Wednesday, September 8th, 2004

INTERNATIONAL DB2 USERS GROUP

San Francisco DB2 User Group

The next meeting for the San Francisco Area DB2 User Group will be:

Wednesday September 15th, 2004

Register: click here

Topics: Wednesday September 15th, 2004

"SOX, SOA, and SarbOx and IT – What does it mean to DB2? "

A Practical Solution that Facilitates Database Compliance to Security Mandates and Industry Initiatives

Speaker: Ulf T. Mattsson – Chief Technology Officer – Protegrity

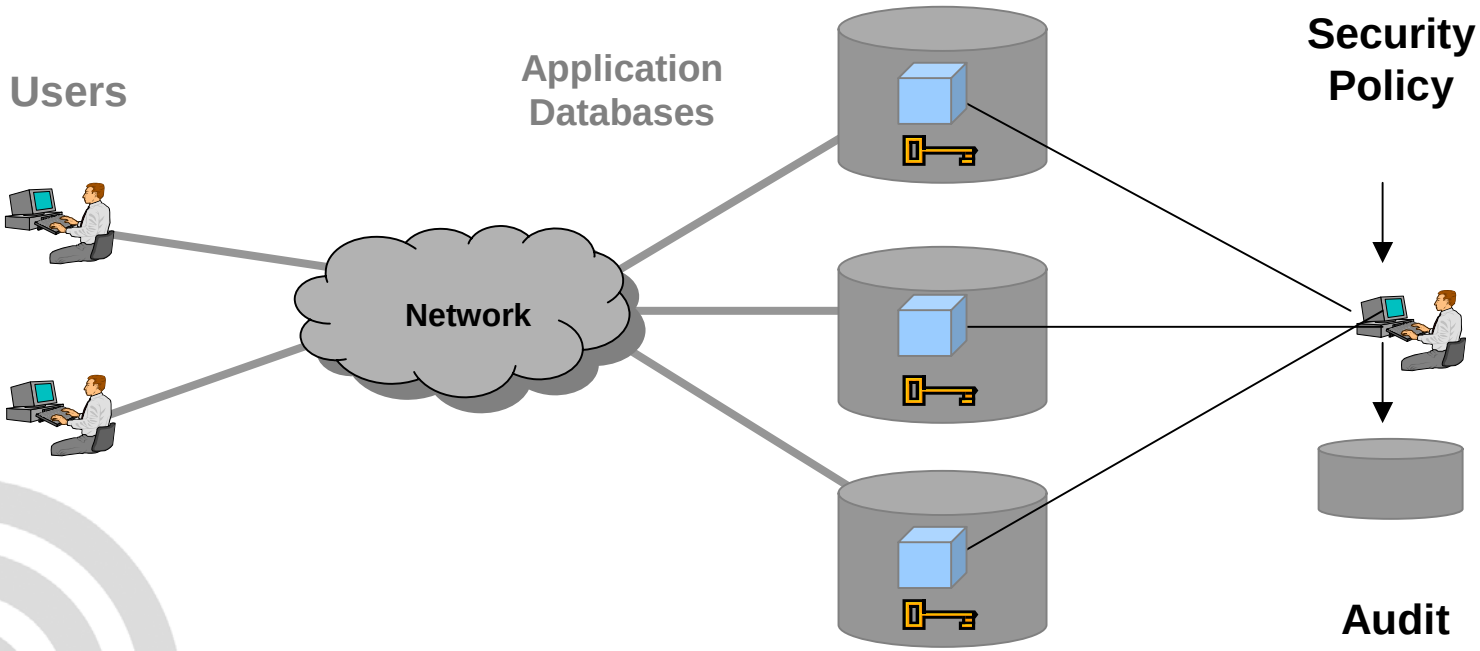
Ulf T. Mattsson, holds a master's degree in physics and a number of patents in the IT security area. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security. He 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 WSEAS, Medical Records Institute, and the IBM Privacy Management Advisory Council.

Agenda

- Review of Critical and Practical Requirements for Data-layer Security
- Technology Overview - Data-layer Security
- Technology issues - Data-layer Security
- Review of Requirements for Data Type Preserving Security Technology
- How Protegrity can meet these Requirements

Securing Enterprise Data

Protegrity provides enterprise-wide, policy-driven data security solutions for organizations that need to protect sensitive data



Corporate Overview

- Ten years experience developing database protection solutions
- We own fundamental data protection patents
- Over sixty customers
- HQ in Connecticut with offices in North Carolina and Sweden
- Wholly-owned subsidiary of Xcelera Inc. (AMEX:XLA)

Protegrity and IBM

- Protegrity is an Advanced Partner of IBM PartnerWorld for Software
- Protegrity is an Advanced Partner of IBM PartnerWorld for Developers
- Protegrity and IBM has signed the IBM Passport Advantage Solution Selling Agreement
- Protegrity is part of the IBM IPASS program where IBM will manage all orders, invoicing and Protegrity will ship the products
- Protegrity is certified by the IBM Start Now Solution Proven Program
- Secure.Data for DB2 is certified on The Solution Advantage Server Proven program

DB2 magazine

DB2 is a registered trademark of IBM and is used here under license

- → Magazine
- → E-Newsletter
- → Technical Tips
- → Skills & Education
- → Books
- → Career Center
- → Subscribe
- → Advertise

DB2 20th Anniversary Poster

Features

An Anniversary Message to the DB2 Community

Janet Perna

After 20 years, the innovations keep coming. IBM Data Management Solutions general manager Janet Perna sets the stage for what's coming next.

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?

Columns

Data Miner
Experimental Design
Elizabeth Obee

Web Developer
Are XML Databases Necessary?
Michael S. Dougherty

Content Management
You Say CM, I Say DM ...
Priscilla Emery

DB2 DBA
Seeing the DB2 Light
Robert Catterall

Programmers Only
More Joys of Commitment
Bonnie Baker

DB2 Trivia

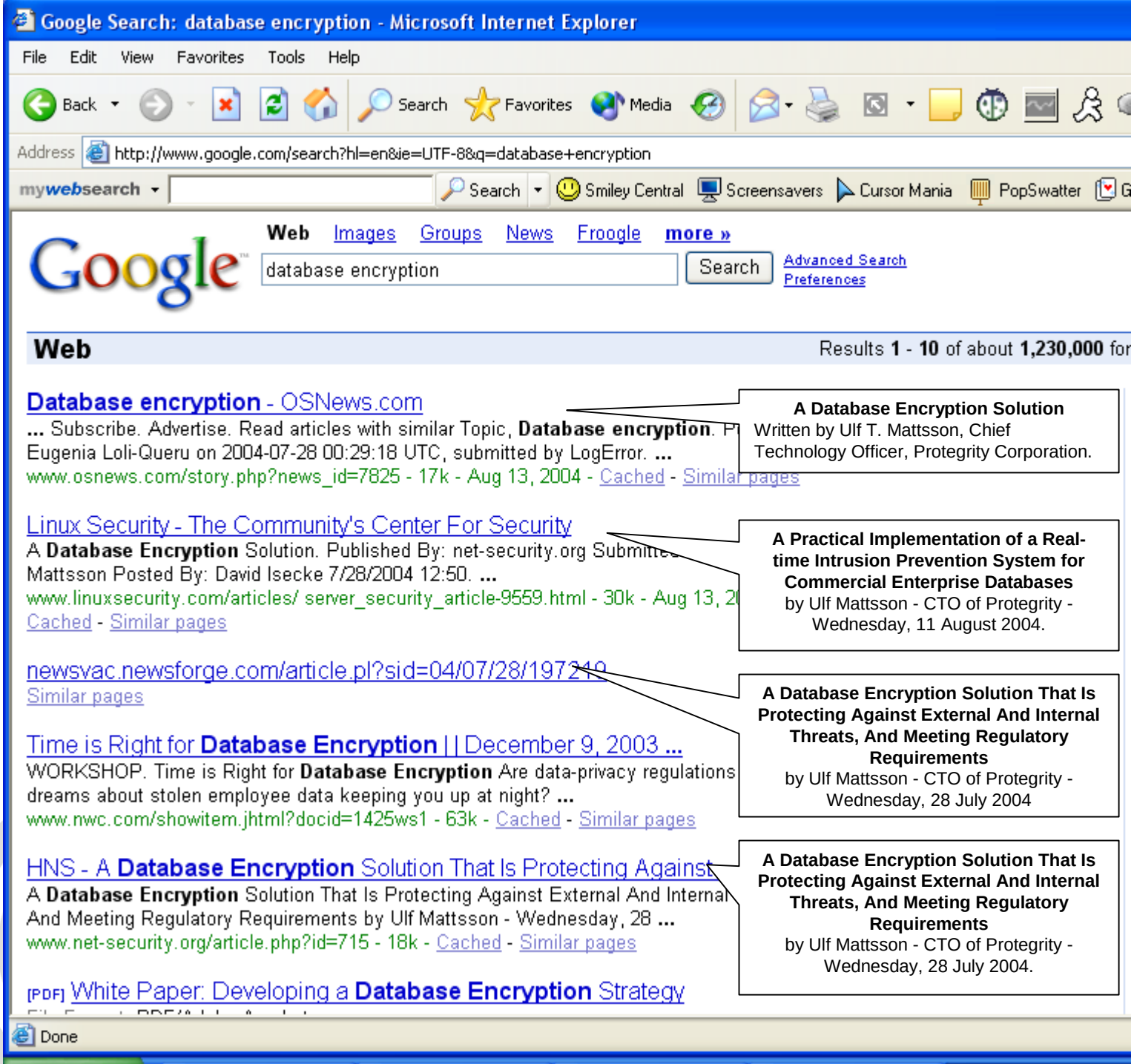
By what name was DB2 known at IBM before its 1983 unveiling to the public?

