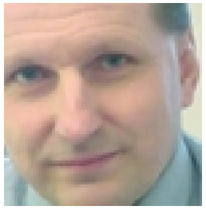
FISSEA Awareness, Training, and Education -

CSI COMPUTER SECURITY INSTITUTE

Encrypting for Database Security

Intrusion Prevention for Databases



Ulf Mattsson
Chief Technology Officer
Protegrity,
ulf.mattsson@protegrity.se
www.protegrity.com

FISSEA Conference

Awareness, Training and Education
The *Driving Force* Behind Information Security

NIST National Institute of Standards and Technology

Safeguarding Enterprise Data

protegrity securing digital assets

Encrypting for Database Security

Abstract

Modern intrusion detection systems are comprised of three basically different approaches, host based, network based, and a third relatively recent addition called procedural based detection. The first two have been extremely popular in the commercial market for a number of years now because they are relatively simple to use, understand and maintain. However, they fall prey to a number of shortcomings such as scaling with increased traffic requirements, use of complex and false positive prone signature databases, and their inability to detect novel intrusive attempts. This intrusion detection systems represent a great leap forward over current security technologies by addressing these and other concerns. This paper presents an overview of our work in creating a true database intrusion detection system. Based on many years of Database Security Research, the proposed solution detects a wide range of specific and general forms of misuse, provides detailed reports, and has a low false-alarm rate. Traditional database security mechanisms are very limited in defending successful data attacks. Authorized but malicious transactions can make a database useless by impairing its integrity and availability. **The proposed solution offers the ability to detect misuse and subversion through the direct monitoring of database operations inside the database host, providing an important complement to host-based and network-based surveillance.**

Biography

Ulf T. Mattsson, Chief Technology Officer, Protegrity Inc., holds a master's degree in physics and a number of patents in the IT security area. 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, in the areas of IT Architecture and IT Security. Mattsson also architected database security enhancements with IBM, Microsoft, Oracle, Informix, and Sybase. Mattsson is an IBM Certified IT Architect and a research member of the International Federation for Information Processing (IFIP) WG 11.3 Data and Application Security, and a member of the IBM Privacy Management Advisory Council.

Encrypting for Database Security

1. Requirements - Case Studies
2. Liability Aspects & Computer Security Breaches
3. Some Solution Alternatives – Positioning & Issues
4. Time, Cost & Performance Aspects - Case Studies
5. The Hybrid IPS - Overview
6. Intrusion Prevention – Database Server Side
7. An Evidence-Quality Audit Log

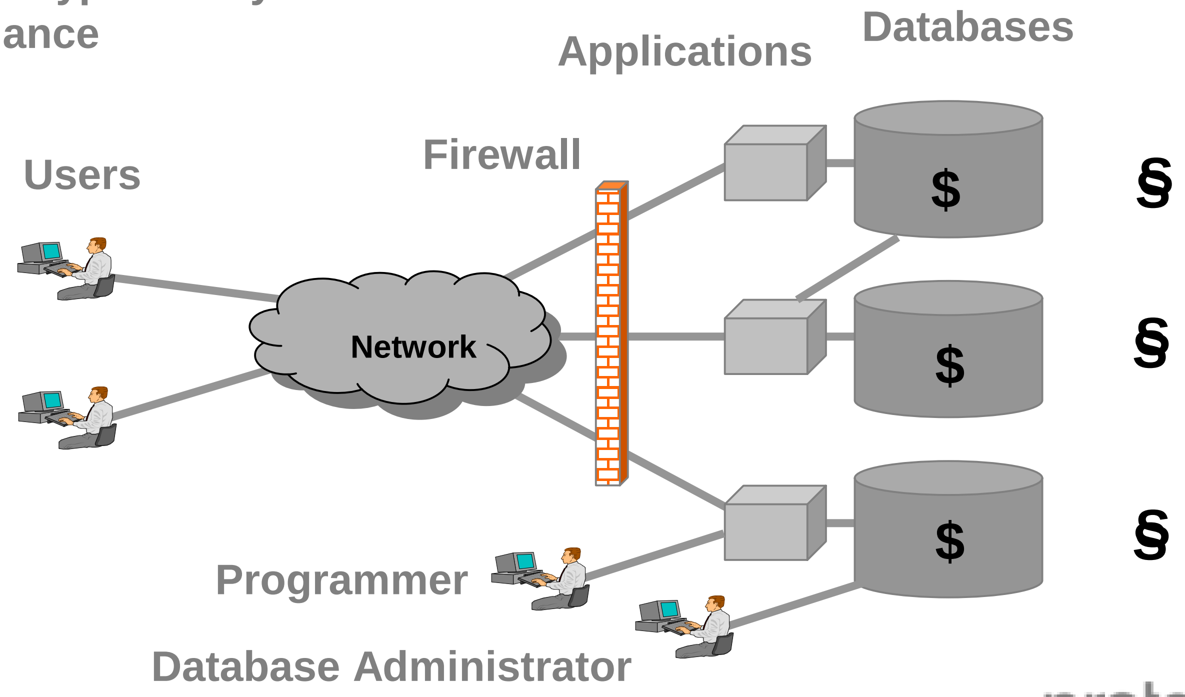
The 1994 Mission – Early European Legislation

Mission:

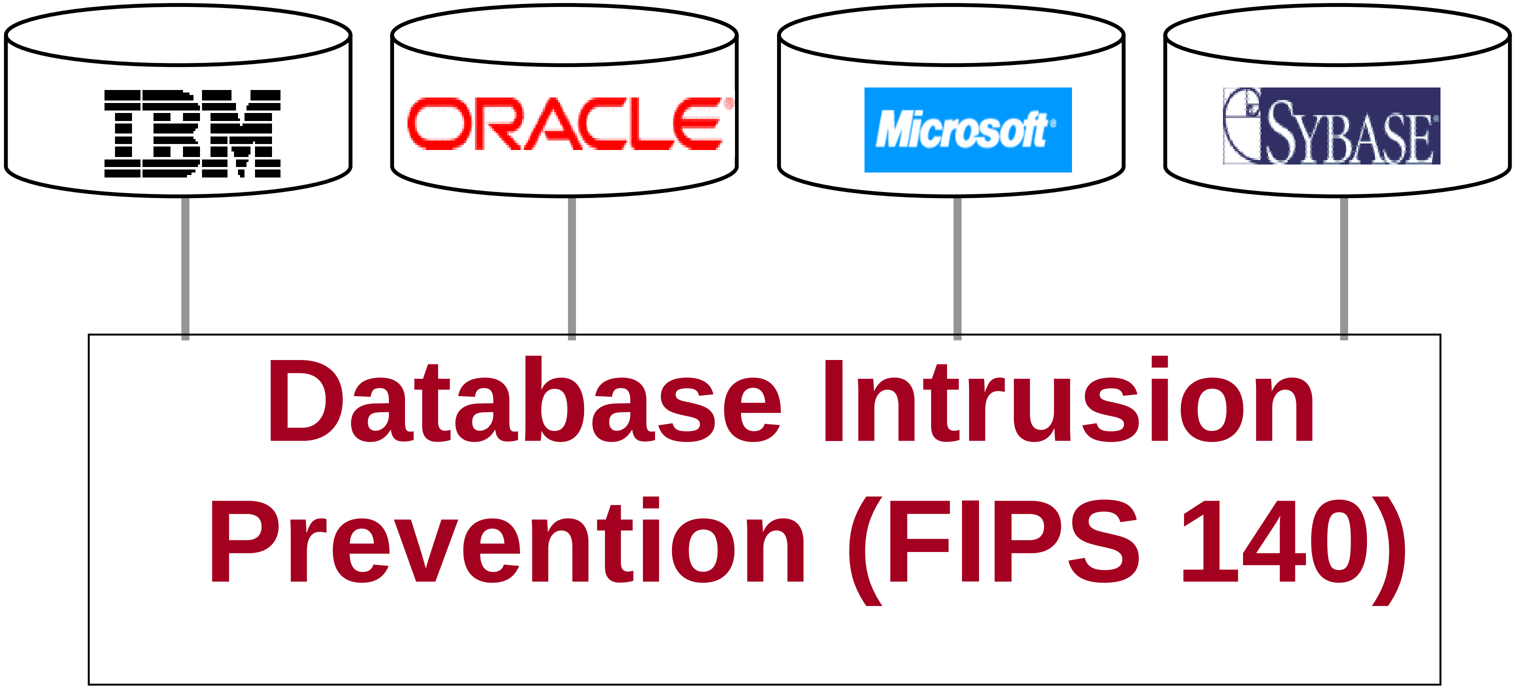
- Protection of Critical Database Information from **External and Internal Threats**
- Regulatory **Compliance and Accountability**

Main Issues:

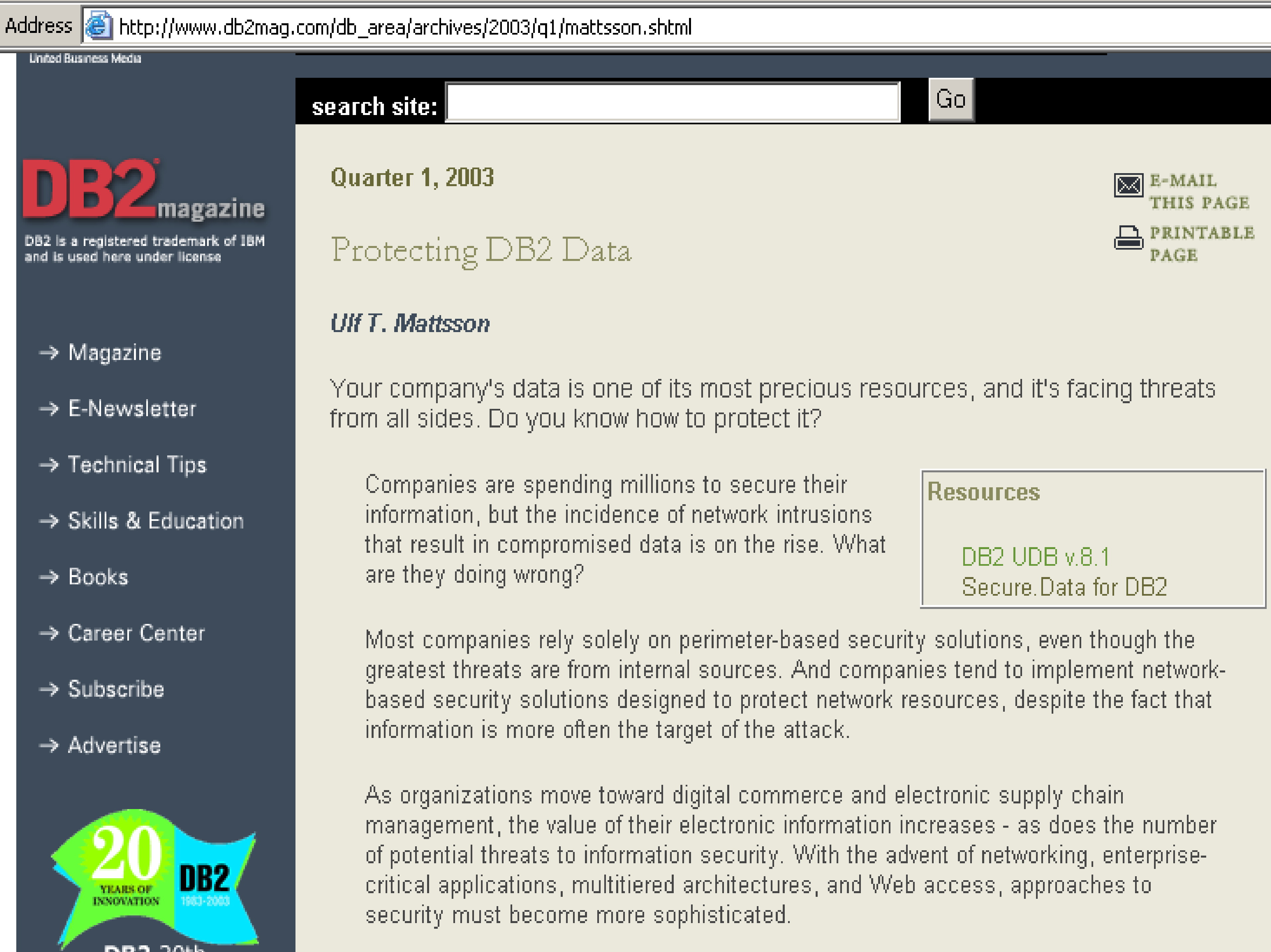
- **Legacy** Support - Application Transparency
- **Data Sharing** Across Applications
- Protection of Data **Encryption Keys**
- Operational **Performance**



‘The 1994 Mission – Early European Legislation’



Database Intrusion Prevention (FIPS 140)



Quarter 1, 2003

Protecting DB2 Data

Ulf T. Mattsson

Your company's data is one of its most precious resources, and it's facing threats from all sides. Do you know how to protect it?

Resources

DB2 UDB v.8.1
Secure.Data for DB2

Companies are spending millions to secure their information, but the incidence of network intrusions that result in compromised data is on the rise. What are they doing wrong?

Most companies rely solely on perimeter-based security solutions, even though the greatest threats are from internal sources. And companies tend to implement network-based security solutions designed to protect network resources, despite the fact that information is more often the target of the attack.

As organizations move toward digital commerce and electronic supply chain management, the value of their electronic information increases - as does the number of potential threats to information security. With the advent of networking, enterprise-critical applications, multitiered architectures, and Web access, approaches to security must become more sophisticated.

Sensitive Information

What are Protegrity's clients protecting?

- The Investment Banker: While allowing each broker access to the corporate database, Secure.Data restricts permissions to the non-public personal information of clients belonging to other associates not required to view such sensitive data.
- The Communications Services Provider: Billing is charged to client credit cards on a monthly basis. Secure.Data was implemented to enforce the separation of duties between database administrators and the Accounts Payable department, by only allowing access to credit card information in Finance.

Sensitive Information

What are Protegrity’s clients protecting?

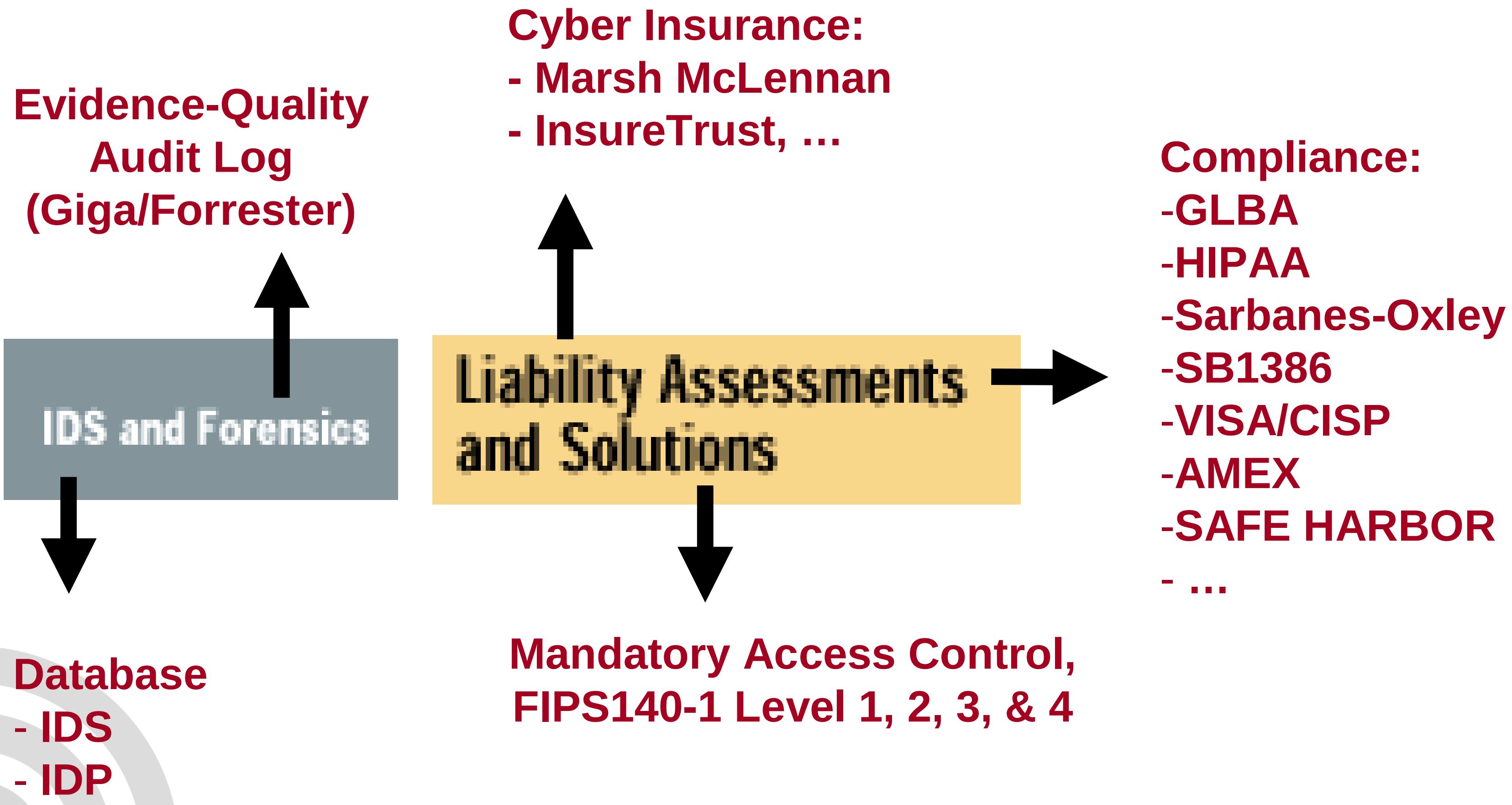
- The Telecom: Adhering to the Telecom Act of 1996 by protecting client data through selective encryption.
- The Computer Software & Services Provider: Our client is using Secure.Data along with their Human Resources application to prevent salary information from being disclosed within any area other than HR.
- The Food and Beverage Company: In the soft drink space, providing access to sensitive formula information must be strictly controlled. Protegrity’s Secure.Data protects this mission critical asset from both internal and external threats.

Sensitive Information

What are Protegrity’s clients protecting?

- Human Services: As a solutions provider to state social services agencies, our client is required by law to protect the confidentiality and integrity of client data.
- Pharmaceutical: The research arm of one of our clients uses Secure.Data to protect the identities of chronically ill patients suffering from a deadly disease.
- Transportation: Our client in the railroad industry protects details regarding the cargo manifest and the shipping schedule. Especially today, protecting this information is a primary security concern.

Case Studies



Evidence-Quality
Audit Log
(Giga/Forrester)

Cyber Insurance:
- Marsh McLennan
- InsureTrust, …

IDS and Forensics

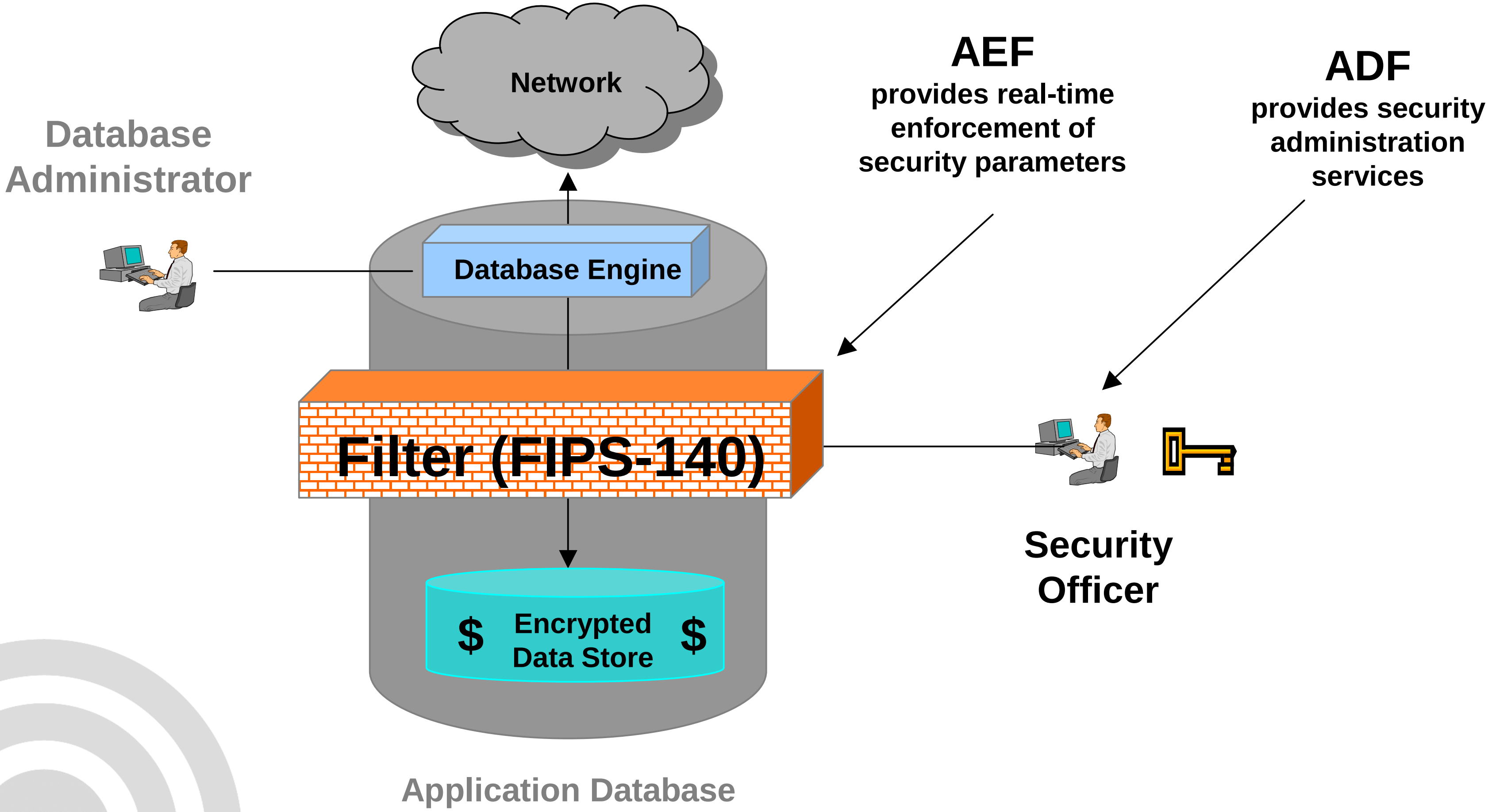
Liability Assessments and Solutions

Compliance:
-GLBA
-HIPAA
-Sarbanes-Oxley
-SB1386
-VISA/CISP
-AMEX
-SAFE HARBOR
- …

Database
- IDS
- IDP

Mandatory Access Control,
FIPS140-1 Level 1, 2, 3, & 4

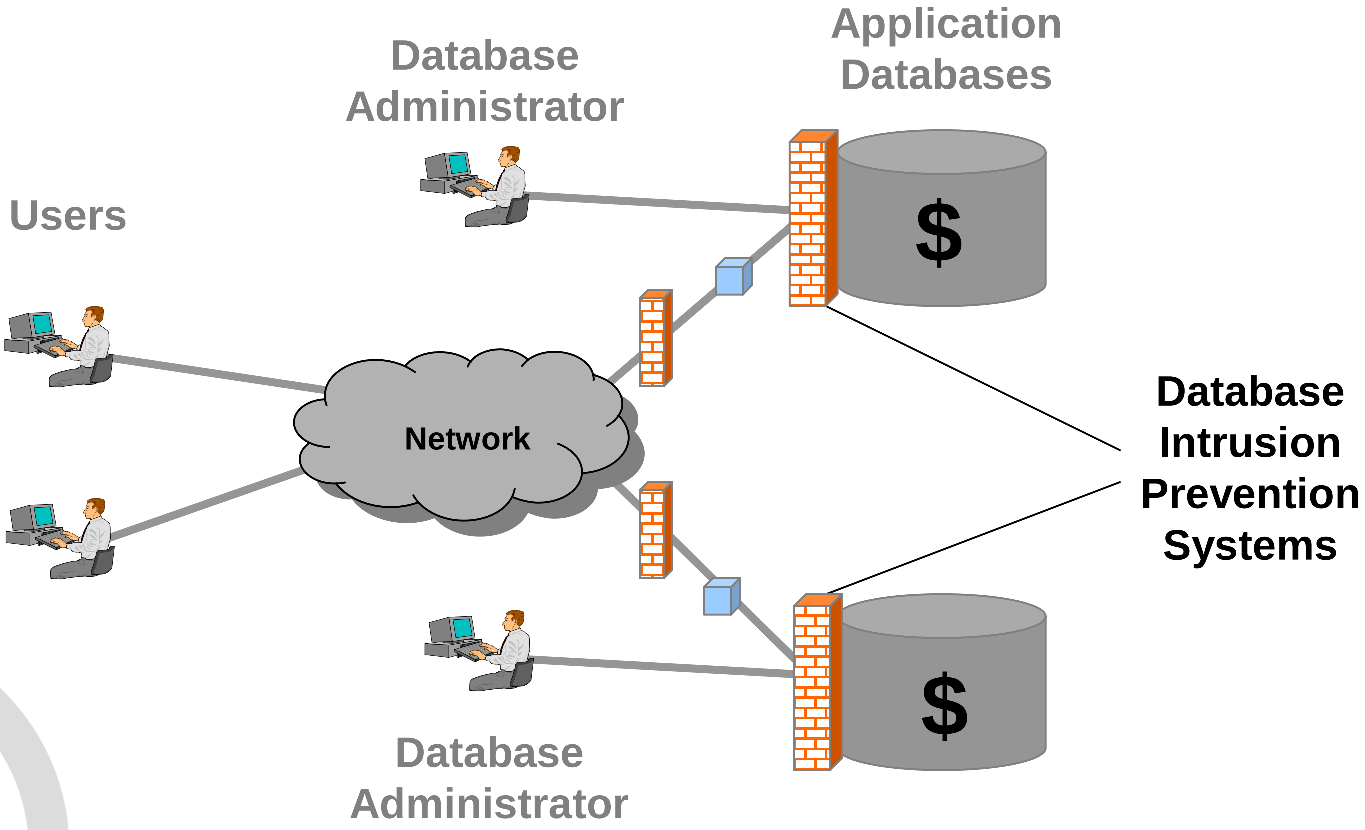
Security Management Standard - ISO/IEC 10181-31



Down and Popek: Design of a Secure Database

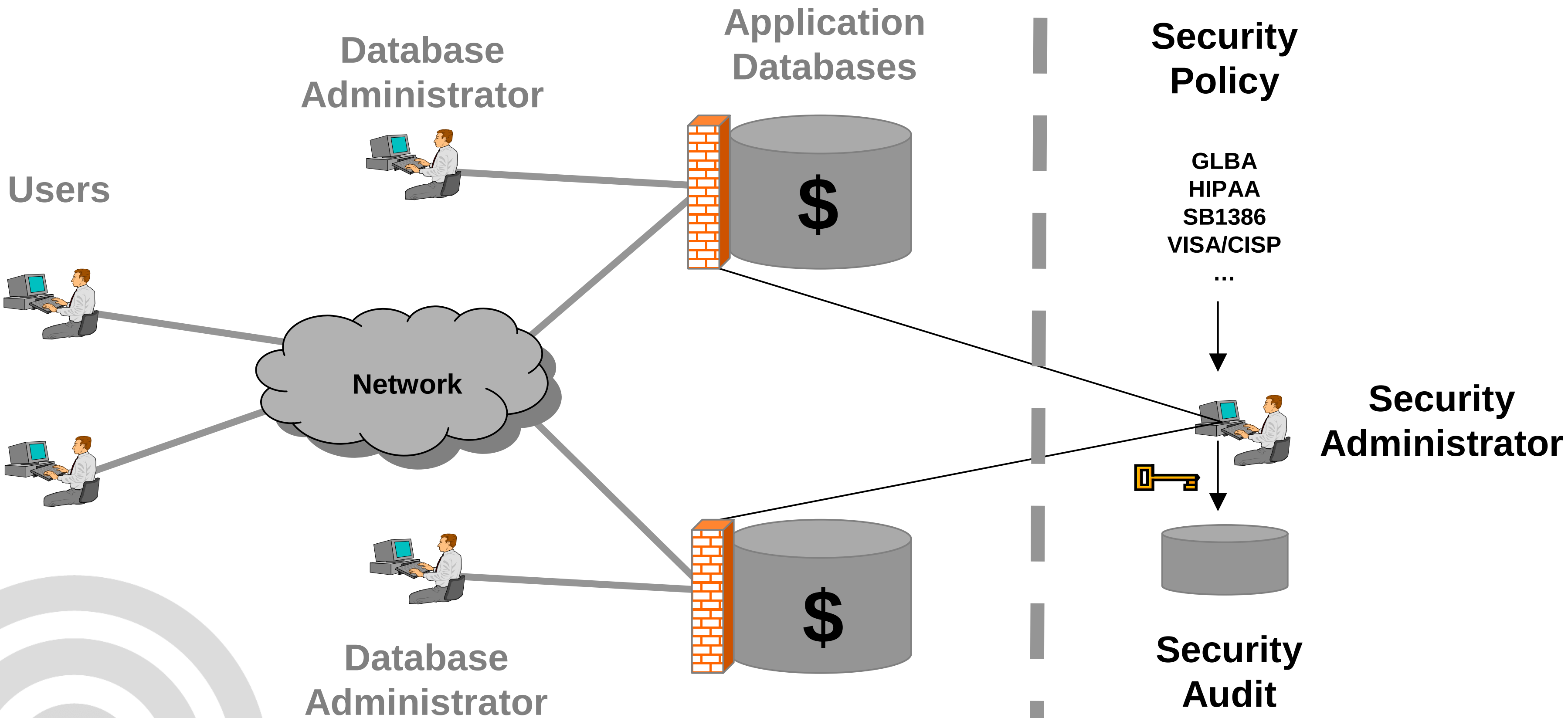
The Database Intrusion Prevention System

The proposed solution locks down the database to both enforce correct behavior and block abnormal behavior. The default policy ensures rapid deployment.

