

**Ulf Mattsson**



**SQL Intrusion Prevention**

# Encrypting for Database Security

Intrusion Prevention for Databases



**Ulf Mattsson**

*Chief Technology Officer*

Protegrity,

[ulf.mattsson@protegrity.se](mailto:ulf.mattsson@protegrity.se)

[www.protegrity.com](http://www.protegrity.com)

# Agenda

---

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

## Project 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**

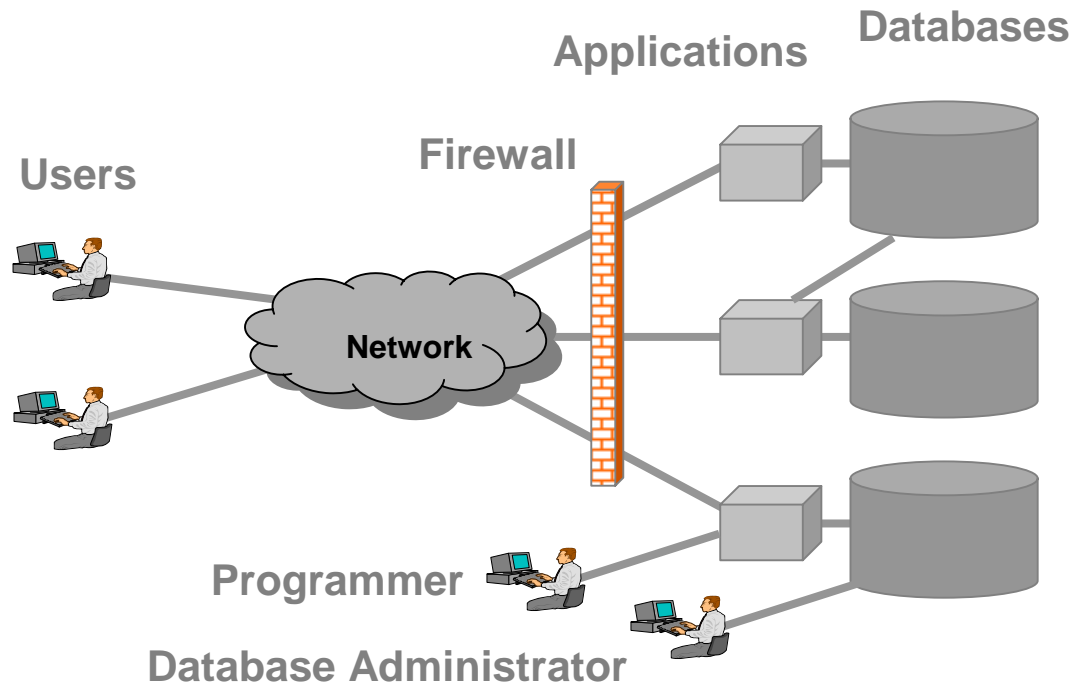
**Administrator  
Access  
Control & Audit**

**Response when  
unauthorized  
access is  
suspected or  
detected**

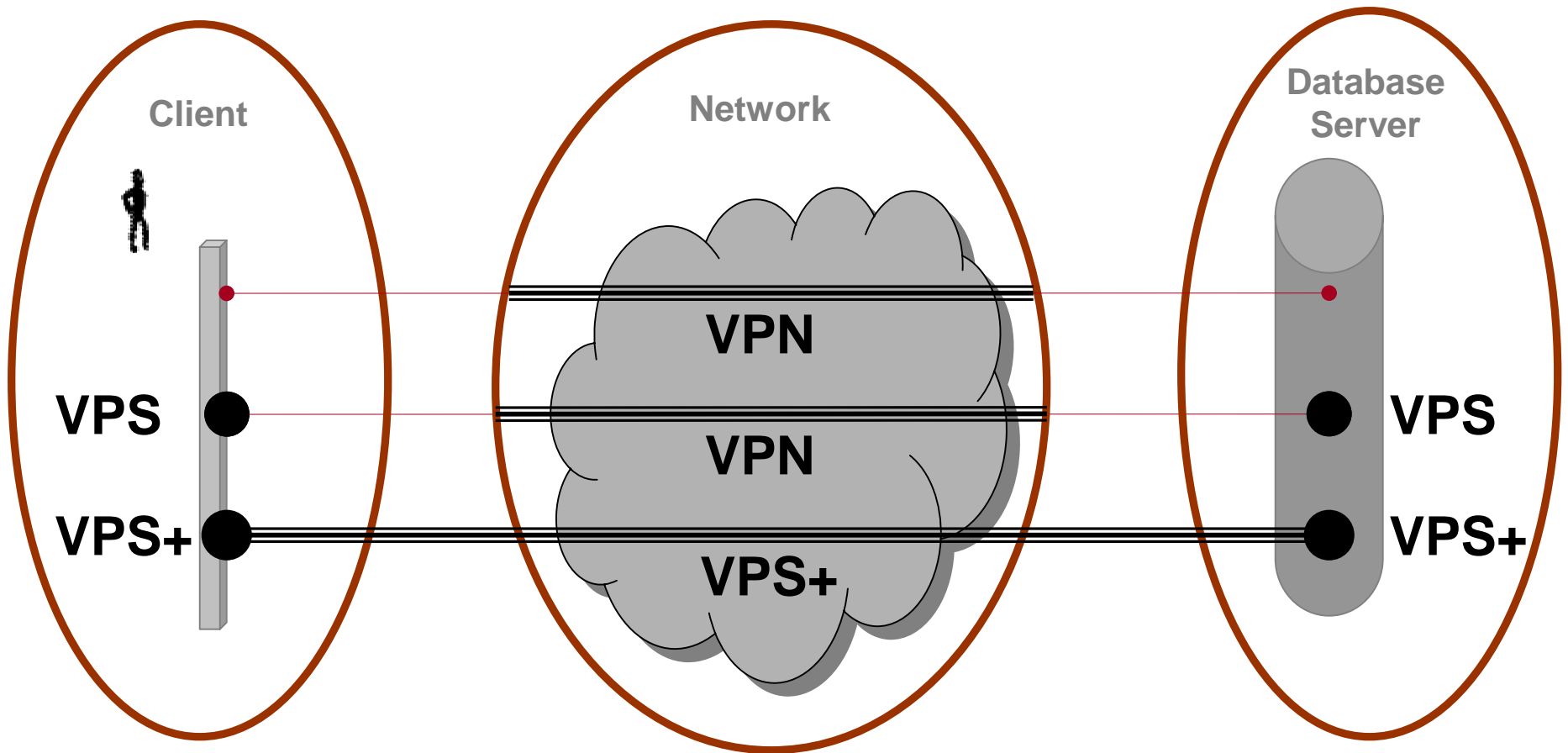
**Data  
Confidentiality**

# The 1994 Mission – The Target Environment

---



# Case Studies: End to End Security



Data Transported Encrypted:



Data Stored Encrypted:



Data Transported in Clear:



Data Stored in Clear:



VPS+ : Virtual Private Storage

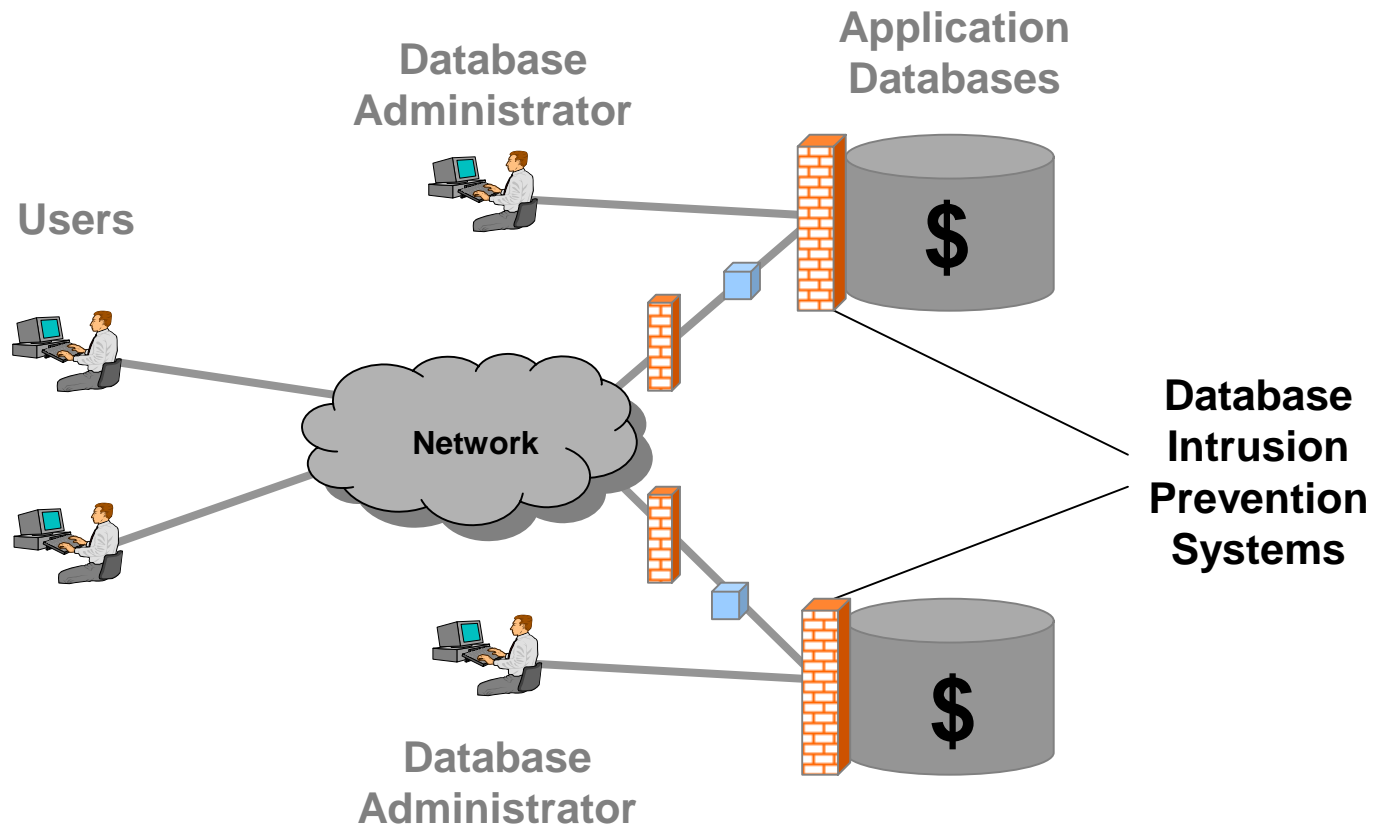


Safeguarding Enterprise Databases



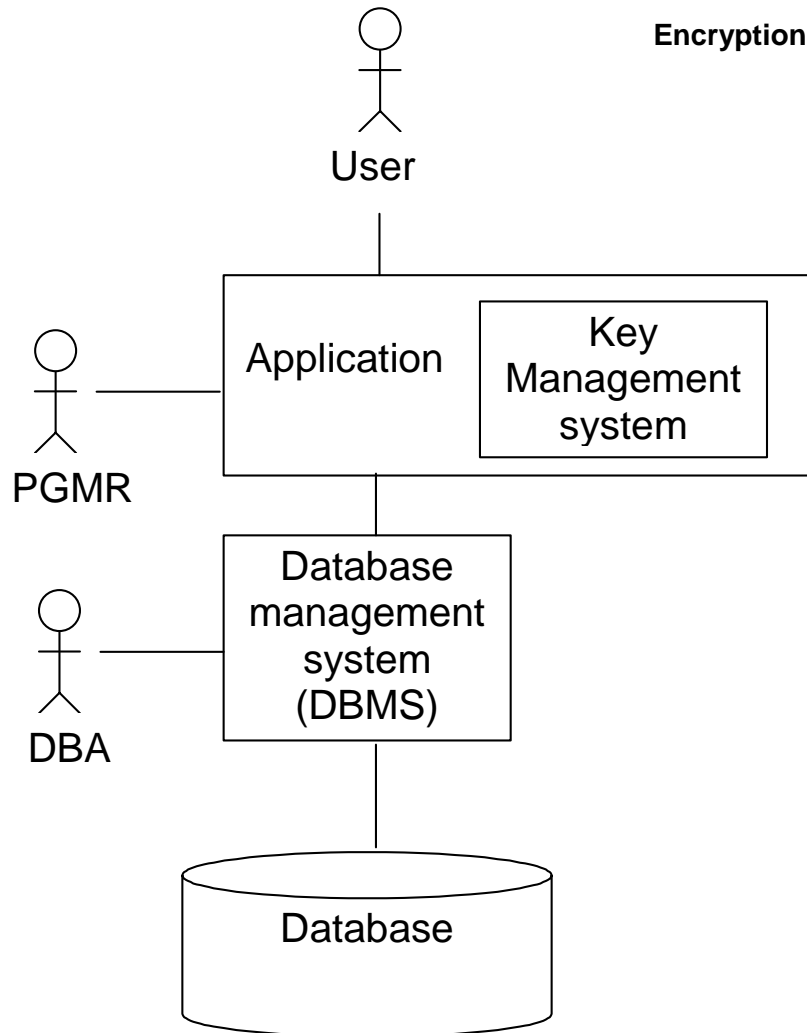
# The Database Intrusion Prevention System

