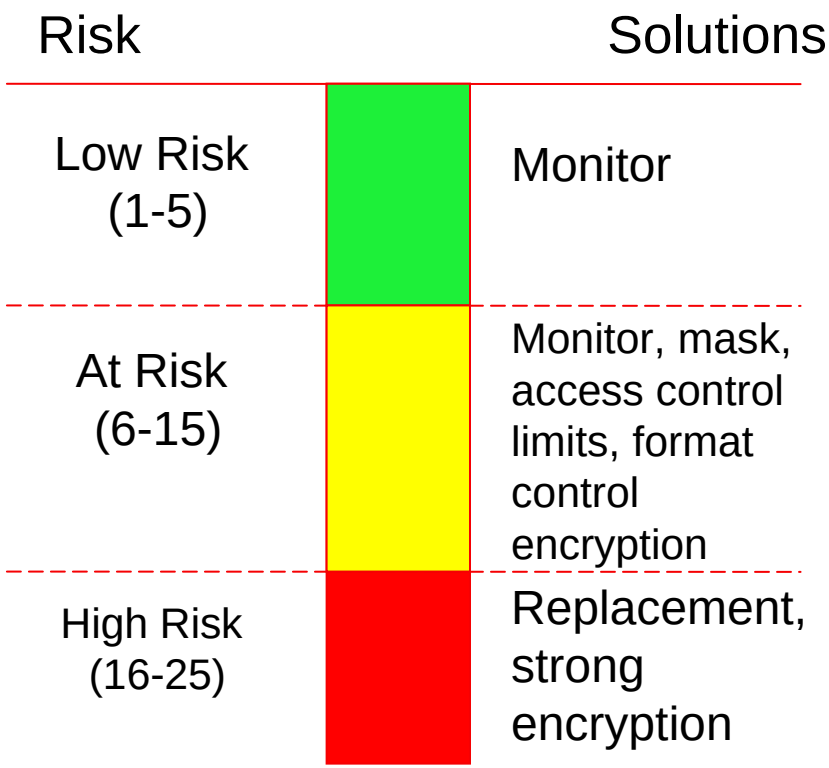
Choose Your Defenses – Find the Balance



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

Protegrity Data Security Value & Approach

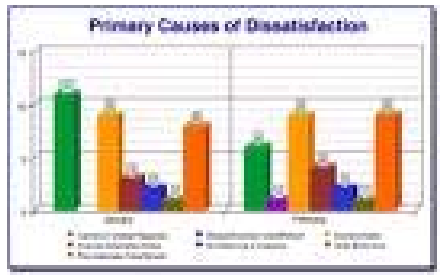
protegrity

Protegrity Value Proposition

- Protegrity delivers, application, database, file protectors across all major enterprise platforms.
- Protegrity's Risk Adjusted Data Security Platform continuously secures data throughout its lifecycle.
- Underlying foundation for the platform includes comprehensive data security policy, key management, and audit reporting.
- Enables customers to achieve data security compliance (*PCI, HIPAA, PEPIDA, SOX and Federal & State Privacy Laws)*

Data Protection Challenges

- Actual protection is not the challenge
- Management of solutions
  - Key management
  - Security policy
  - Auditing and reporting
- Minimizing impact on business operations
  - Transparency
  - Performance vs. security
- Minimizing the cost implications
- Maintaining compliance
- Implementation Time



protegrity

Protect Sensitive Data

PCI & Customer Data

- Credit & Loyalty cards
- Banking/mortgage data
- Customer profiles
- Prospect information

PII

- Social security number
- Drivers license number
- Private account numbers
- Date of birth