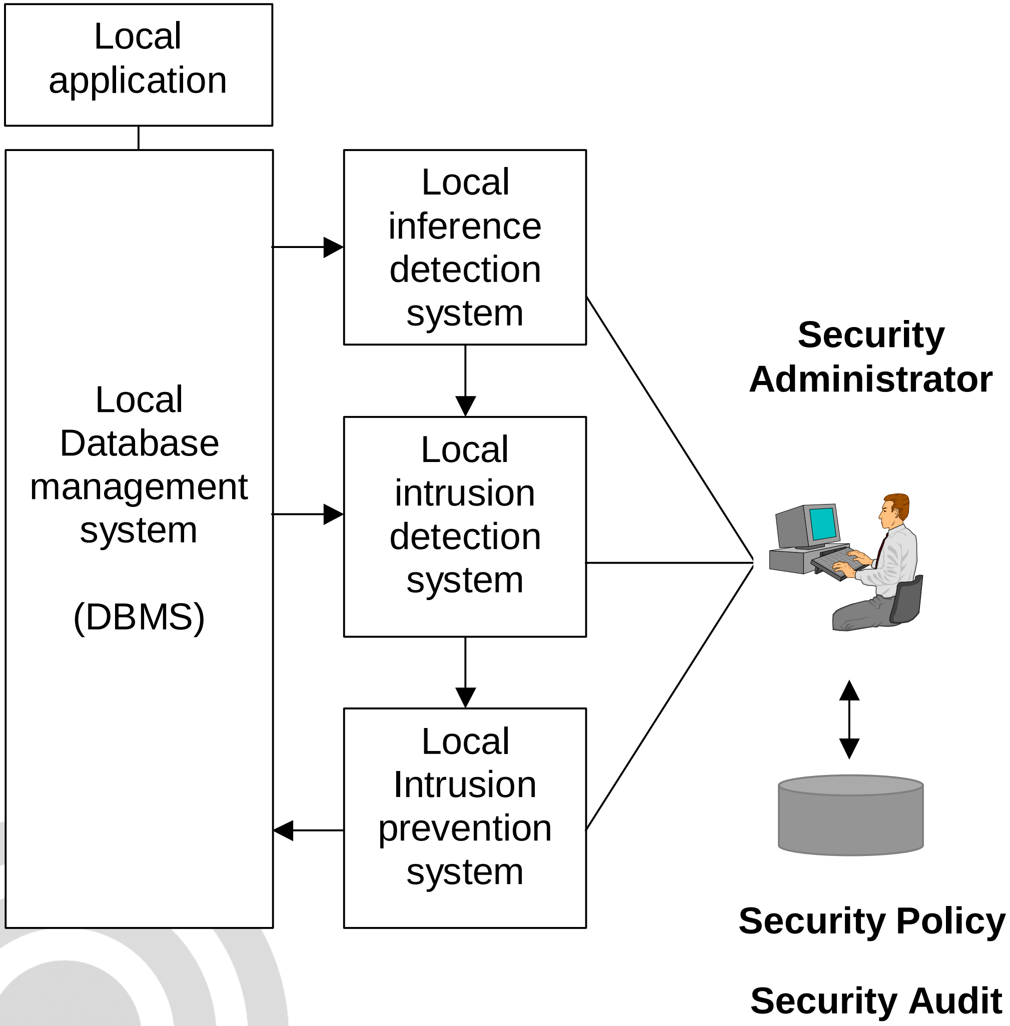


Best Practice (Visa USA) – Dual Control

Use ‘split knowledge” or “dual control” to preserve system security.



Database Intrusion Prevention - Components



Local application

Local Database management system

(DBMS)

Local inference detection system

Local intrusion detection system

Local Intrusion prevention system

Security Administrator

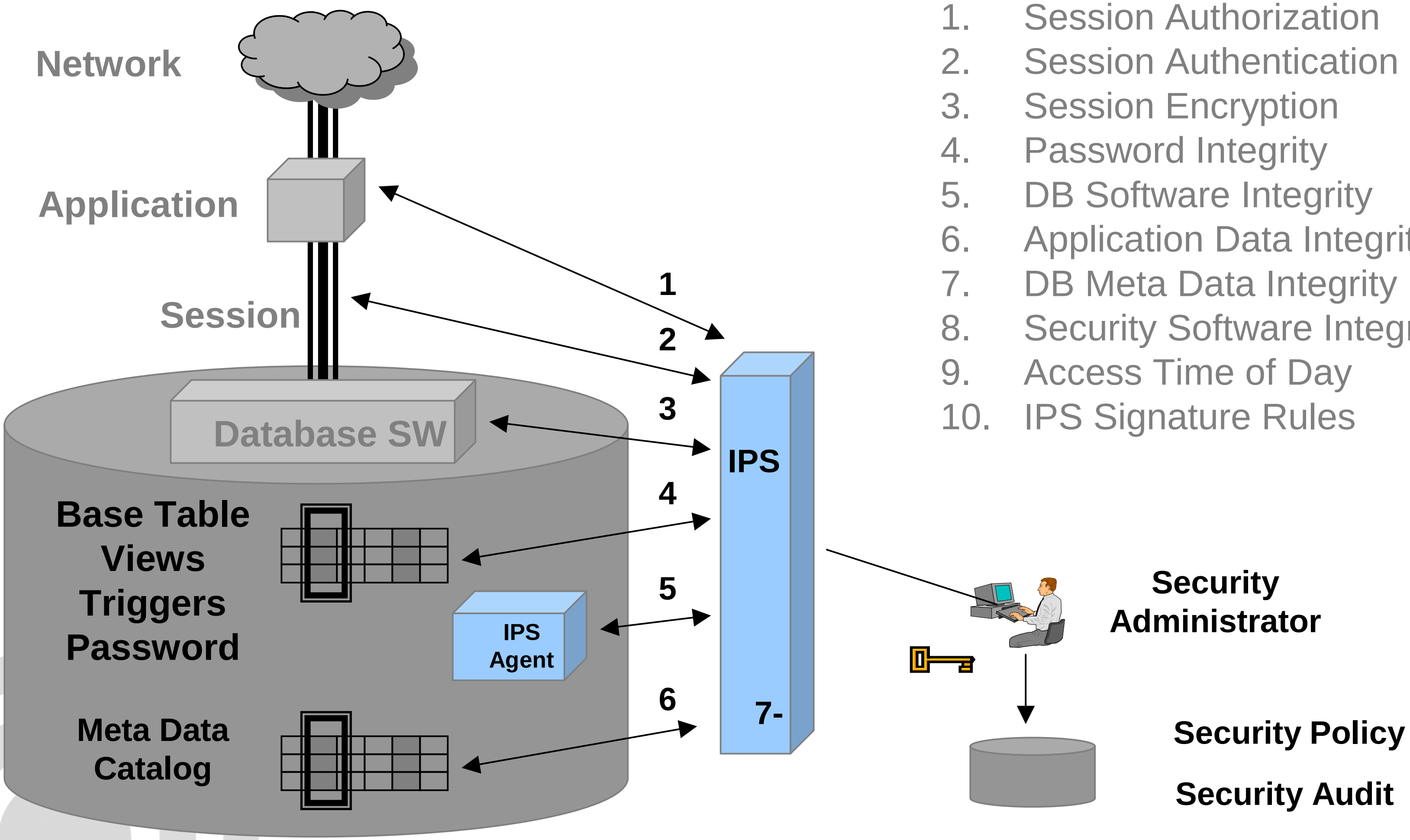
Security Policy

Security Audit

Security Policy Enforcement:

1. Session Authorization
2. Session Authentication
3. Session Encryption
4. Password Integrity
5. DB Software Integrity
6. Application Data Integrity
7. DB Meta Data Integrity
8. Security Software Integrity
9. Access Time of Day
10. IPS Signature Rules

Database Intrusion Prevention - Implementation



Security Policy Enforcement:

1. Session Authorization
2. Session Authentication
3. Session Encryption
4. Password Integrity
5. DB Software Integrity
6. Application Data Integrity
7. DB Meta Data Integrity
8. Security Software Integrity
9. Access Time of Day
10. IPS Signature Rules

Privacy & Security Legislation

- **New legislation demands it**
  1. GLBA
  2. HIPAA
  3. Safe Harbor
- **Business partners and trade associations require it**
  1. VISA CISP
  2. American Express MDSS
  3. MasterCard SDPS
- **International businesses assume it**
- **Customers expect it**

Protecting Privacy

Health-care and financial-services companies turn to security vendors to bring them into compliance with new federal rules

rontEnd

THE WALL STREET JOURNAL

POLITICS & P

Identity Theft Dogs Credit Firms In the Supreme Court, Congress

rcuits

THE Inside News

STRATEGIC NEWS AND ANALYSIS

Privacy's Guarded Prognosis

With More Medical Records Stored on Computer Networks, Whose Eyes Will See Them?

Security concerns top agenda

Health care industry braces for privacy rules

administration moves ahead with HIPAA regulations despite IT concerns

The price of medical records privacy

ZIFF DAVIS MEDIA

February 16, 2004

eWEEK®

THE ENTERPRISE NEWSWEEKLY

OPINION

ERIC LUNDQUIST

Offshore: A better deal? 27

PETER COFFEE

Exposing source code serves development 34

NEWS & ANALYSIS

Microsoft in security hot seat

Windows flaw found; code leaked to Web 9

Push for grid computing is on

Database makers add grid features 12

Securing the wireless network

Symbol, Cisco upgrades take aim at SMBs 14

FCC to move quickly on VOIP

Ready, set, comply

SARBANES-OXLEY: ROAD TO COMPLIANCE

PART 1 IN A SERIES

By Dennis Callaghan

S THE INITIAL JUNE DEAD-

Not surprisingly, IT depart-

more costly and time-consuming

ZIFF DAVIS MEDIA

eW

THE ENTERPRISE

As part of the compliance process, Volt IT personnel needed to document security and application access as well

NEWS & ANALYSIS

Microsoft in security hot seat

Windows flaw found;

Ready, set, comply

Keeping up with Sarbanes-Oxley

Five steps to compliance

- **Planning** Form compliance committee, select software to assist in compliance process
- **Scoping** Determine what information needs to be documented and is material to company
- **Documentation** Document business processes and controls in place to ensure information is accurate
- **Gap analysis** Identify and remediate inadequate controls
- **Implementation, evaluation and monitoring of controls** Document and update controls as needed, then turn them over to audit team, which evaluates depth and effectiveness of controls; develop ongoing process for monitoring controls

Breaking it down

The average billion-dollar public company ...

- **Manages** 48 disparate financial systems
- **Manages** 2.7 enterprise resource planning systems
- **Uses** stand-alone spreadsheets for financial reporting (47 percent)

California's Database Security Breach Notification Act

Effective July 1, 2003, SEC. 2. Section 1798.29 is added to the Civil Code:

- Any agency that owns or licenses computerized data that includes personal information shall **disclose any breach of the security** of the system following discovery or notification of the breach in the security of the data to any resident of California whose **<u>unencrypted</u>** personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

- 1798.82. A. Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall **disclose any breach of the security** of the system following discovery or notification of the breach in the security of the data to any resident of California whose **<u>unencrypted</u>** personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

GLBA/OCC IT Requirements

1. **Access control** and authentication
2. **<u>Encryption, including transit and storing</u>**
3. Implementation to confirm modifications consistent with InfoSecPol
4. **Segregation of duties for access control management**
5. **Mechanism to protect the security by service provider**
6. **Monitoring system to detect actual attempted attacks**
7. Response when **unauthorized access is suspected or detected**
8. Response to **preserve integrity and security**

OCC Data Security Regulations II.A-B; III.A-D for GLBA

HIPAA IT Requirements

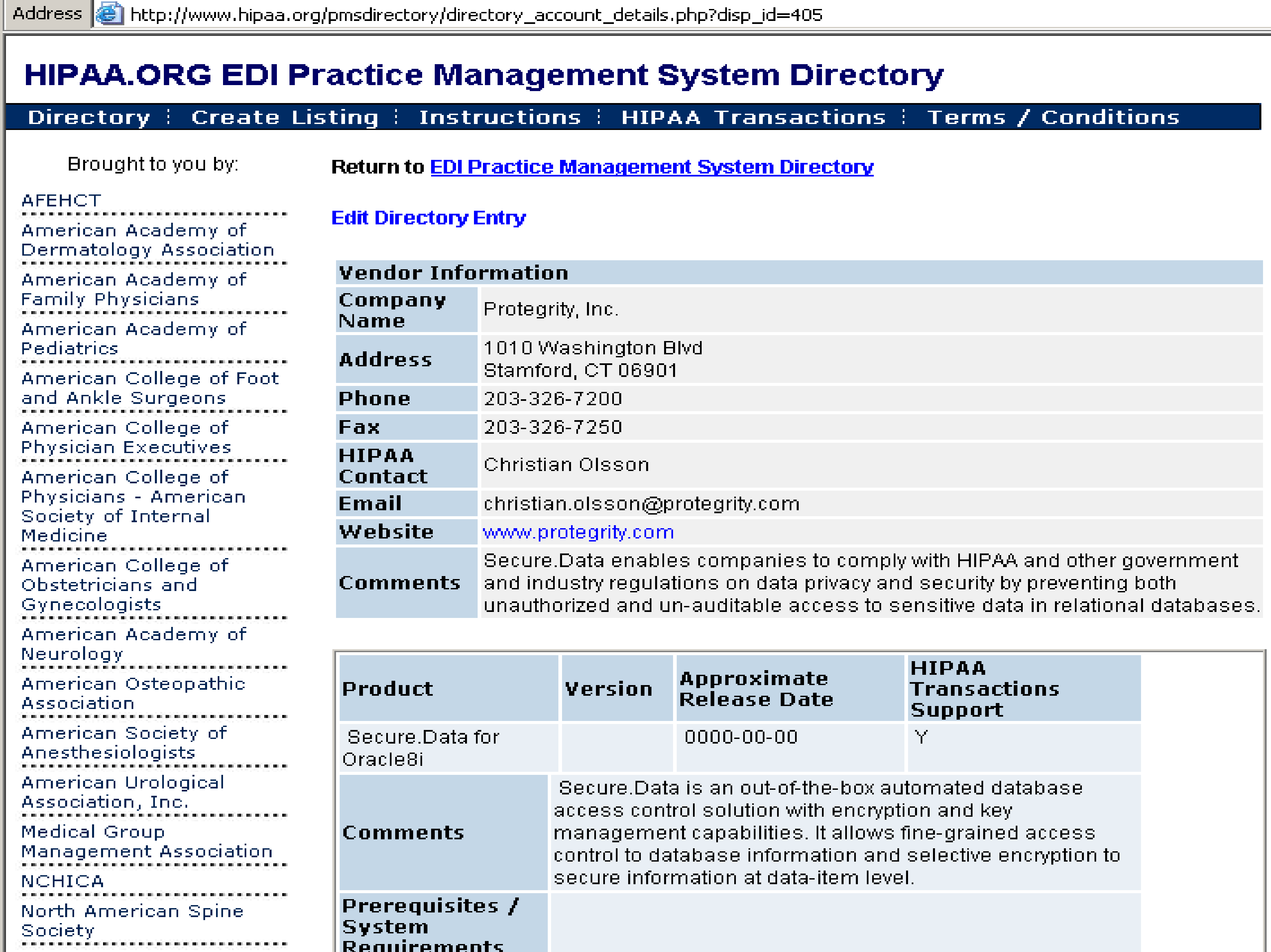
1. Data to be Protected - “patient identifiable information”, not necessarily medical records
2. Healthcare is Data Driven & Data Intensive
3. Shorthand for security requirements:
   - Confidentiality
   - Integrity
   - Individual Accountability
4. Current Interpretation is Data at Rest as well as Data during Transmission
5. Protegrity provides trusted functionality (access control, integrity, confidentiality, audit trails) as required by HIPAA and as needed by business requirements
6. Protegrity provides the means for this functionality across several applications and platforms

Visa USA CISP Requirements

ISSUE

1. Install and maintain a working network firewall to protect data accessible via the Internet
2. Keep security patches up-to-date
3. **Encrypt stored data**
4. Encrypt data sent across open networks
5. Use regularly update anti-virus software
6. **Restrict access to data by business “need to know”**
7. Assign unique ID to each person with computer access to data.
8. Don’t use vendor-supplied defaults for system passwords and other security parameters
9. **Track access to data by unique ID**
10. Regularly test security systems and processes
11. **Maintain a policy that addresses information security for employees and contractors**
12. Restrict physical access to cardholder information

Best Practice: **Use ‘split knowledge” or “dual control” to preserve system security.**



Address
http://www.hipaa.org/pmsdirectory/directory_account_details.php?disp_id=405

HIPAA.ORG EDI Practice Management System Directory

Directory | Create Listing | Instructions | HIPAA Transactions | Terms / Conditions

Brought to you by:

- AFEHCT
- American Academy of Dermatology Association
- American Academy of Family Physicians
- American Academy of Pediatrics
- American College of Foot and Ankle Surgeons
- American College of Physician Executives
- American College of Physicians - American Society of Internal Medicine
- American College of Obstetricians and Gynecologists
- American Academy of Neurology
- American Osteopathic Association
- American Society of Anesthesiologists
- American Urological Association, Inc.
- Medical Group Management Association
- NCHICA
- North American Spine Society

Return to EDI Practice Management System Directory

Edit Directory Entry

Vendor Information	
Company Name	Protegrity, Inc.
Address	1010 Washington Blvd Stamford, CT 06901
Phone	203-326-7200
Fax	203-326-7250
HIPAA Contact	Christian Olsson
Email	christian.olsson@protegrity.com
Website	www.protegrity.com
Comments	Secure.Data enables companies to comply with HIPAA and other government and industry regulations on data privacy and security by preventing both unauthorized and un-auditable access to sensitive data in relational databases.

Product	**Version**	**Approximate Release Date**	**HIPAA Transactions Support**
Secure.Data for Oracle8i		0000-00-00	Y
Comments	Secure.Data is an out-of-the-box automated database access control solution with encryption and key management capabilities. It allows fine-grained access control to database information and selective encryption to secure information at data-item level.		
Prerequisites / System Requirements			

Privacy Legislation & Industry Initiatives

Privacy Legislation:

- U.S. Gramm-Leach-Bliley Act, (GLBA) extended with the U.S. Office of the Comptroller of Currency (OCC) requirements for the financial services industry
- U.S. Healthcare Insurance Portability and Accountability Act (HIPAA)
- U.S. Food & Drug Administration (FDA) 21CFR 11 Electronic Records; Electronic Signatures for Clinical Trials
- U.S. State of California SB 1386 Disclosure Law
- E.U. 95/46/EC Directive on Data Privacy (Safe Harbor) and individual E.U. member state privacy legislation
- Canada's Personal Information Protection and Electronic Document Act (PIPEDA)

Industry Initiatives:

- ISO 17799 Code of Practice for Security Management
- American Express Merchant Data Security Standards
- MasterCard Site Data Protection Service
- VISA Cardholder Information Security Program (CISP)
- VISA 3D Secure specifications for cardholder data protection
- U.S. Software and Information Industry Association (SIIA) - A method for securing credit card and private consumer data in e-business sites

Typical Compliance Requirements:

User Access Control & Audit

Data Integrity

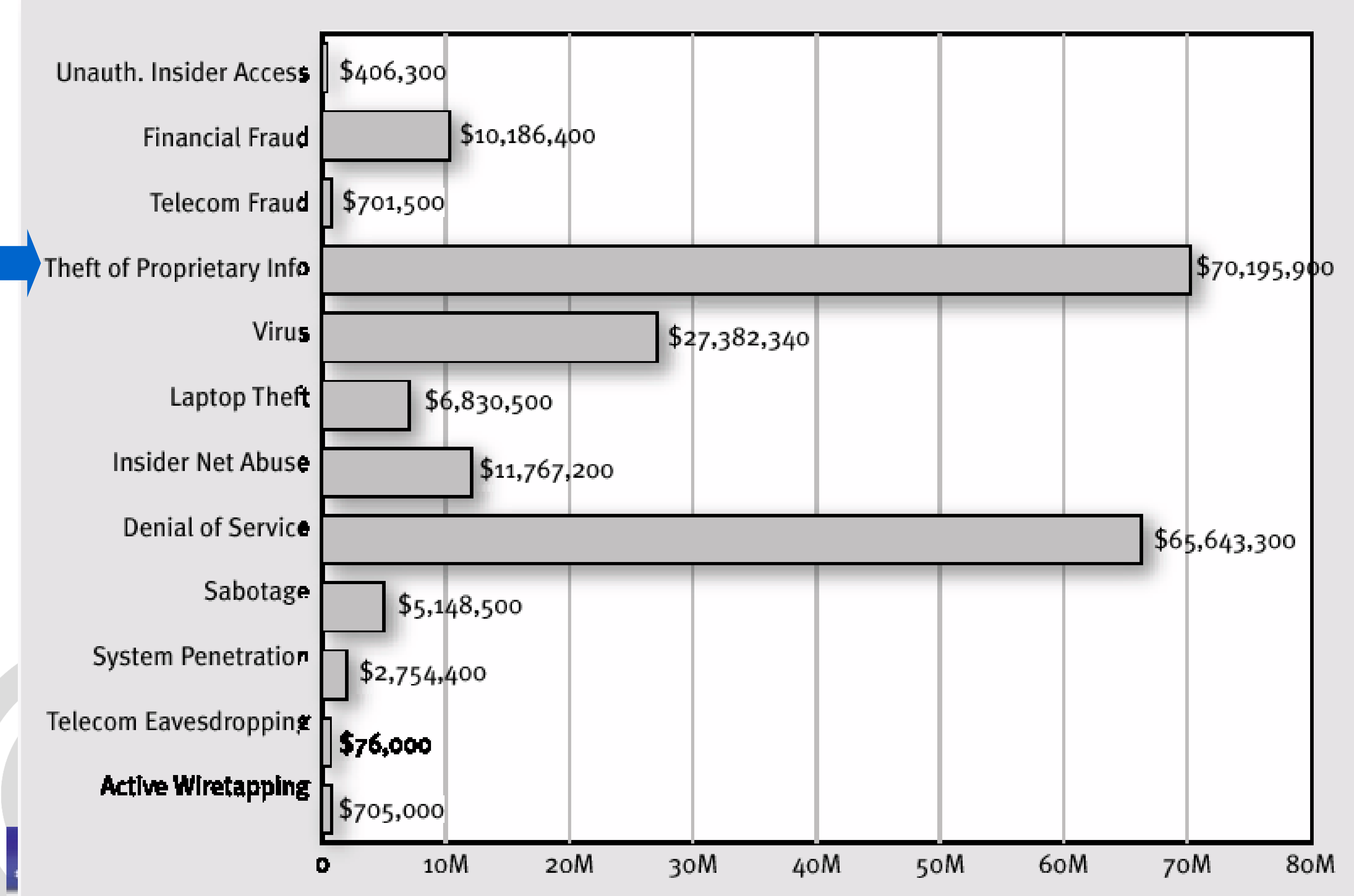
Administrator Access Control & Audit

Response when unauthorized access is suspected or detected

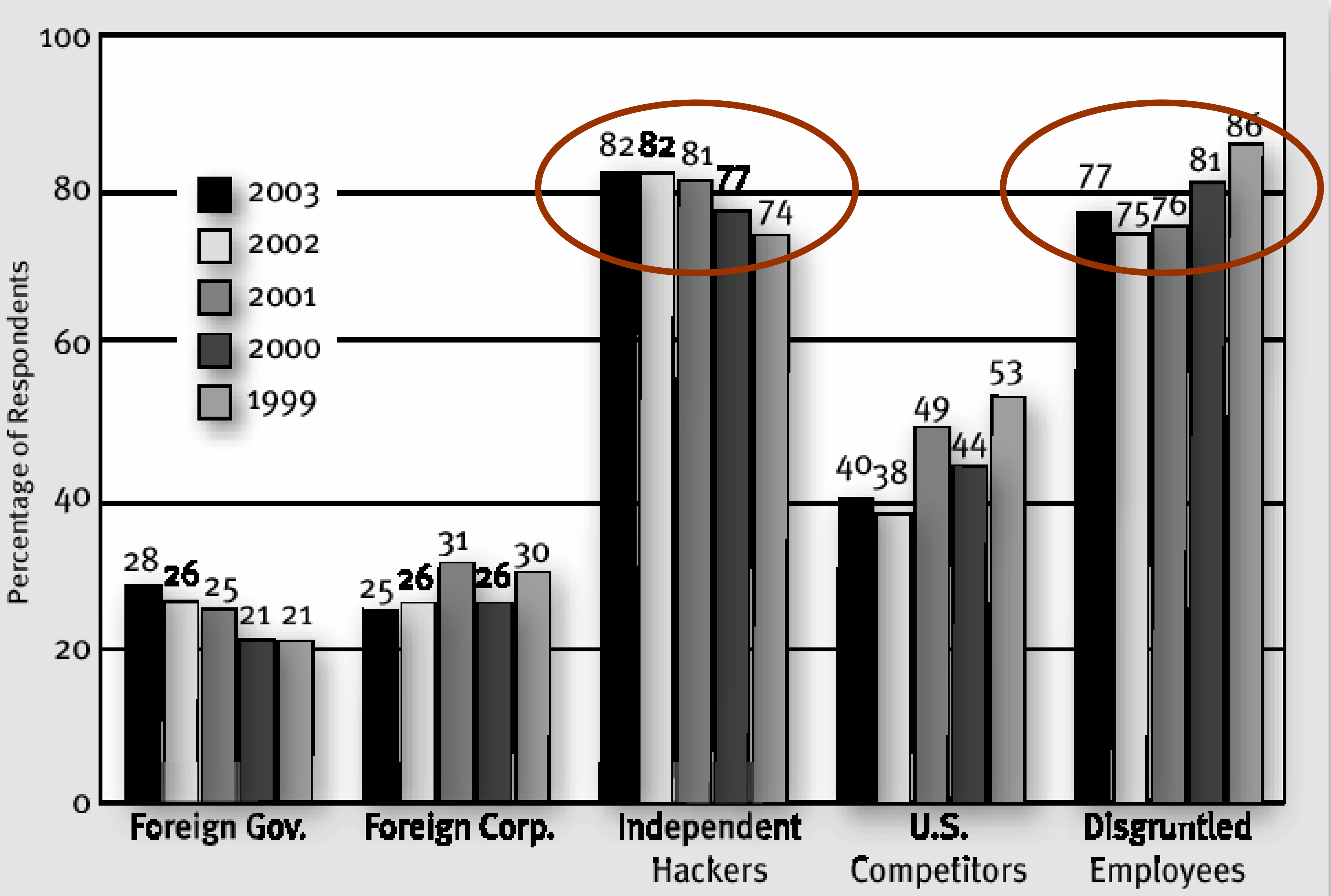
Data Confidentiality

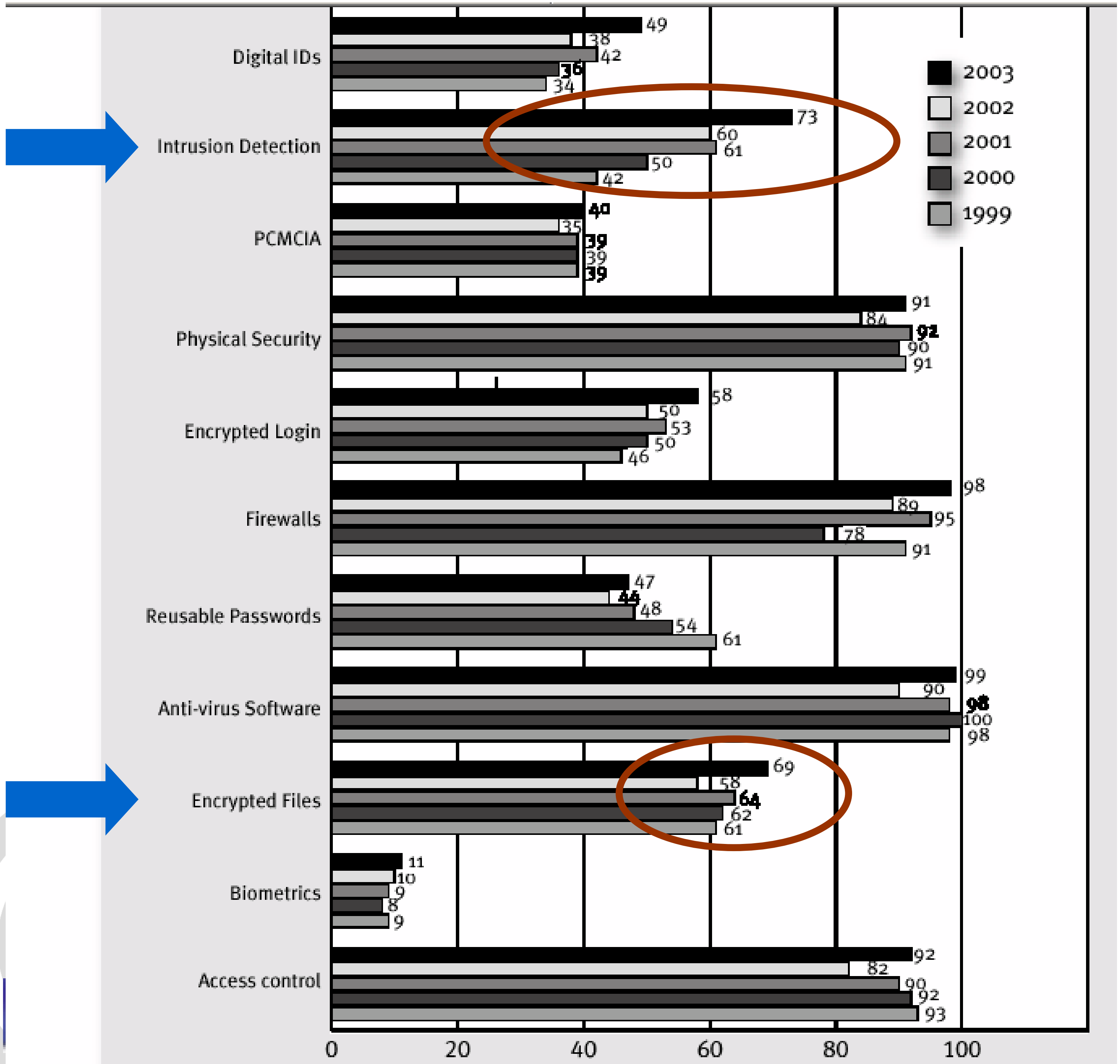
Dollar Amount of Losses by Type

2003 CSI/FBI Computer Crime And Security Survey



Likely Sources of Attack



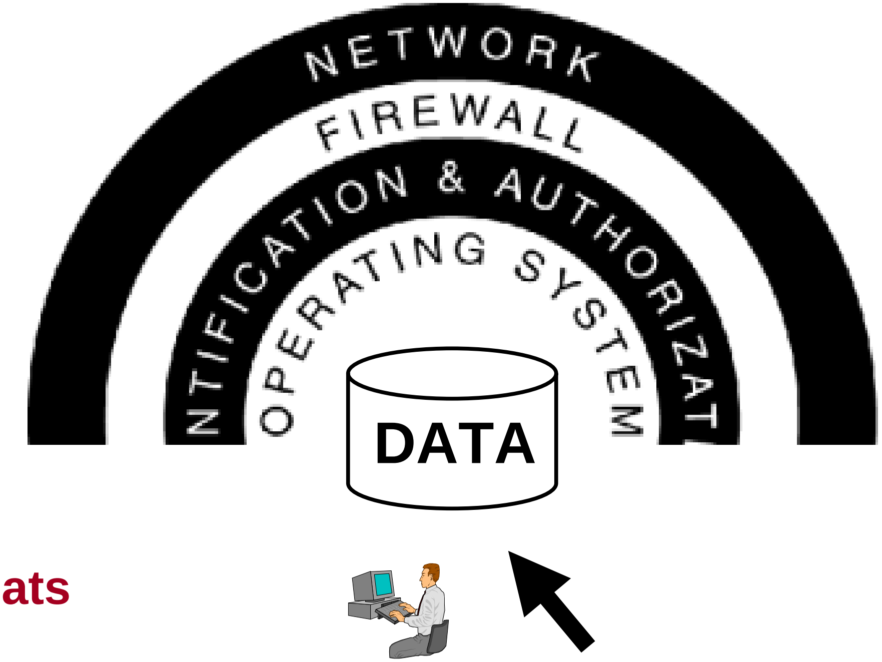


Security Technologies Used,

2003 CSI/FBI Computer Crime And Security Survey

FBI/CSI Statistics - Inside Threats

Outside Threats

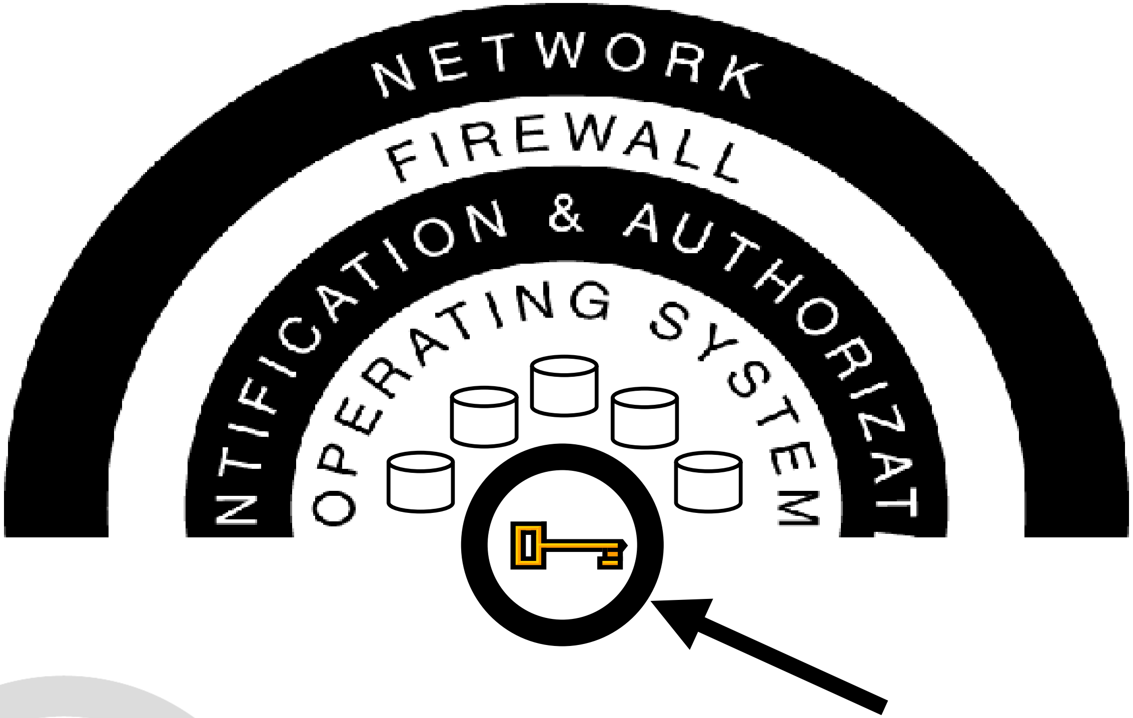


Inside Threats

The most serious financial losses occurred through theft of proprietary information.