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



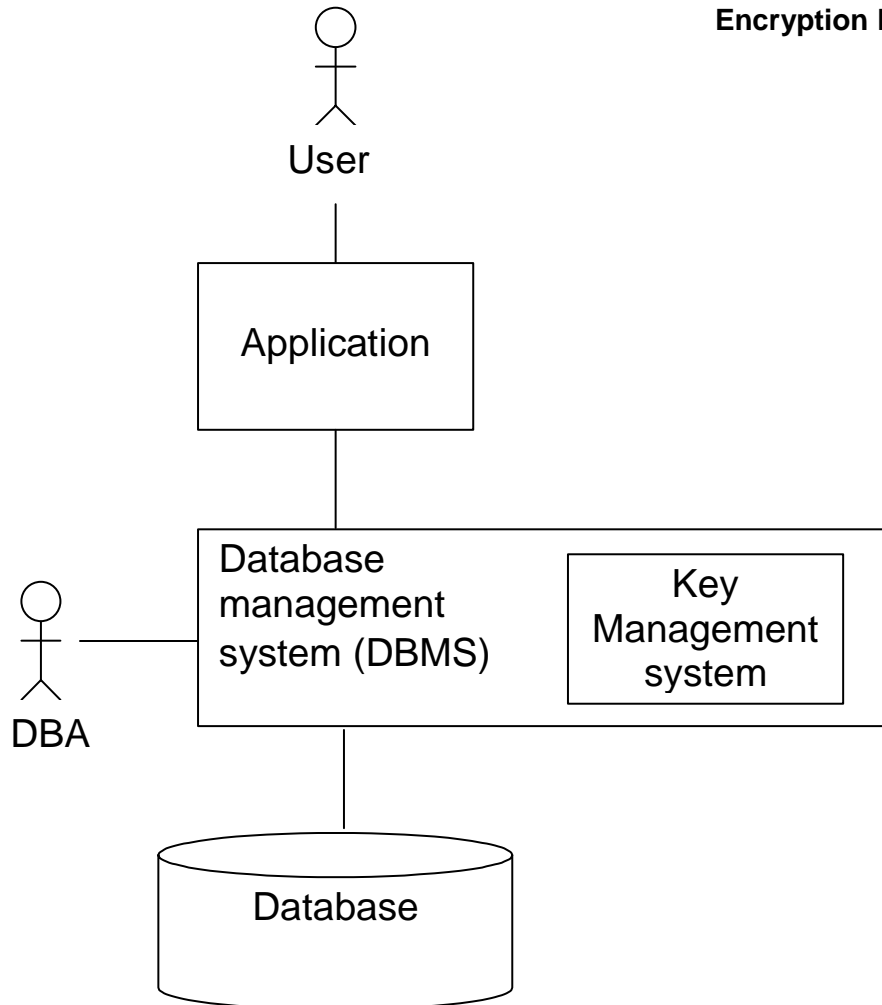
# Case Studies - 4 Server Solution Alternatives

Encryption Keys exposed in the application environment.

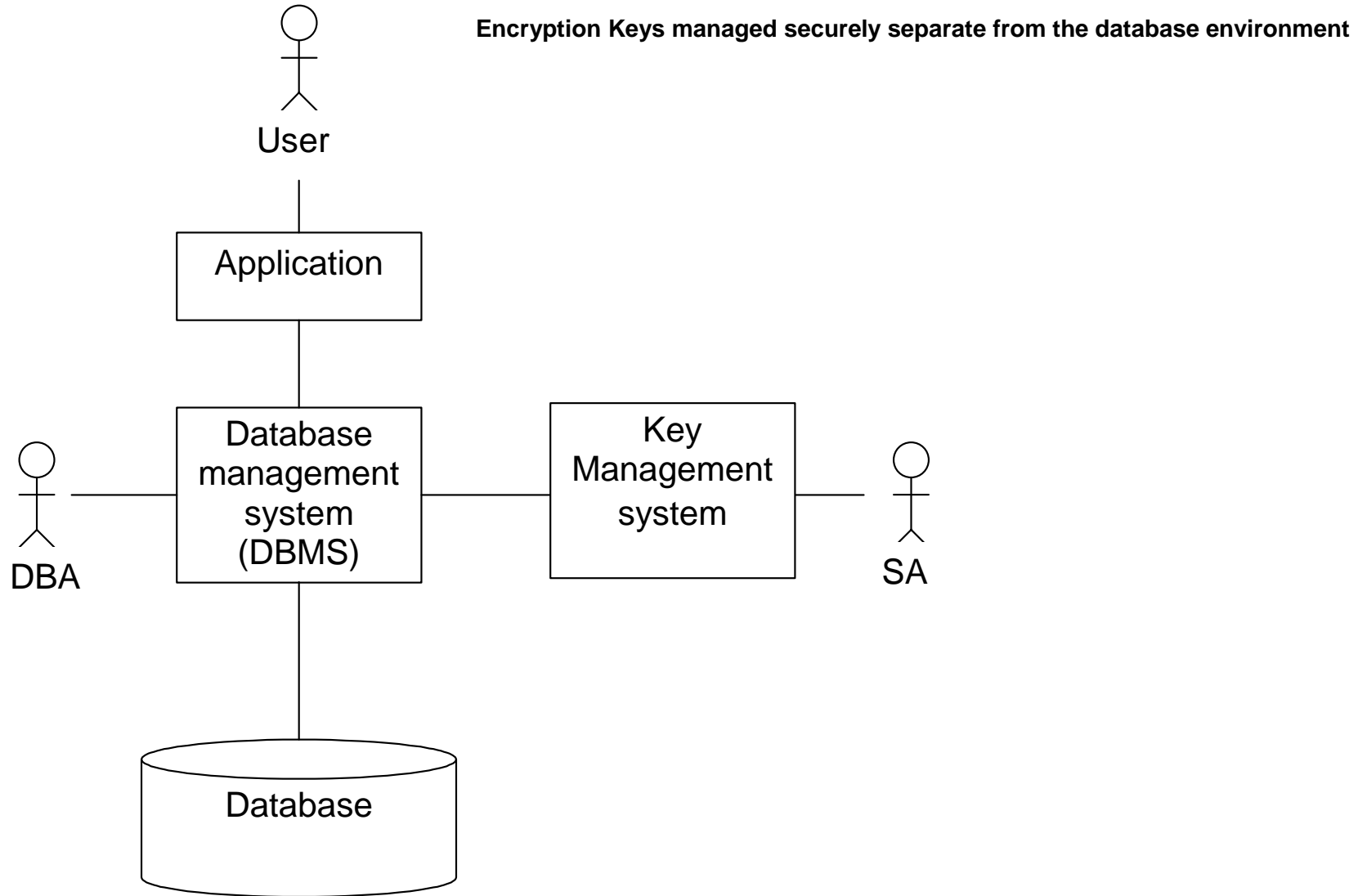


# Case Studies - 4 Server Solution Alternatives

Encryption Keys exposed in the database environment.