- A. Falcon
- B. Eagle
- C. Hawk
- D. Kestrel

Answer correctly to enter a drawing for a $100 American Express Gift Cheque!

Grade Me

E-Newsletter



A Database Encryption Solution
Written by Ulf T. Mattsson, Chief Technology Officer, Protegrity Corporation.

A Practical Implementation of a Real-time Intrusion Prevention System for Commercial Enterprise Databases
by Ulf Mattsson - CTO of Protegrity - Wednesday, 11 August 2004.

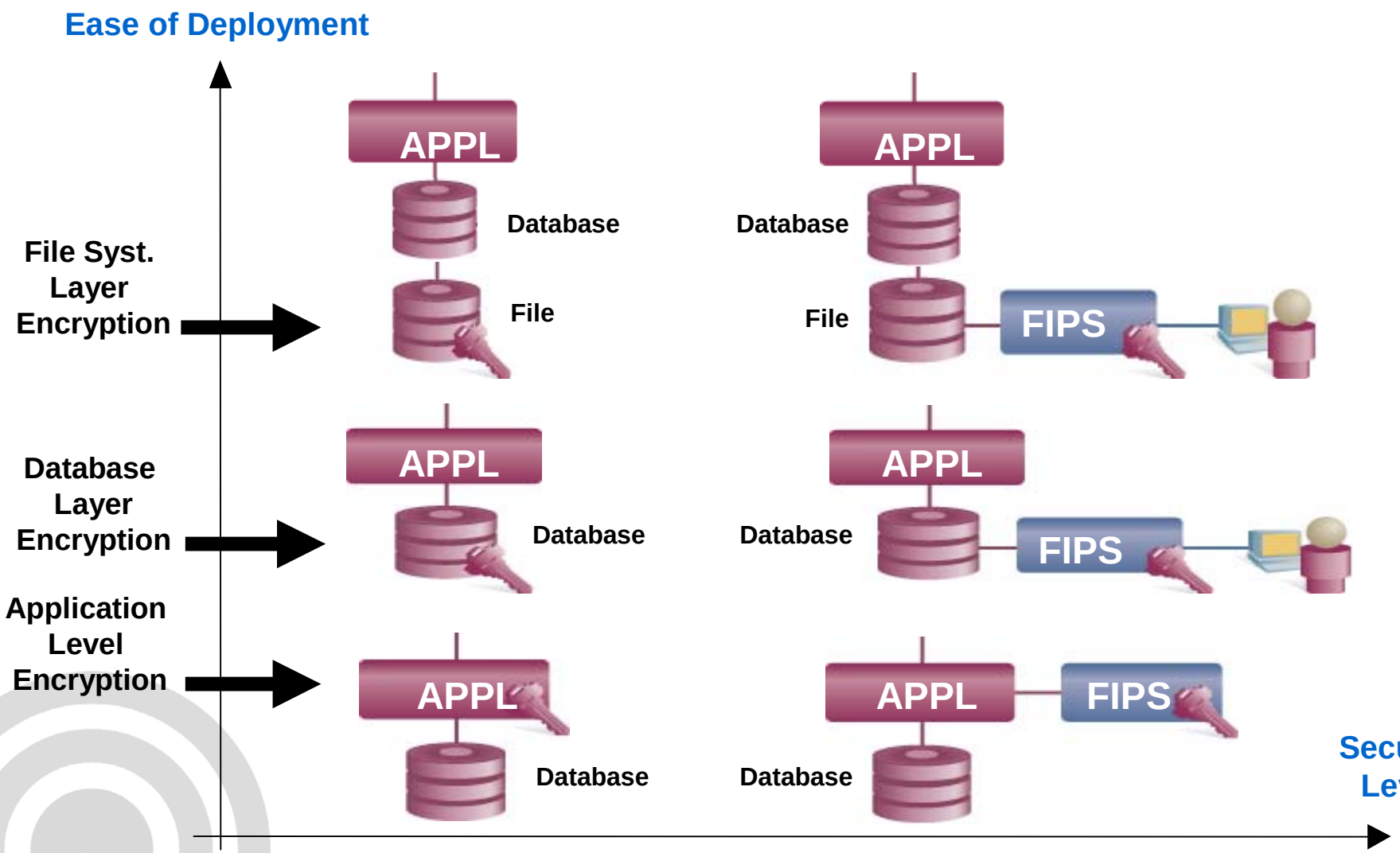
A Database Encryption Solution That Is Protecting Against External And Internal Threats, And Meeting Regulatory Requirements
by Ulf Mattsson - CTO of Protegrity - Wednesday, 28 July 2004

A Database Encryption Solution That Is Protecting Against External And Internal Threats, And Meeting Regulatory Requirements
by Ulf Mattsson - CTO of Protegrity - Wednesday, 28 July 2004.