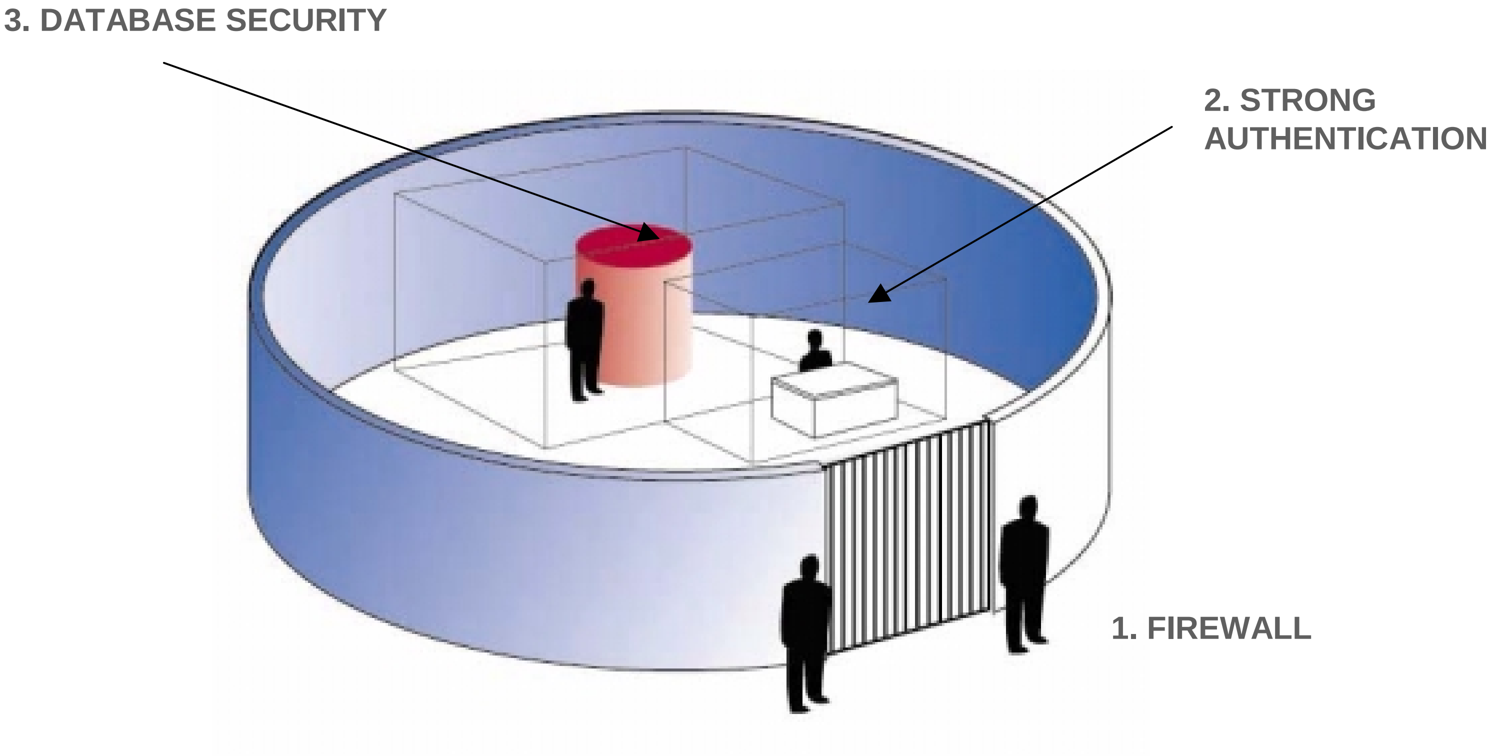
SECURE ’THE KEYS’ TO YOUR CRITICAL DATA

Clear separation of Authentication, Authorization, and Encryption Key Management

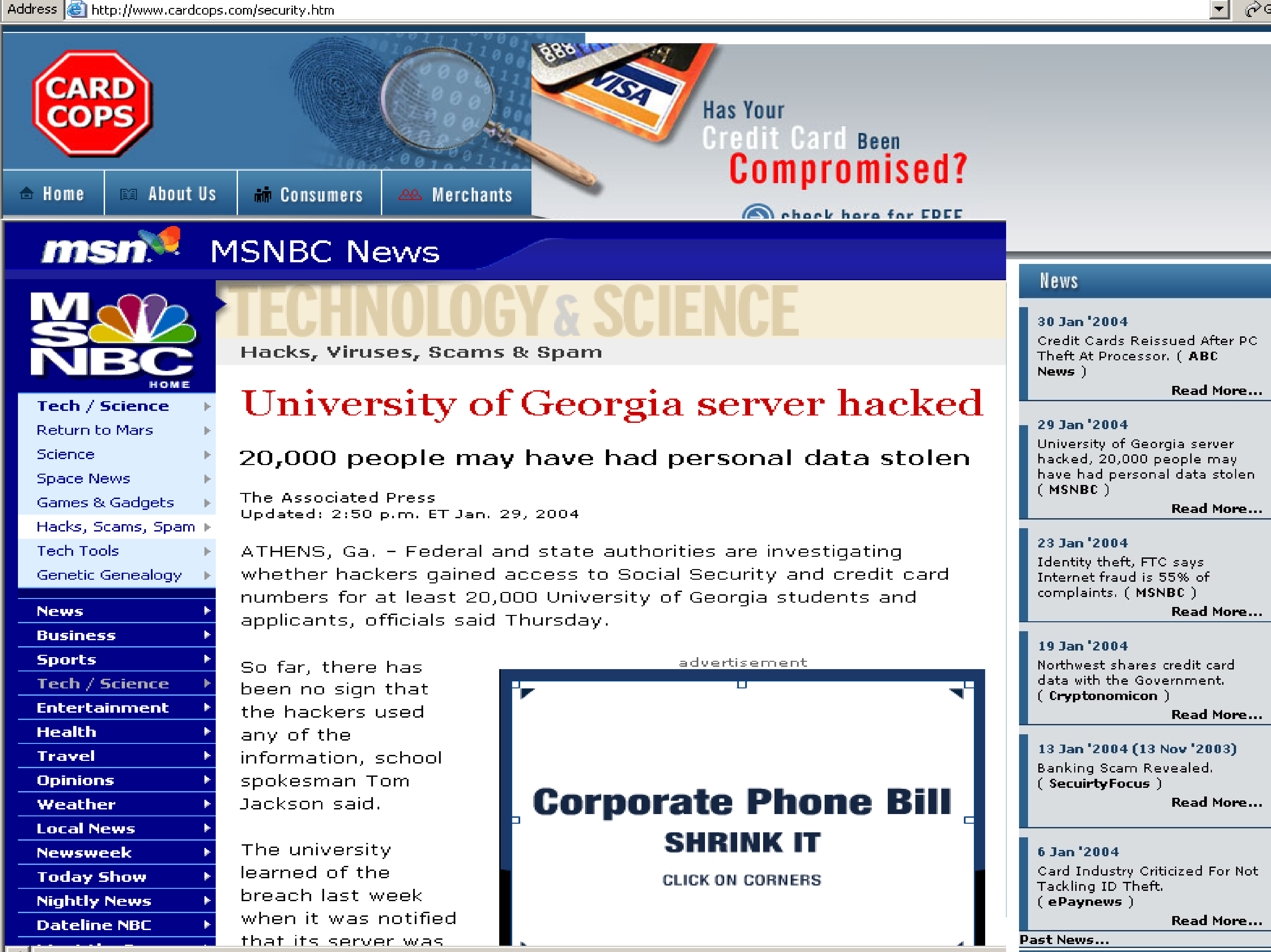


Your platforms may never be secure,
But the keys to your data can be secure.

Security Trend: ‘Inside Out’ – Like a Bank



‘… we are loosing against security each day ...
we need to re-think: inside-out …’



University of Georgia server hacked

20,000 people may have had personal data stolen

The Associated Press
Updated: 2:50 p.m. ET Jan. 29, 2004

ATHENS, Ga. - Federal and state authorities are investigating whether hackers gained access to Social Security and credit card numbers for at least 20,000 University of Georgia students and applicants, officials said Thursday.

So far, there has been no sign that the hackers used any of the information, school spokesman Tom Jackson said.

The university learned of the breach last week when it was notified that its server was

News

30 Jan '2004
Credit Cards Reissued After PC Theft At Processor. (**ABC News**)
Read More...

29 Jan '2004
University of Georgia server hacked, 20,000 people may have had personal data stolen (**MSNBC**)
Read More...

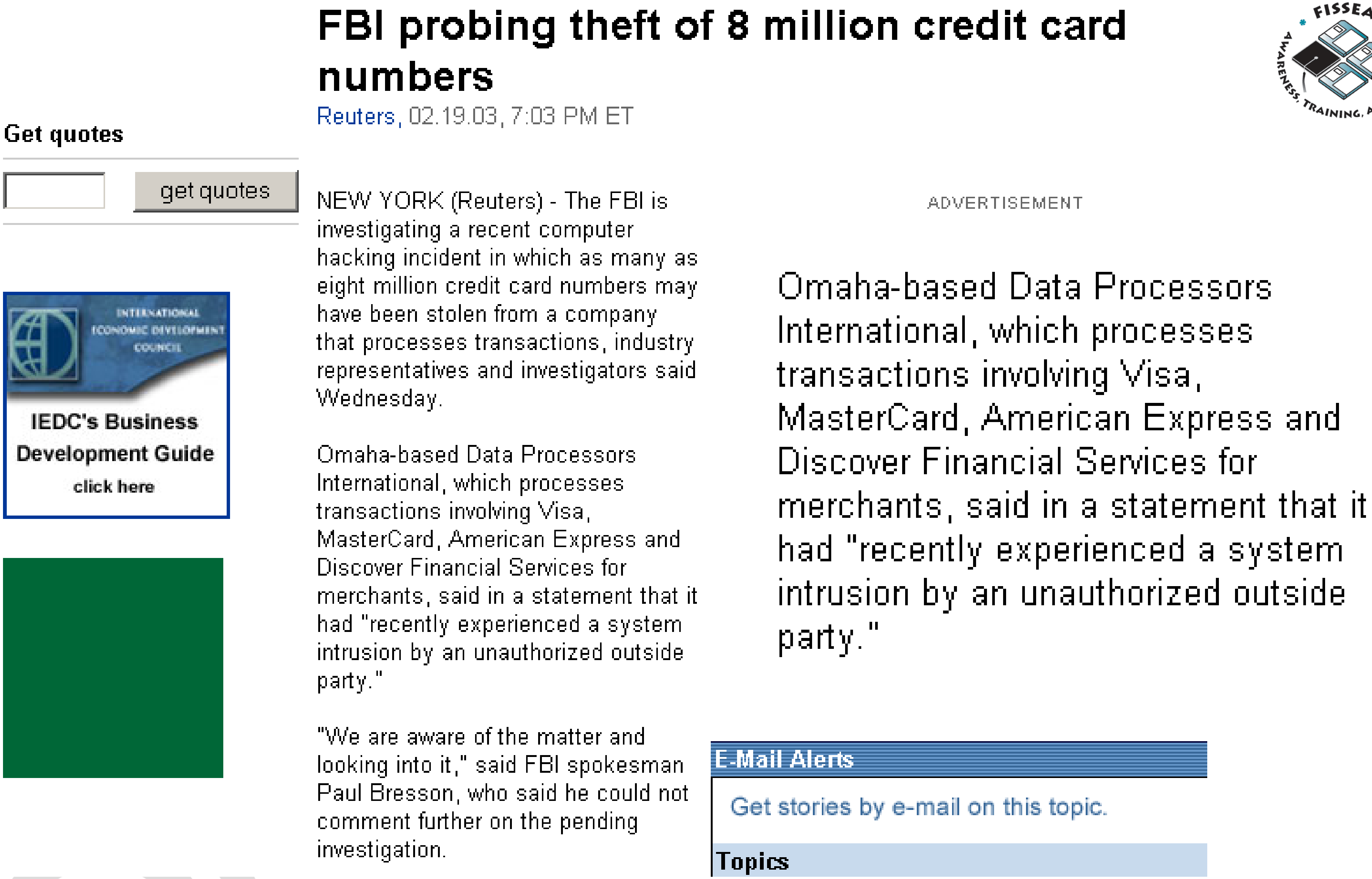
23 Jan '2004
Identity theft, FTC says Internet fraud is 55% of complaints. (**MSNBC**)
Read More...

19 Jan '2004
Northwest shares credit card data with the Government. (**Cryptonomicon**)
Read More...

13 Jan '2004 (13 Nov '2003)
Banking Scam Revealed. (**SecuirtyFocus**)
Read More...

6 Jan '2004
Card Industry Criticized For Not Tackling ID Theft. (**ePaynews**)
Read More...

Past News...



FBI probing theft of 8 million credit card numbers

Reuters, 02.19.03, 7:03 PM ET

Get quotes

get quotes

NEW YORK (Reuters) - The FBI is investigating a recent computer hacking incident in which as many as eight million credit card numbers may have been stolen from a company that processes transactions, industry representatives and investigators said Wednesday.

Omaha-based Data Processors International, which processes transactions involving Visa, MasterCard, American Express and Discover Financial Services for merchants, said in a statement that it had "recently experienced a system intrusion by an unauthorized outside party."

"We are aware of the matter and looking into it," said FBI spokesman Paul Bresson, who said he could not comment further on the pending investigation.

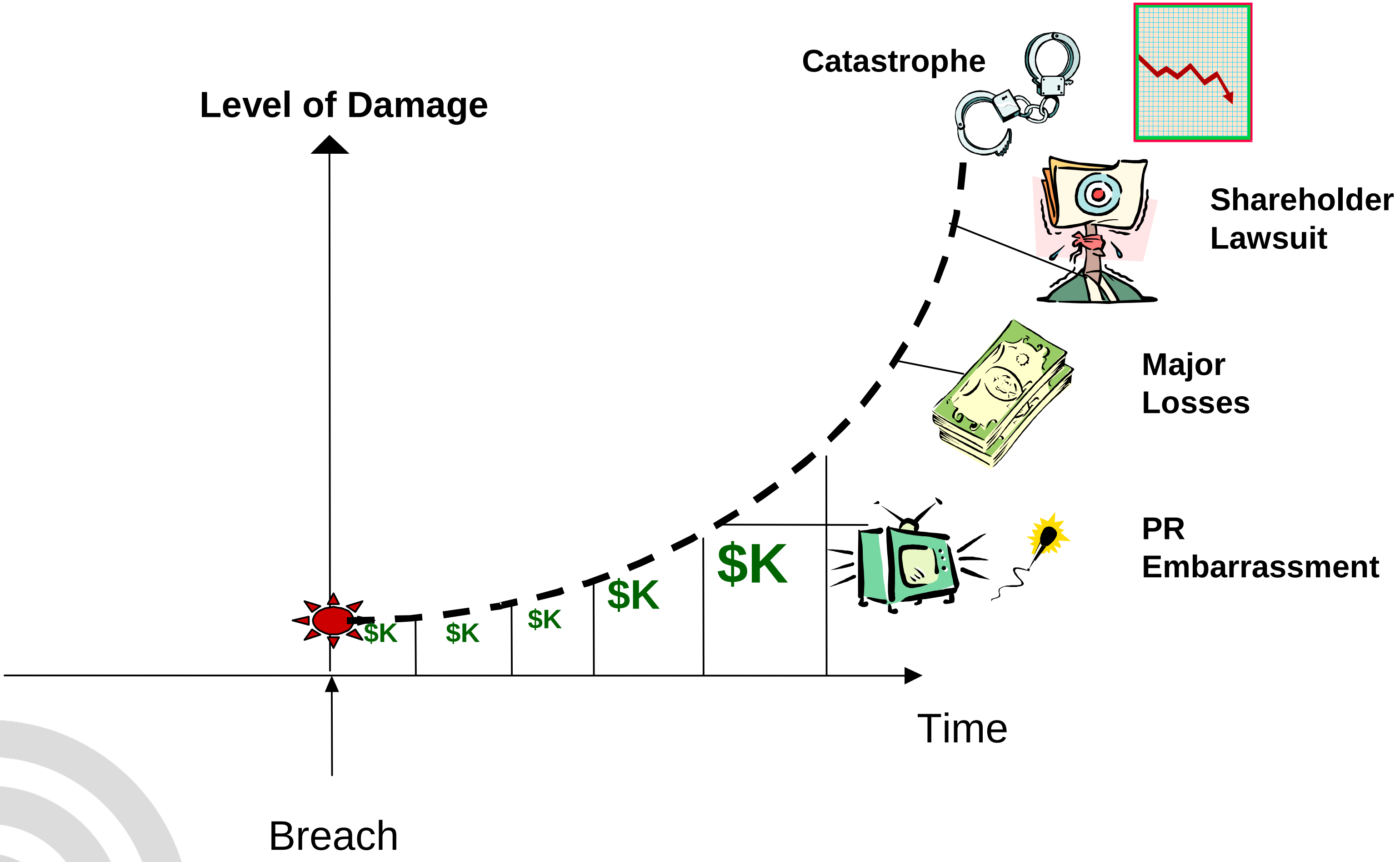
Omaha-based Data Processors International, which processes transactions involving Visa, MasterCard, American Express and Discover Financial Services for merchants, said in a statement that it had "recently experienced a system intrusion by an unauthorized outside party."

E-Mail Alerts

Get stories by e-mail on this topic.

Topics

Liability of a Critical Data Breach



Liability Issues executives need to consider

1. Class and individual action suits
2. Loss of network/database integrity and availability
3. Loss of intellectual capital
4. Loss of employee productivity
5. Defamation of brand name and reputation

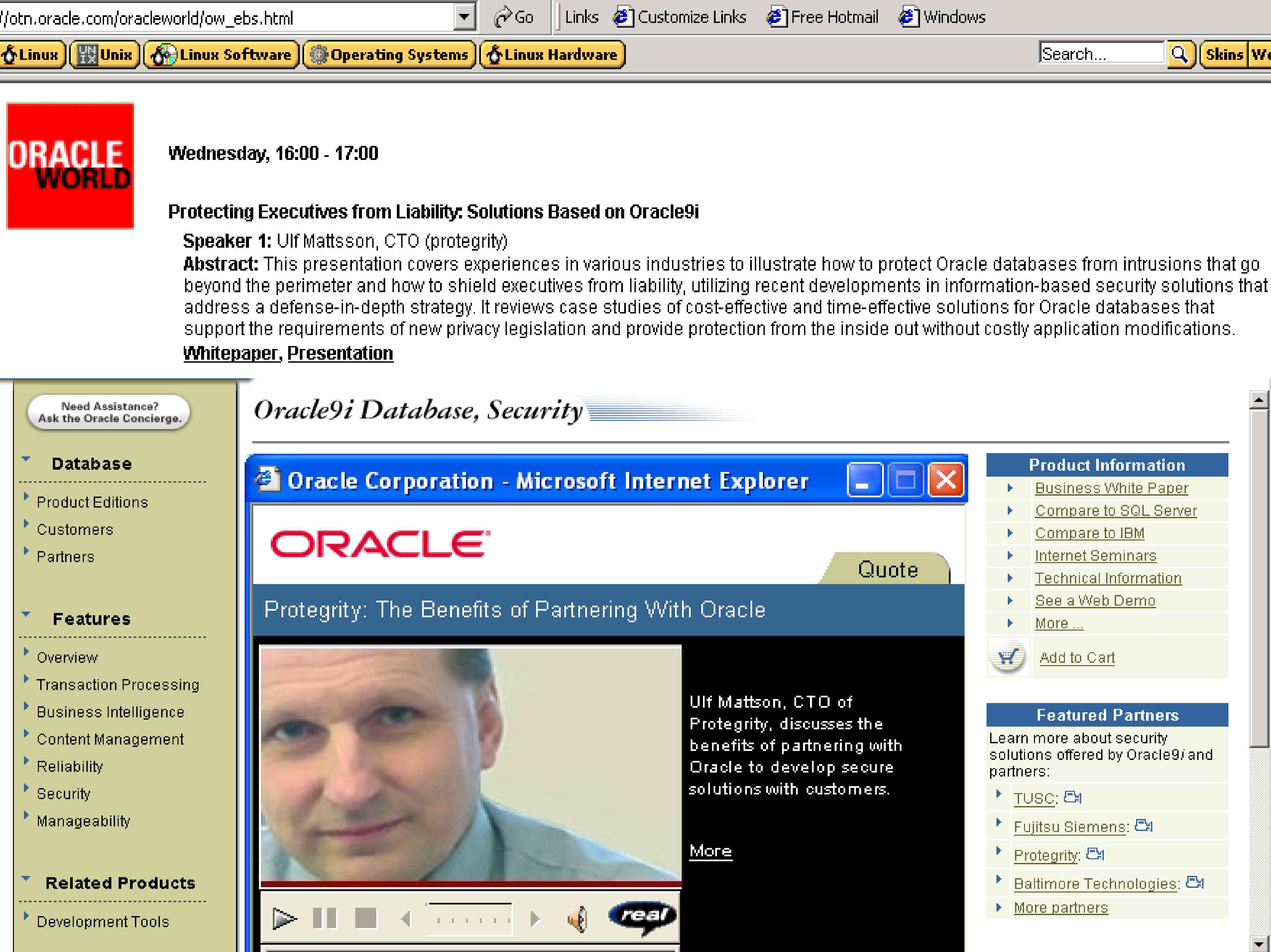
Liability Coverage: Computer Security Insurance

Customers utilizing the
Database Intrusion Prevention Technology
for data-privacy will qualify for up to a
40% discount on breach of
computer security insurance coverage.

Placed with Lloyd's of London, this policy provides the insured broad first party e-business Prevention for highly secure risks. Coverage includes Prevention against losses resulting from computer hacking, illegitimate use of computer systems and other Information Technology security risks.

INSUREtrust, Marsh McLennan, …

, …



Wednesday, 16:00 - 17:00

Protecting Executives from Liability: Solutions Based on Oracle9i

Speaker 1: Ulf Mattsson, CTO (protegrity)

Abstract: This presentation covers experiences in various industries to illustrate how to protect Oracle databases from intrusions that go beyond the perimeter and how to shield executives from liability, utilizing recent developments in information-based security solutions that address a defense-in-depth strategy. It reviews case studies of cost-effective and time-effective solutions for Oracle databases that support the requirements of new privacy legislation and provide protection from the inside out without costly application modifications.

Whitepaper, Presentation

Oracle9i Database, Security

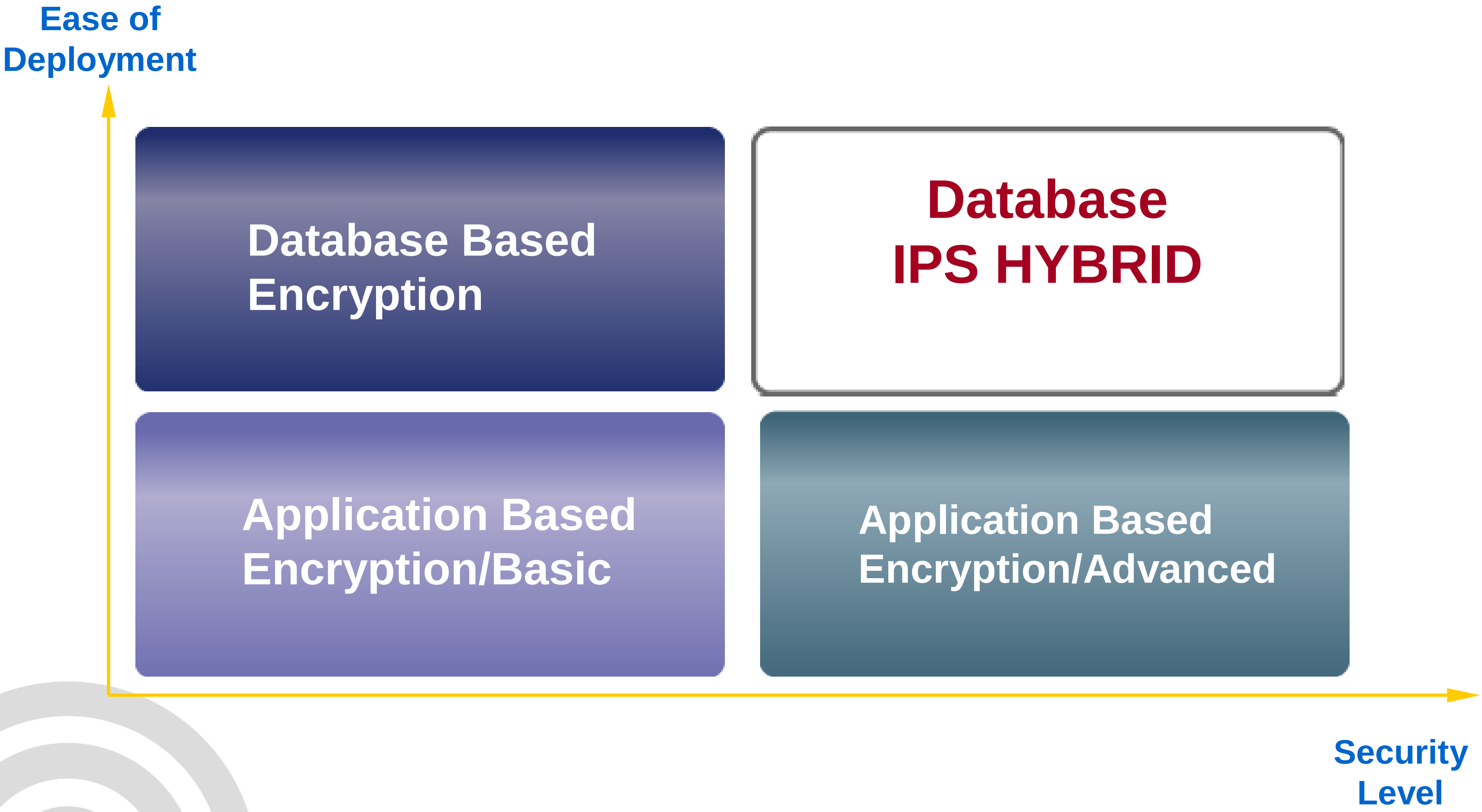
Protegrity: The Benefits of Partnering With Oracle

Ulf Mattson, CTO of Protegrity, discusses the benefits of partnering with Oracle to develop secure solutions with customers.