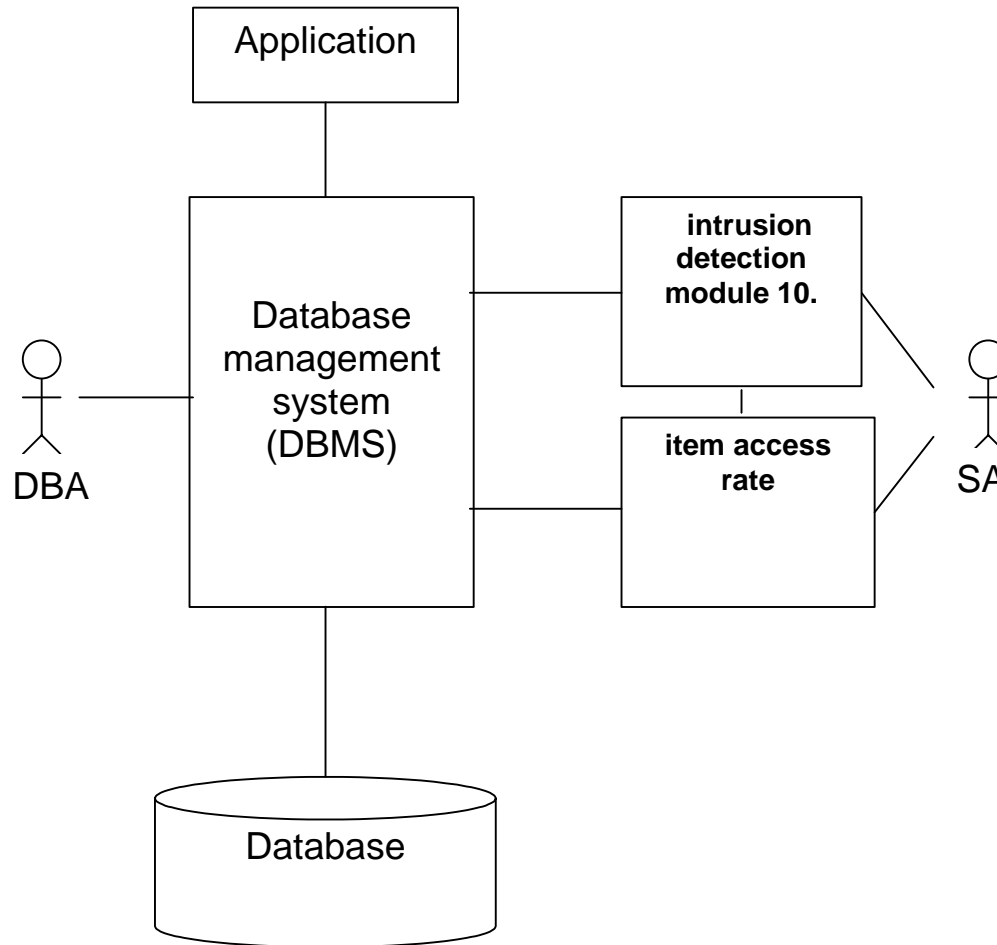


# Case Studies - 4 Server Solution Alternatives

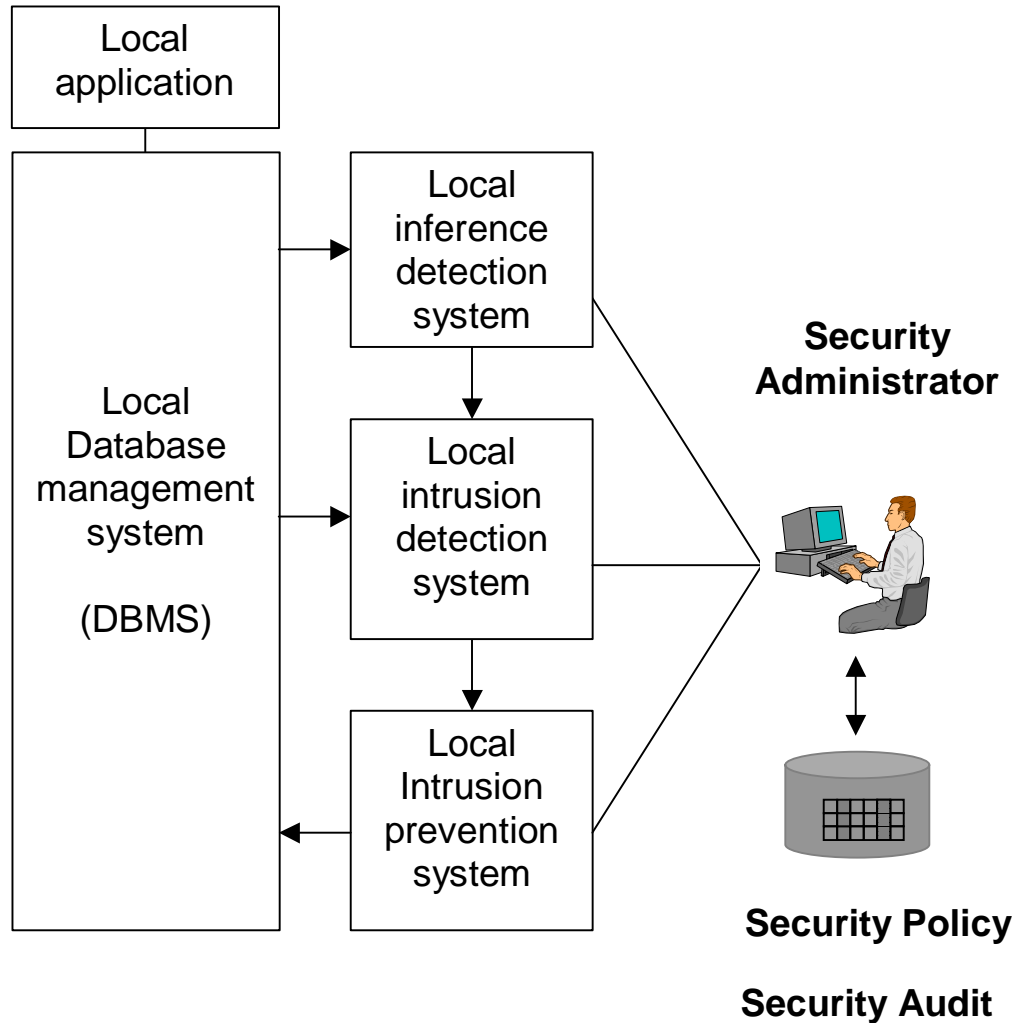


# Case Studies - Solution Alternatives

---



# Database Intrusion Prevention - Components



## Security Policy Enforcement:

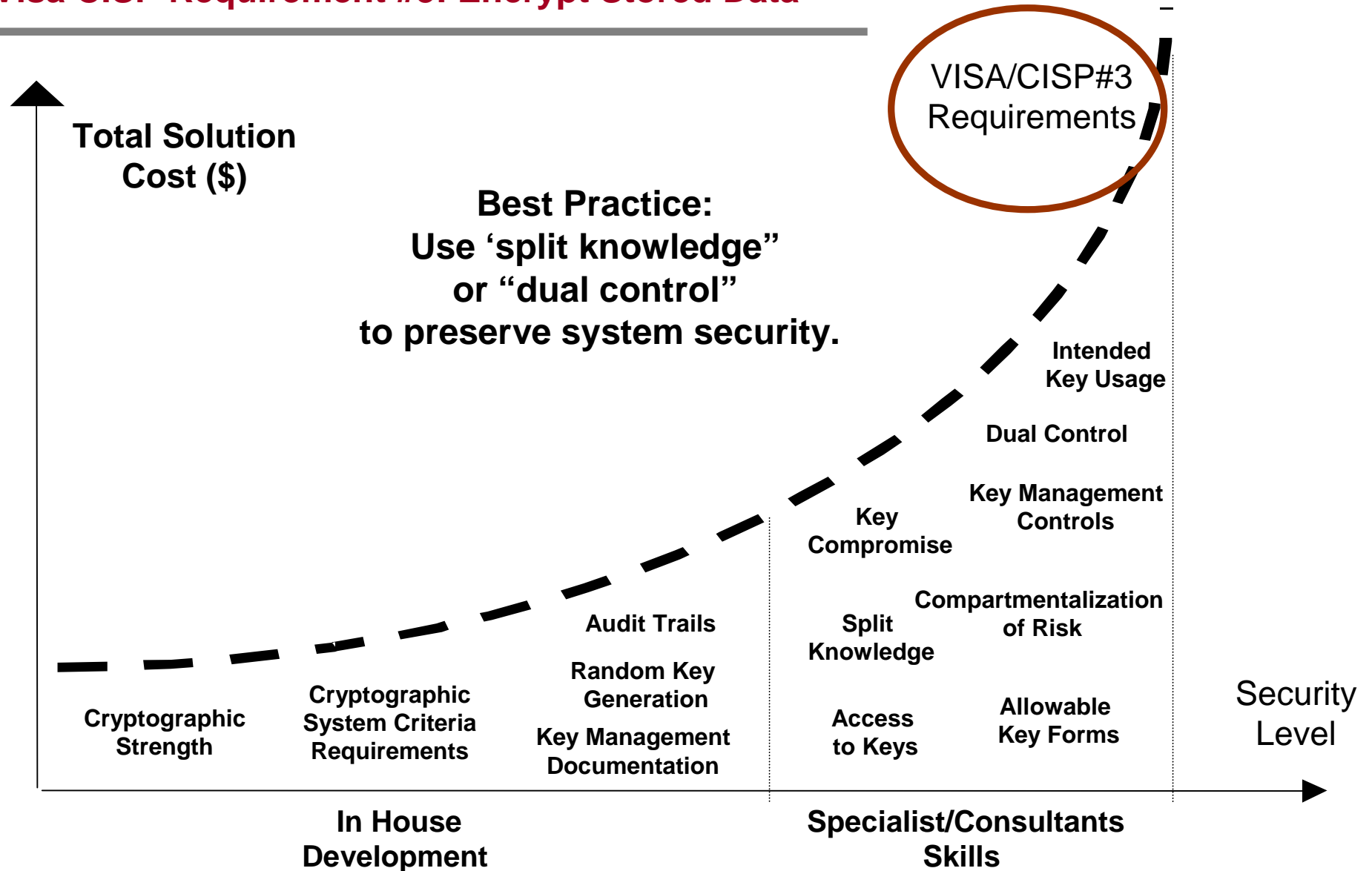
1. Session Authorization
2. Session Authentication
3. Session Encryption
4. Password Integrity
5. DB Software Integrity
6. Application Data Integrity
7. DB Meta Data Integrity
8. Security Software Integrity
9. Access Time of Day
10. IPS Signature Rules

# 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
Requirements 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.

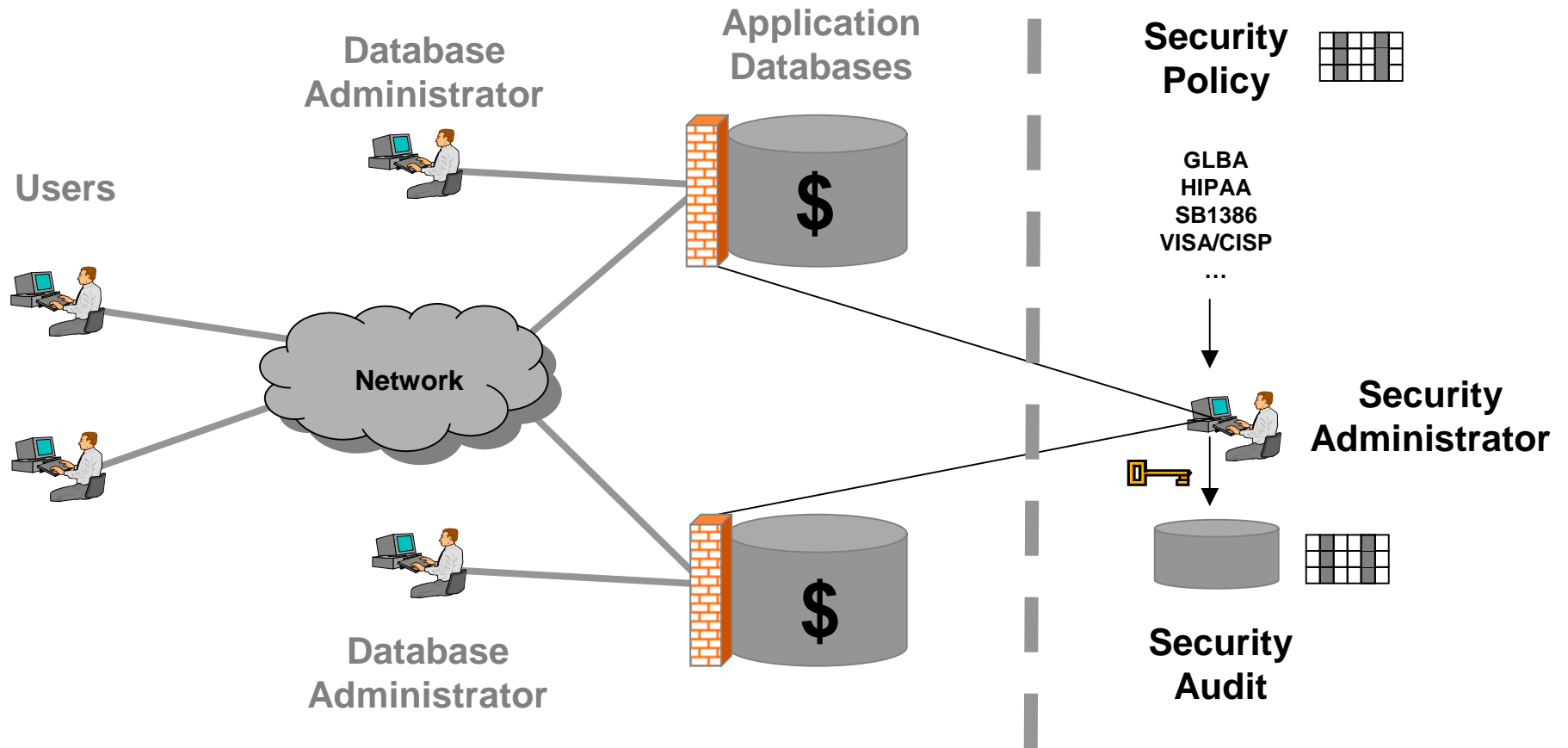
Legend	Recommended	Not Recommended	Only as a secondary alternative
--------	-------------	-----------------	---------------------------------

# Visa CISP Requirement #3: Encrypt Stored Data



# Best Practice (Visa USA) – Dual Control

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



## Case Studies - Solution Alternatives

---

*Network-Based Detection* - Network intrusion monitors are attached to a packet-filtering router or packet sniffer to detect suspicious behavior on a network as they occur. They look for signs that a network is being investigated for attack with a port scanner, that users are falling victim to known traps like .url or .lnk, or that the network is actually under an attack such as through SYN flooding or unauthorized attempts to gain root access (among other types of attacks). Based on user specifications, these monitors can then record the session and alert the administrator or, in some cases, reset the connection. Some examples of such tools include Cisco's NetRanger and ISS' RealSecure as well as some public domain products like Klaxon that focus on a narrower set of attacks.

*Server-Based Detection* - These tools analyze log, configuration and data files from individual servers as attacks occur, typically by placing some type of agent on the server and having the agent report to a central console. Some examples of these tools include Axent's OmniGuard Intrusion Detection (ITA), Security Dynamic's Kane Security Monitor and Centrax's eNTrax as well as some public domain tools that perform a much narrower set of functions like Tripwire which checks data integrity. Tripwire will detect any modifications made to operating systems or user files and send alerts to ISS' RealSecure product. Real-Secure will then conduct another set of security checks to monitor and combat any intrusions.

## Case Studies - Solution Alternatives

---

*Security Query and Reporting Tools* - These tools query NOS logs and other related logs for security events or they glean logs for security trend data. Accordingly, they do not operate in real-time and rely on users asking the right questions of the right systems. A typical query might be "how many failed authentication attempts have we had on these NT servers in the past two weeks." A few of them (e.g., SecurIT) perform firewall log analysis. Some examples of such tools include Bindview's EMS/NOSadmin and Enterprise Console, SecureIT's SecureVIEW and Security Dynamic's Kane Security Analyst.

*Inference detection* - A variation of conventional intrusion detection is detection of specific patterns of information access, deemed to signify that an intrusion is taking place, even though the user is authorized to access the information. A method for such inference detection, i.e. a pattern oriented intrusion detection, is disclosed in US patent 5278901 to Shieh et al. None of these solutions are however entirely satisfactory. The primary drawback is that they all concentrate on already effected queries, providing at best an information that an attack has occurred.