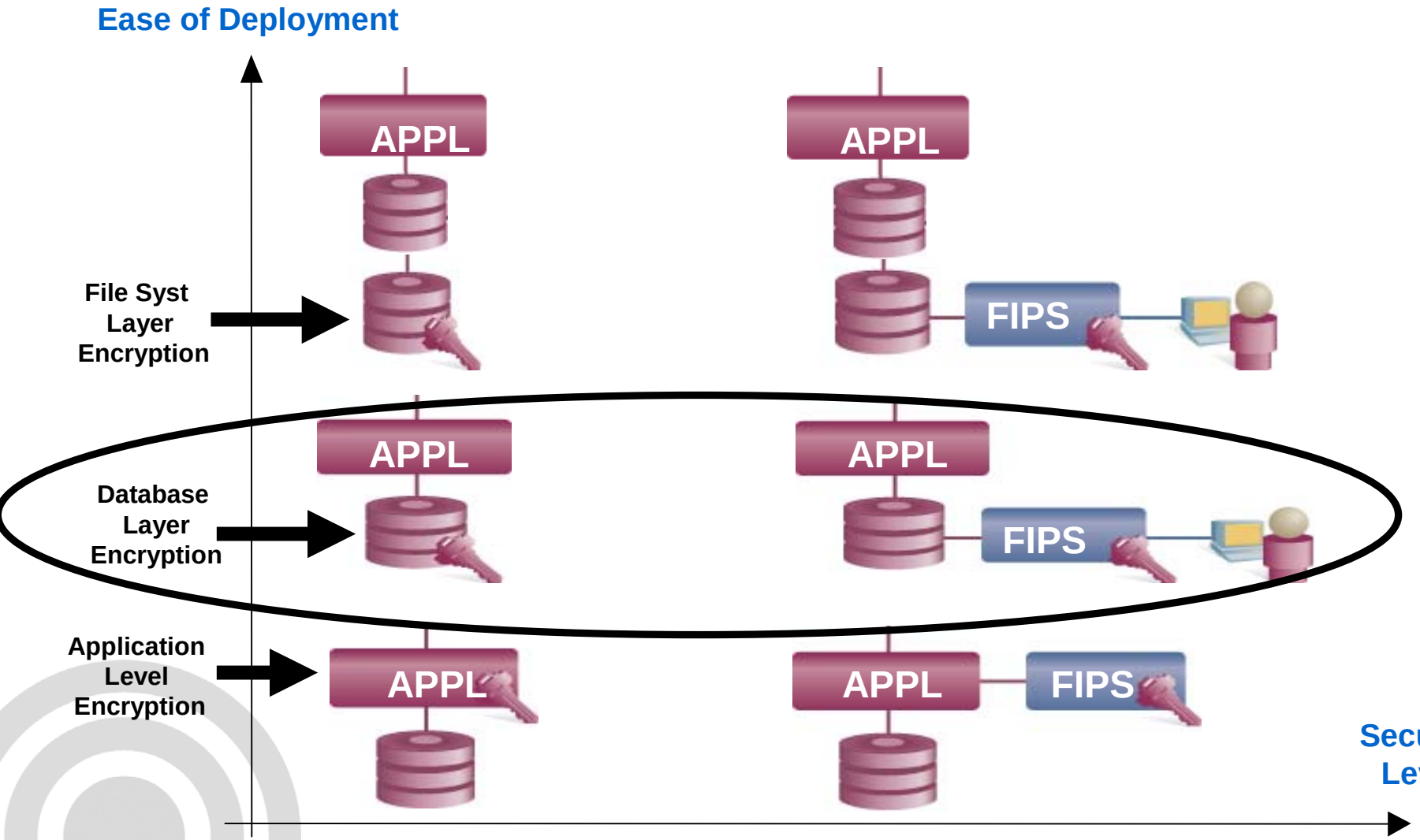
IBM Business Partner

protegrity
securing digital assets

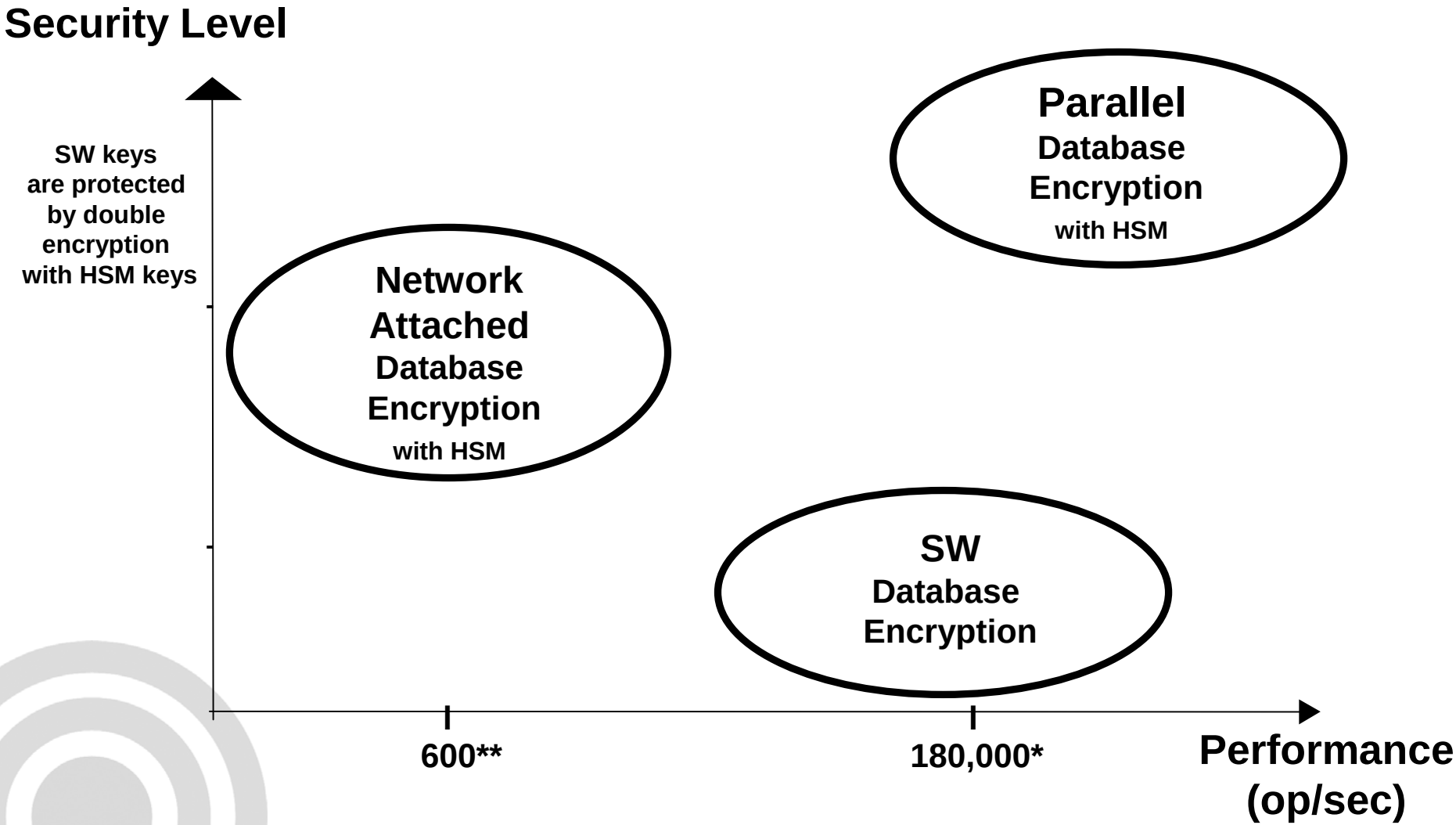
Case Studies – 3 Solution Alternatives



Case Studies – Database Encryption Solutions



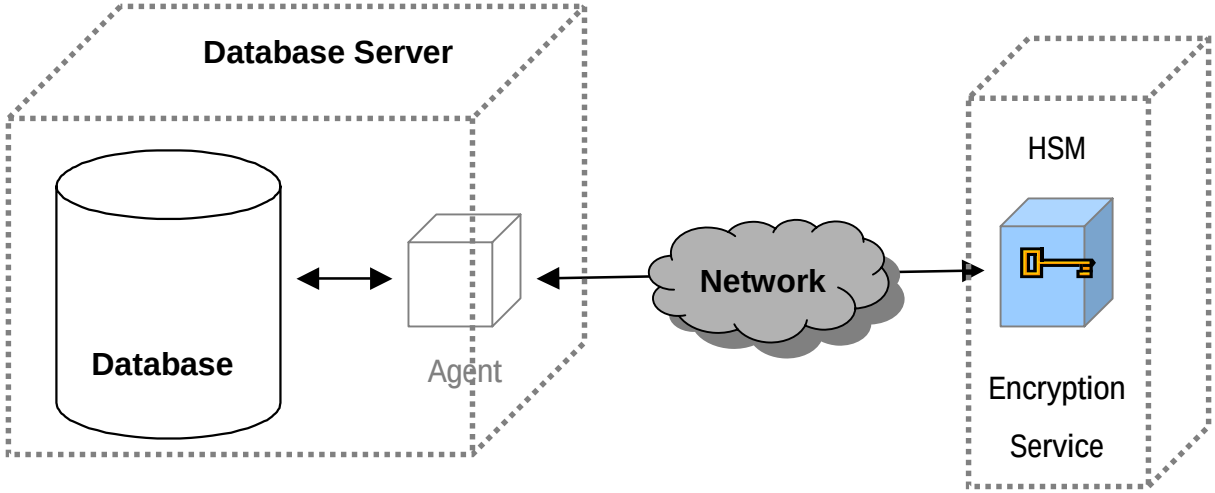
Security & Performance of Database Encryption Solutions