Learn more about security solutions offered by Oracle9*i* and partners:

1. Requirements based on Privacy & Security Legislation
2. Liability Aspects & Computer Security Breaches
3. → Some Solution Alternatives – Positioning & Issues
4. Case Studies – Time, Cost & Performance Aspects
5. A Solution - Overview
6. Intrusion Prevention – Database Server Side
7. Intrusion Prevention – Client Side
8. An Evidence-Quality Audit Log

Case Studies - 4 Solution Alternatives



Ease of Deployment

Database Based Encryption

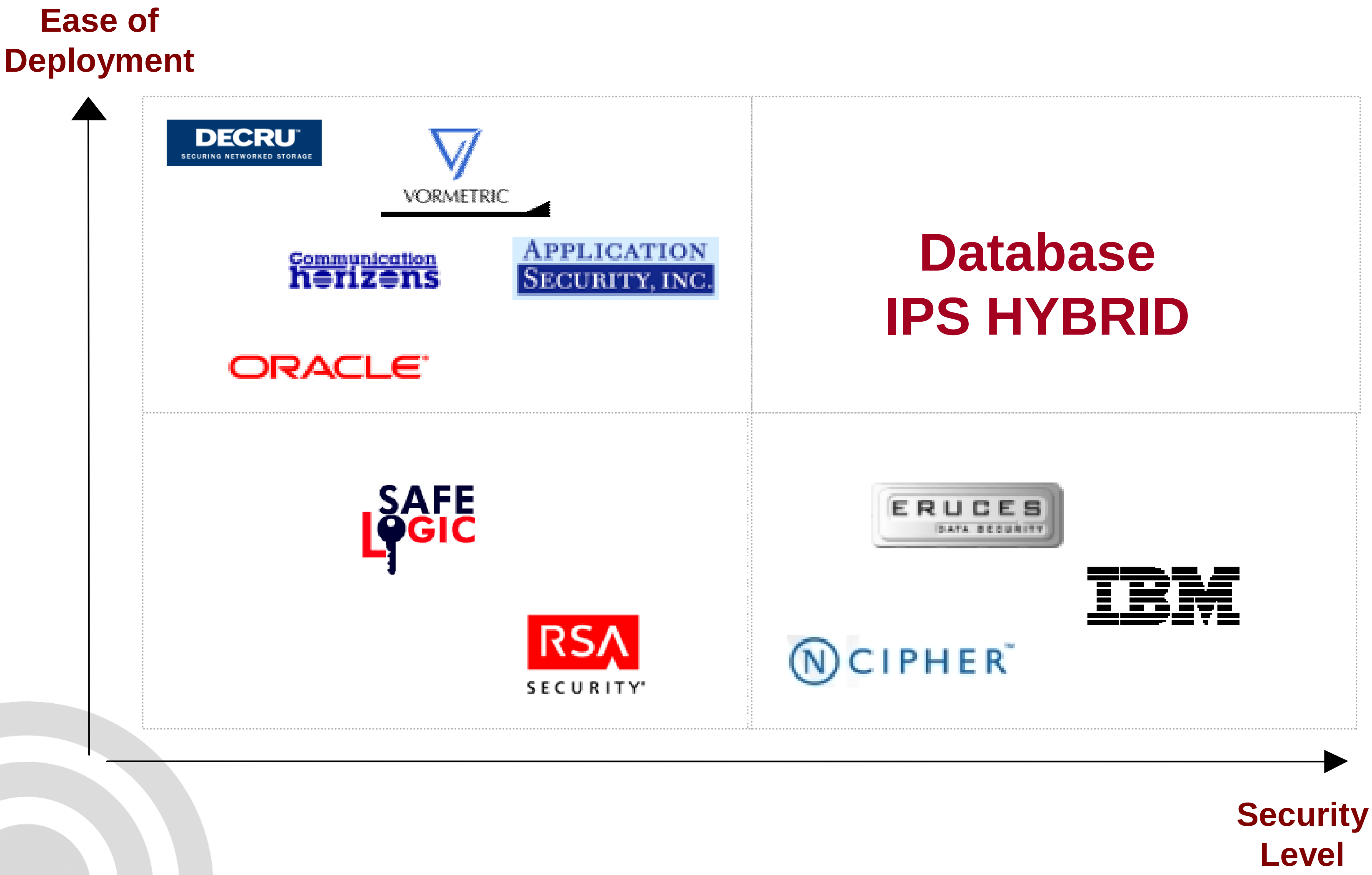
Database IPS HYBRID

Application Based Encryption/Basic

Application Based Encryption/Advanced

Security Level

Case Studies - Solution Alternatives

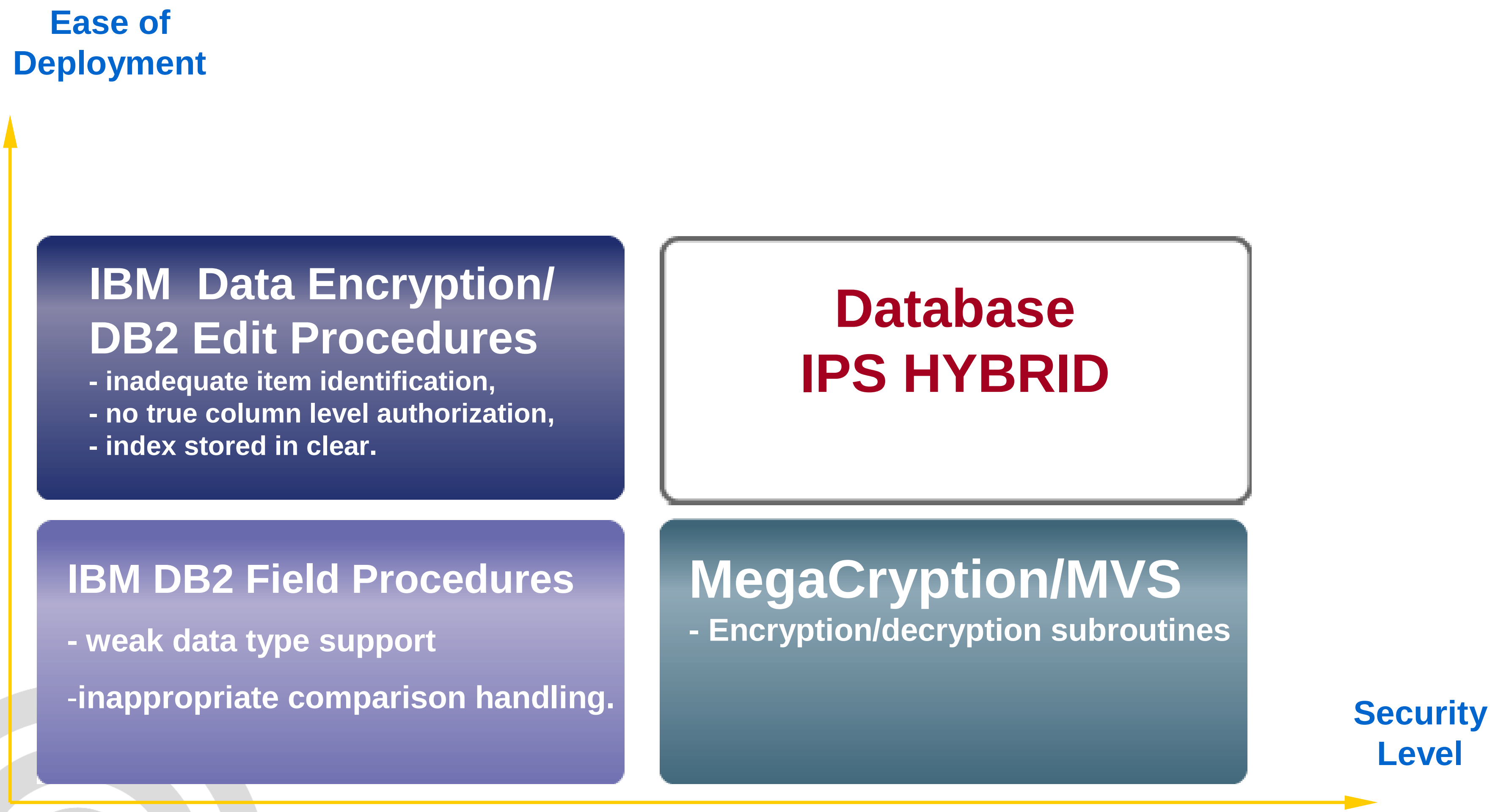


Ease of Deployment

Database
IPS HYBRID

Security Level

Case Studies – DB2/390 Solution Alternatives



Ease of Deployment

IBM Data Encryption/ DB2 Edit Procedures

- inadequate item identification,
- no true column level authorization,
- index stored in clear.

Database IPS HYBRID

IBM DB2 Field Procedures

- weak data type support

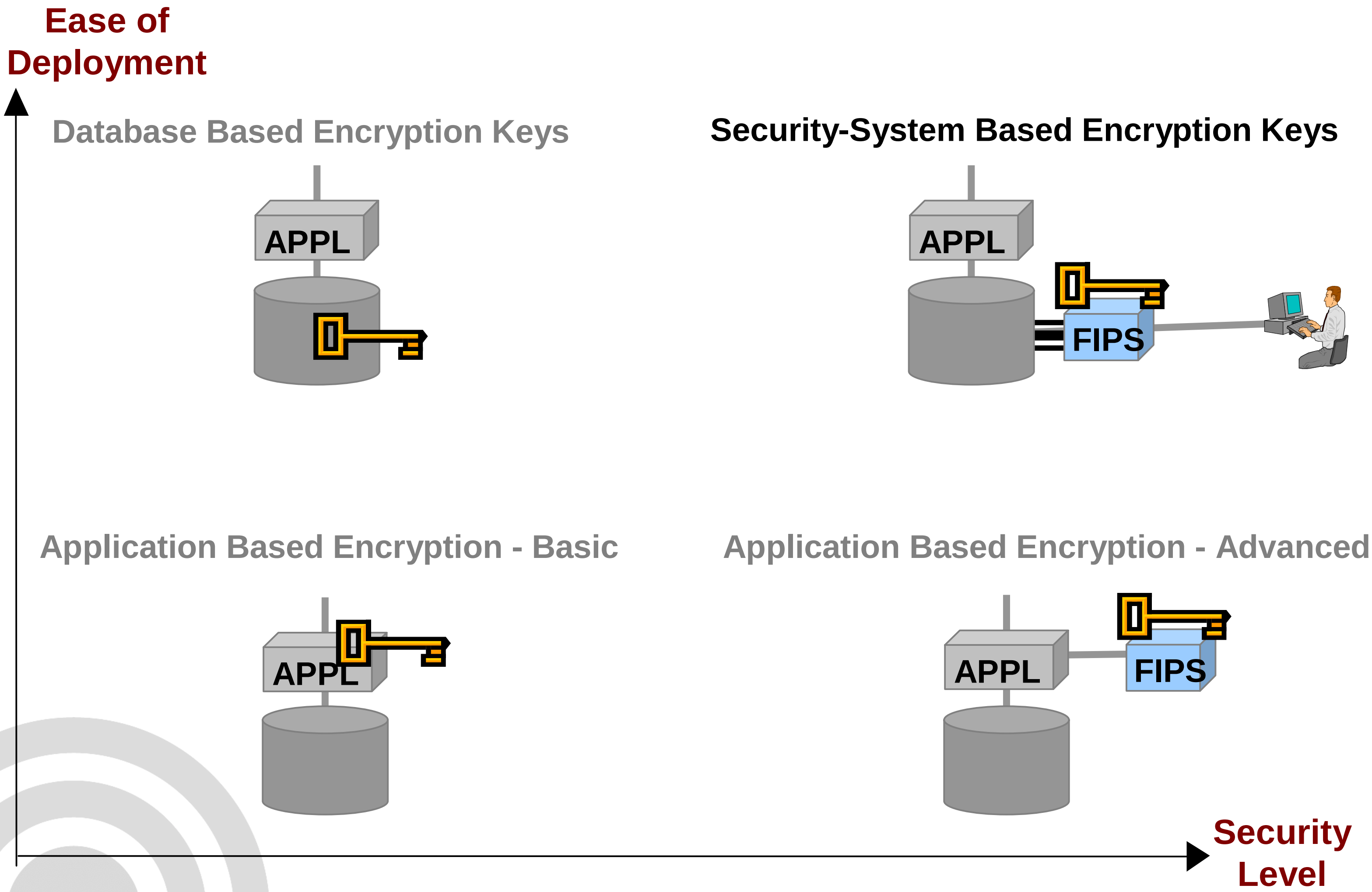
-inappropriate comparison handling.

MegaCryption/MVS

- Encryption/decryption subroutines

Security Level

Case Studies - 4 Server Solution Alternatives



Ease of Deployment

Database Based Encryption Keys

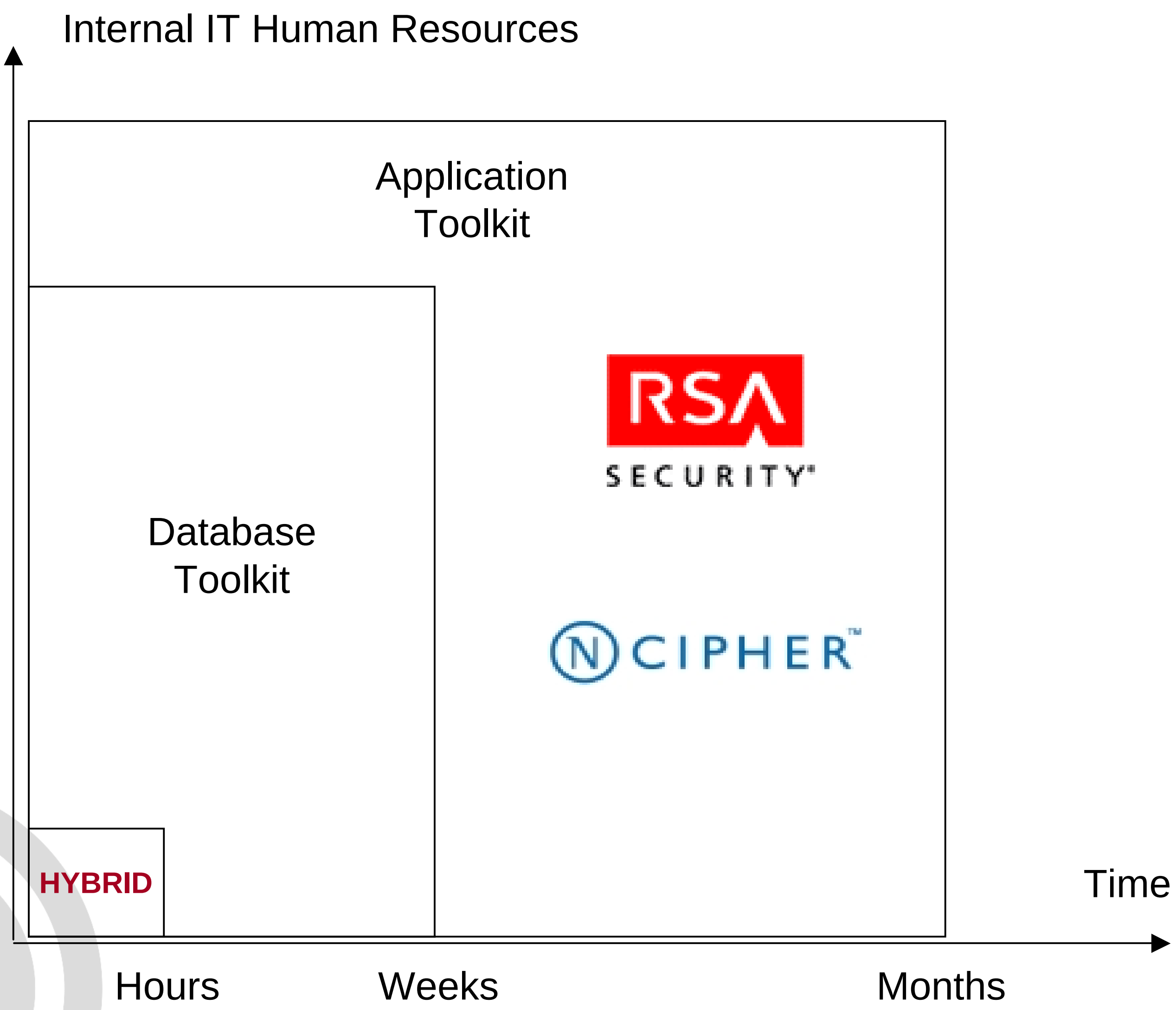
Security-System Based Encryption Keys

Application Based Encryption - Basic

Application Based Encryption - Advanced

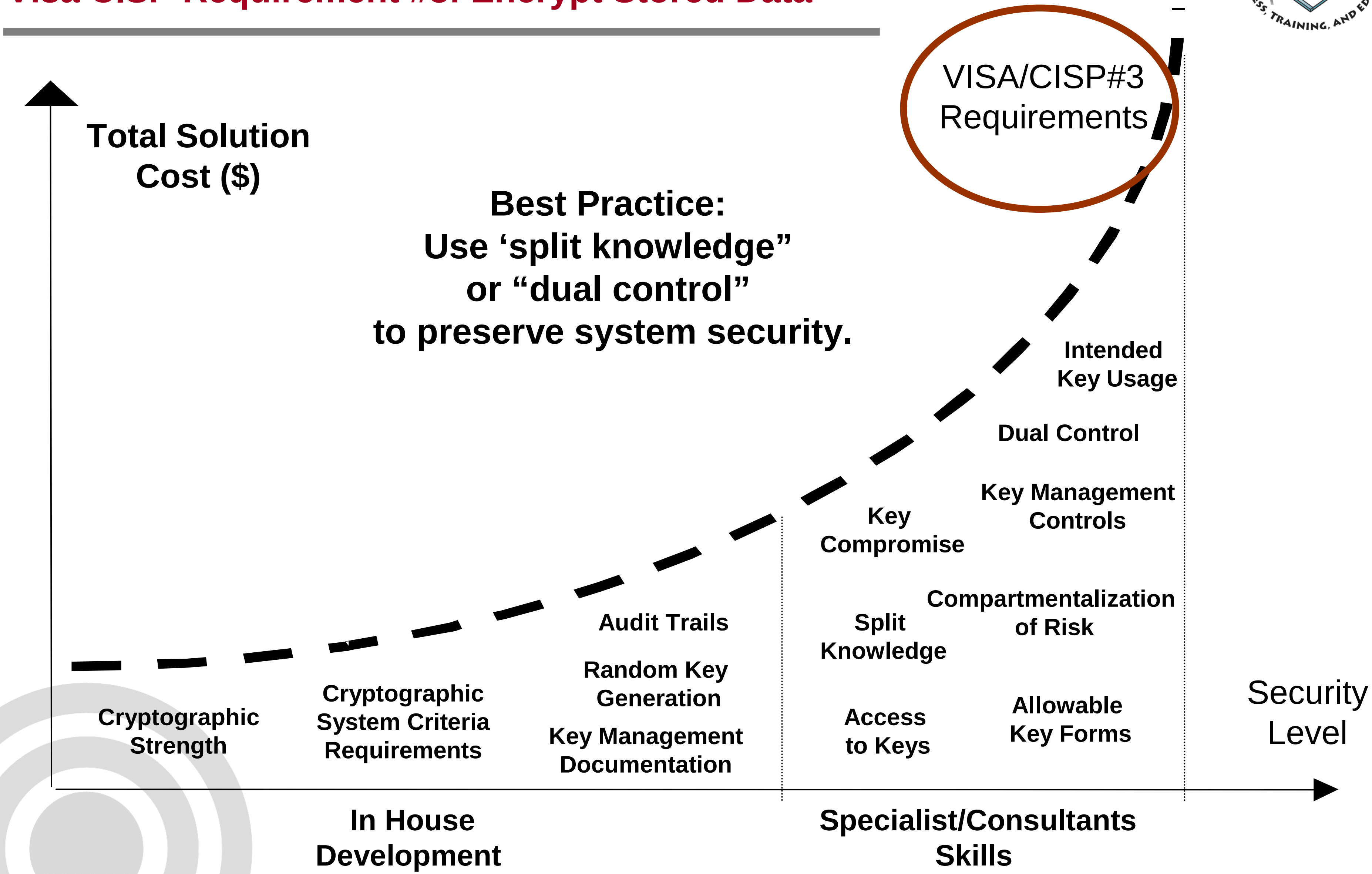
Security Level

Implementation and Migration Tools



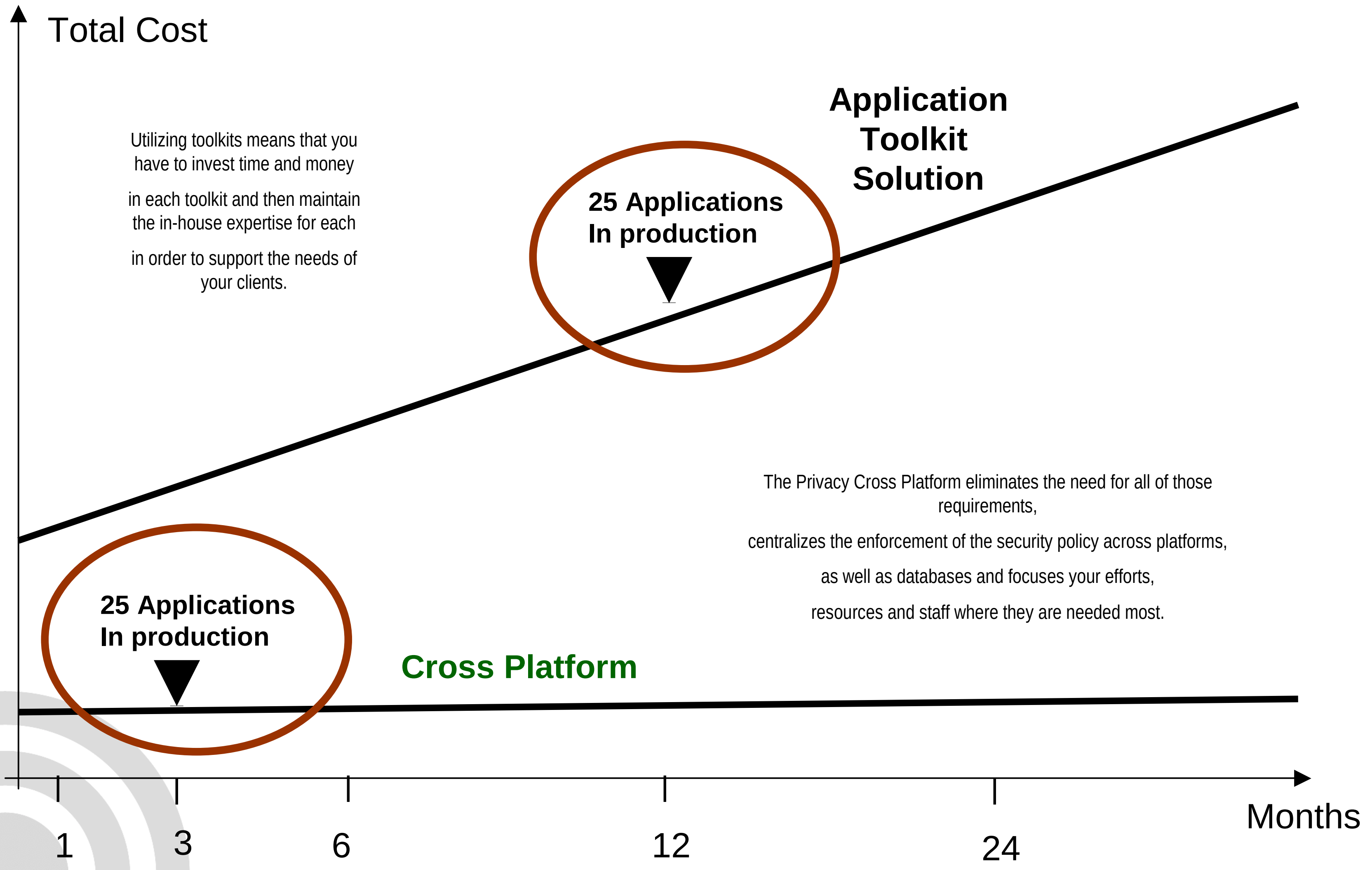
Implementation Time & Resources – Case Study

Visa CISP Requirement #3: Encrypt Stored Data



Best Practice:
Use ‘split knowledge” or “dual control” to preserve system security.

Implementation Time: 25 Applications Visa Compliant



Utilizing toolkits means that you have to invest time and money

in each toolkit and then maintain the in-house expertise for each

in order to support the needs of your clients.

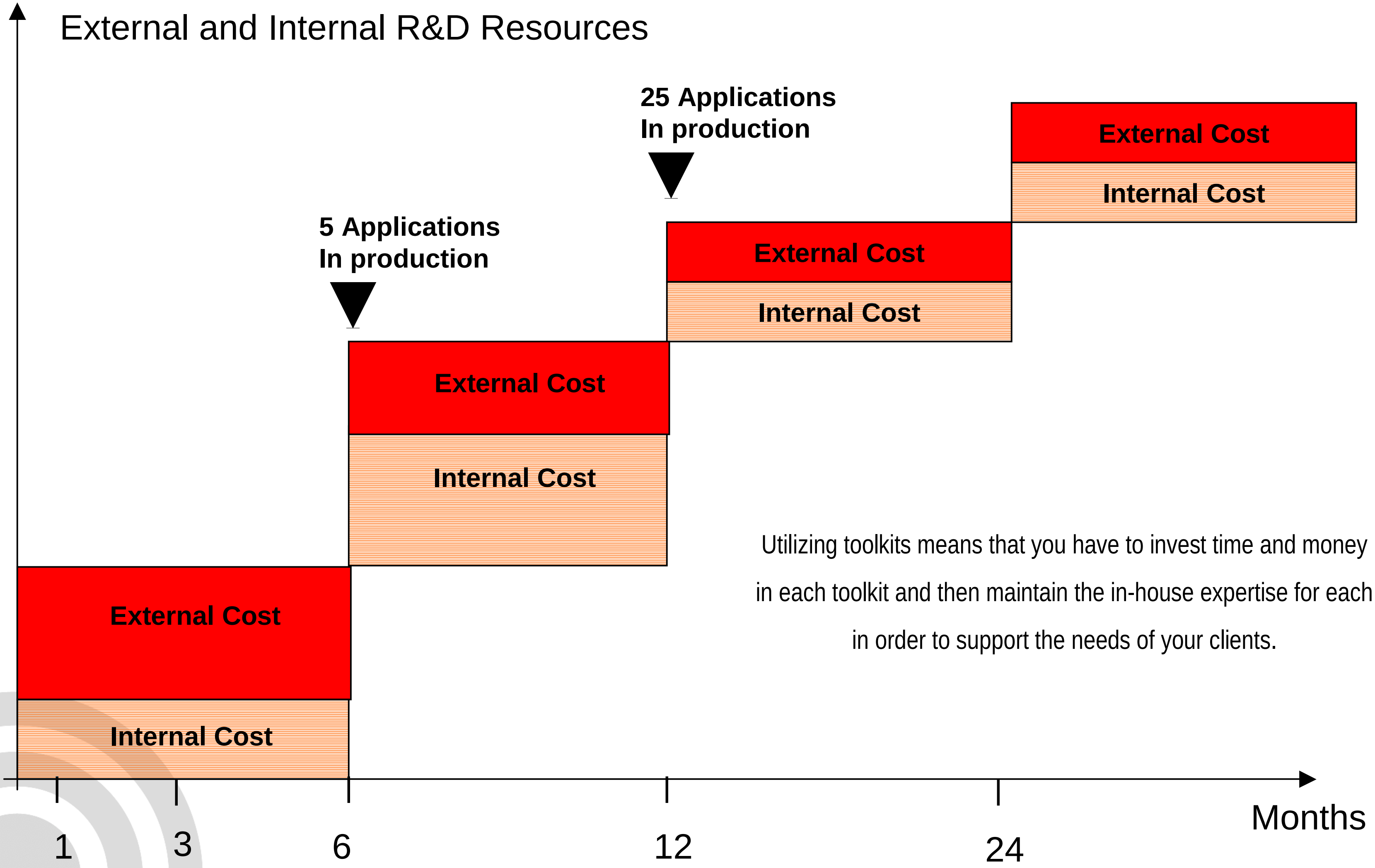
The Privacy Cross Platform eliminates the need for all of those requirements,

centralizes the enforcement of the security policy across platforms,

as well as databases and focuses your efforts,

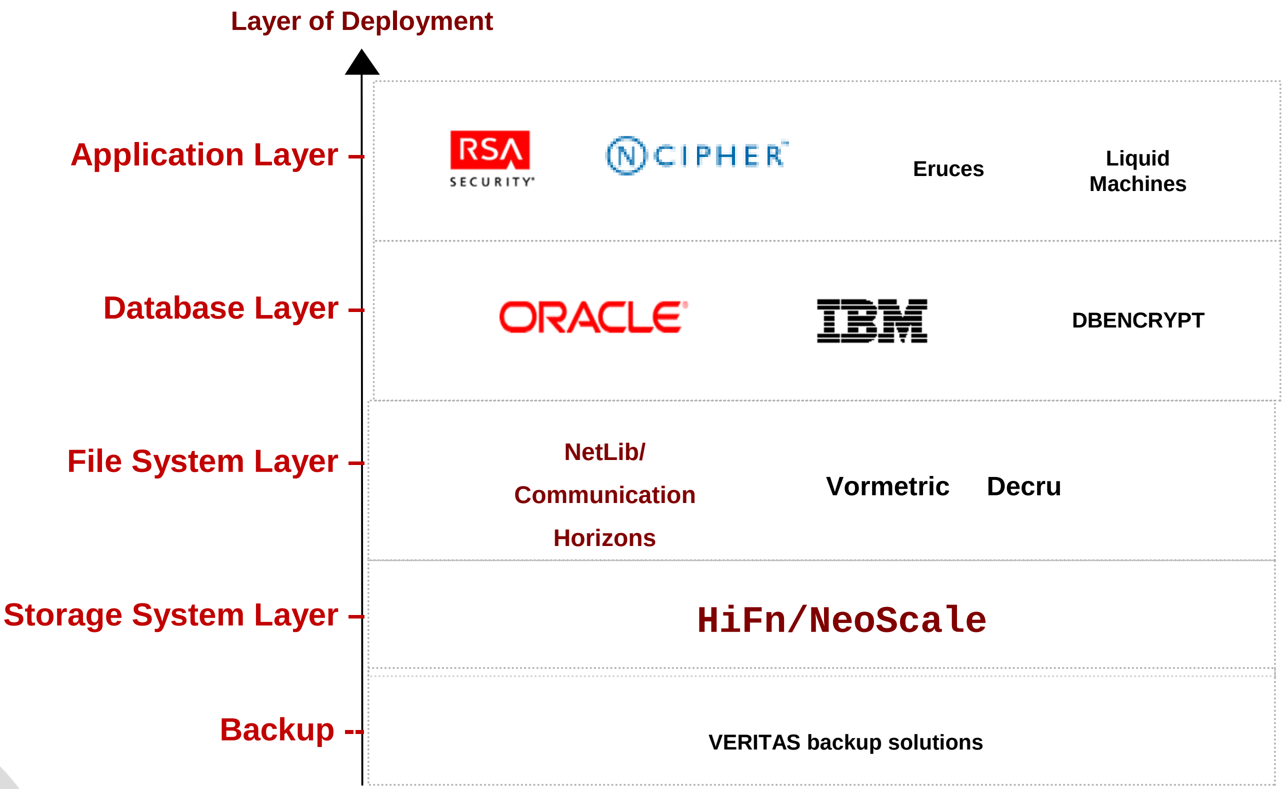
resources and staff where they are needed most.

Implementation Time & Cost: Application Toolkit



Utilizing toolkits means that you have to invest time and money in each toolkit and then maintain the in-house expertise for each in order to support the needs of your clients.