# 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**

# 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

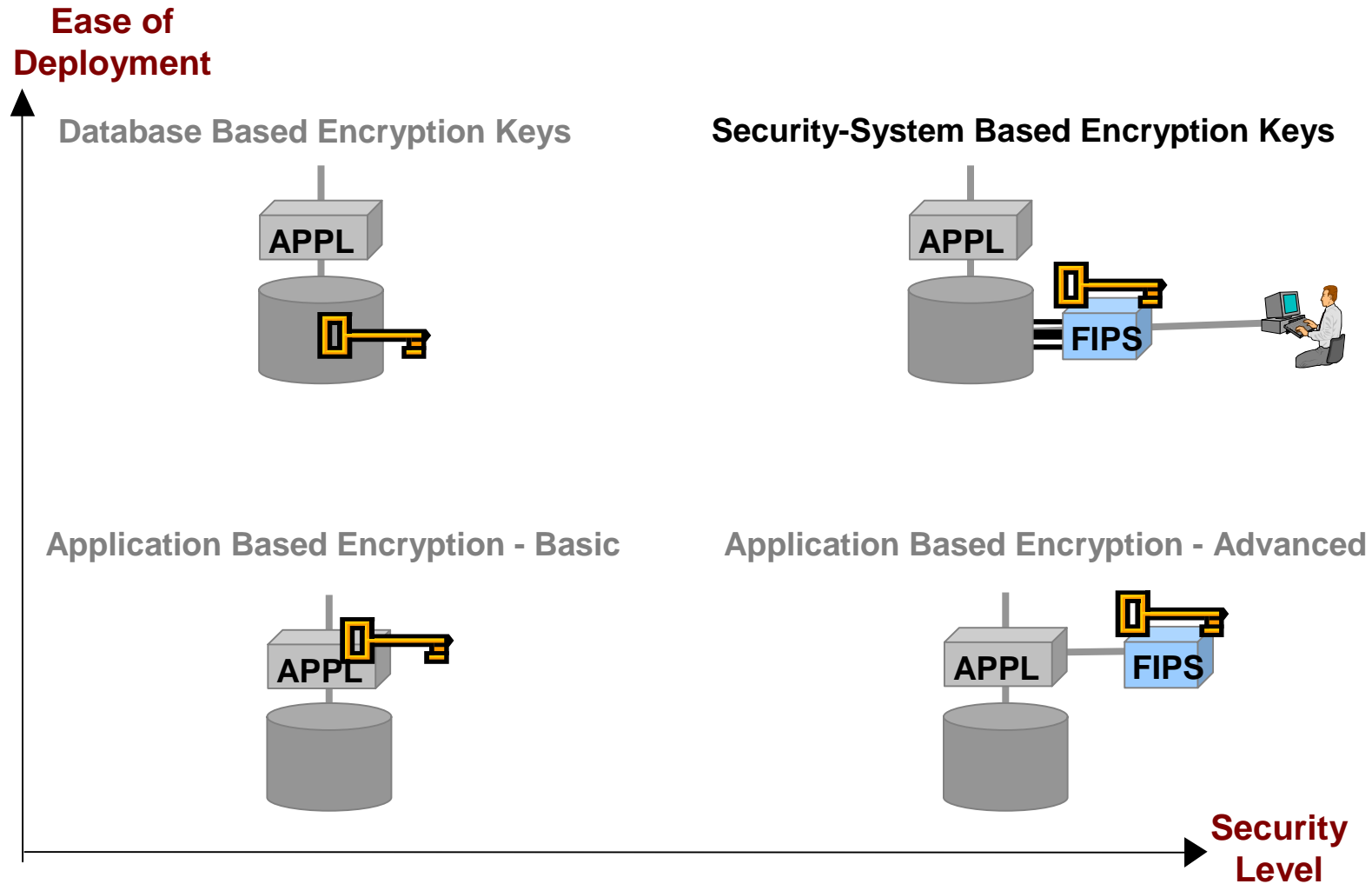
***Best Practice: Use ‘split knowledge’ or ‘dual control’ to preserve system security.***