Company Data

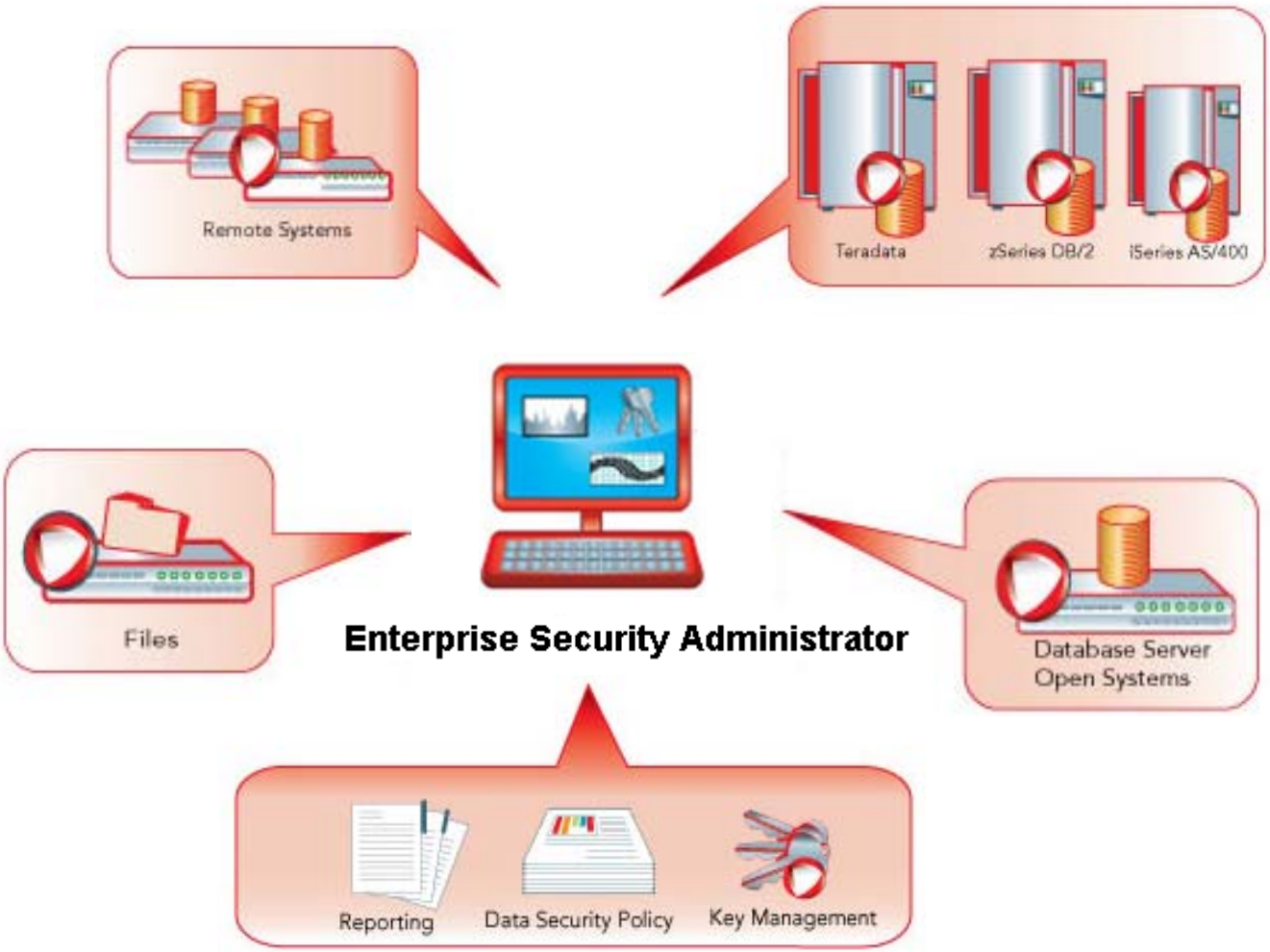
- Salary / bonus
- HR data
- Corporate secrets
- Financial results

Health Records

- Insurance claims
- Medical records
- Prescriptions
- Billing information

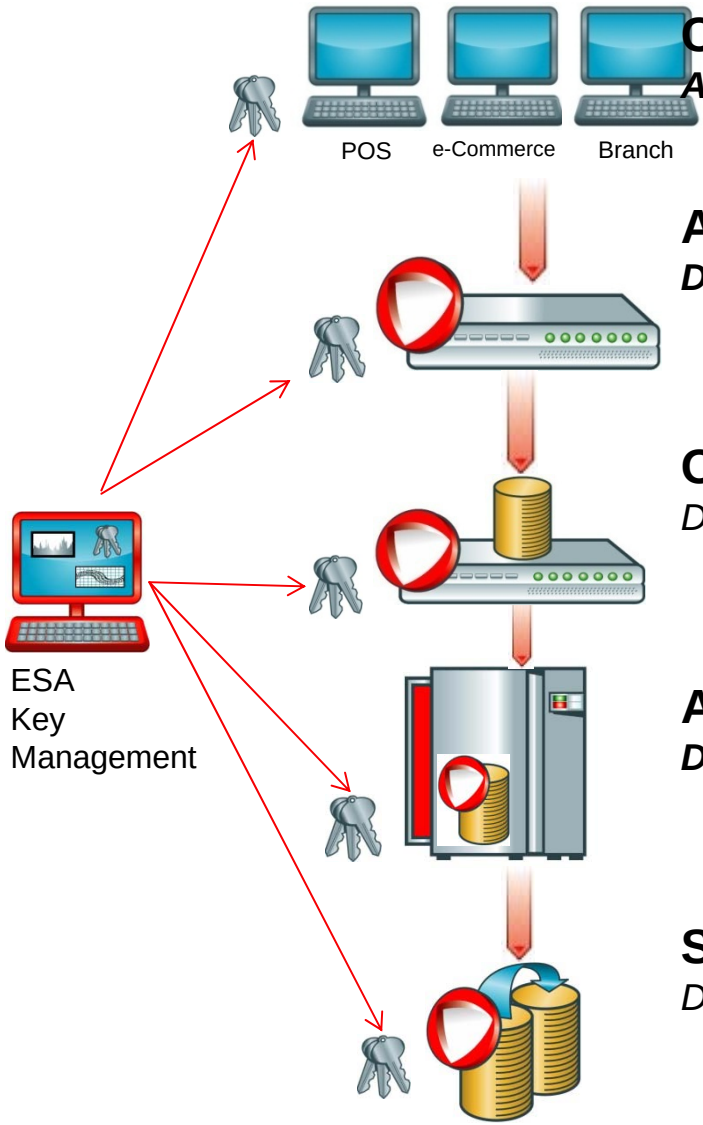
protegrity

Protegrity Data Security Solutions



protegrity

Protecting the Enterprise Data Flow



Collection

Application Protection

Protect data from collection to aggregation

Aggregation

Database and Application Protection

Change Security Zone, protect data at aggregation, distribute to different operational sys. on different zones

Operations

Database, File and Application Protection

Protect data in different security zones, and in different business applications and technologies

Analysis

Database Protection

High performance column level protection is required for these large analytical systems

Storage

Database and File Protection

Archive protected systems with the ability to restore

protegrity