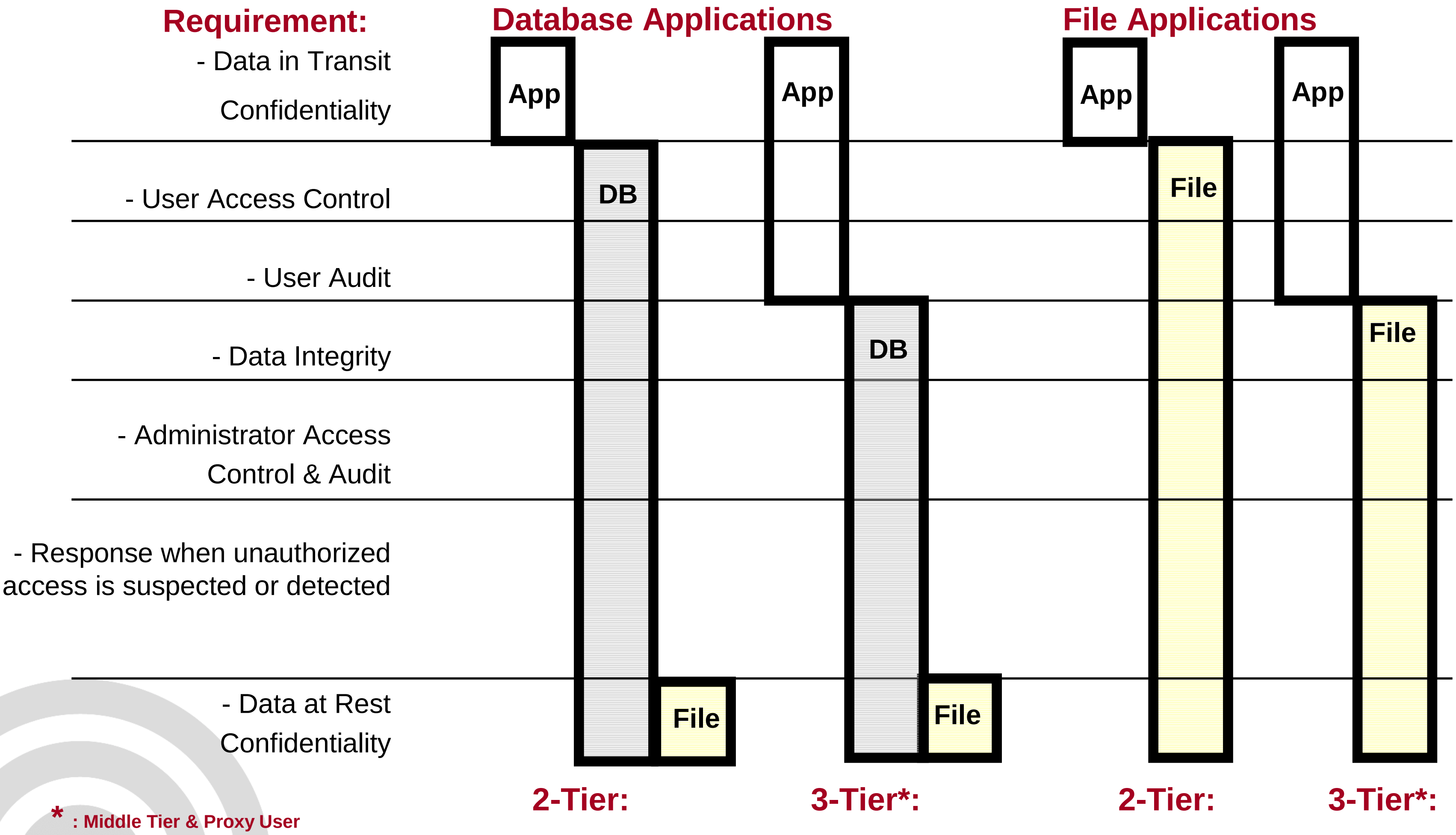
Server Side Solutions – Some Alternatives



Layer of Deployment

Application Layer	RSA SECURITY	NCIPHER	Eruces	Liquid Machines
Database Layer	ORACLE	IBM	DBENCRYPT	
File System Layer	NetLib/ Communication Horizons	Vormetric	Decru	
Storage System Layer	HiFn/NeoScale			
Backup	VERITAS backup solutions			

Case Studies – Typical Implementation Layer



Requirement:

- Data in Transit Confidentiality
- User Access Control
- User Audit
- Data Integrity
- Administrator Access Control & Audit
- Response when unauthorized access is suspected or detected
- Data at Rest Confidentiality

Database Applications

File Applications

* : Middle Tier & Proxy User

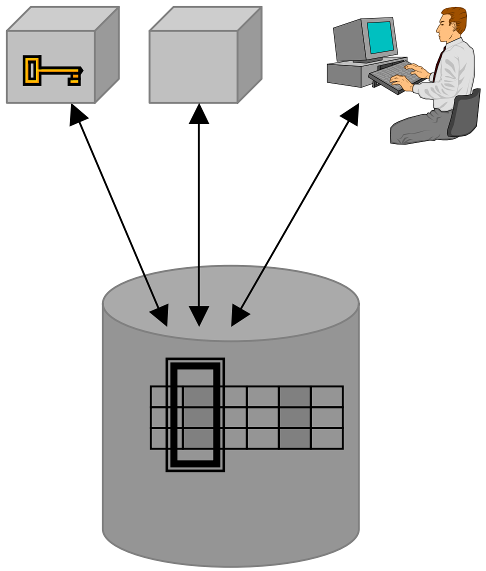
Compliance Requirements vs. Alternative Solutions

Requirement Type	User Access Control & Audit	Administrator Access Control & Audit	Response when unauthorized access is suspected or detected	Data Confidentiality & Encryption
Requirents in US OCC/GLBA/C - Manage and Control Risk	Access controls on customer/member information	Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer/member information.	Response programs that specify actions for you to take when you suspect or detect that unauthorized individuals have gained access to customer/member information systems, including appropriate reports to regulatory and law enforcement agencies.	Encryption of electronic customer/member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.
Application Level Encryption	🟩 **3-Tier Applications**	🟥 **High Risk, High Cost**	🟥 **High Risk, High Cost**	🟥 **High Risk, High Cost**
Databases Level Encryption	🟩 **2-Tier Applications**	🟩 **All Applications**	🟩 **All Applications**	🟩 **Accountability for database administrators.**
File Level Encryption	🟥 **Non Compliant**	🟥 **Non Compliant**	🟥 **Non Compliant**	▨ **No accountability for database administrators.**

Legend	🟩 **Recommended**	🟥 **Not Recommended**	▨ **Only as a secondary alternative**

Case Study: Application Encryption – Advanced

Applications



Source Code Changes

Prevention of Encryption Keys?

No Data Sharing with Application Packages, Database Utilities and Report Generators …

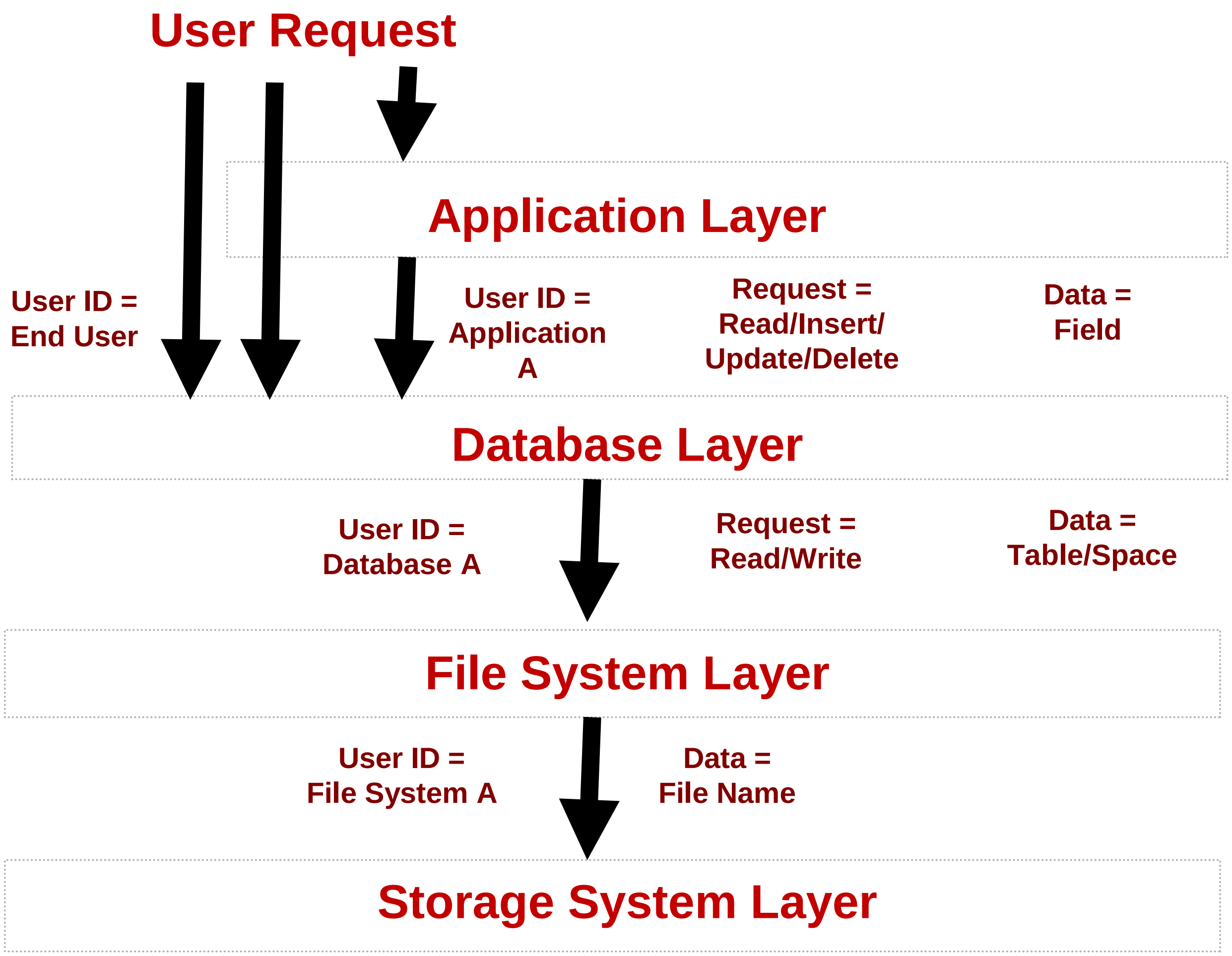
No Search on Encrypted Data

No JOIN on Encrypted Data

No Stored Procedures

Applications stop working …

Solution Layers – Information Request Granularity



User Request

Application Layer

User ID =
End User

User ID =
Application
A

Request =
Read/Insert/
Update/Delete

Data =
Field

Database Layer

User ID =
Database A

Request =
Read/Write

Data =
Table/Space

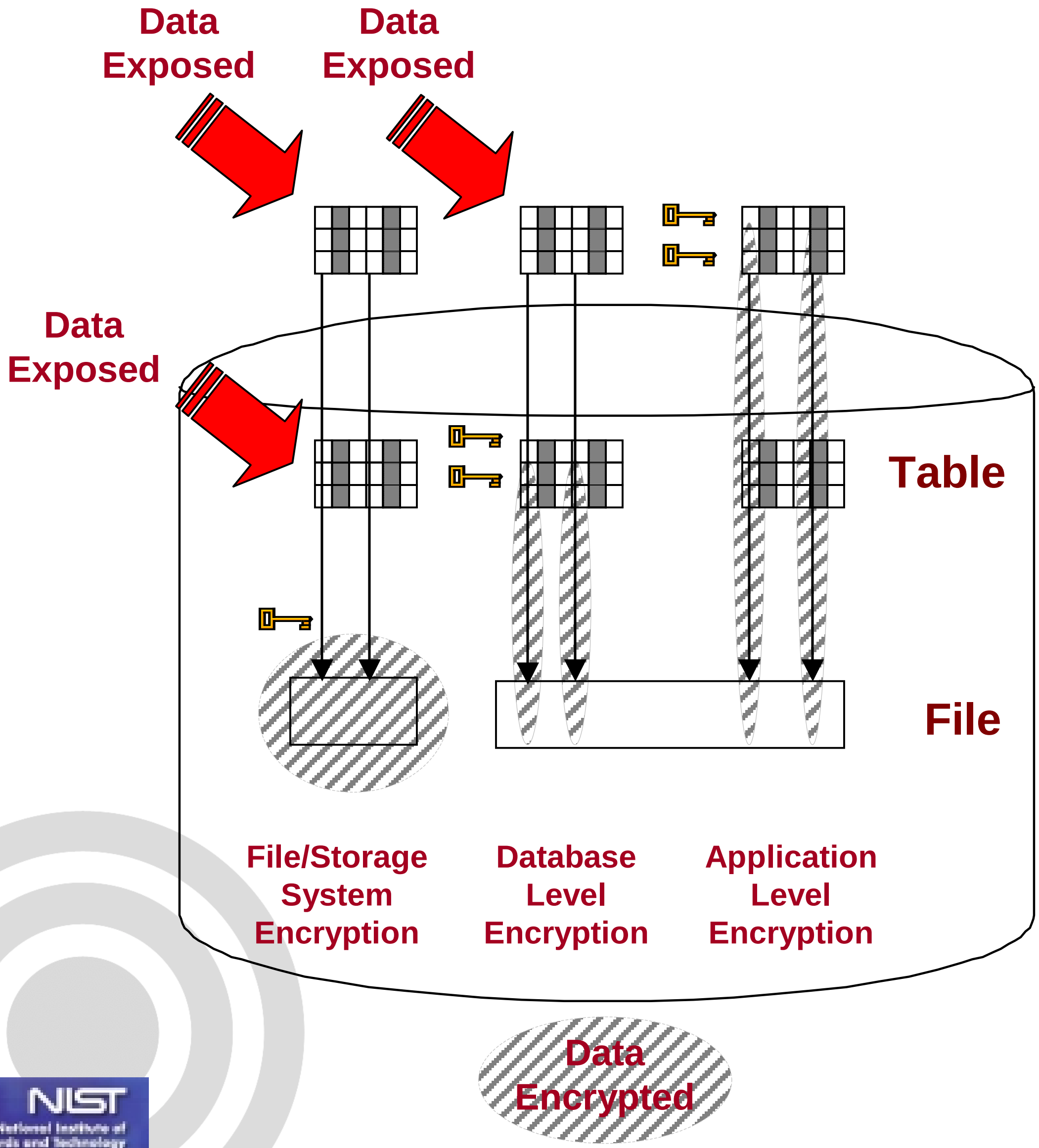
File System Layer

User ID =
File System A

Data =
File Name

Storage System Layer

Data Exposed with Alternative Solutions

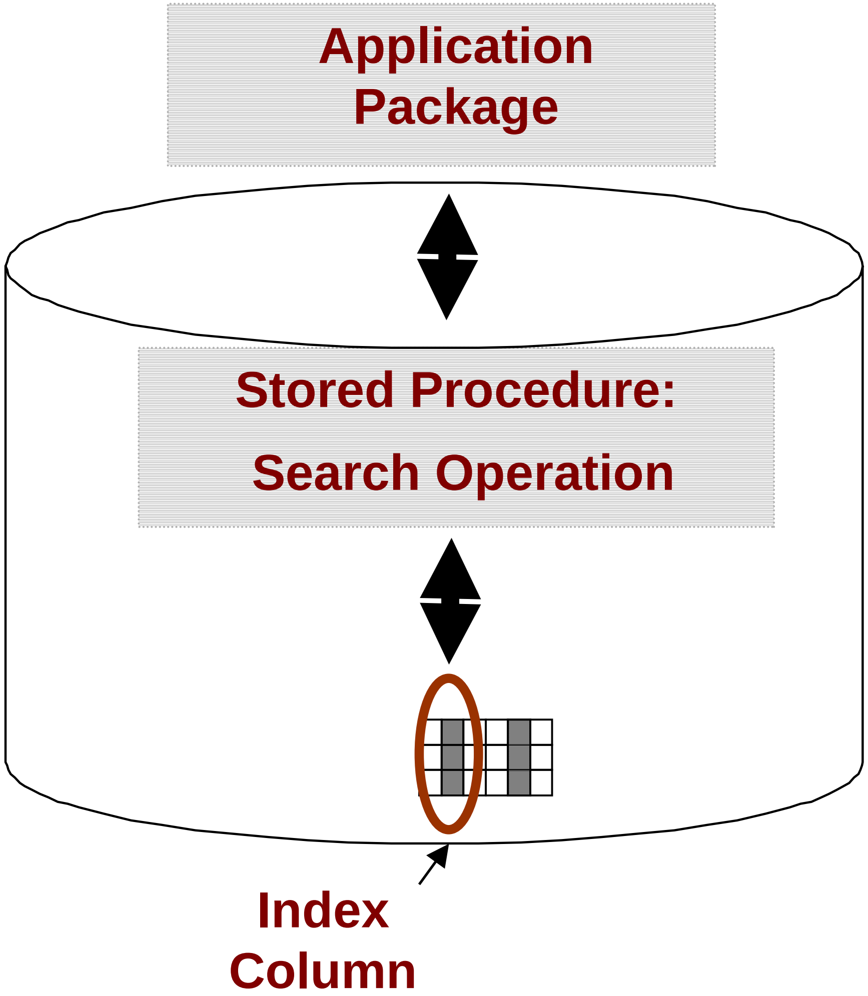

Data Exposed
Data Exposed
Data Exposed
Table
File
File/Storage System Encryption
Database Level Encryption
Application Level Encryption
Data Encrypted

Application Layer

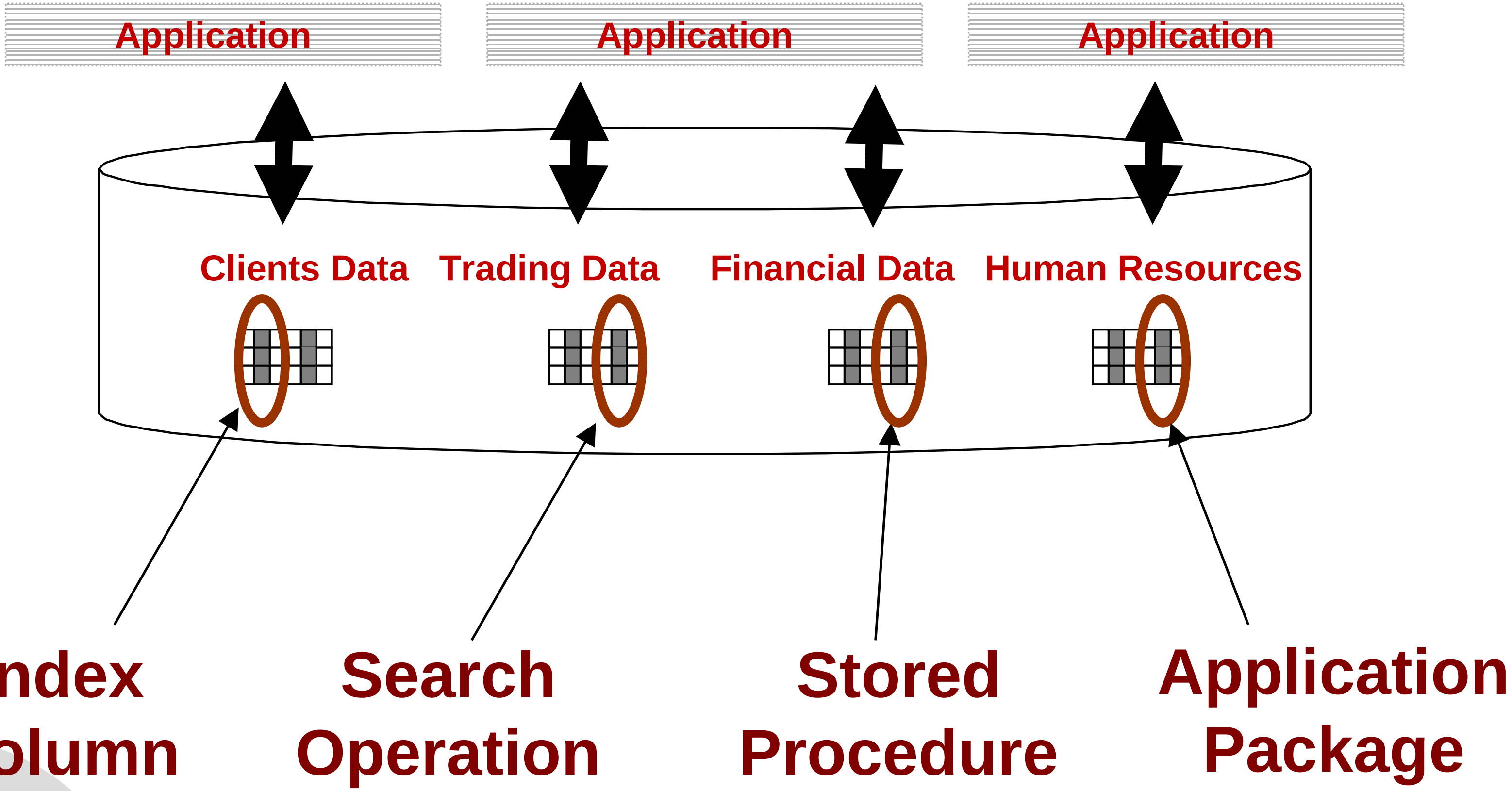
Database Layer

File / Storage Sys Layer

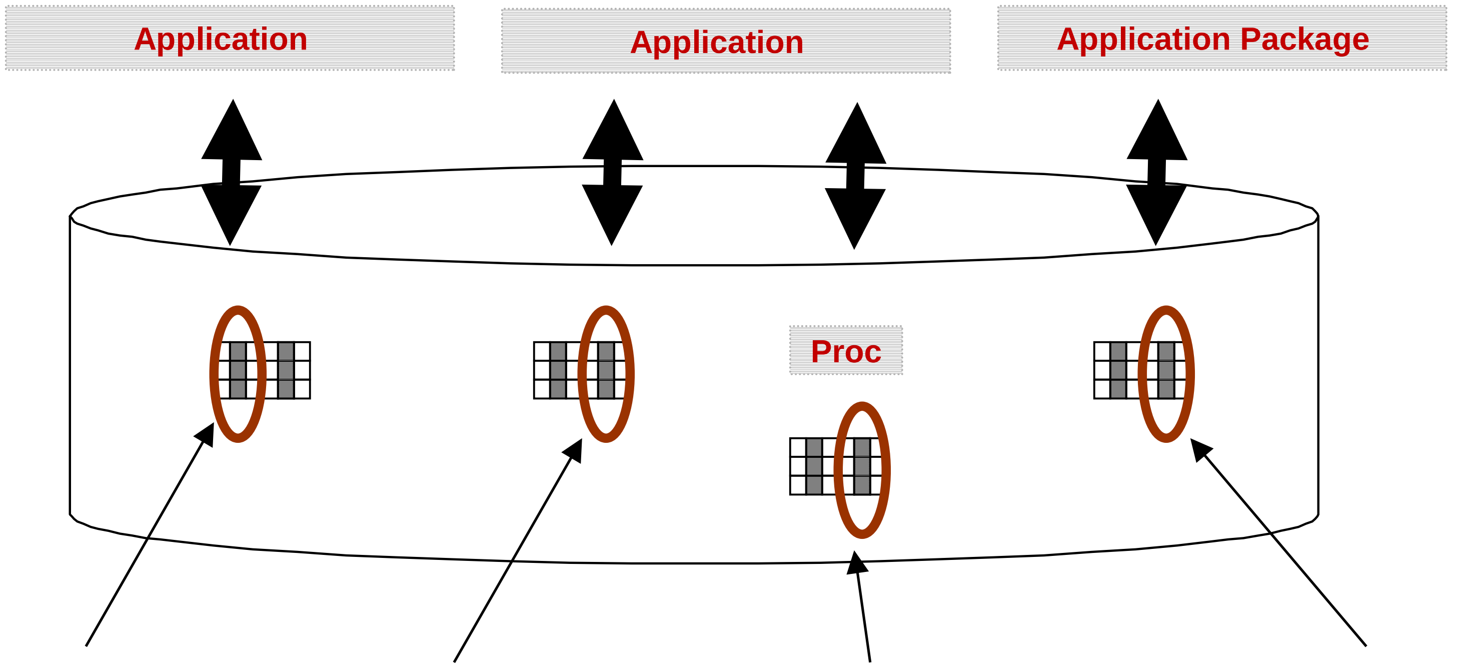
Case Study – Issues with Application Level Encryption



Case Study - Typical Line of Business Applications:



Case Study - Typical Applications and Databases:



Index
On Encrypted Column

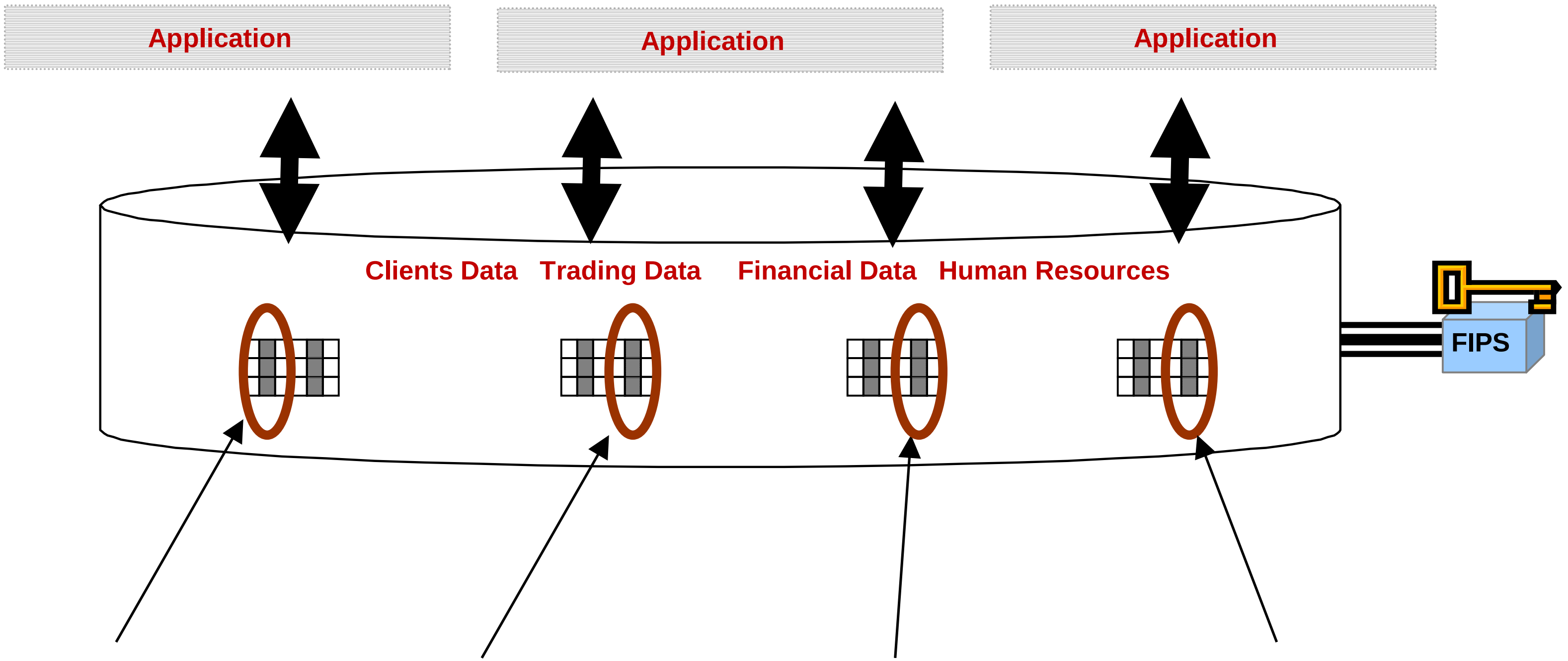
Search Operation
Operating on Clear-text values of Encrypted Data

Stored Procedure
Operating on Clear-text values of Encrypted Data

Application Package
Operating on Clear-text values of Encrypted Data

○ : Column to be encrypted

Case Study - Why Database Level Encryption is Needed:



Index
On Encrypted Column

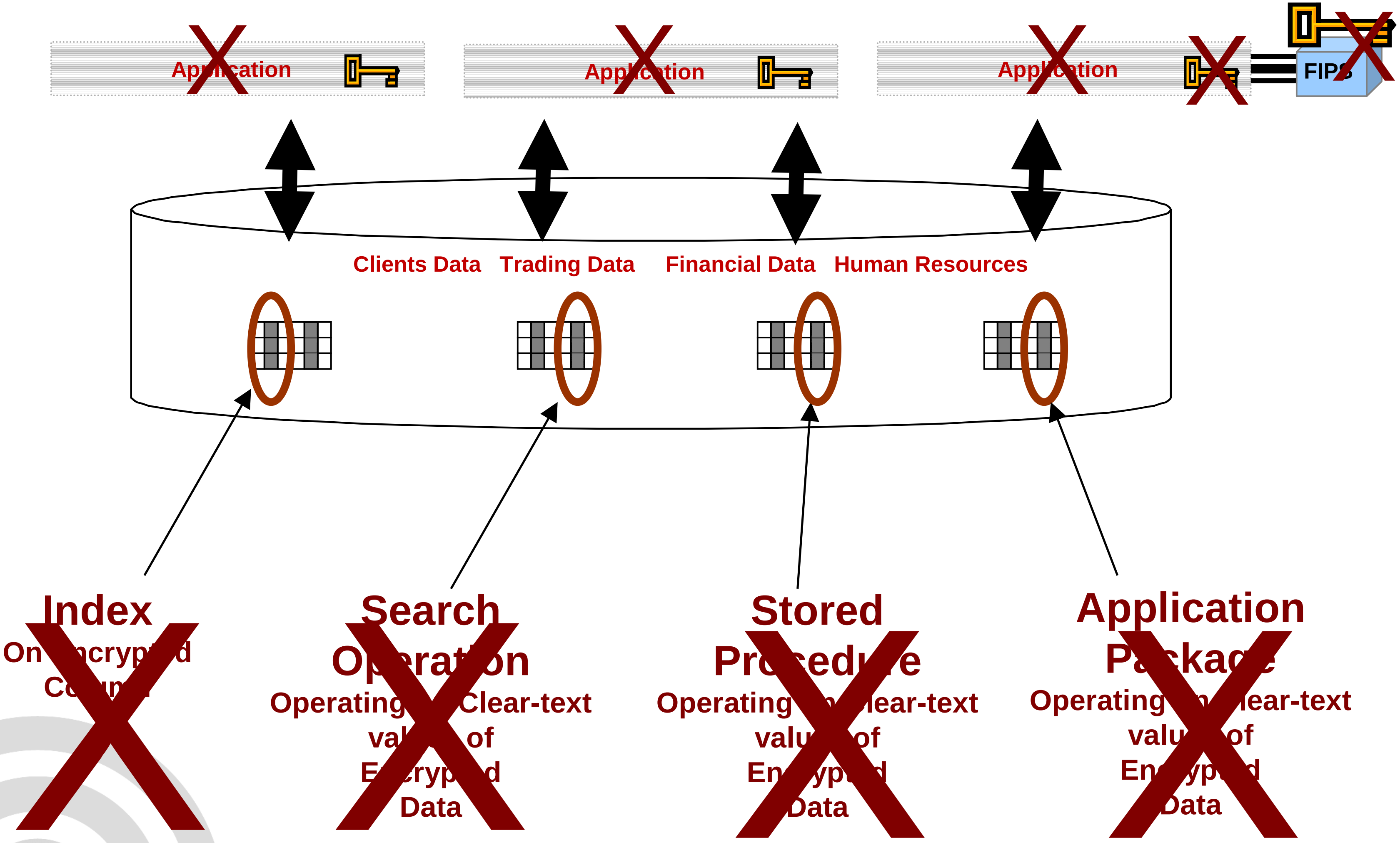
Search Operation
Operating on Clear-text values of Encrypted Data