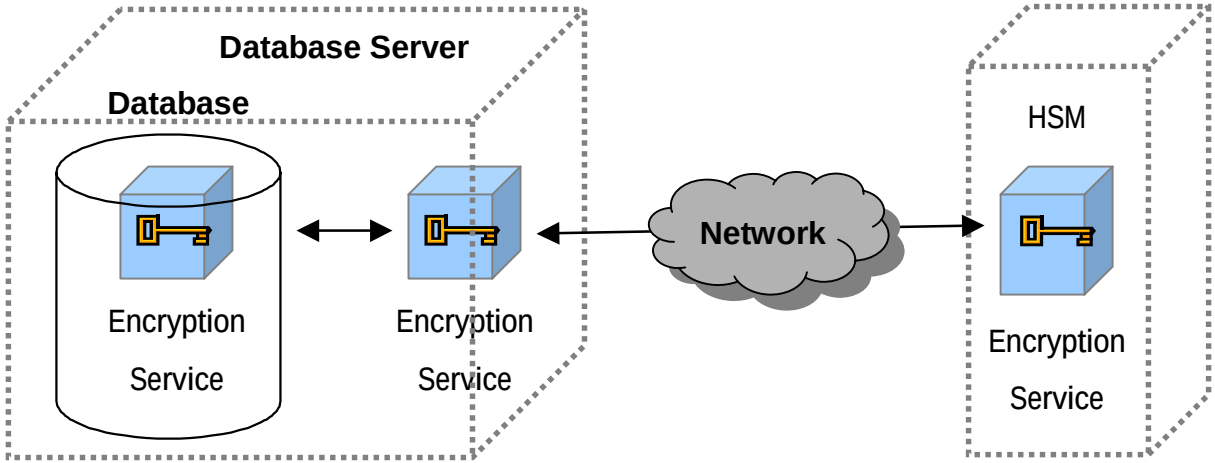
*: Source - IBM Waltham, Protegrity Secure.Data Benchmark on UNIX
**: Based on Publicly available information and Protegrity Benchmarks

Performance – Database Encryption

Network Attached Database Encryption (600 op/sec**)



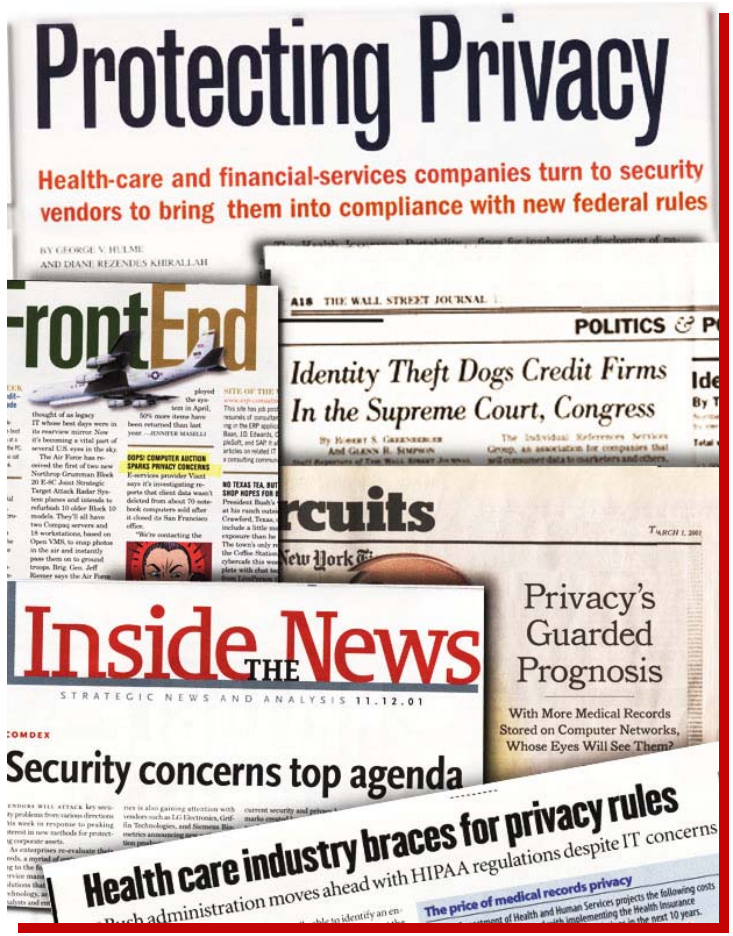
Integrated Parallel Database Encryption (180,000 op/sec*)



*: Source - IBM Waltham, Protegrity Secure.Data Benchmark on UNIX
**: Based on Publicly available information and Protegrity Benchmarks

Privacy & Security Legislation

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



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 **unencrypted** 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 **unencrypted** 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. Encryption, including transit and storing
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

Customer 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.**

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

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
- Customer Cardholder Information Security Program (CISP)
- Customer 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

IBM Business Partner

Typical Compliance Requirements:

User Access Control & Audit

Data Integrity

Administrator Access Control & Audit

Response when unauthorized access is suspected or detected

Data Confidentiality

FBI/CSI Statistics - Inside Threats

Outside Threats

Inside Threats

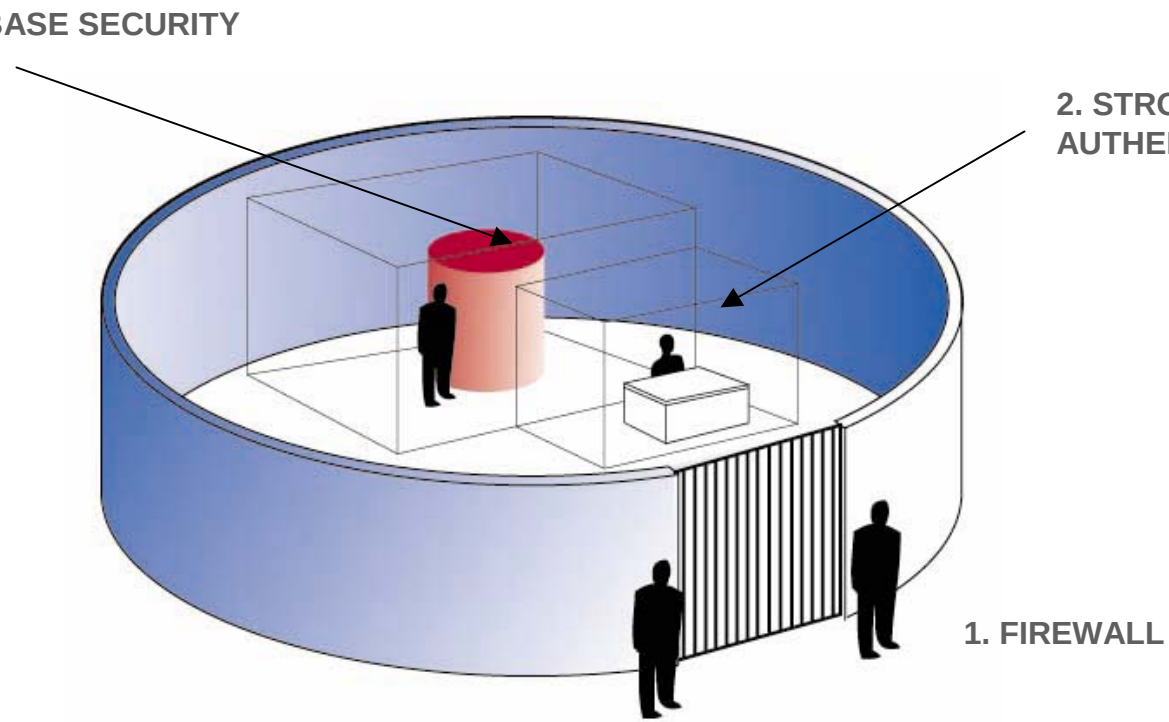
The most serious financial losses occurred through theft of proprietary information.