## Liability Issues executives need to consider

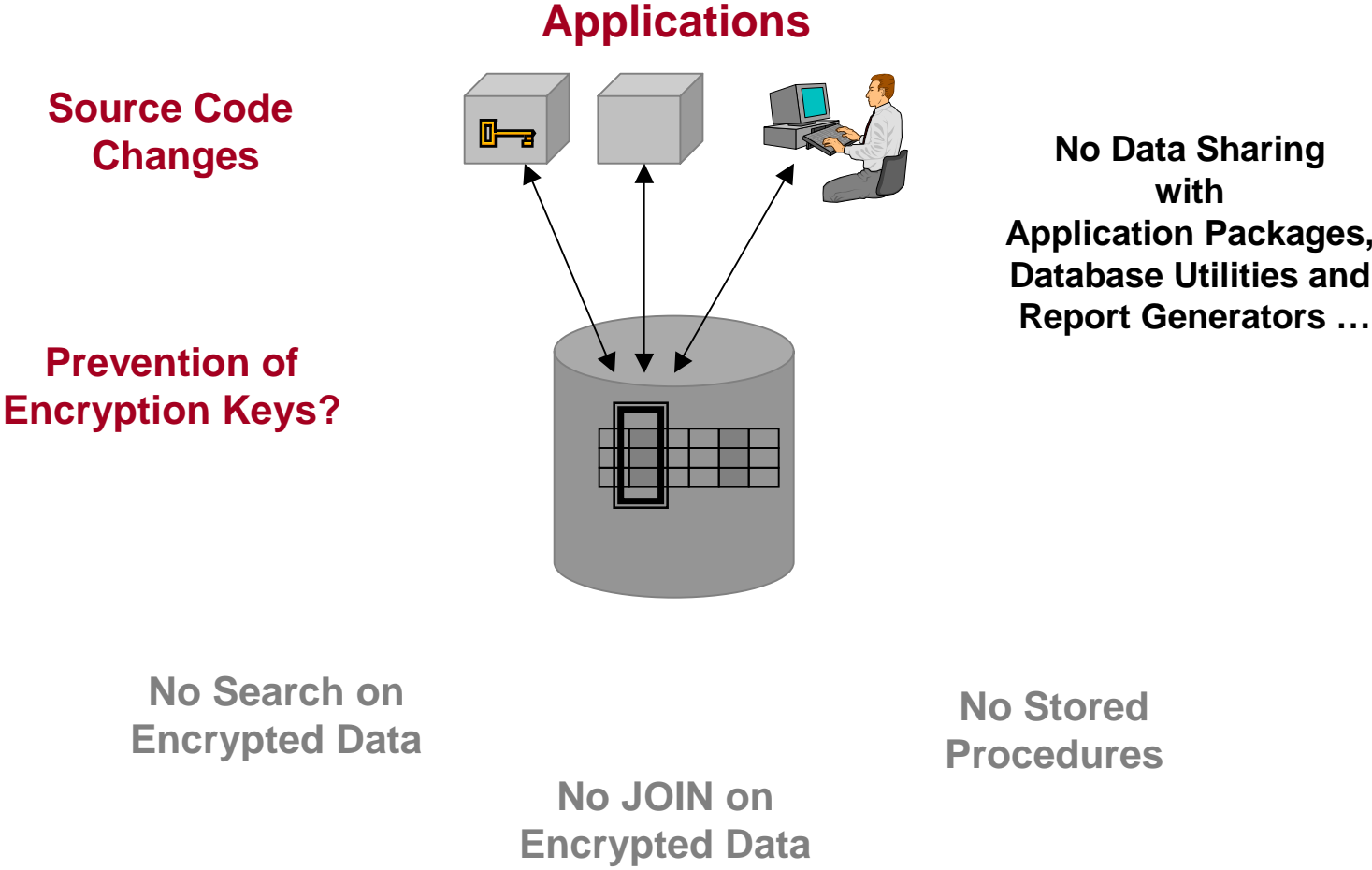
---

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

# Case Studies - 4 Server Solution Alternatives



# Case Study: Application Encryption – Advanced



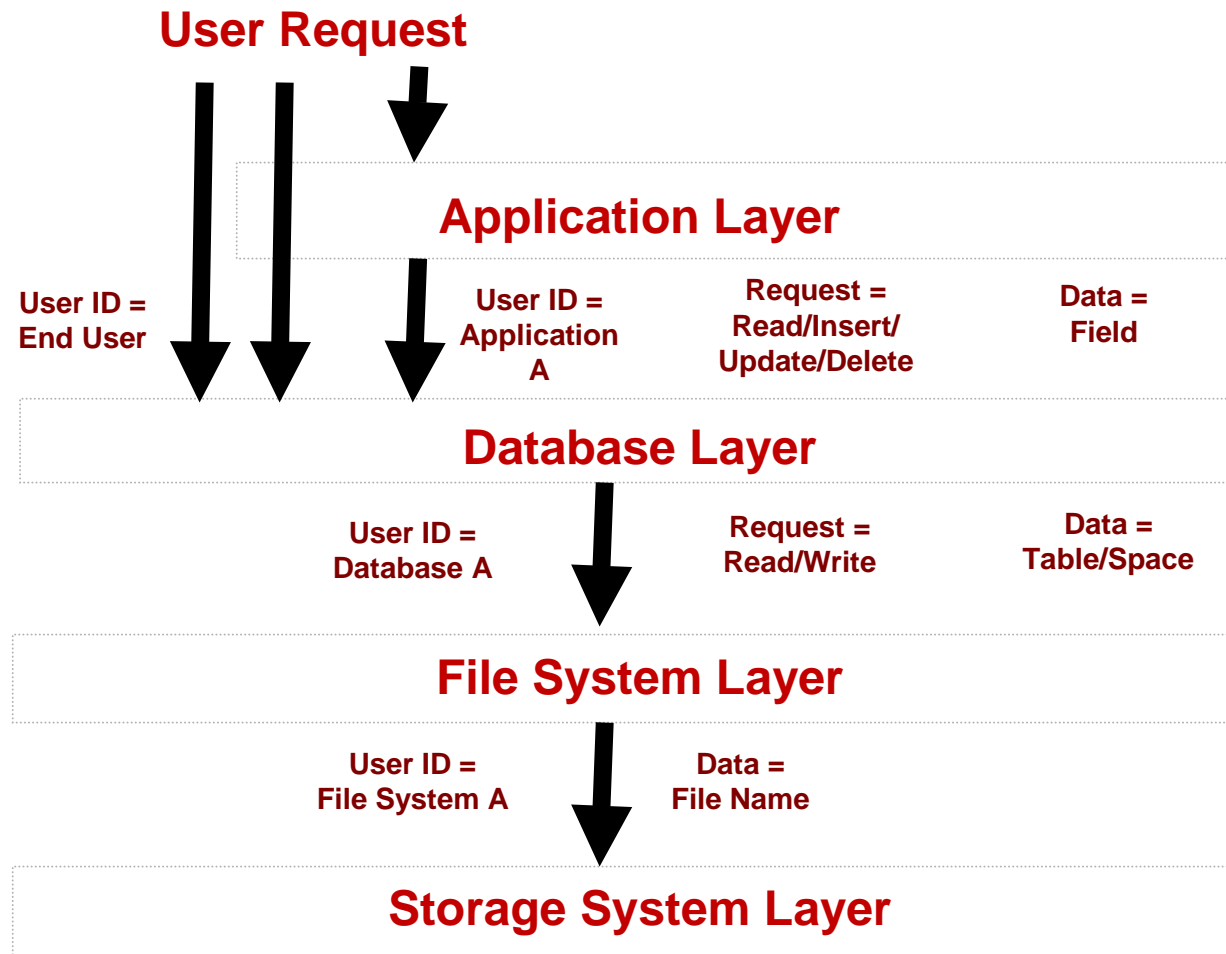
**Applications stop working ...**



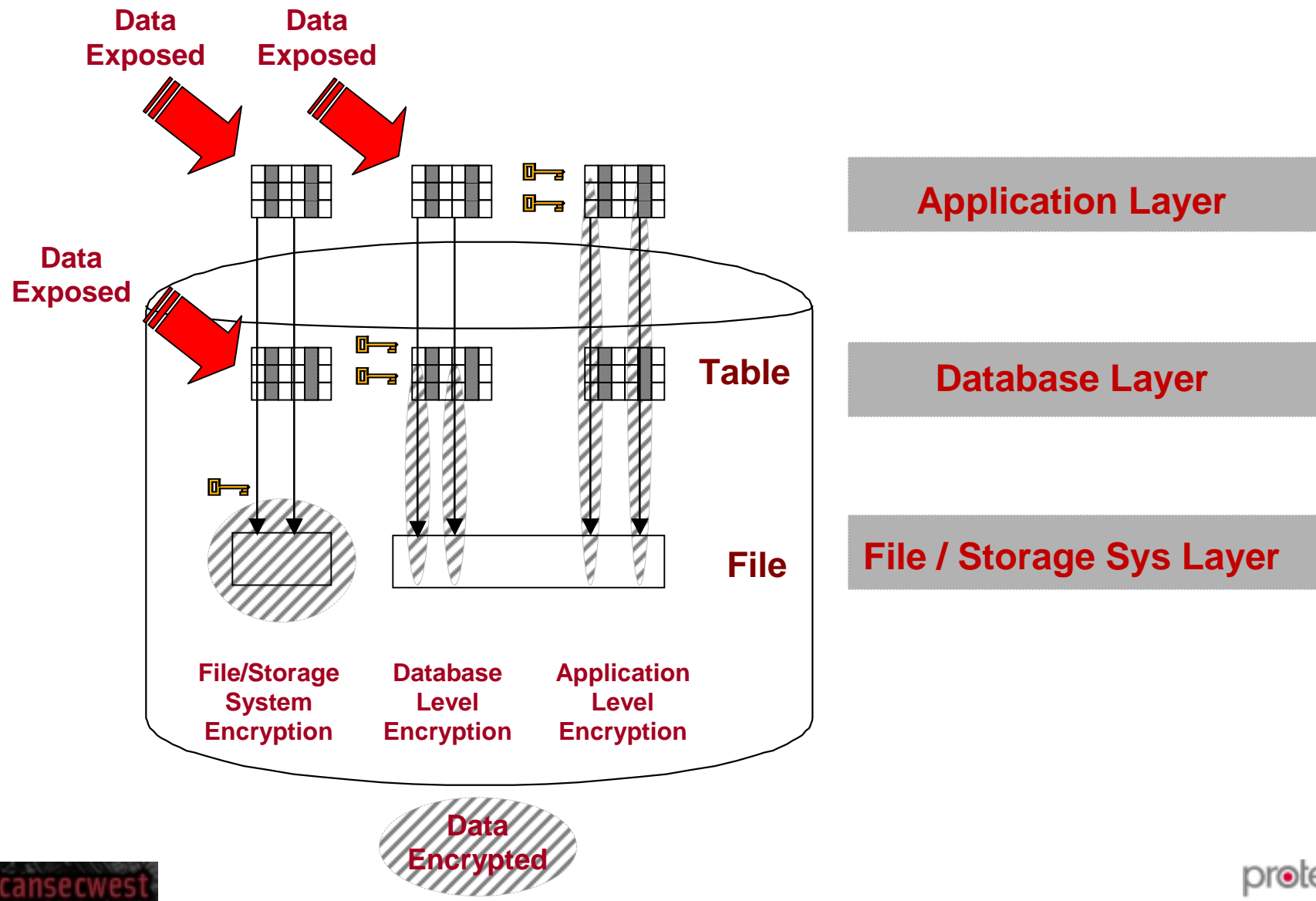
Safeguarding Enterprise Databases



## Solution Layers – Information Request Granularity

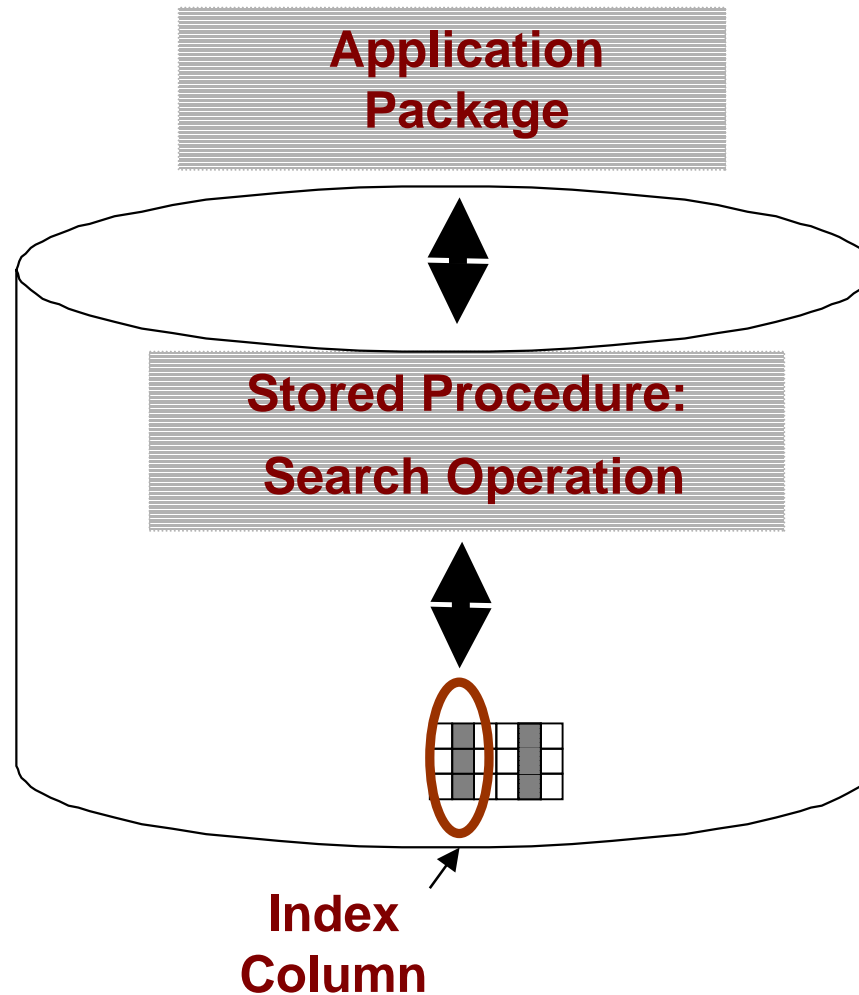


# Data Exposed with Alternative Solutions

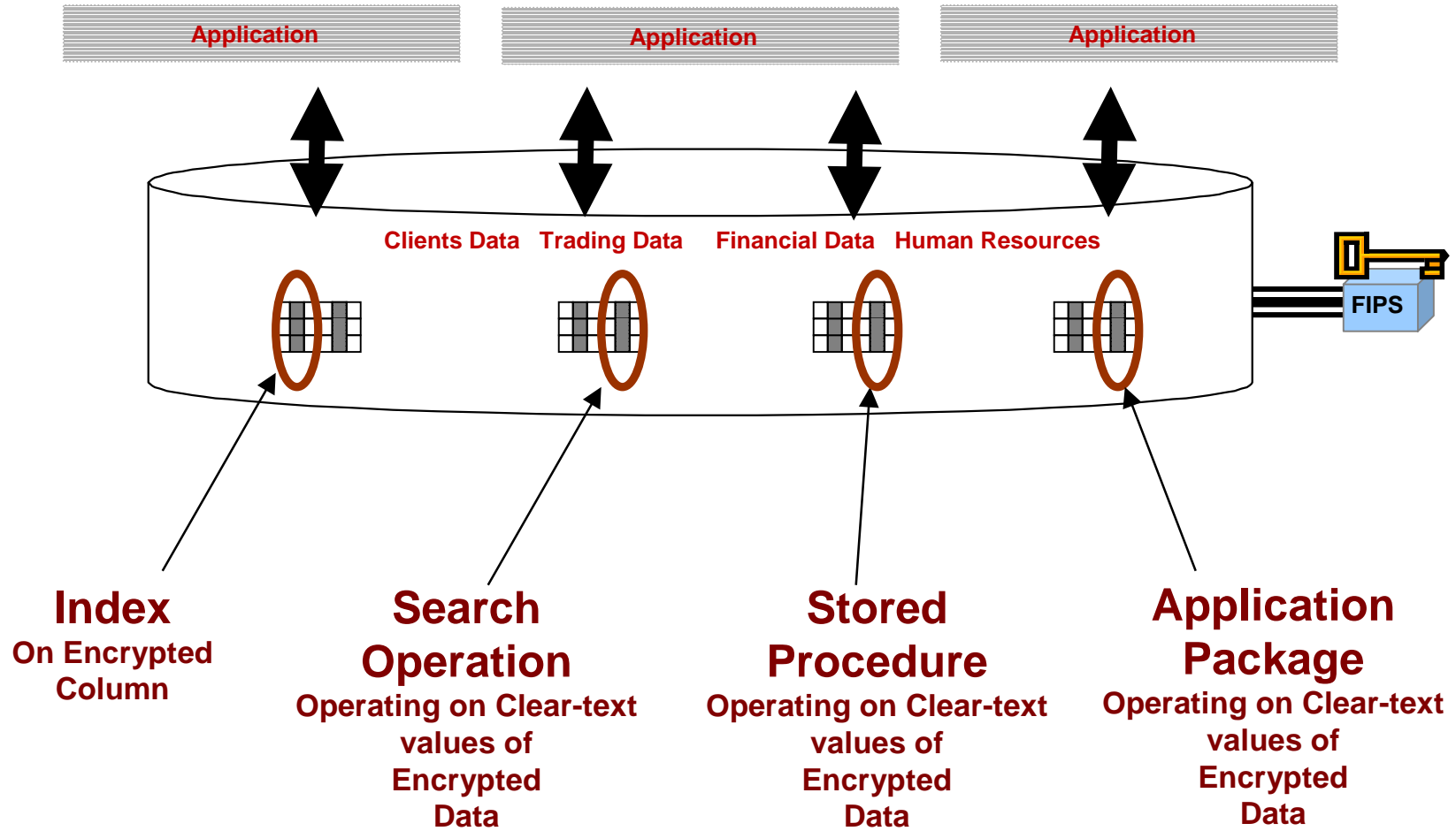


## Case Study – Issues with Application Level Encryption

---

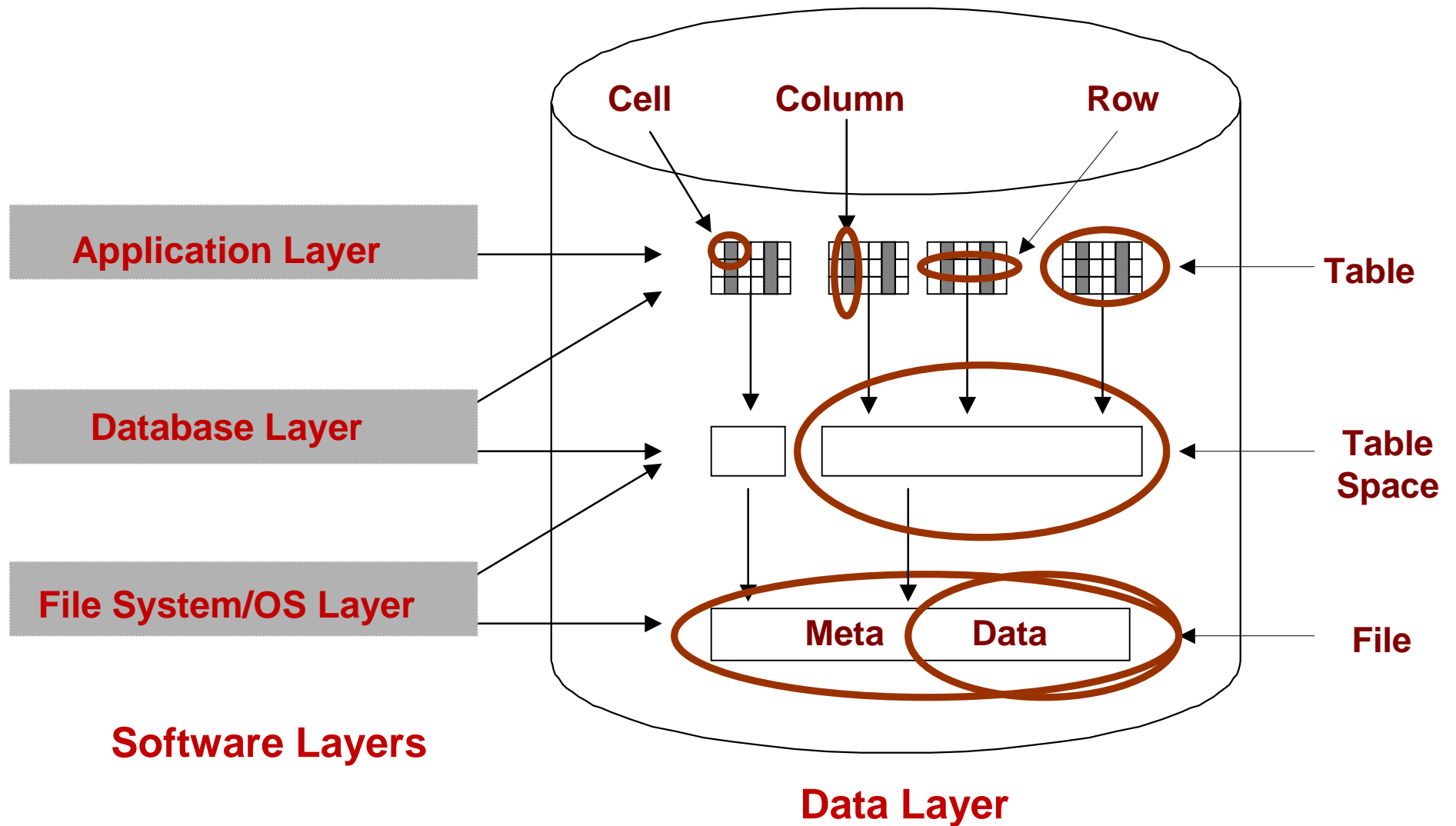