Stored Procedure
Operating on Clear-text values of Encrypted Data

Application Package
Operating on Clear-text values of Encrypted Data

🔑 : Key Management & Crypto Operation

Case Study - Why Application Level Encryption Failed:



Application

Application

Application

FIPS

Clients Data

Trading Data

Financial Data

Human Resources

Index
On Encrypted Column

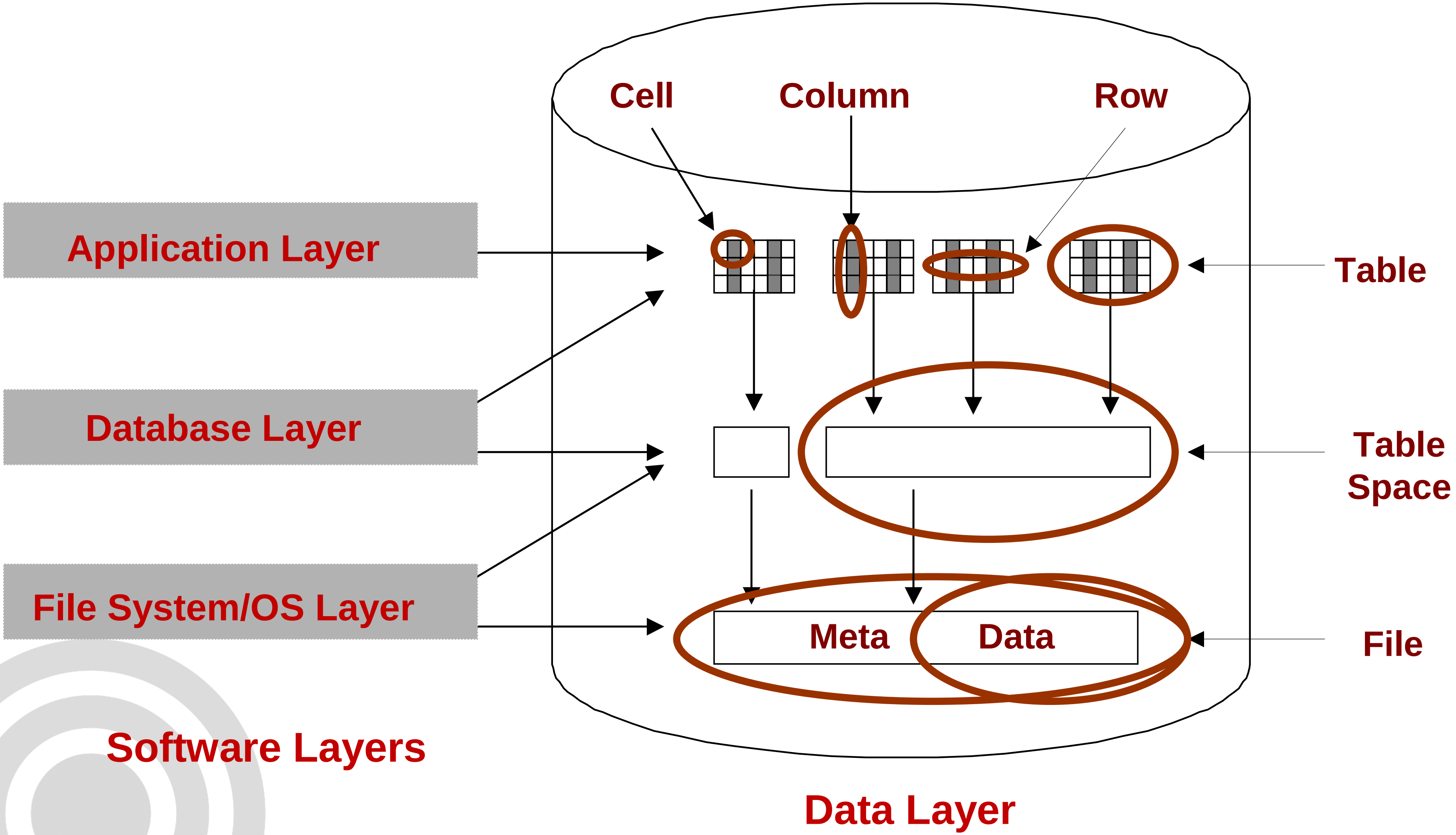
Search Operation
Operating on Clear-text value of Encrypted Data

Stored Procedure
Operating on Clear-text value of Encrypted Data

Application Package
Operating on Clear-text value of Encrypted Data

: Key Management & Crypto Operation

Data at Rest Encryption at Different Layers



Cell

Column

Row

Application Layer

Database Layer

File System/OS Layer

Table

Table Space

File

Meta

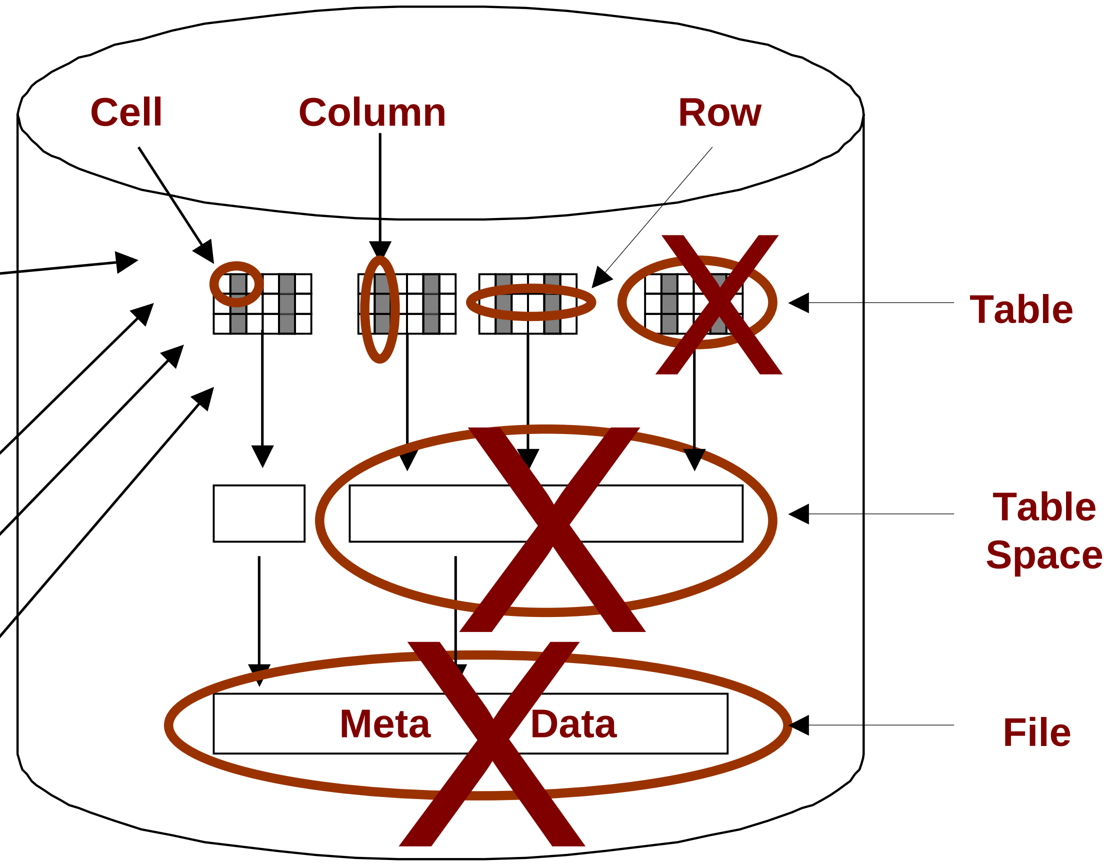
Data

Software Layers

Data Layer

Encryption Key Management Requirements

VISA/CISP#3
Cryptographic System Criteria
Key Management Controls
Access to Keys
Random Key Generation
Allowable Key Forms
Dual Control
Split Knowledge
Audit Trails
Intended Key Usage
Key Compromise
Compartmentalization of Risk
Cryptographic Strength



Same Key Rotation/Aging for all columns?

Same encryption key for all columns?

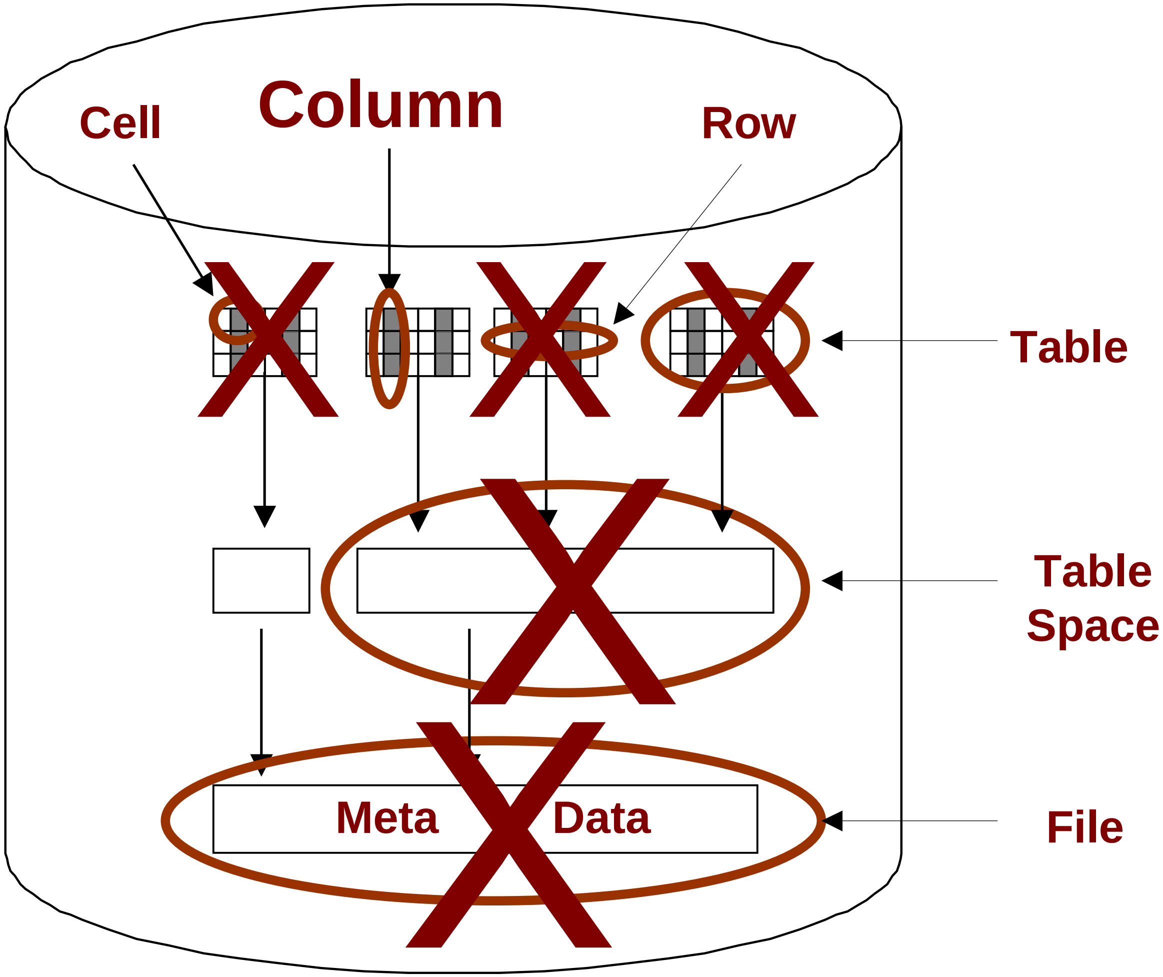
Decrypt all columns and rows for a every user?

Issues with Security and Deployment

Issues when Searching Encrypted Data

Encryption Key Management Issues

Issues with Audit, Segregation of Duties

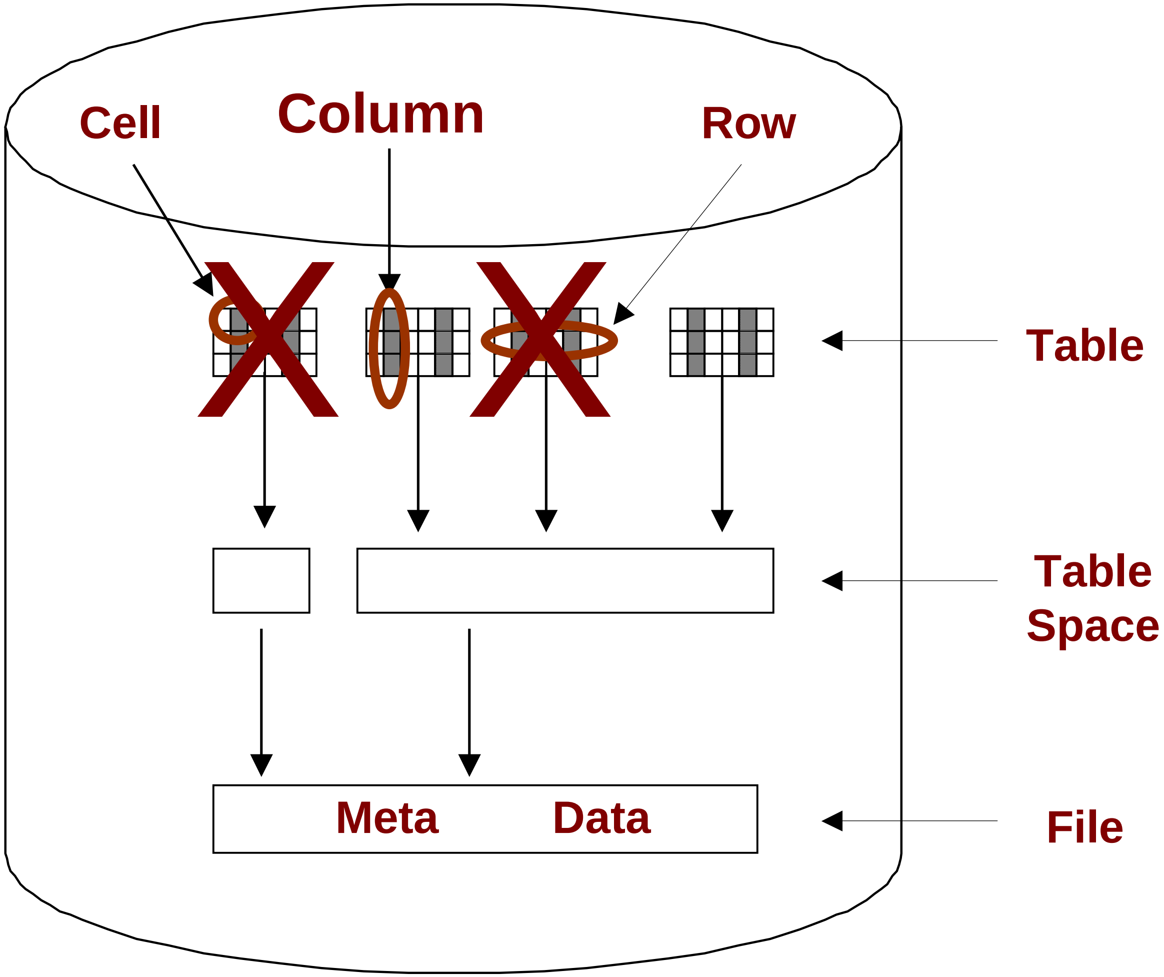


Issues when Searching Encrypted Data

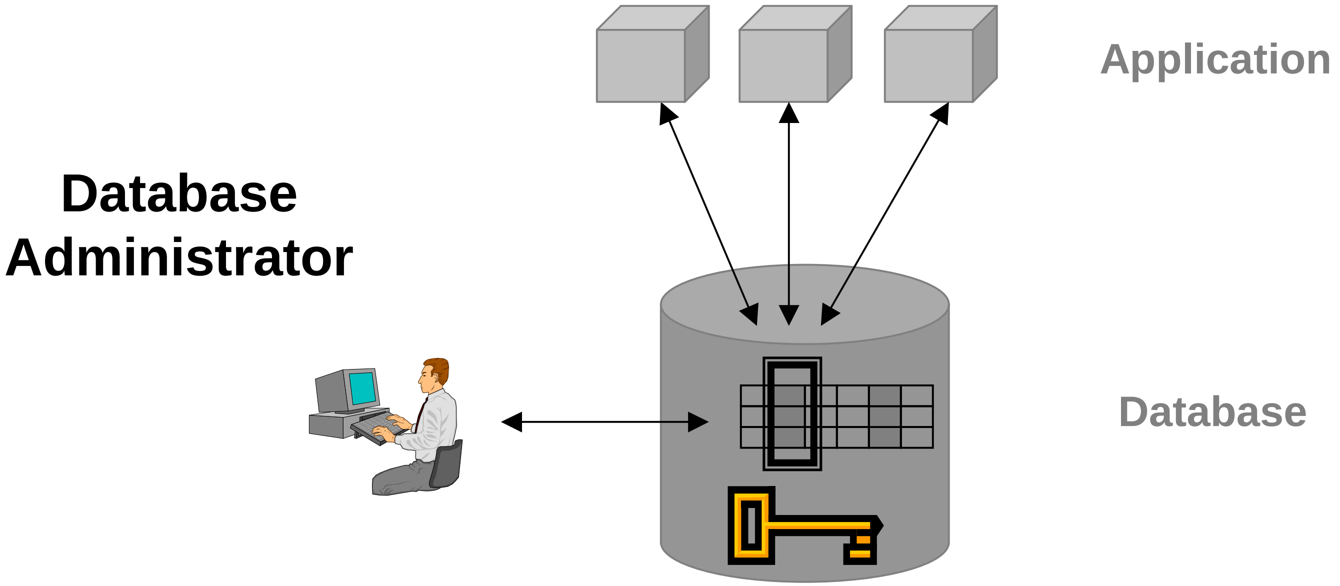
Search Operations?

Index?

Data Type?



Case Study: Database Encryption – Advanced



**Do NOT leave
'The Keys to The Store'
in the Database!**

Questions with Database Encryption

1. Is there there a concept of access control with Read, write, update, delete as separate functions, or will a user either has **100% access or 0%?**
2. Are **keys are stored in in clear text** for the duration of the session. This is readily accessible to any DBA! No point in locking the data if the key is accessible!
3. Is key storage password protected (requires second authentication), In on OS file (**unsecured from root**), or in the database in clear text (**accessible by the DBA**)? None of these are secure solutions.
4. Are keys generated by a **random number generator in the OS?** Not secure.
5. Is there a key recovery system? If you delete all the current users (private key and the associated copy of the "data" key) of a column will you have destroyed the keys and now have **unrecoverable data**?
6. Is there a **secure audit** around sensitive data or changes to access policy? Is there a central control of access, or can any defined user change access to the tables they own.
7. Is a private key required for key protection? Must the key be supplied to access data? This infers that **application changes** must be made to handle the key management. FIPS 140 level 3 support?
8. Is there **support for encrypted indexes acceleration?**
9. Is there **wizard support for automated deployment and migration of data and database definitions?**
10. Is there only **limited support of data types**, (or only Varchar2, raw or numeric (without parameters) are supported)?
11. Is the product **supporting all major database brands?**
12. Is the product **supported by major database vendors?**
13. Is the product **supported by major security vendors?**
14. Can I talk to multiple **reference customers in my industry segment?**

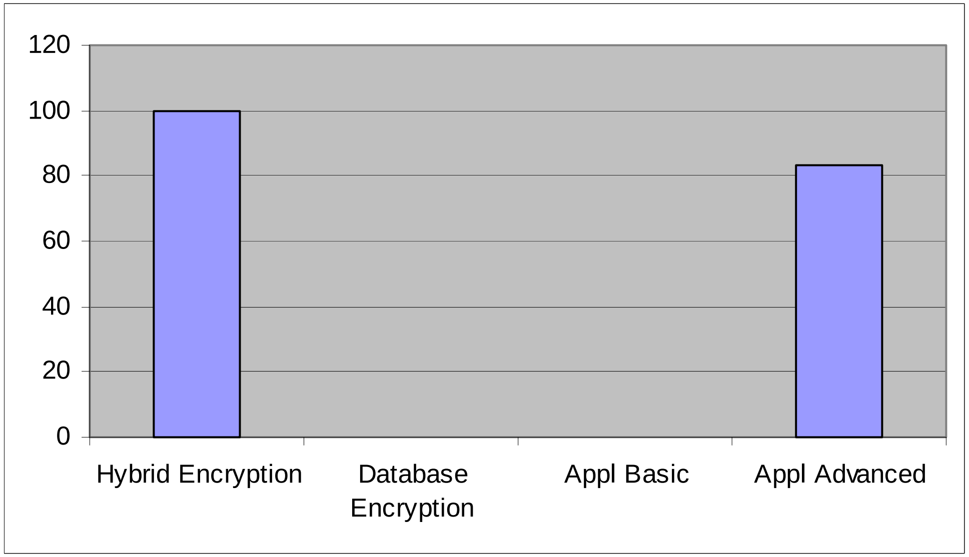
Case Study: Database Encryption – Advanced

	The FAQ Scorecard (High Score is Most Favorable)	Hybrid Encryption	Database Encryption
Deployment	Do I need to change my applications?	100	0
	Support for several major database brands?	100	0
	Support for all major data types?	100	0
	Support for encrypted index?	100	0
Security	Are encryption keys protected exposure in clear text?	100	0
	Support for recovery of encryption keys?	100	0
	Support for random generation of encryption keys?	100	0
	Support for separation of users and encryption keys?	100	0
	Insert/update/delete/select support in security policy?	100	0
Audit	Audit support for all access to data?	100	0
	Audit support for all changes to security policy?	100	0

High Score is Most Favorable

Case Studies: Scorecard – Security

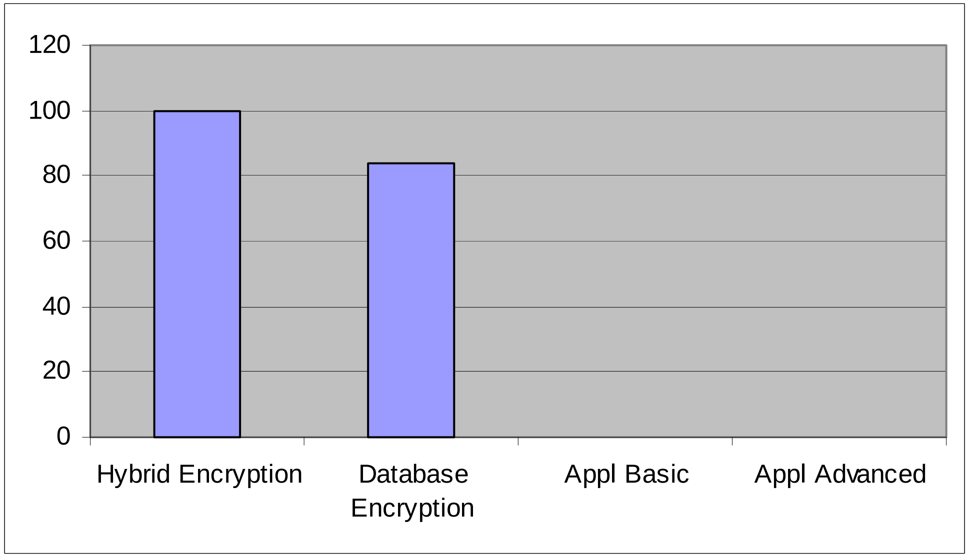
The FAQ Scorecard (High Score is Most Favorable)	Hybrid Encryption	Database Encryption	Application Encryption Basic	Application Encryption Advanced
Can I audit all changes to the access policy?	100	0	0	0
Can I audit the key management?	100	0	0	100
Are the encryption keys protected?	100	0	0	100
Is the encryption FIPS 140 level 3?	100	0	0	100
Is separation of duties enforced?	100	0	0	100
Can I prevent both external and internal attacks?	100	0	0	100



High Score is Most Favorable

Case Studies: Scorecard – Deployment

The FAQ Scorecard (High Score is Most Favorable)	Hybrid Encryption	Database Encryption	Application Encryption Basic	Application Encryption Advanced
Do I need to change my applications?	100	60	0	0
Can all applications & tools still access the encrypted data?	100	60	0	0
Will searches on encrypted data still work?	100	100	0	0
Will my stored procedures, joins, and where/like/between still work?	100	100	0	0
Can I easily reencrypt archived data?	100	100	0	0



High Score is Most Favorable

Visa/CISP#3 – Case Study – Development

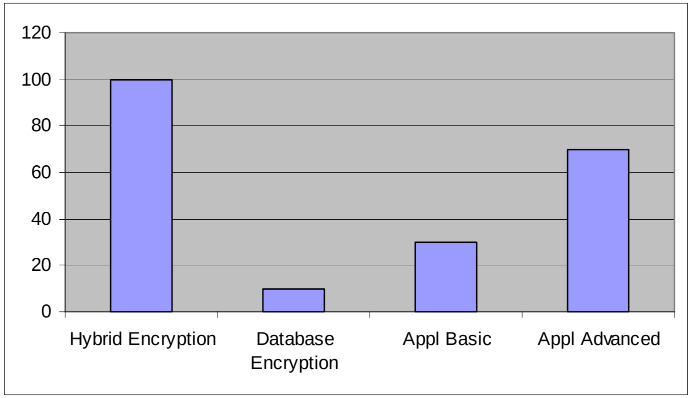
Training, analysis, design, programming, test, documentation, and installation:

- **Application Integration Development: 4 man-weeks/application**
- **Cryptographic Solution Development (man weeks):**

Cryptographic Vector Functions:	2
Key Management Control Functions:	12
Access to Keys Isolation:	11
Random Key Generation:	2
Allowable Key Forms Functions :	9
Intended Key Usage Functions :	10
Key Compromise Prevention Functions	10
Dual Control Functions :	6
Split Knowledge Functions :	8
Compartmentalization Functions:	10
Secure Audit System:	11

Visa/CISP#3 – Case Study Scorecard (% Compliance)

VISA/CISP#3	Hybrid Encryption	Database Encryption	Application Encryption Basic	Application Encryption Advanced
Cryptographic System Criteria	100	40	100	100
Key Management Controls	100	0	0	3
Access to Keys	100	0	60	60
Random Key Generation	100	40	100	100
Allowable Key Forms	100	0	0	100
Dual Control	100	0	0	40
Split Knowledge	100	0	0	40
Audit Trails	100	0	0	40
Intended Key Usage	100	0	0	40
Key Compromise	100	0	0	100
Compartmentalization of Risk	100	0	0	60
Cryptographic Strength	100	40	100	100



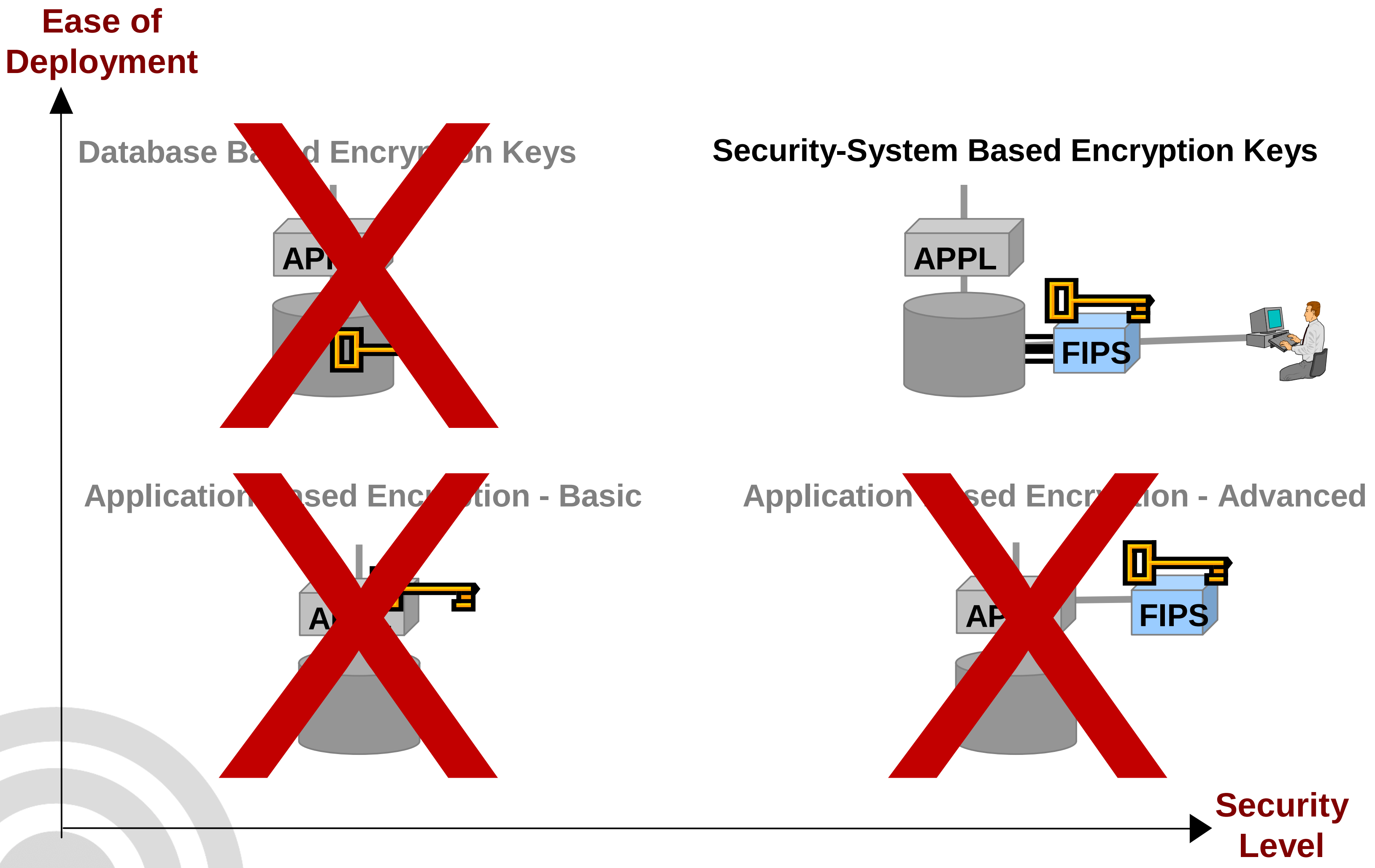
IDS and Forensics - Liability Assessments and Solutions