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 …'

Data Security Critical Requirements

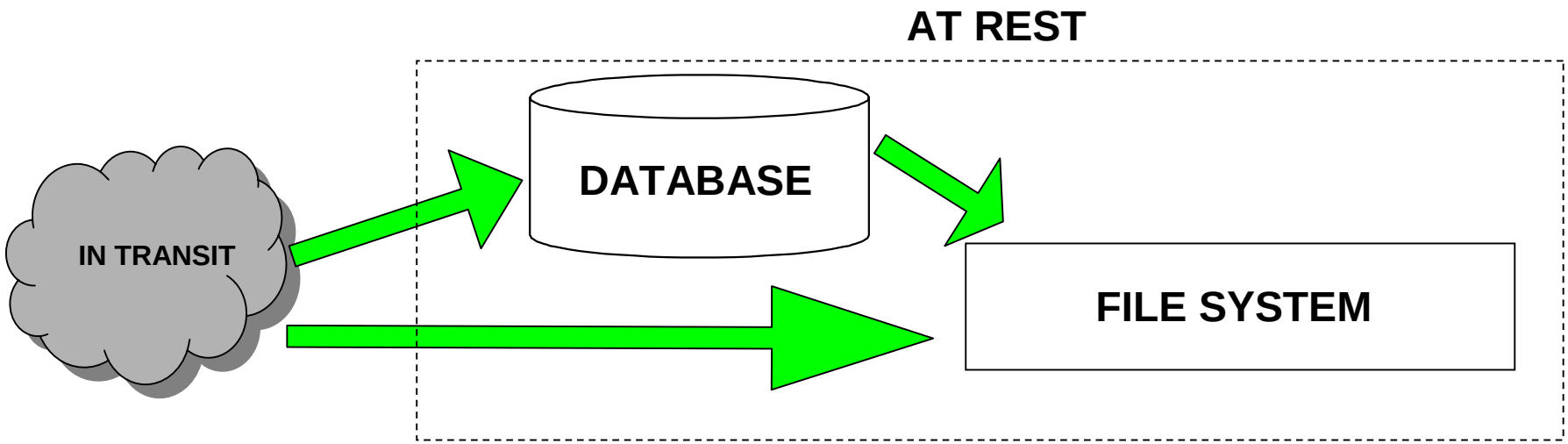
- Protect data in both the database and storage system
- Enforce privileges at the field/user level
- Separate security policy from data management
- Protect encryption keys
- Audit & report access to secure data

Data Security Practical Requirements

IBM Business Partner

- Transparent to applications and infrastructure
- Minimal impact on performance
- Enforce security policies across the enterprise
- Support multiple data stores and operating systems
- Cost effective to deploy and maintain

Different Threats to Database and File System



Database Threats

- ✓Hackers
- ✓Employees,
- ✓Contractors
- ✓Customers
- ✓Suppliers
- ✓Partners
- ✓Outsourcers
- ✓Trojan Horses
- ✓Application errors

File System Threats

- ✓Physical Theft – file / backup
- ✓Root/Admin

Data Security Requirements

- The requirements are divided between critical requirements, “must-haves” for a solution to effectively secure the data, and practical requirements, factors that make it feasible for an enterprise to deploy a solution. The three different approaches reviewed are:
  - Application-Layer
  - Database-Layer
  - Storage-Layer
- The database-layer approach proves to be the most comprehensive and versatile in meeting the broad needs of most heterogeneous environments found in today’s large complex organizations.

Conclusion - Data Security Requirements

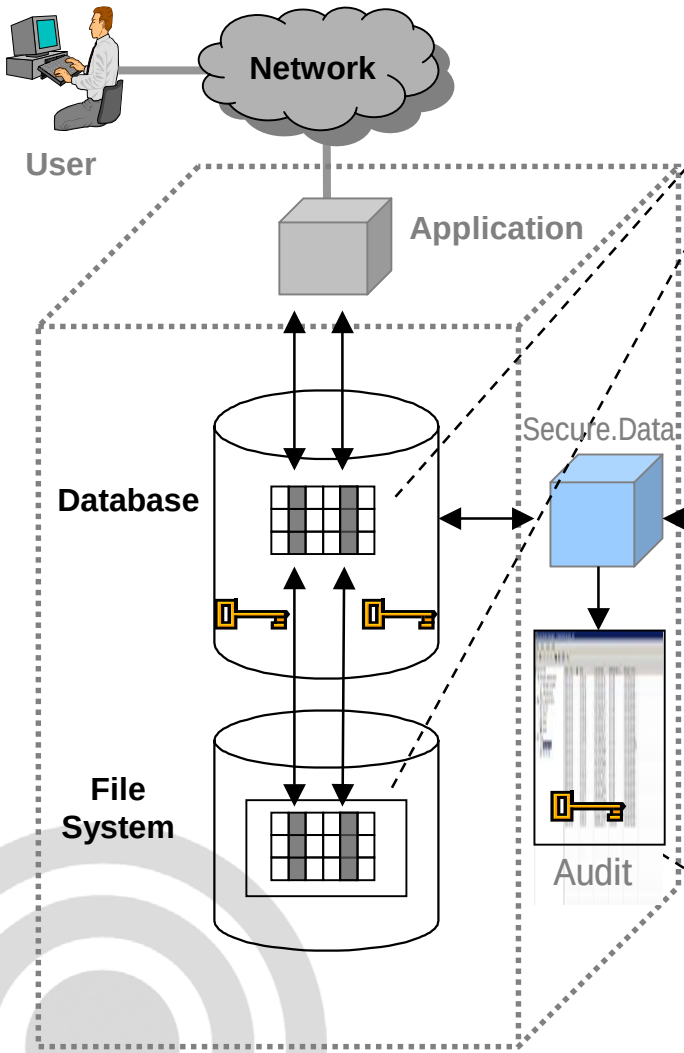
- *Application-layer encryption*:
  - Requires rewrite of existing applications
  - Rewriting applications is also very risky and introduces an implementation time delay factor.
  - All applications that access the encrypted data must also be changed to support the encryption/decryption model.

- *Storage-layer encryption* alone can only protect against a narrow range of threats:
  - Media theft and
  - Storage system attacks.

- *Database-layer encryption* protects the data within the DBMS and also protects against a wide range of threats, including:
  - Storage media theft,
  - Storage attacks,
  - Database-layer attacks, and
  - Malicious DBAs.

Deployment at the column level within a database table, coupled with access controls will prevent theft of critical data.