# Case Study - Why Database Level Encryption is Needed:



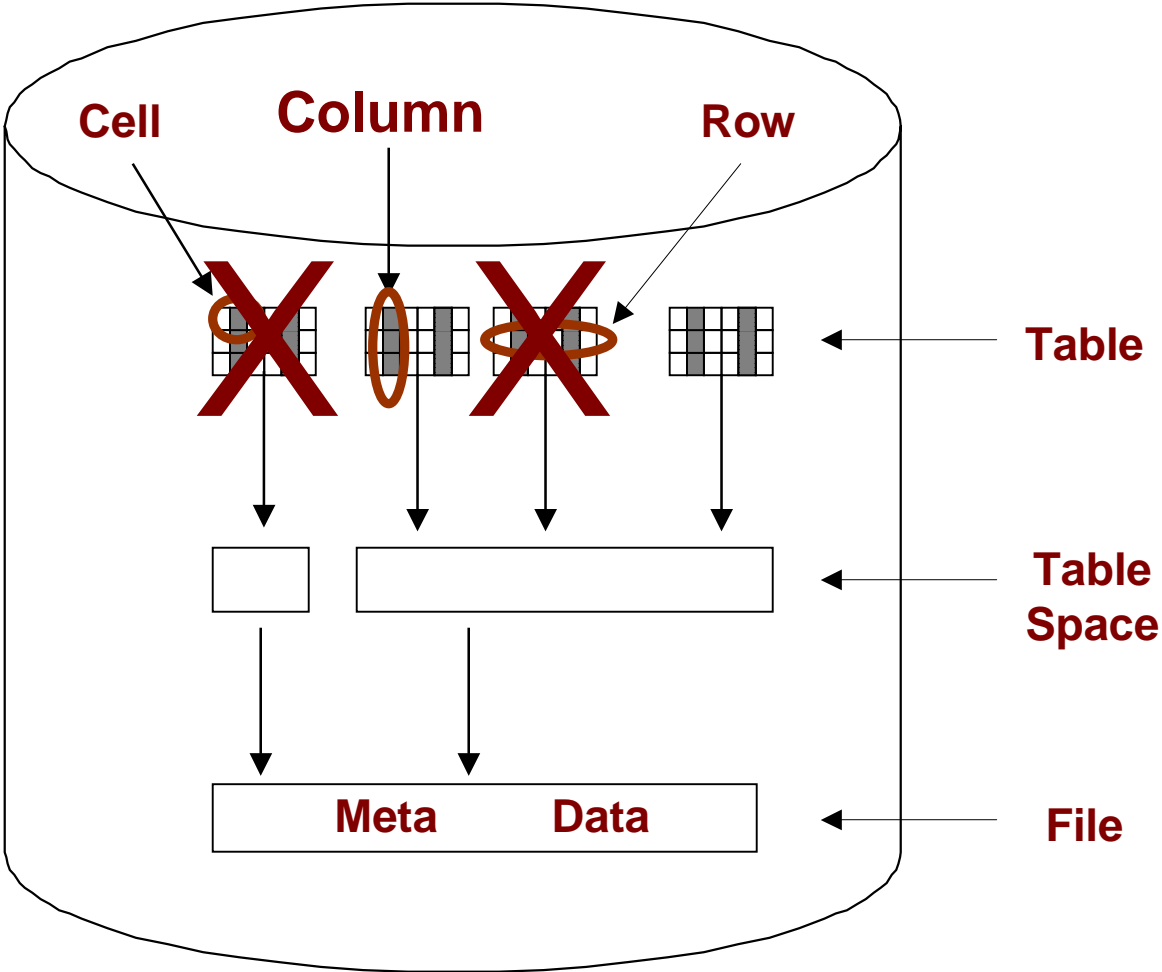
: Key Management & Crypto Operation

# Data at Rest Encryption at Different Layers

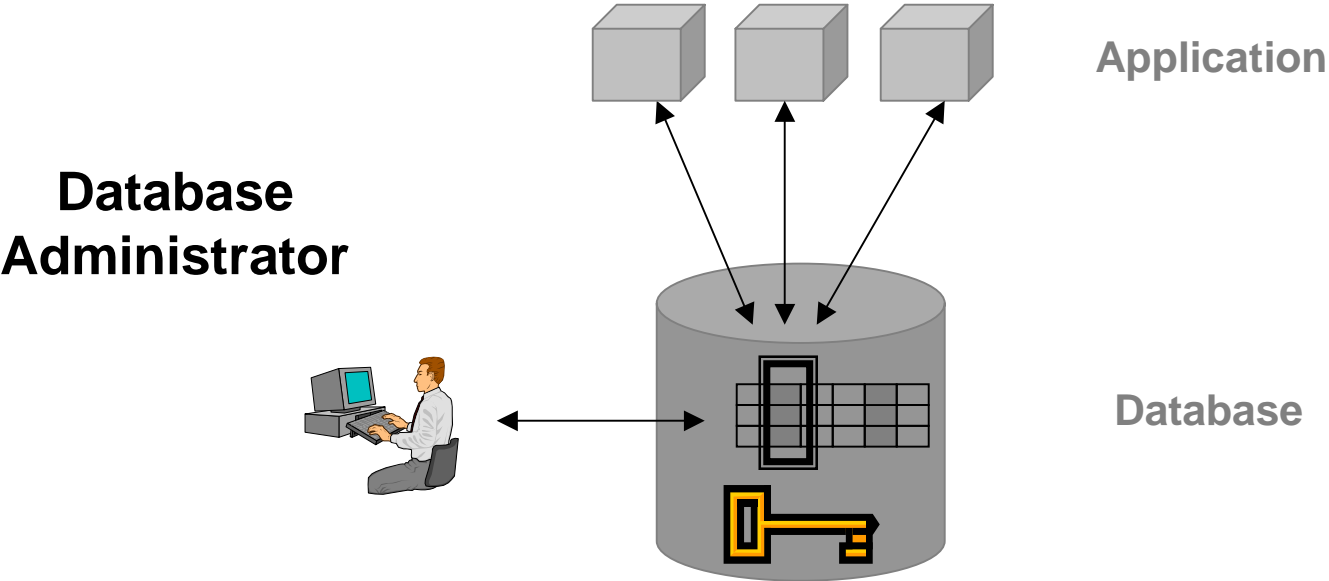


# Issues when Searching Encrypted Data

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
<b>Deployment</b>	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
<b>Security</b>	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
<b>Audit</b>	Audit support for all access to data?	100	0
	Audit support for all changes to security policy?	100	0

High Score is Most Favorable



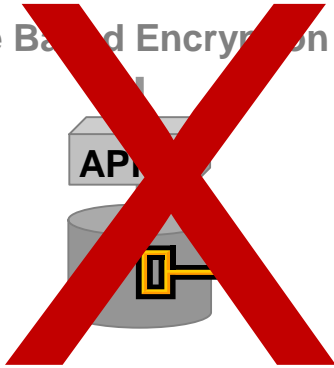
Safeguarding Enterprise Databases



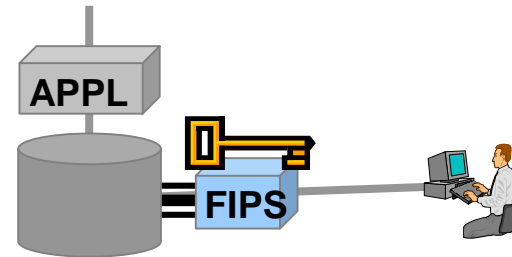
# Case Studies - 4 Solution Alternatives