1. Requirements based on Privacy & Security Legislation
2. Liability Aspects & Computer Security Breaches
3. Some Solution Alternatives – Positioning & Issues
4. Case Studies – Time, Cost & Performance Aspects
5. ➡ A Solution - Overview
6. Intrusion Prevention – Database Server Side
7. Intrusion Prevention – Client Side
8. An Evidence-Quality Audit Log

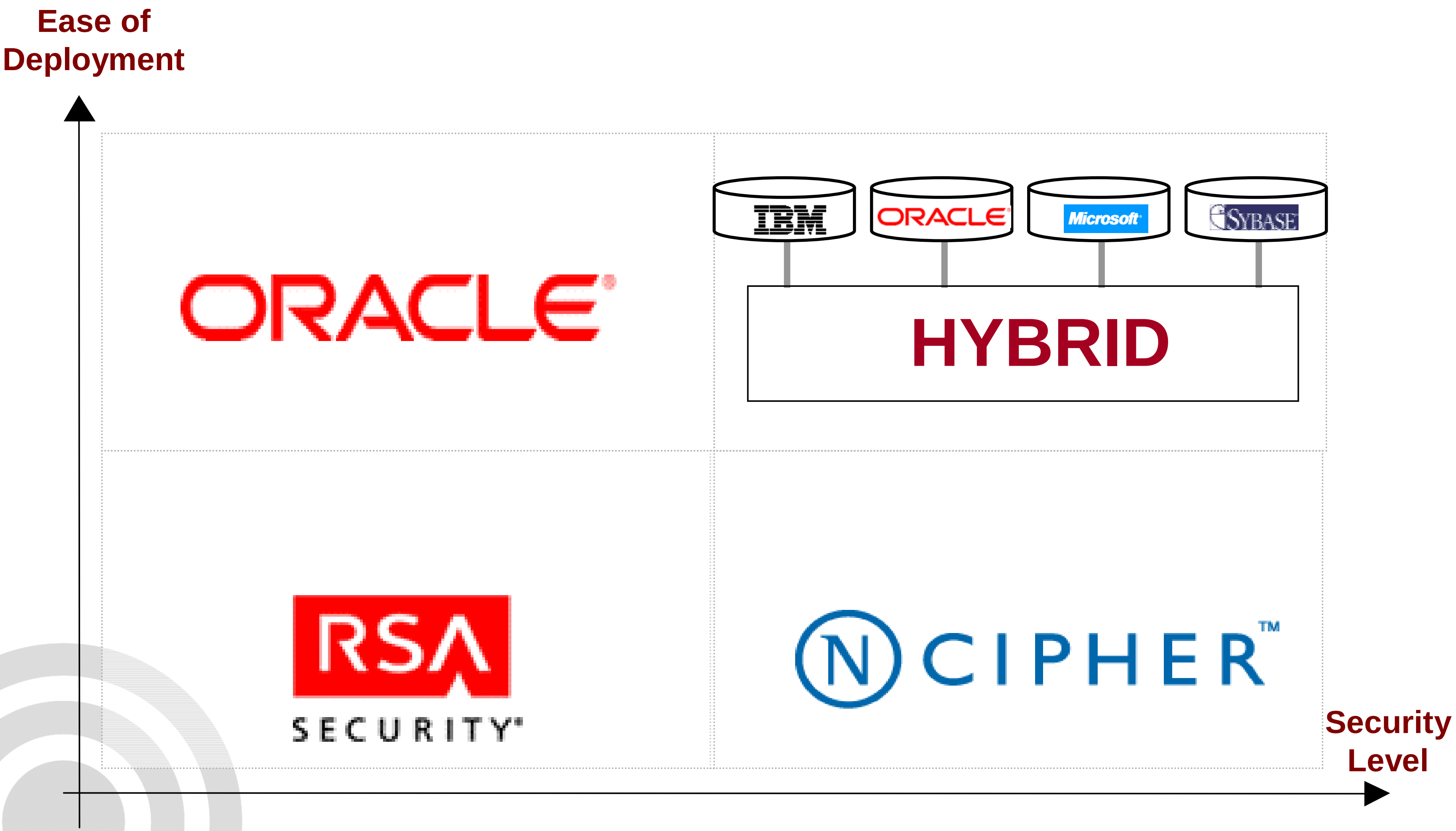
Solution Alternatives Summary

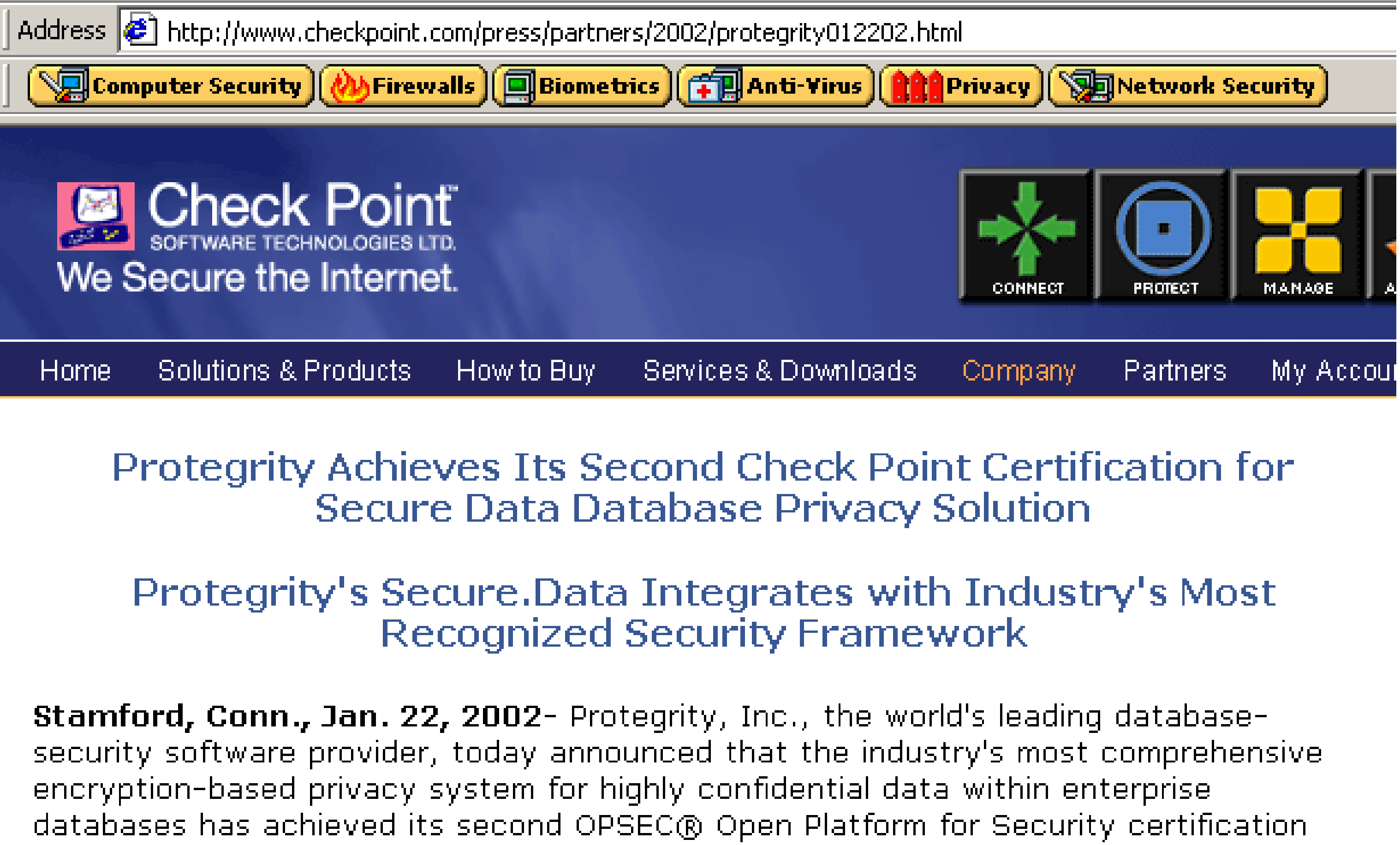
1. **Database toolkits?**
2. **Application toolkits?**
3. **Toolkit drawbacks include:**
   - Limited and rudimentary Prevention when deployed at the data level
   - Time-consuming development and expensive maintenance
   - Lack of flexibility
   - Don’t address issues such as key management, dual control and separation of duties

Case Studies - 4 Solution Alternatives


Ease of Deployment
Database Based Encryption Keys
APPL
Security-System Based Encryption Keys
APPL
FIPS
Application Based Encryption - Basic
APPL
Application Based Encryption - Advanced
APPL
FIPS
Security Level

Case Studies - 4 Solution Alternatives

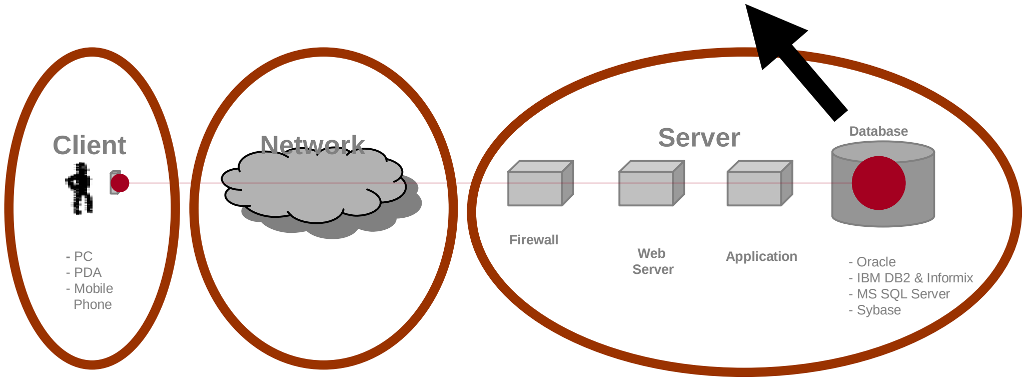




Protegrity Achieves Its Second Check Point Certification for Secure Data Database Privacy Solution

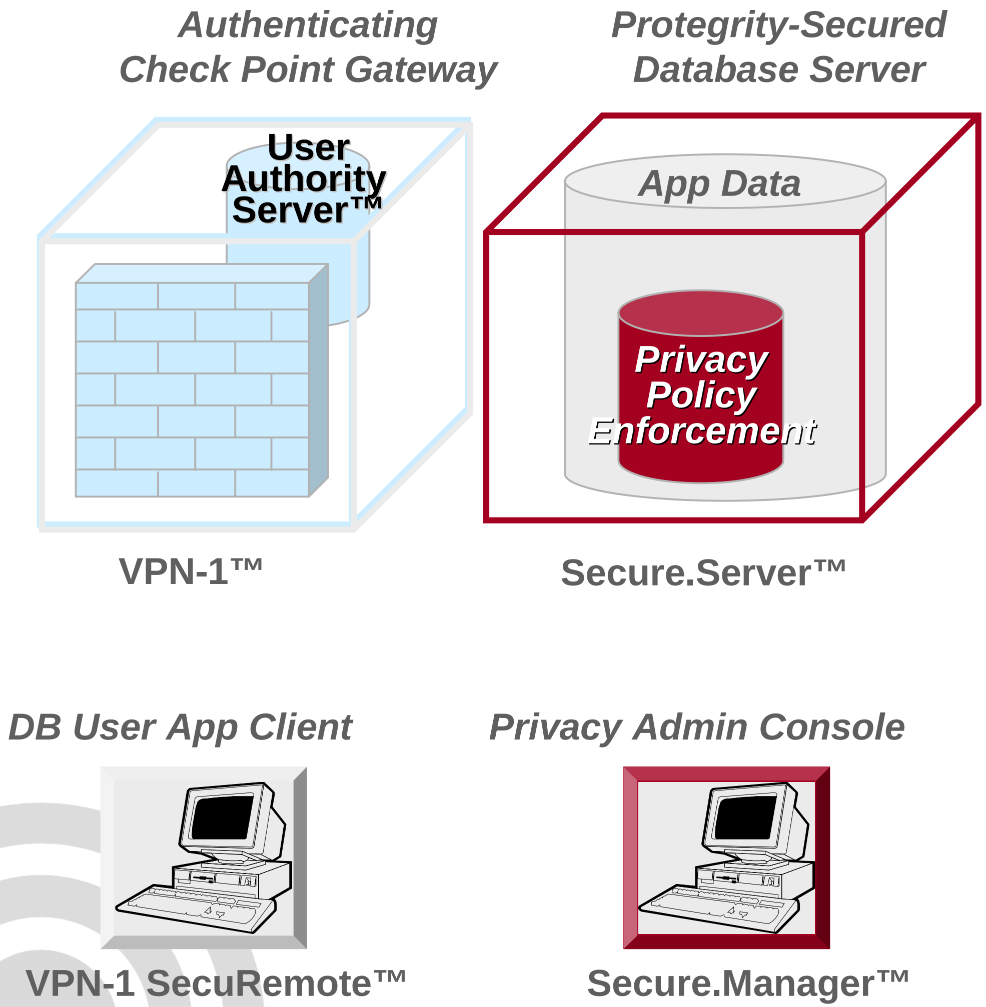
Protegrity's Secure.Data Integrates with Industry's Most Recognized Security Framework

Stamford, Conn., Jan. 22, 2002- Protegrity, Inc., the world's leading database-security software provider, today announced that the industry's most comprehensive encryption-based privacy system for highly confidential data within enterprise databases has achieved its second OPSEC® Open Platform for Security certification



Safeguarding Enterprise Data

Check Point Integration Components



DB User logon requests to Protegrity-secured databases can now be authenticated with Check Point technology

Checkpoint:

- VPN-1 SecuRemote, or
- VPN-1 SecureClient
- VPN-1 Gateway or Firewall-1

Database Server:

- Secure.Server 2.2.1.3

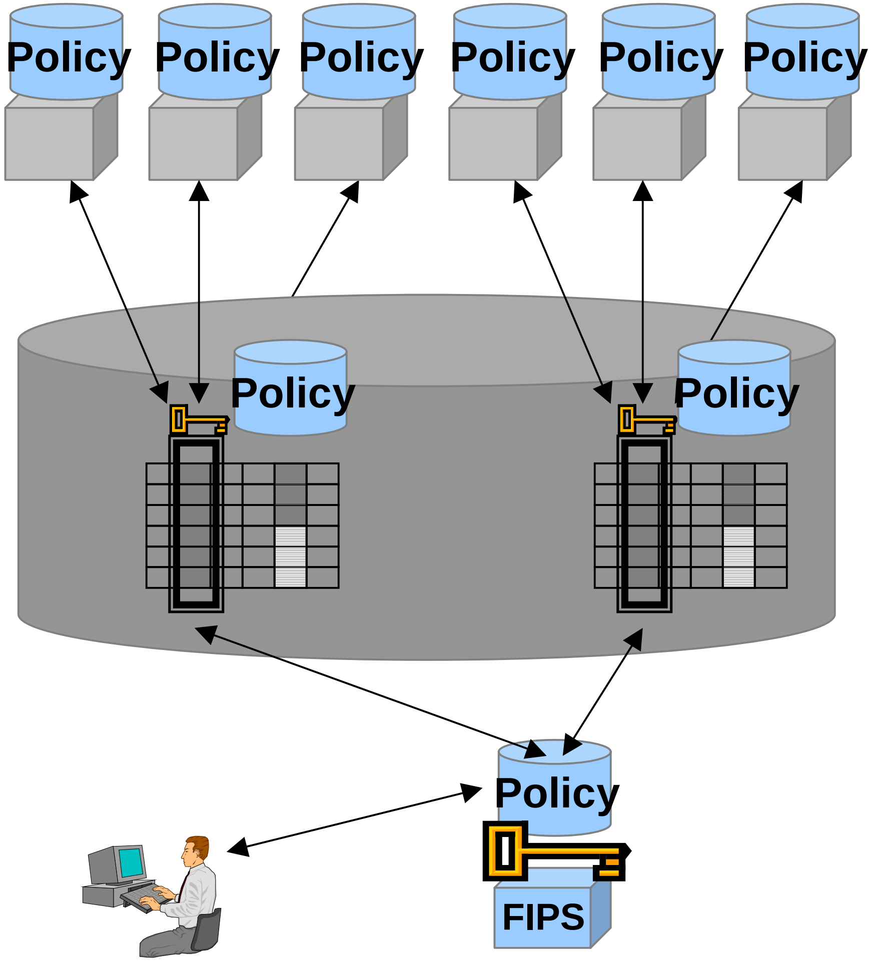
Privacy Administration Console:

- Secure.Manager 2.2.1.3

Check Point UAA Integration Details

- User requests secured application - A client attempts to access an application which is secured by a VPN-1 or FireWall-1 gateway and requires authentication.
- Gateway authenticates user, establishes VPN - Based on the security policy, the gateway authenticates the user.
- In this example, the user is requesting a connection through a VPN-1 Gateway and the policy specifies that a VPN be formed between the client and the Gateway.
- Application asks UserAuthority for user information - The application receives the connection request from the user. A user profile must be configured prior to a login request succeeding.
- Because this application leverages the UserAuthority API, it is a UserAuthority Client capable of making requests to the UserAuthority Server located at the Gateway.
- In this example, the UserAuthority Server knows about the user, so it responds to the application's UserAuthority Client request.
- A UserAuthority Server can also query other UserAuthority Servers, creating a chain of requests, until the UserAuthority Server which knows about the user is found and responds.
- Application makes intelligent authorization decision Based on information UserAuthority supplied. In this release the Secure.Server is able to make an intelligent authorization decision based on the authentication method supplied.
- Additional requests - Additional requests by this user to other applications do not require the user to authenticate. Rather, the UserAuthority-enabled application they want to connect to can make an inquiry to a UserAuthority Server.

Prevention Against Attacks

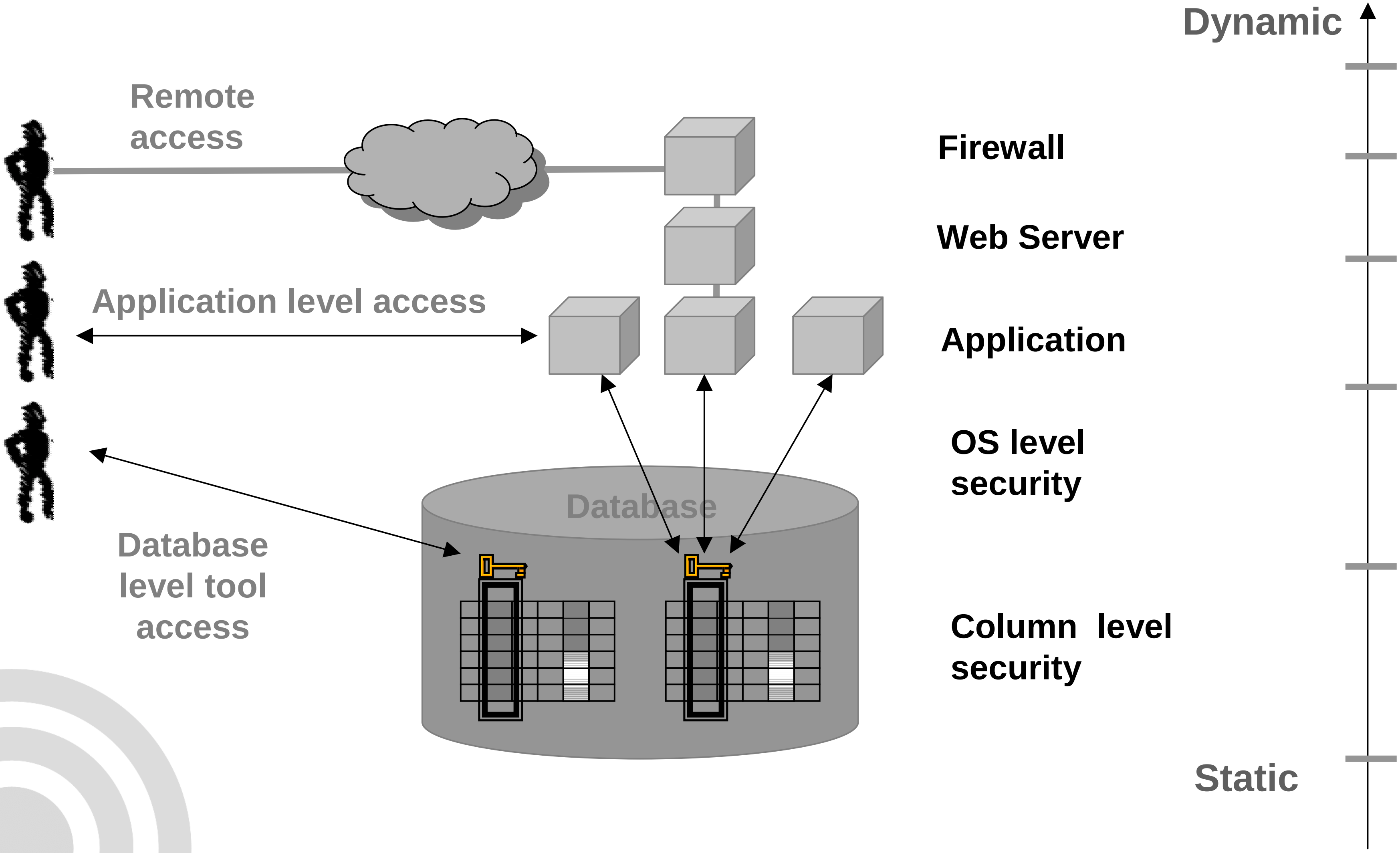


Application

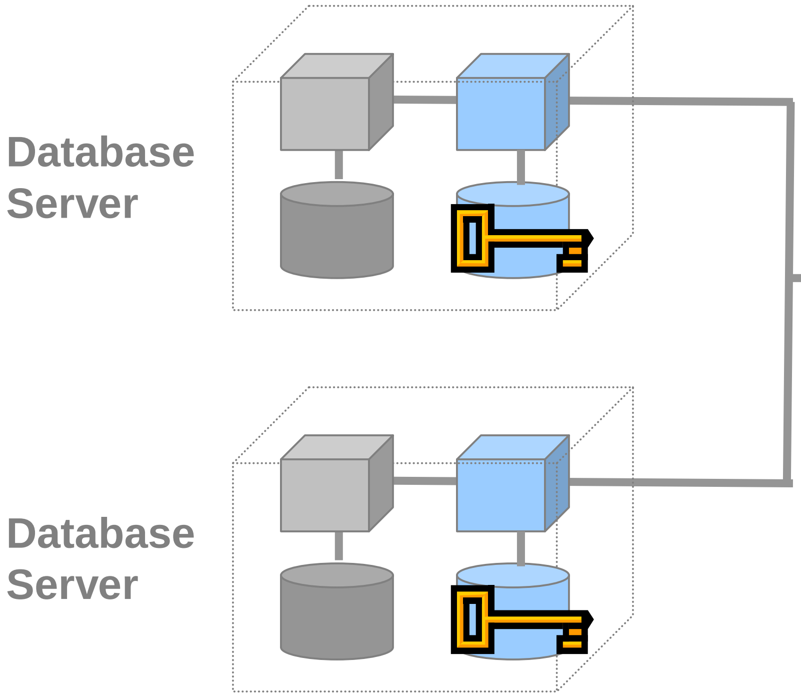
Database

Security
Enforcement
Facility

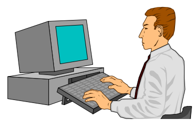
Policy Administration (RBAC)

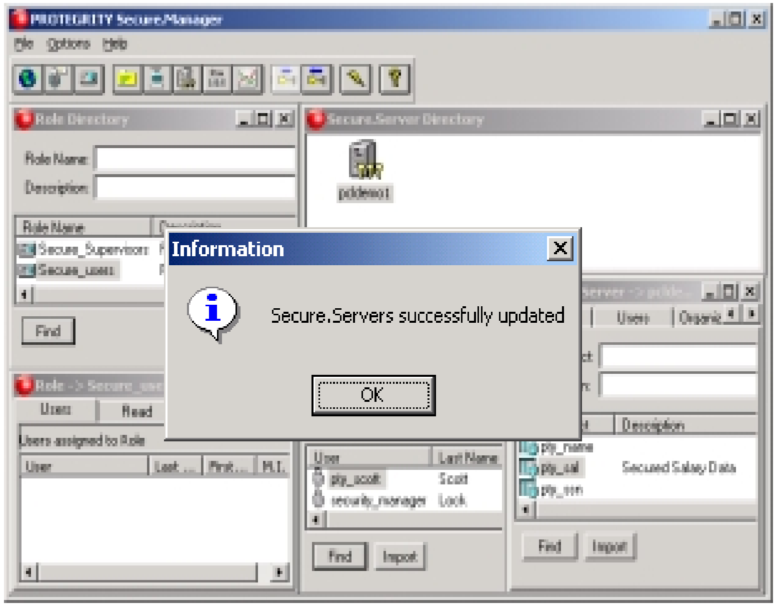


Single point of Privacy Policy Administration



One button update of Enterprise Privacy Policy



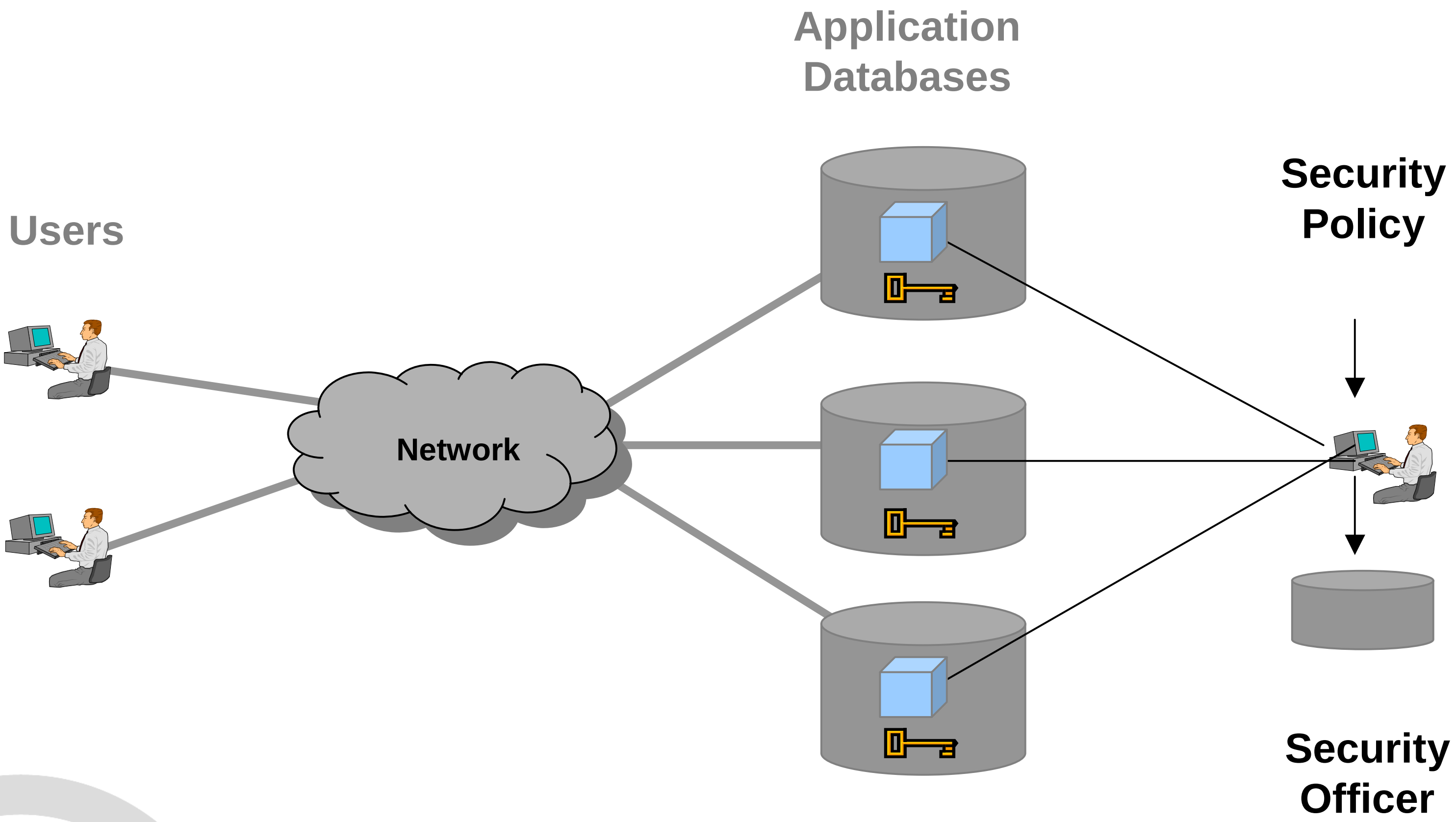


Information

Secure.Servers successfully updated

OK

A Database Intrusion Prevention Solution

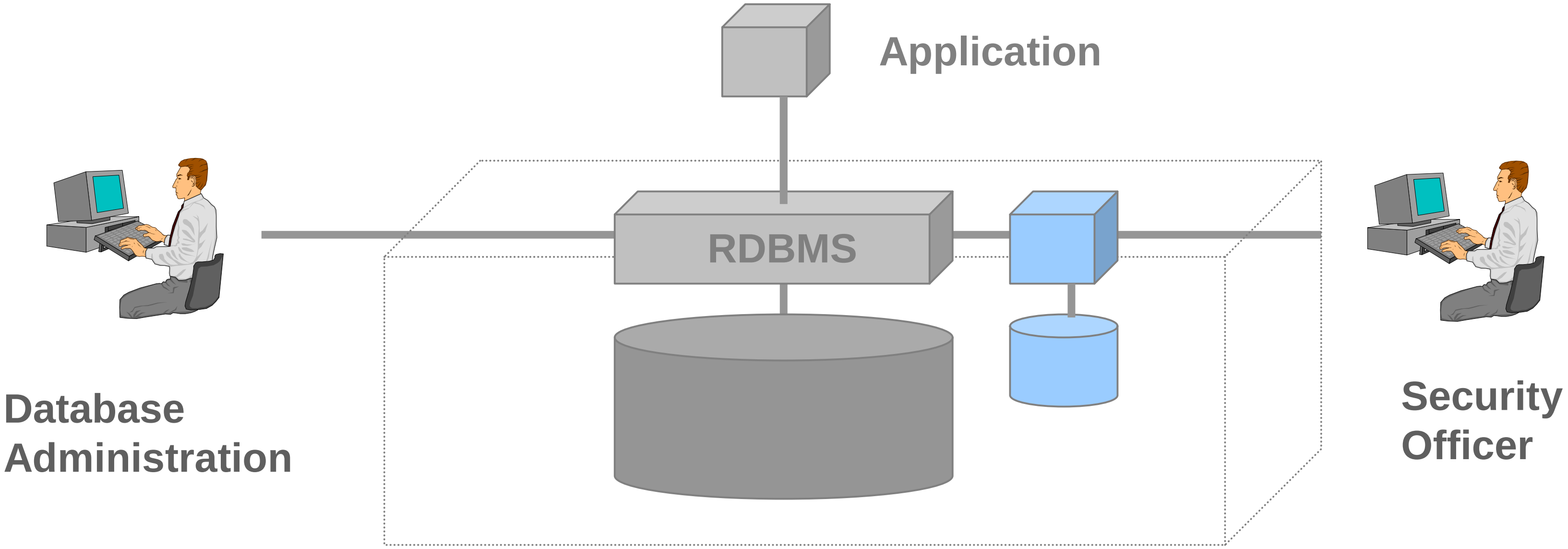


The Hybrid - Much more than data encryption

- The Database Intrusion Prevention provides an effective last line of defense

1. Selective and highly secure, column-level data item encryption
2. Cryptographically enforced authorization
3. Comprehensive key management
4. Secure audit and reporting facility
5. Enforced separation of duties
6. Interoperability with other security technologies
7. Operational transparency to applications