Protegrity Secure.Data – Functionality



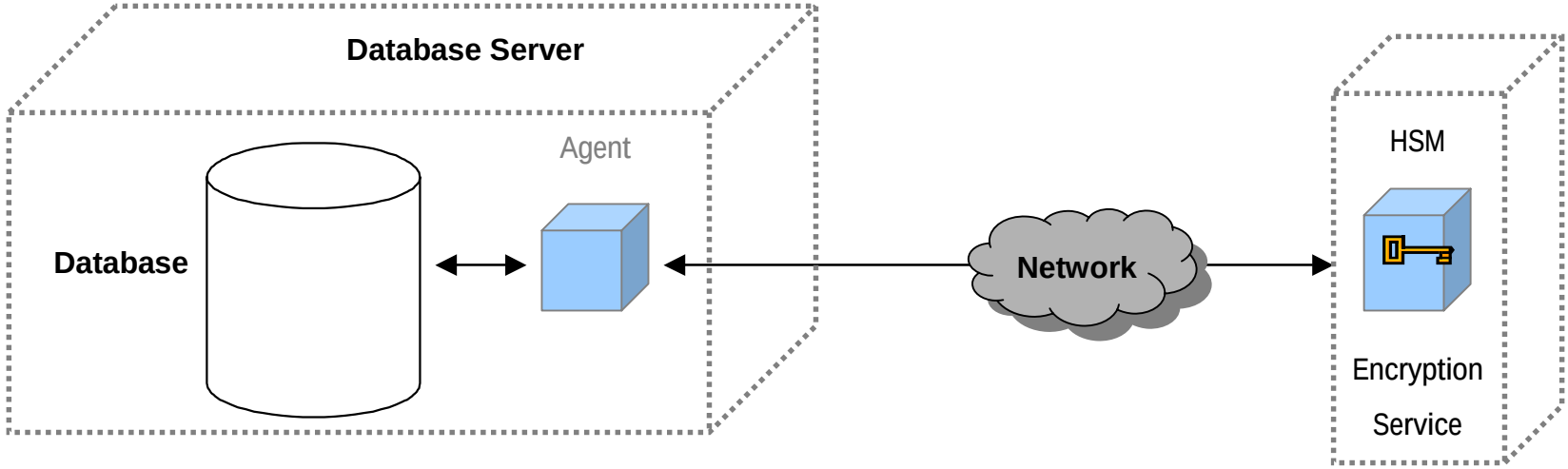
- Secure.Data encrypts data in data stores and file system
- Secure.Manager provides enterprise policy control
  - Control down to the role or user level across applications
  - Control what field the user is accessing and decrypting
- Strong key management system
  - Protect encryption keys from attacks
  - Assign a unique key and key management policy to different fields
- Secure audit information at field/user level
  - Who, what, when, where
  - Fully secure and selective audit trail

Support Multiple Data Stores and Operating Systems

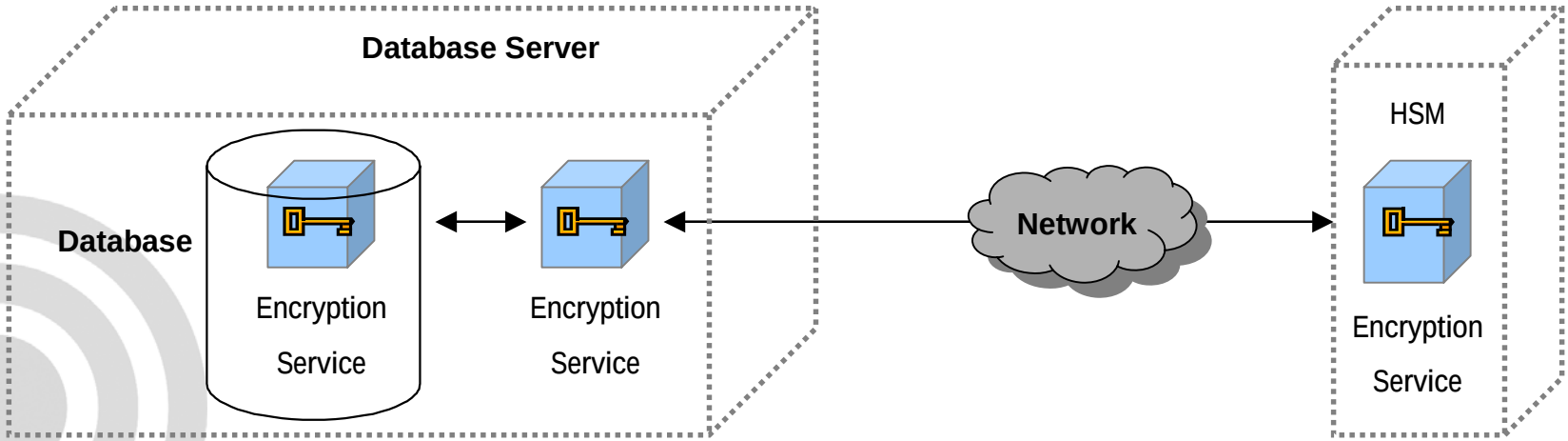
Data Stores	Operating Systems	Status
Oracle 8i and 9i	**AIX 5L, HP-UX 11, Solaris 2.x**	Available
SQL Server 2000	**Windows**	Available
DB2 7	**OS/390 3.x, z/OS 1.x**	Available
DB2 8	**AIX 5L, Windows**	Available
Informix 9	**Solaris 2.x**	Available
Sybase 12	**HP-UX 11, Solaris 2.x Windows**	Available

Performance – Database Encryption

Network Attached Database Encryption (600 op/sec**)

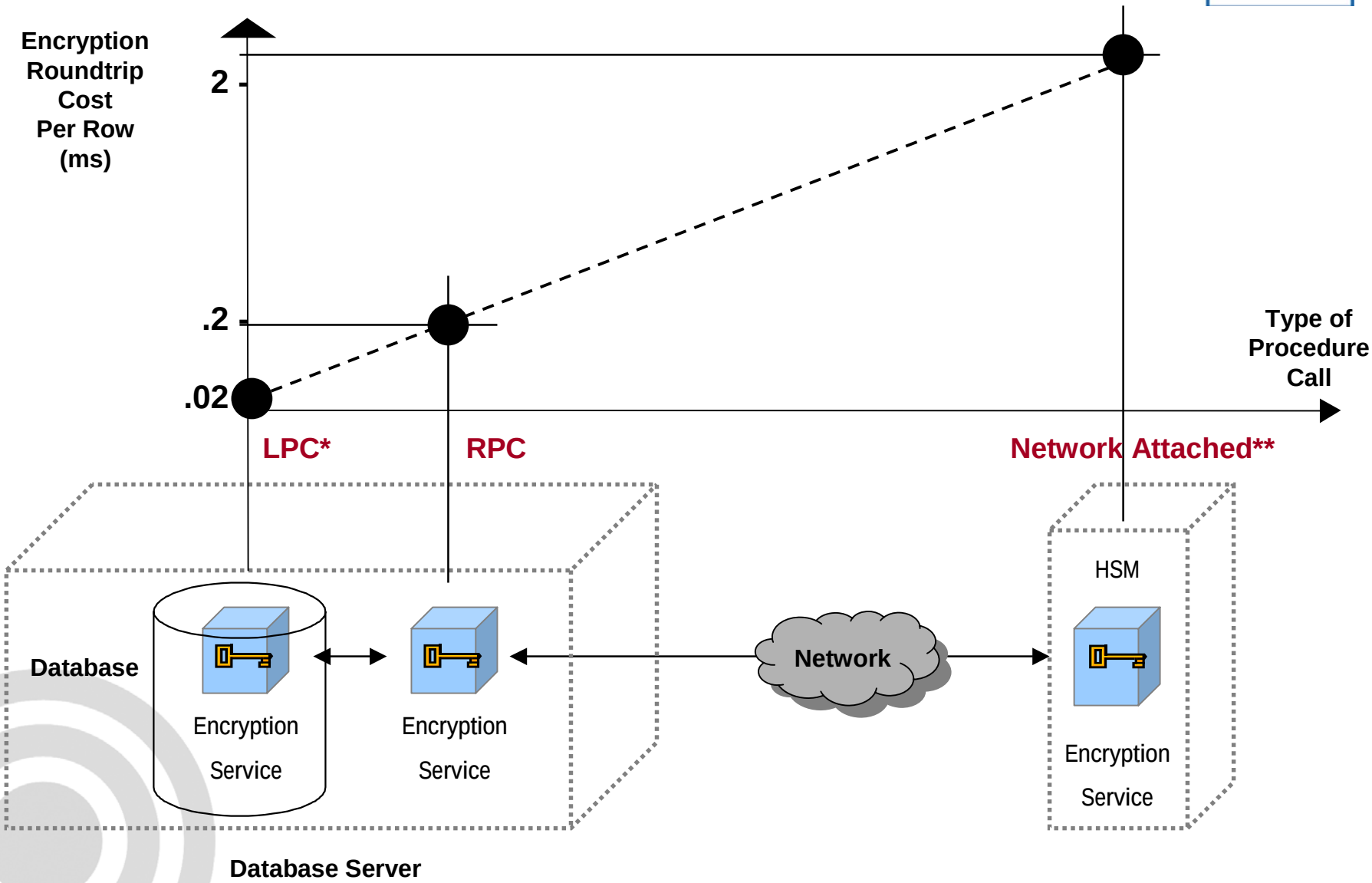


Protegrity Integrated Database Encryption (180,000 op/sec*)