Ease of Deployment

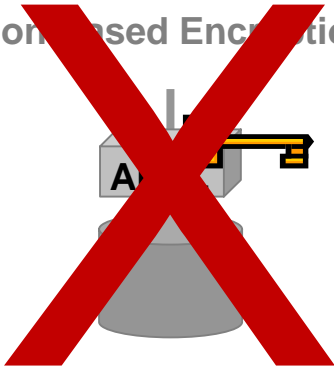
Database Based Encryption Keys



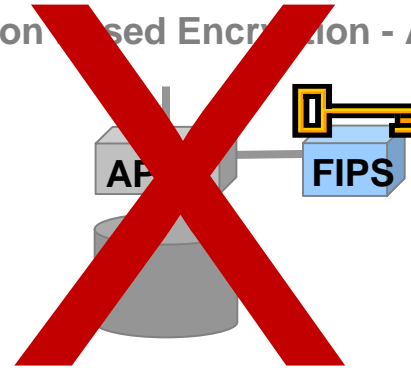
Security-System Based Encryption Keys



Application Based Encryption - Basic



Application Based Encryption - Advanced



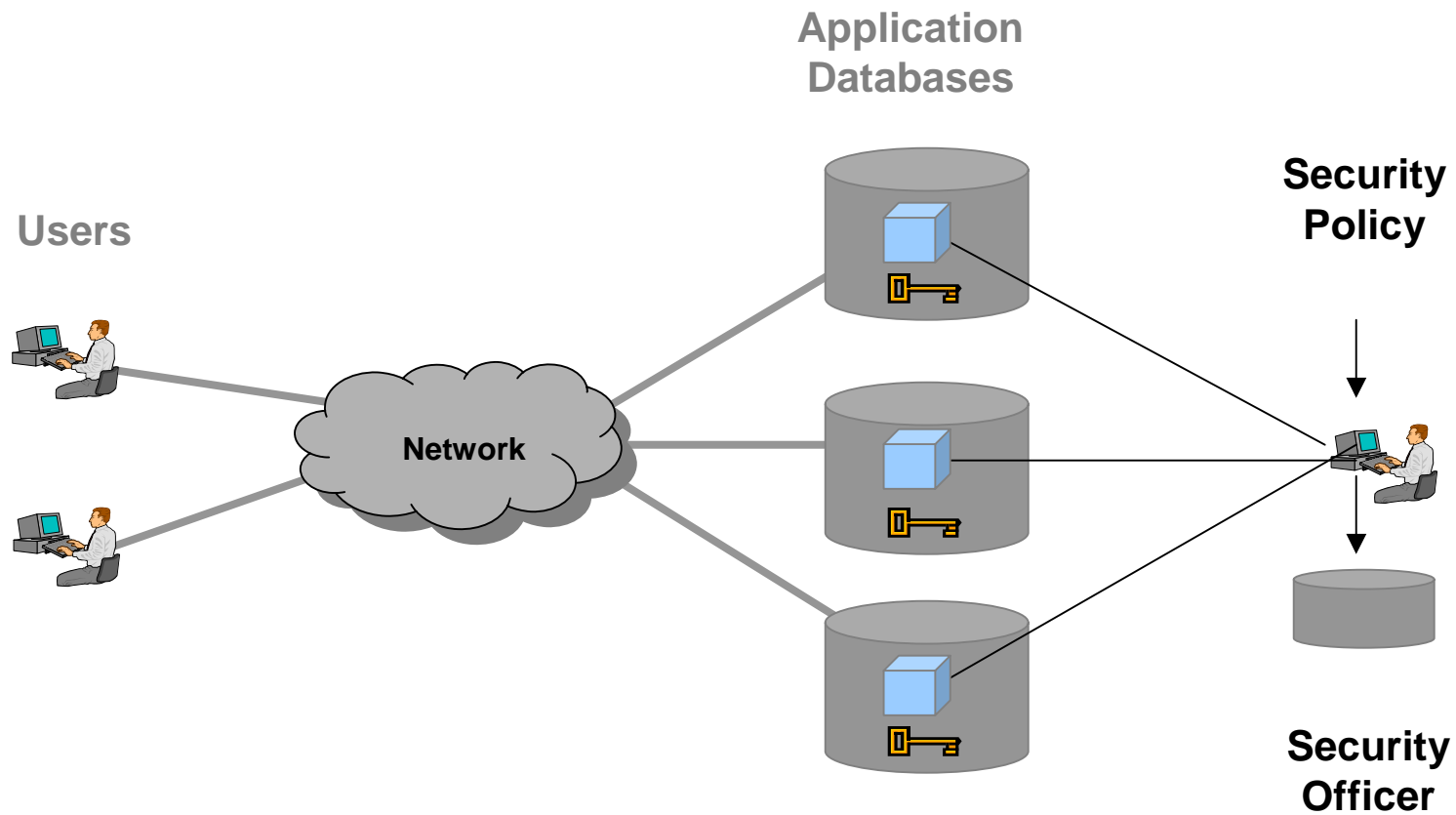
Security Level

# 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.

# A Database Intrusion Prevention Solution

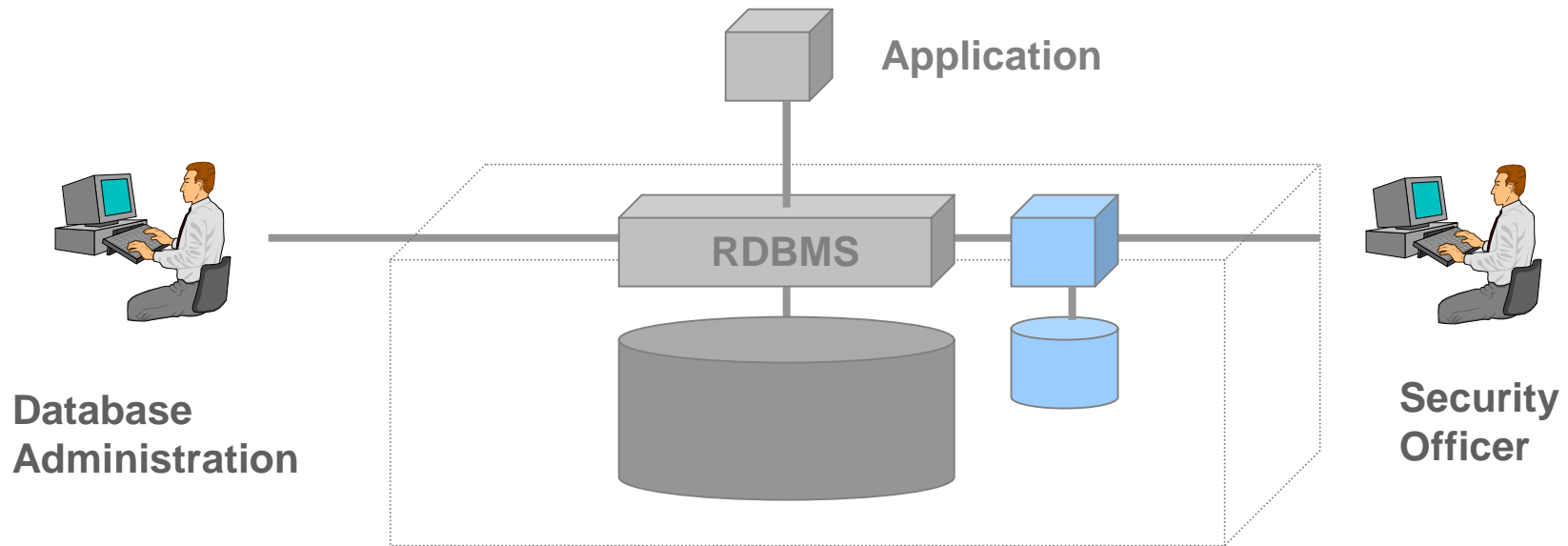


## The Hybrid - Much more than data encryption

---

- 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

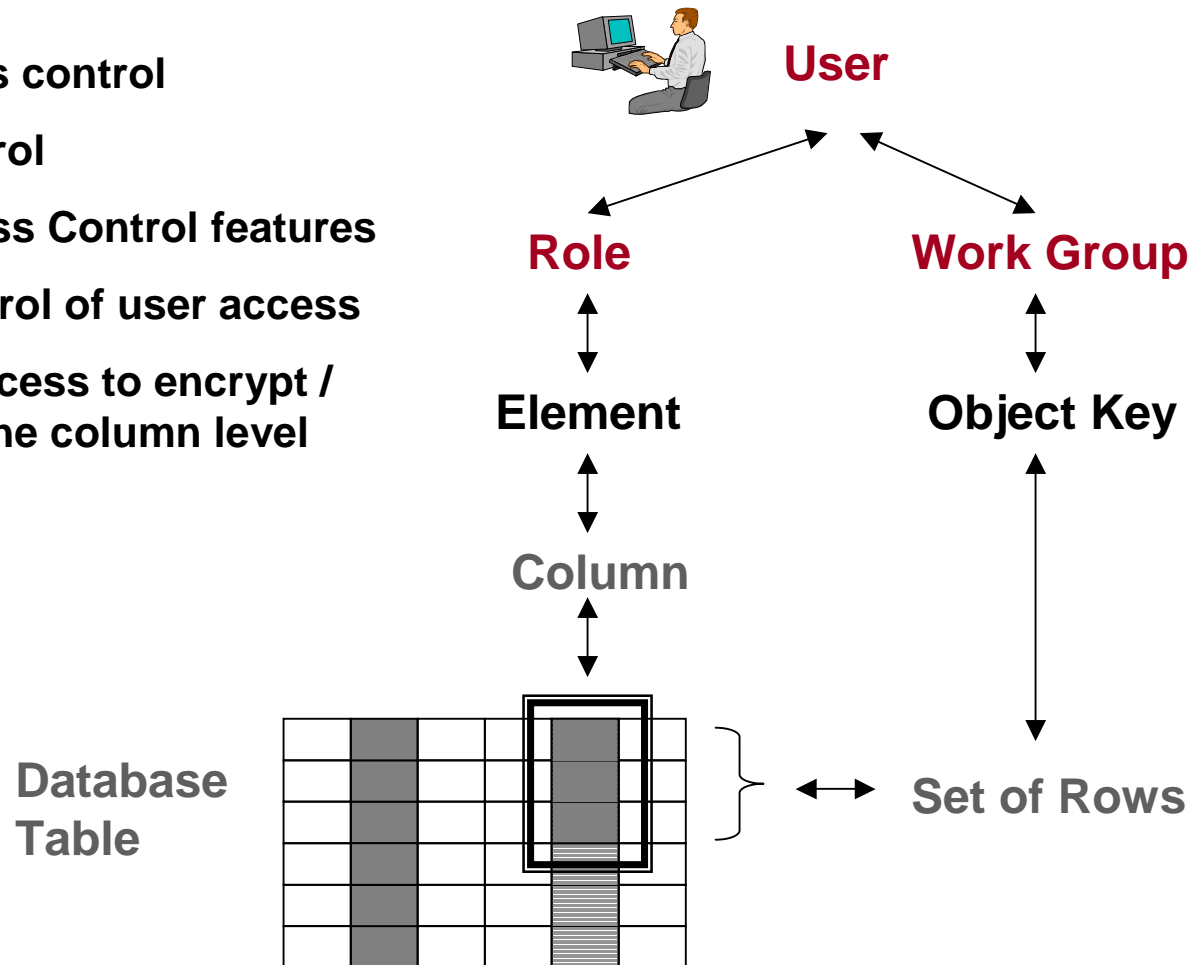
# Separation of Privacy Control Duties



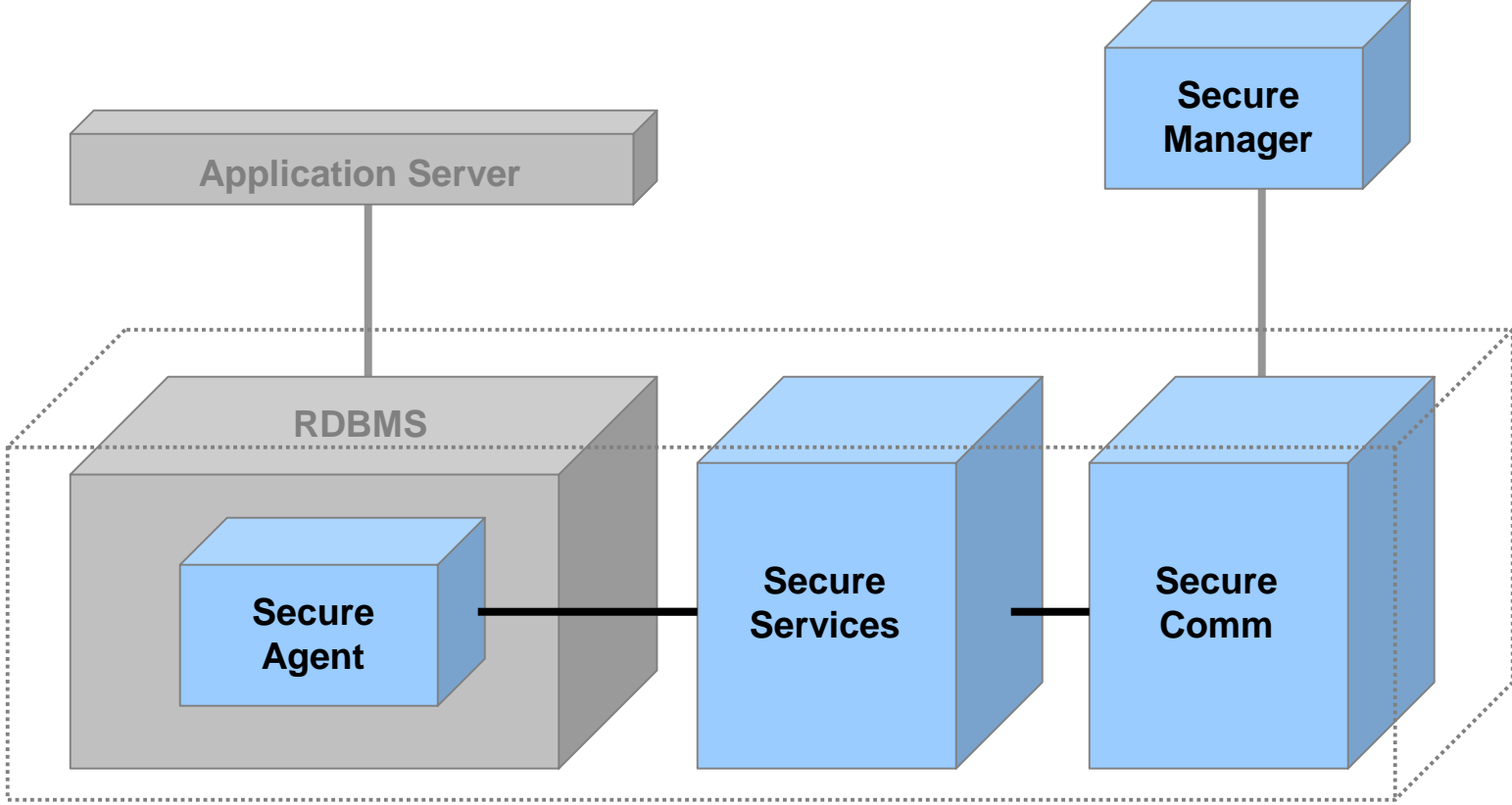
1. Separation of duties for encryption key management
2. Separation of duties for integrity check of selected software executables
3. Separation of duties for access control policy
4. Strong authentication for the security administrator