Separation of Privacy Control Duties

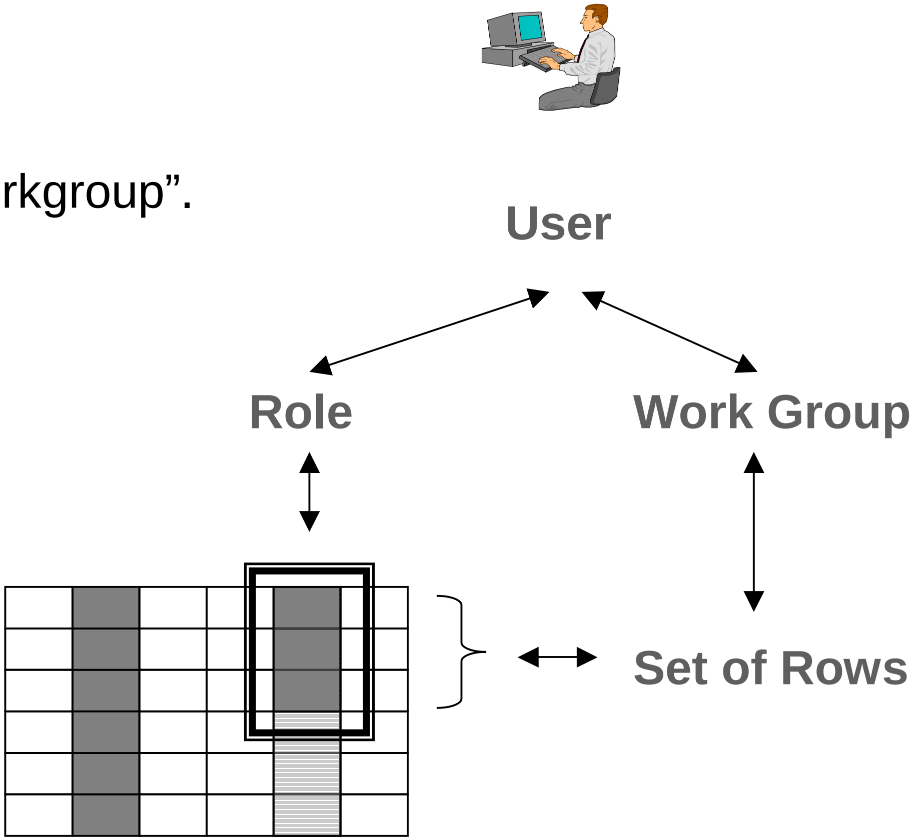


1. Separation of duties for encryption key management
2. Separation of duties for integrity check of selected software executables
3. Separation of duties for access control policy
4. Strong authentication for the security administrator

Easy to Manage - Role Based Access Control

1. Functional roles - “role”

2. Organizational roles - “workgroup”.



User

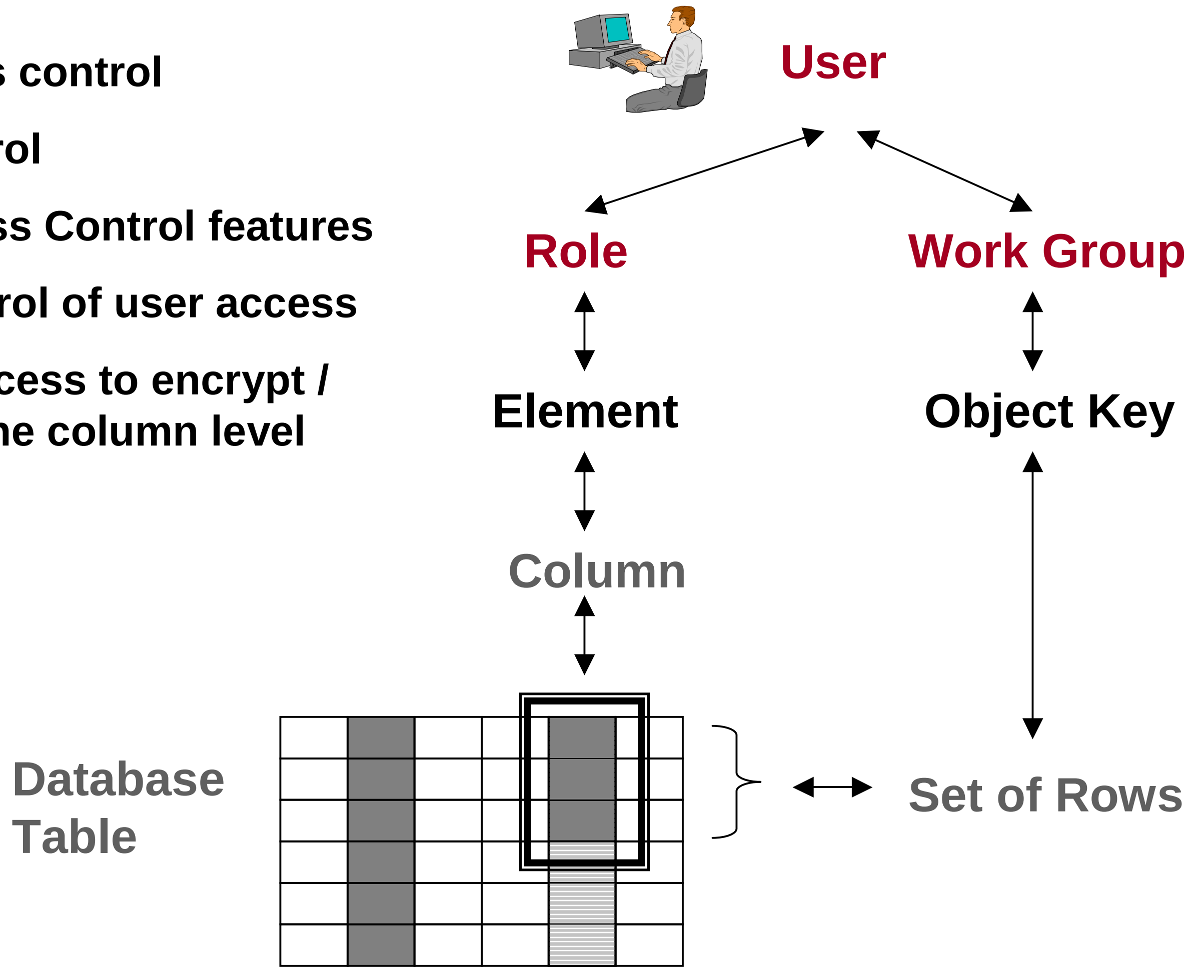
Role

Work Group

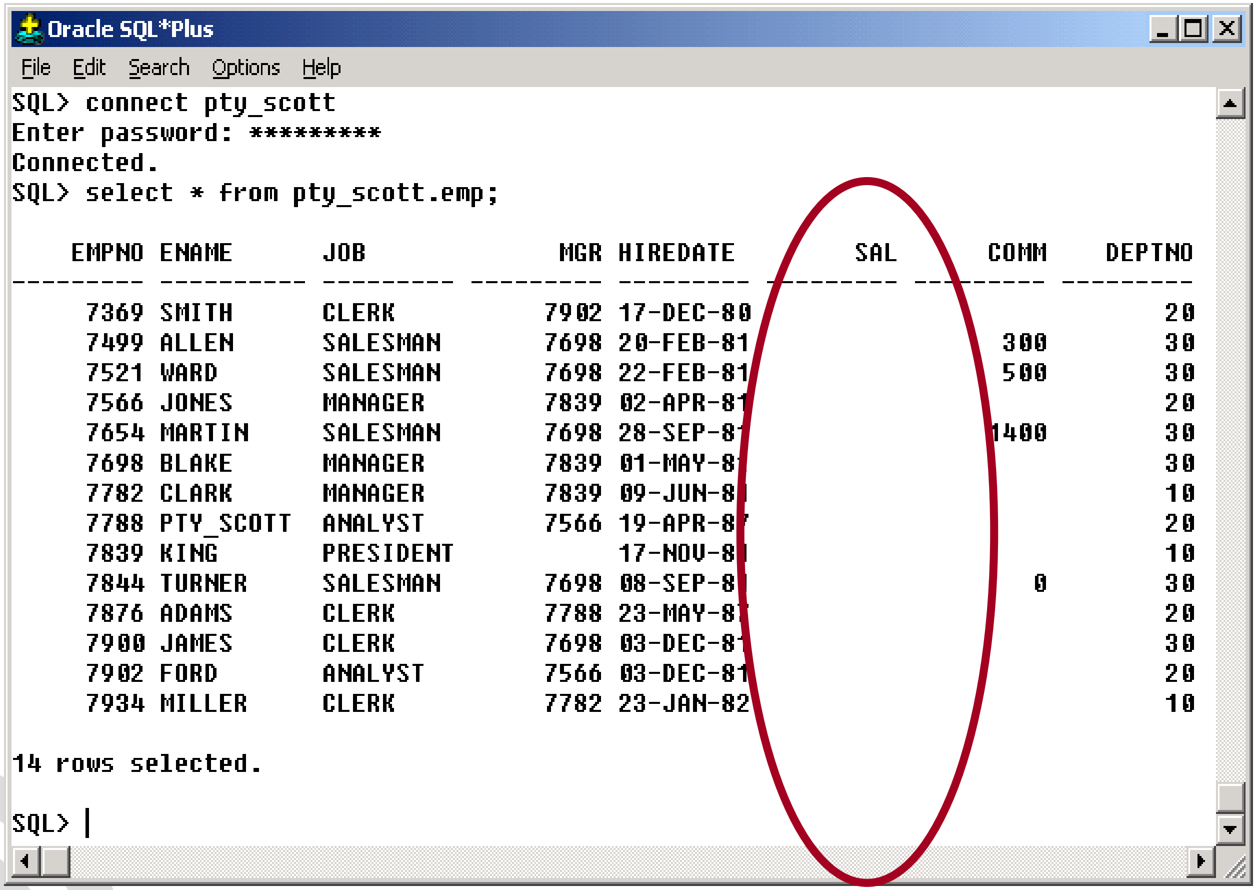
Set of Rows

Easy to Manage - Role Based Access Control

- Row level access control
- Role-based control
- Mandatory Access Control features
- Time-based control of user access
- Controls user access to encrypt / decrypt data at the column level



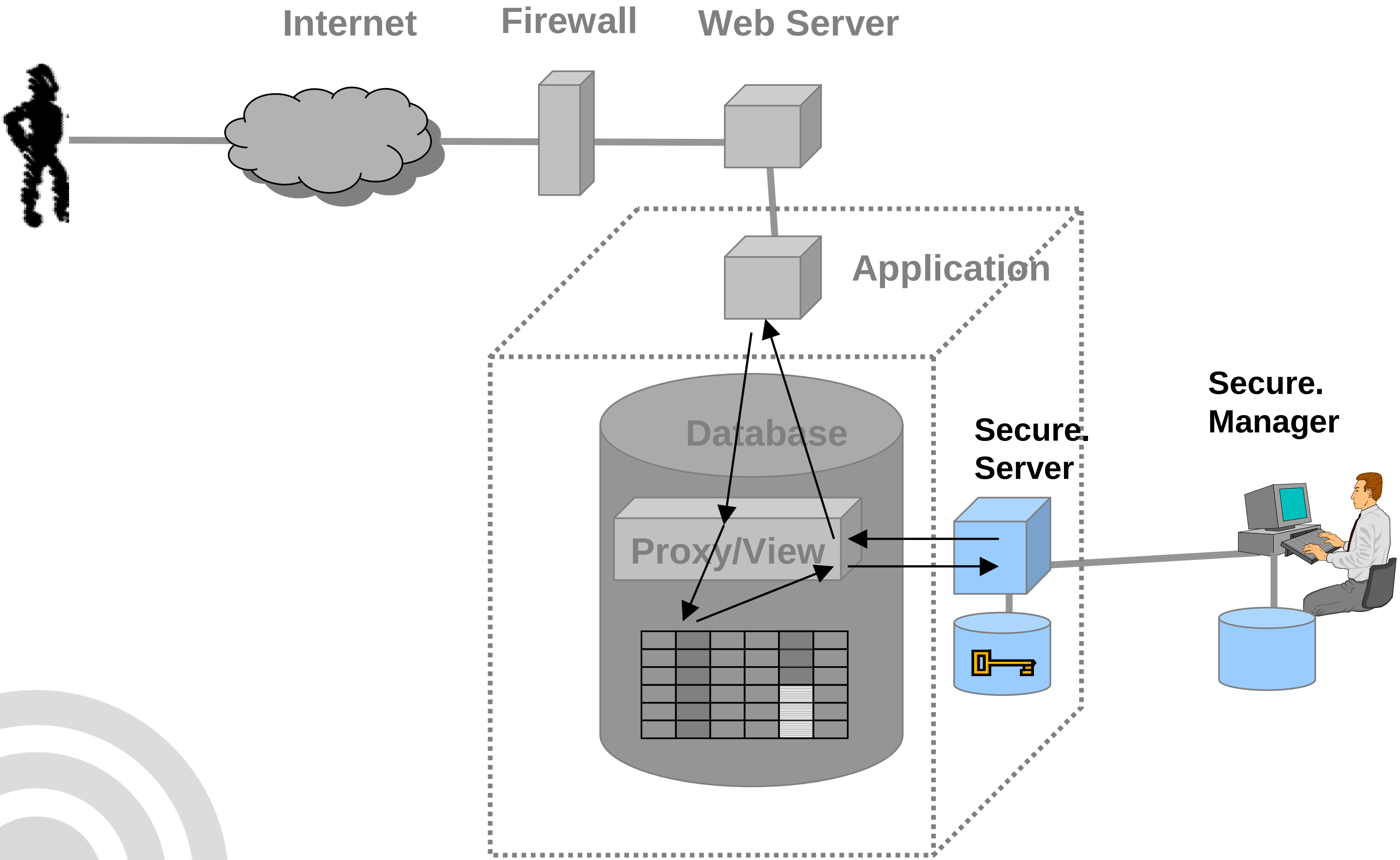
Application Transparent Encryption



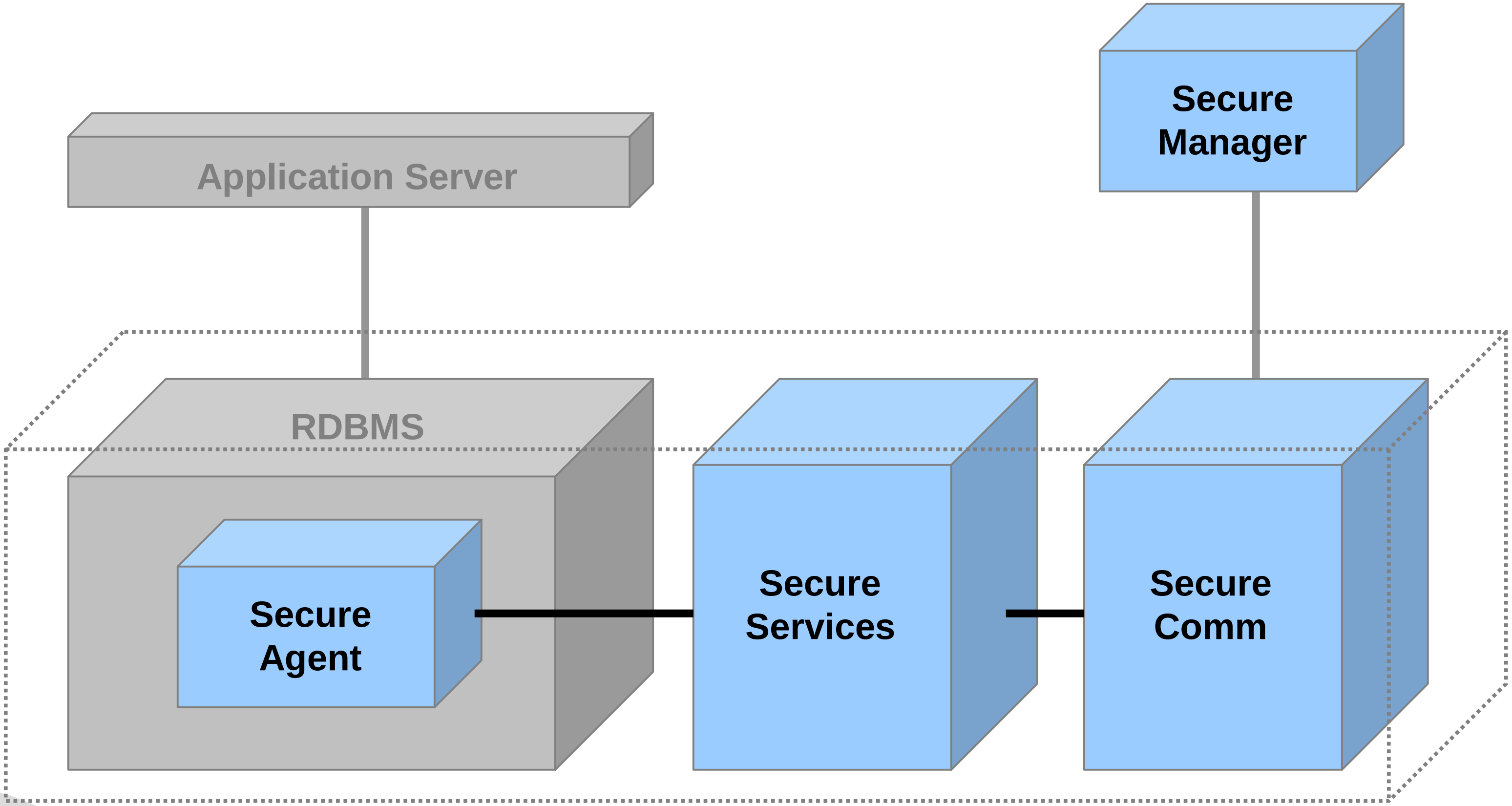
```
SQL> connect pty_scott
Enter password: *********
Connected.
SQL> select * from pty_scott.emp;

    EMPNO ENAME      JOB              MGR HIREDATE         SAL       COMM     DEPTNO
--------- ---------- --------- ---------- --------- ---------- ---------- ----------
     7369 SMITH      CLERK           7902 17-DEC-80                               20
     7499 ALLEN      SALESMAN        7698 20-FEB-81                   300         30
     7521 WARD       SALESMAN        7698 22-FEB-81                   500         30
     7566 JONES      MANAGER         7839 02-APR-81                               20
     7654 MARTIN     SALESMAN        7698 28-SEP-81                  1400         30
     7698 BLAKE      MANAGER         7839 01-MAY-81                               30
     7782 CLARK      MANAGER         7839 09-JUN-81                               10
     7788 PTY_SCOTT  ANALYST         7566 19-APR-87                               20
     7839 KING       PRESIDENT            17-NOV-81                               10
     7844 TURNER     SALESMAN        7698 08-SEP-81                     0         30
     7876 ADAMS      CLERK           7788 23-MAY-87                               20
     7900 JAMES      CLERK           7698 03-DEC-81                               30
     7902 FORD       ANALYST         7566 03-DEC-81                               20
     7934 MILLER     CLERK           7782 23-JAN-82                               10

14 rows selected.

SQL> |
```

Immediate Response on Policy Changes

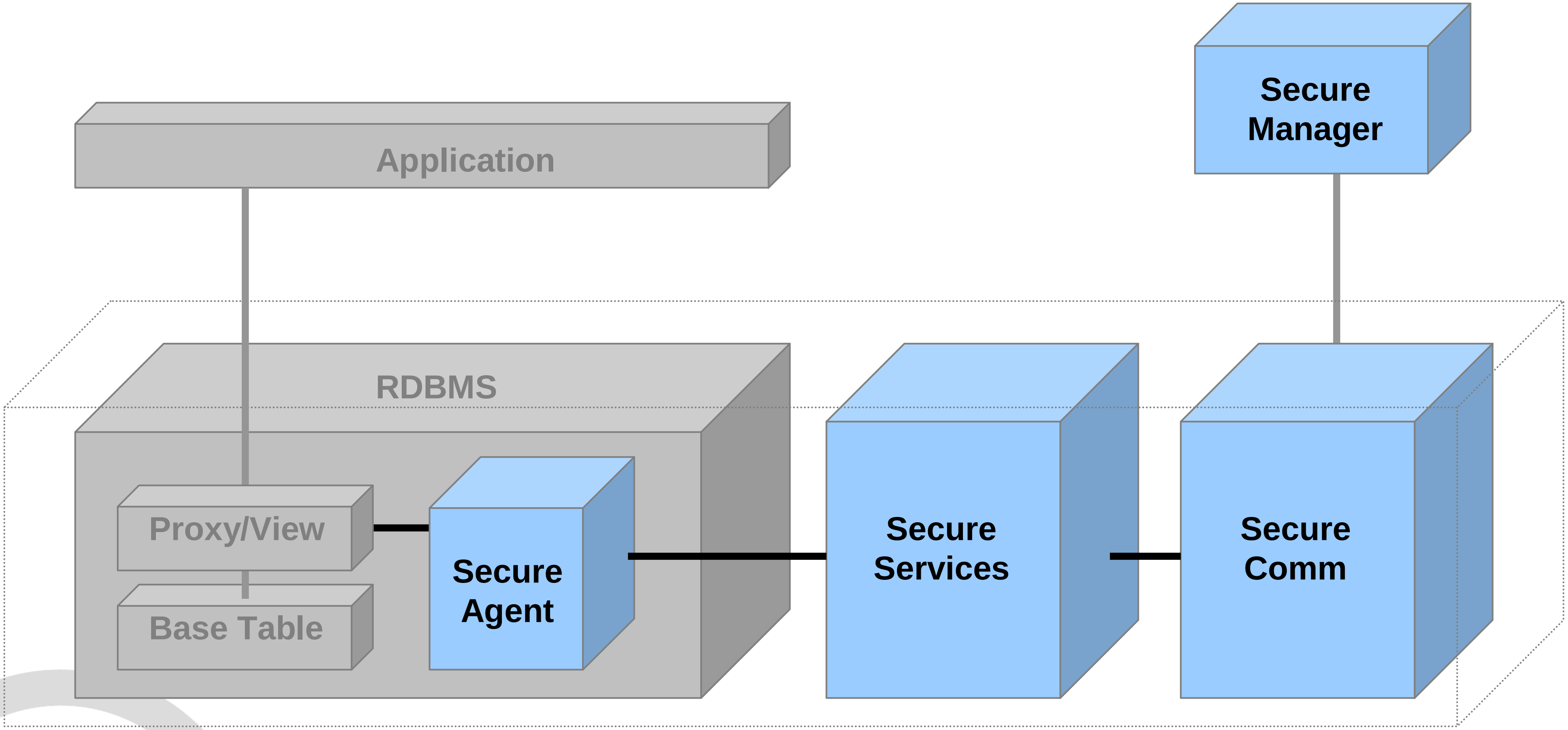
Secure.Data - Implementation



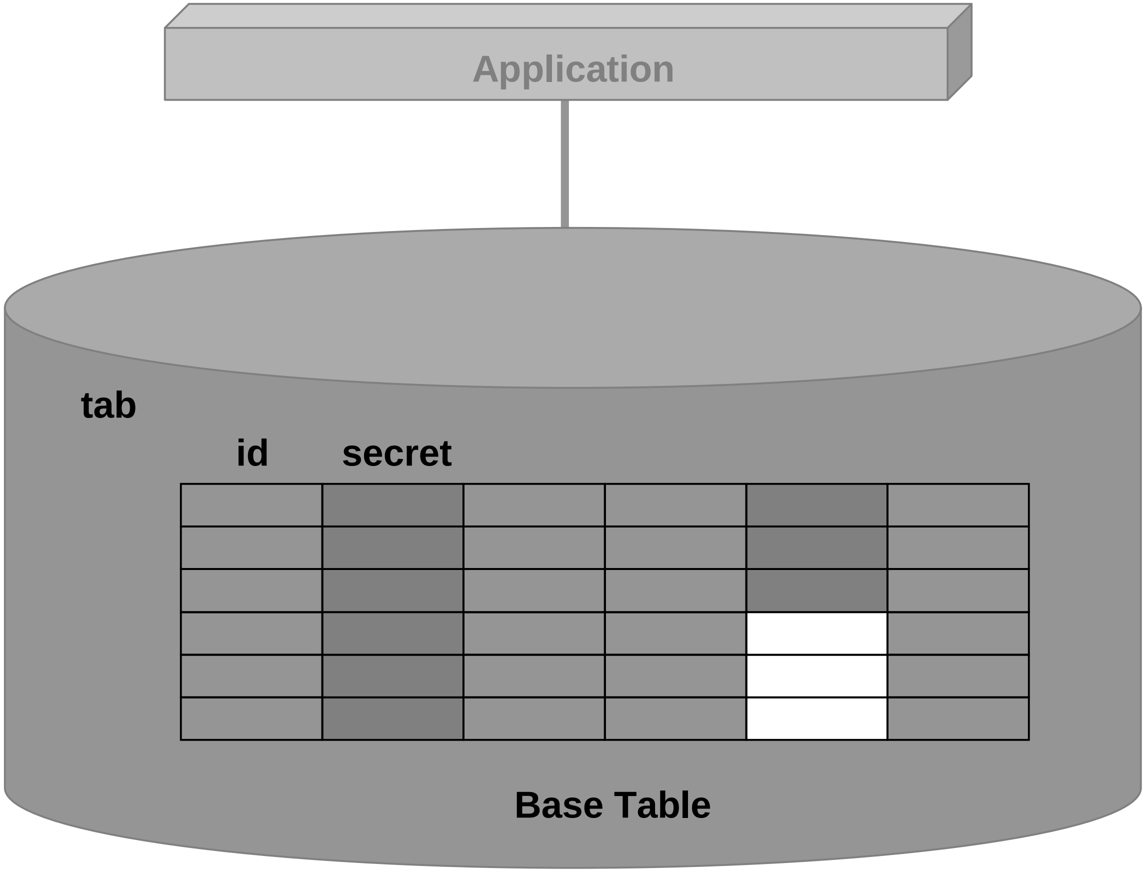
Secure.Data - Implementation



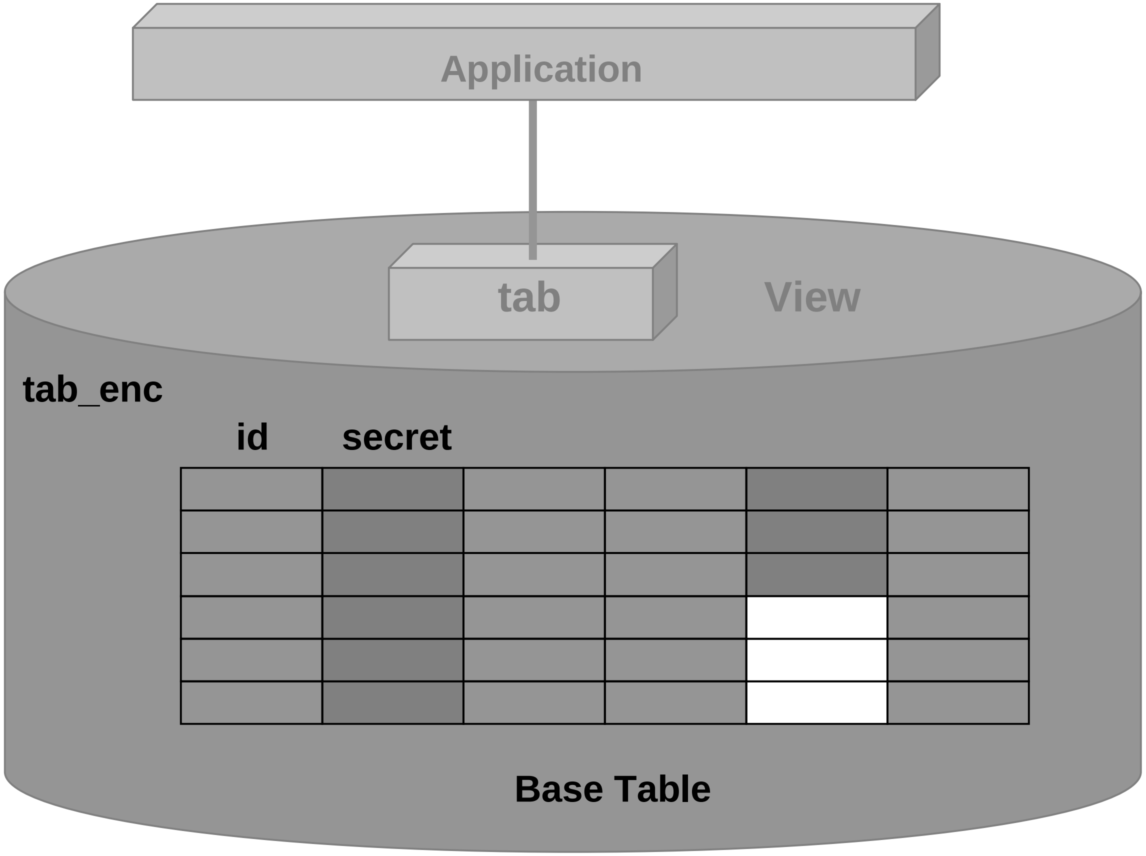
Secure.Data - Implementation



Secure.Data – Implementation - Sample



Secure.Data – Implementation - Sample


Application
tab
View
tab_enc
id
secret
Base Table