*: Source - IBM Waltham, Protegrity Secure.Data Benchmark on UNIX.
**: Based on Publicly available information and Protegrity Benchmarks

Typical Cost of Database Crypto Operations



*: Source - IBM Waltham, Protegrity Secure.Data Benchmark on UNIX
**: Based on Publicly available information and Protegrity Benchmarks

Data Type Preservation

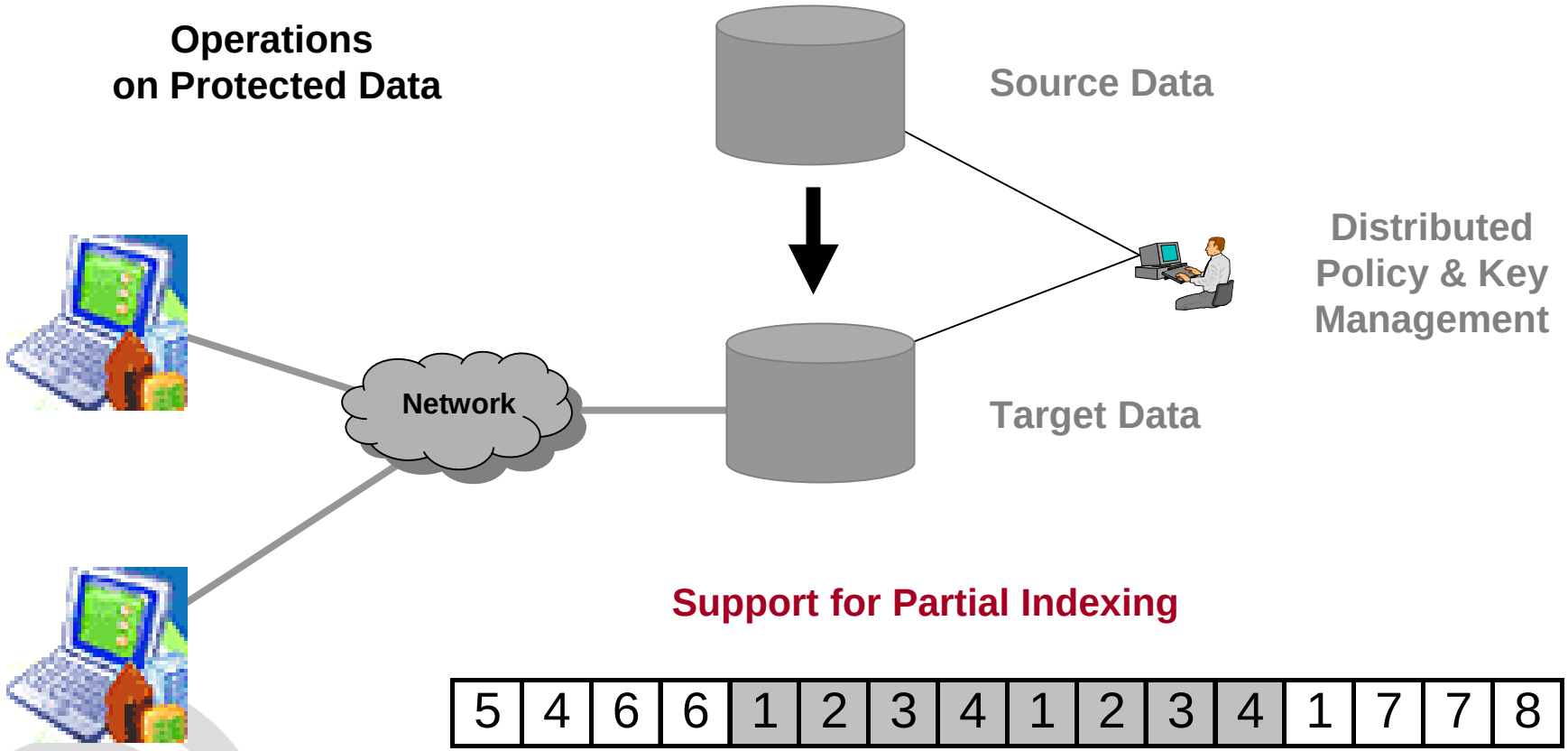
Critical Security Requirements for Data Type Preservation

- Encrypt and decrypt data in existing environments
- No changes to the length of fields or type of data
- No changes required to IT infrastructure or applications
- Supports all databases and file systems
- NIST certified encryption algorithms

DTP Benefits – Customer Case Study

- No impact on IT Infrastructure and Applications
- Scaleable to Terra-bytes of data
- Support for OS/390, UNIX, and Windows
- No Additional Hardware Investment
- Distributed Key-management
- Easy Fail-over (vs. VPN)

Search on Protected Fields

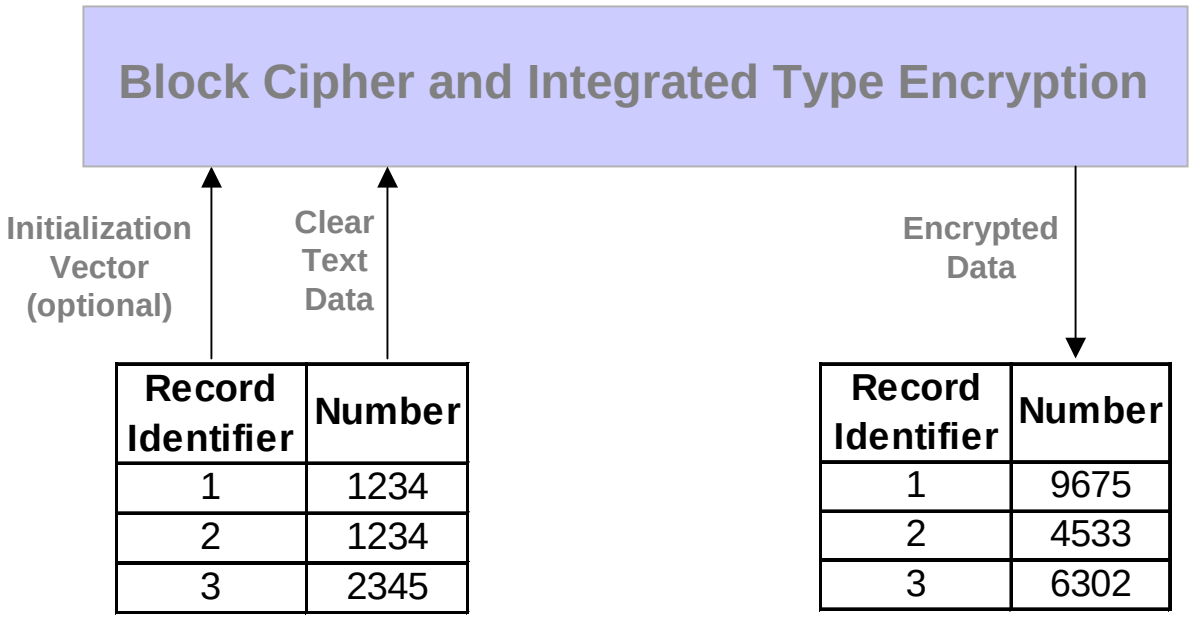


Support for Partial Indexing

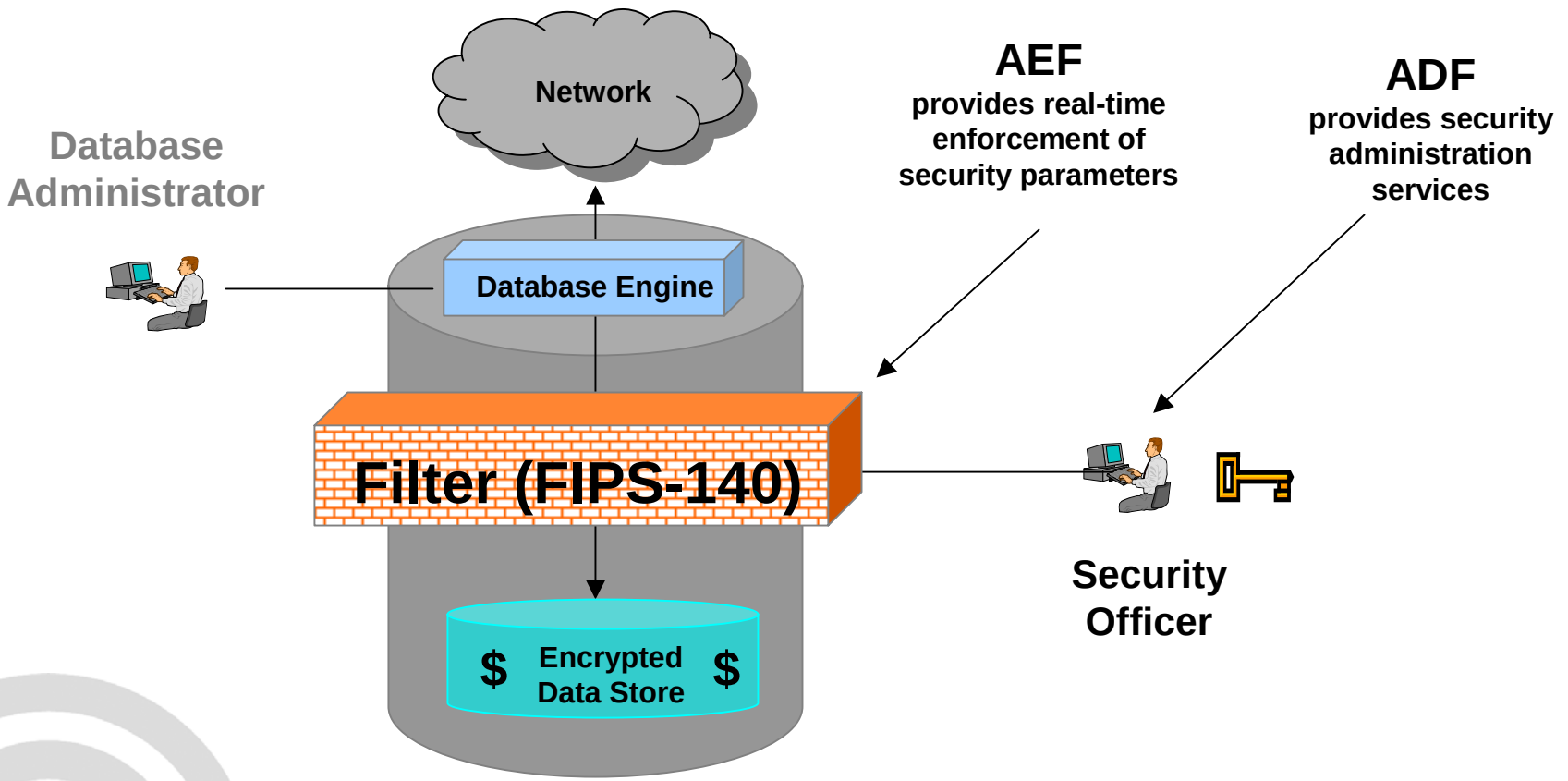
5	4	6	6	1	2	3	4	1	2	3	4	1	7	7	8

Clear Text | Cipher Text | Clear Text

DTP – Optional use of Unique Initialization Vector



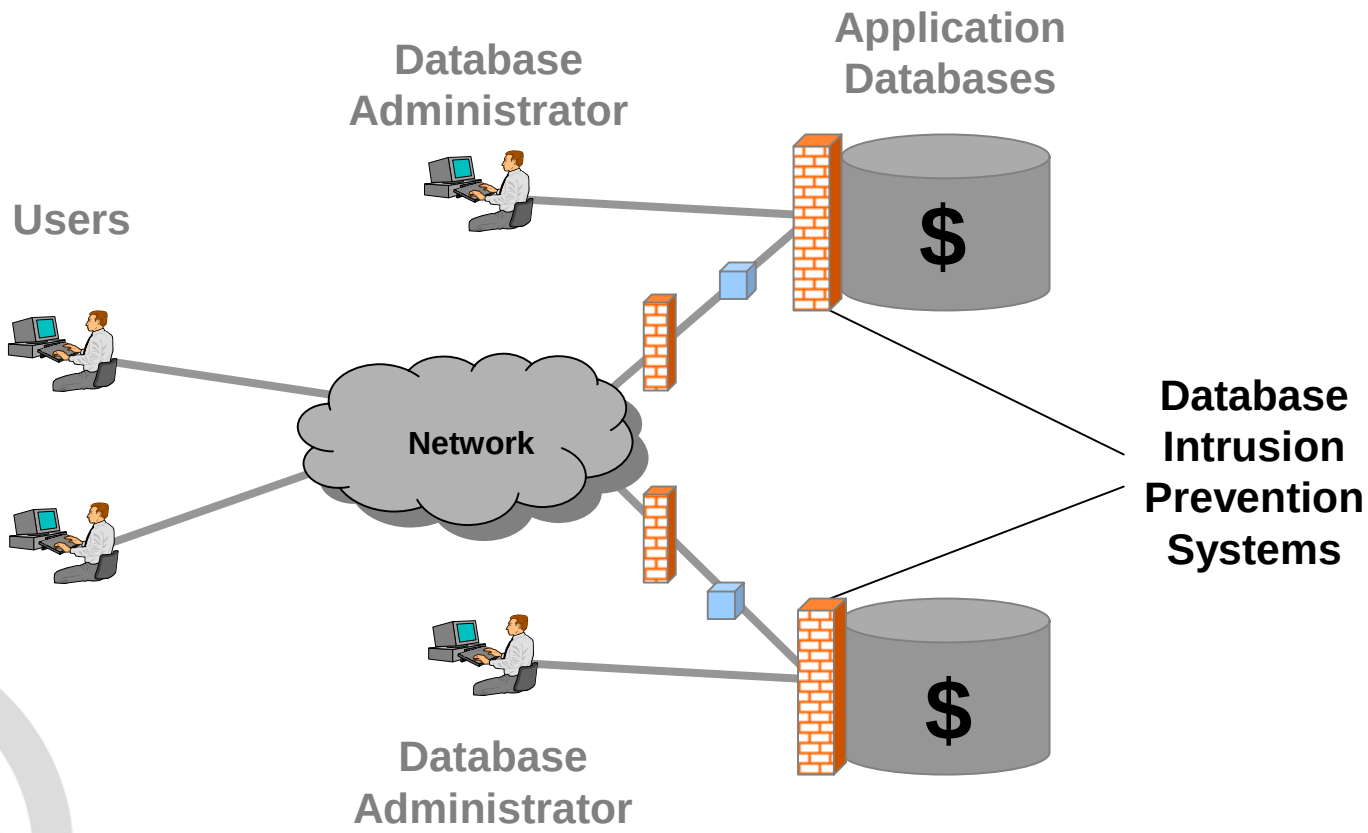
Security Management Standard - ISO/IEC 10181-31



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 (Customer USA) – Dual Control

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