# Easy to Manage - Role Based Access Control

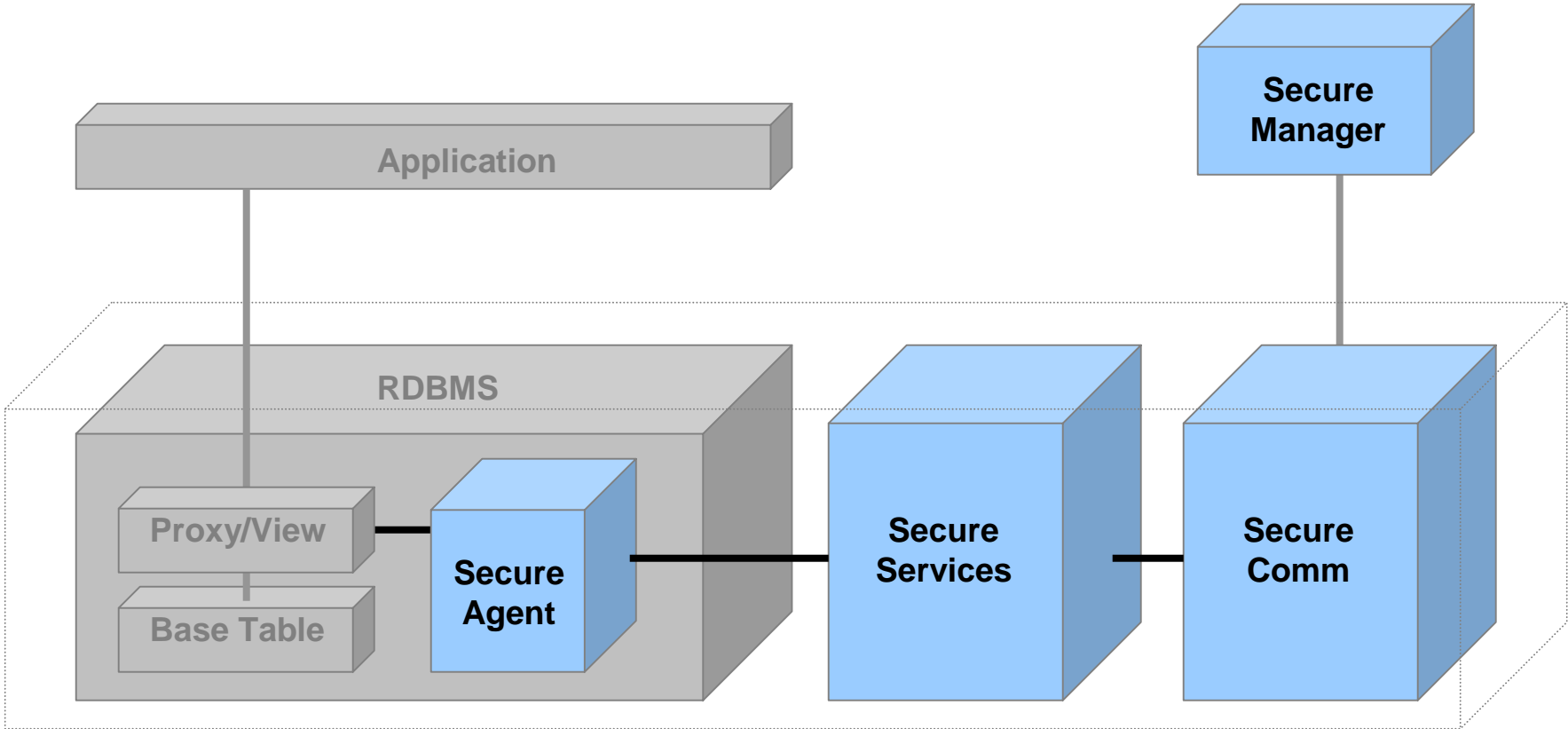
- Row level access control
- Role-based control
- Mandatory Access Control features
- Time-based control of user access
- Controls user access to encrypt / decrypt data at the column level



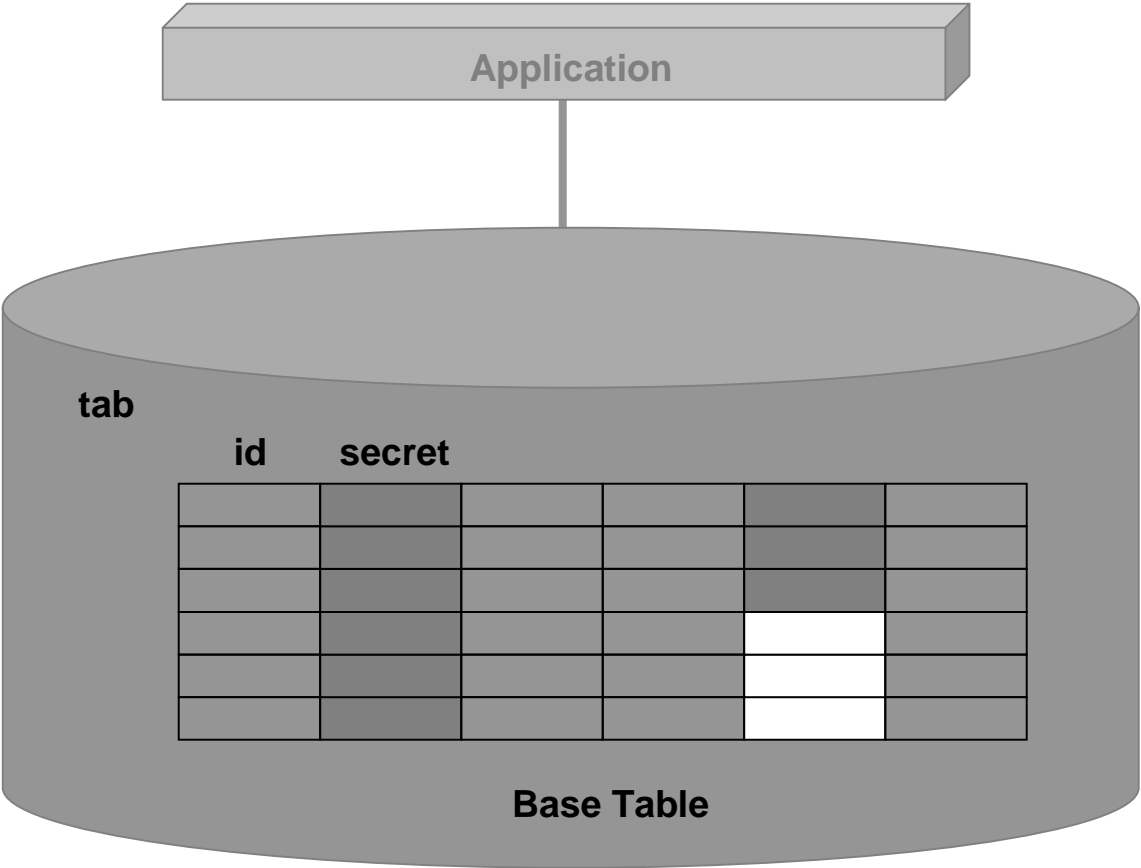
# Secure.Data - Implementation



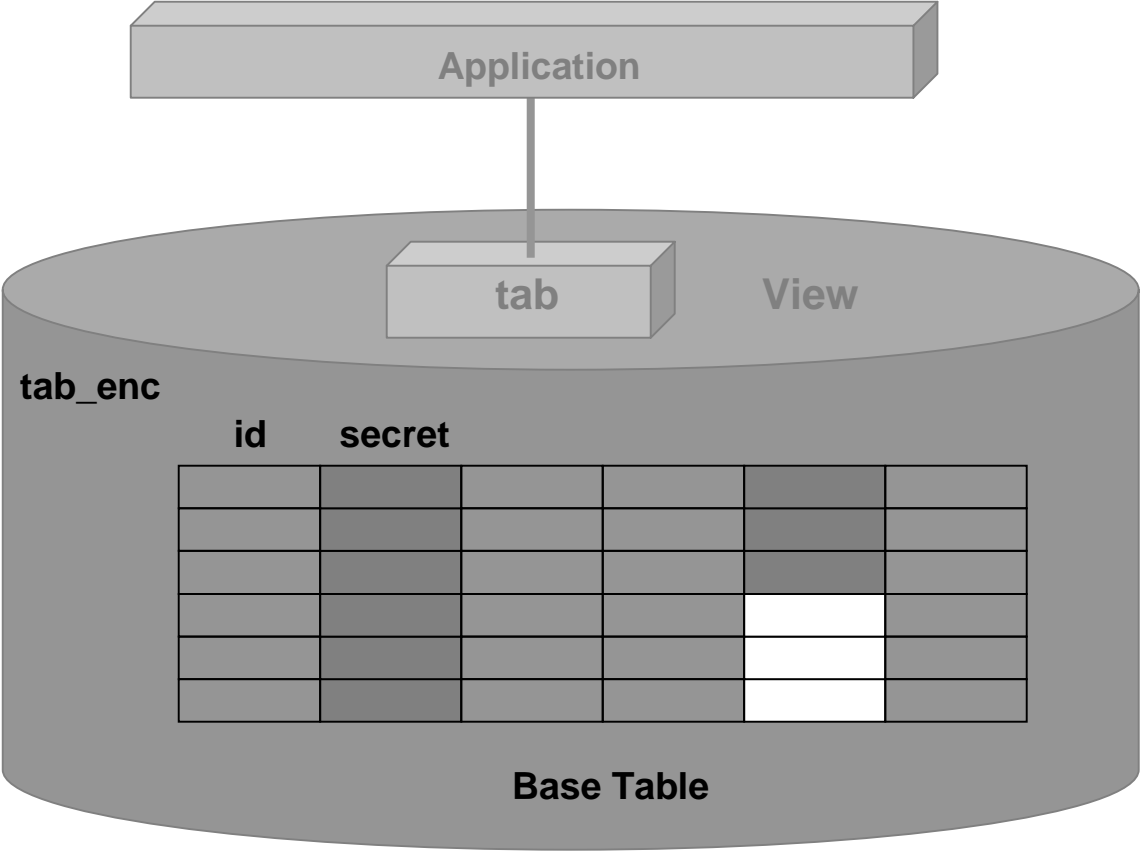
# Secure.Data - Implementation



# Secure.Data – Implementation - Sample



# Secure.Data – Implementation - Sample



## Secure.Data – Implementation – Tables & Views

---

The original base table 'tab' holds an identity 'id' column and a secret code column 'secret':

Create the new base table 'tab\_enc' is defined as:

```
create table tab_enc (  
    id integer,  
    secret varchar (32) for bit data);
```

Create the new base table 'tab\_enc' that will hold encrypted values in the 'secret' column:

```
create table tab_enc (  
    id integer,  
    secret varchar (32) for bit data);
```

Create a view with the same name as the original base table 'tab':

```
create or replace view tab(id, secret) as  
    SELECT id, decrypt('tab_enc.secret', secret)  
    FROM tab_enc;
```

# Secure.Data – Implementation - Triggers

---

Protegrity SQLdirector creates a trigger on the view 'tab' to be able to insert data:

```
create or replace trigger tab_insert
instead of insert on tab
for each row
begin
    insert into tab (
        id,
        secret)
    values (
        :new.id,
        pty.ins_encrypt('secret', :new.secret));
end;
```

Protegrity SQLdirector creates a trigger on the view 'tab' to be able to update data:

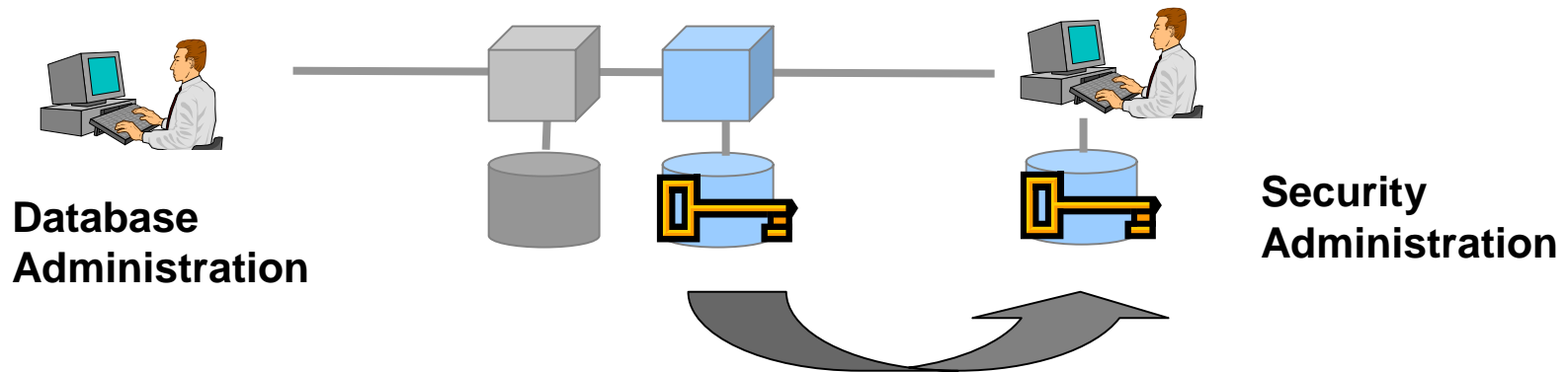
```
create or replace trigger tab_update
instead of update on tab
for each row
begin
    update tab set
    id = :new.id,
    secret = pty.upd_encrypt('secret', :new.secret)
    where id = :old.id;
end;
```

Protegrity SQLdirector creates a trigger on the view 'tab' to be able to delete data:

```
create or replace trigger tab_delete
instead of delete on tab
for each row
begin
    pty.del_check('secret');
    delete tab
    where id = :old.id;
end;
```

# Protected Enterprise Audit

---



1. All logs are of a common format across transaction protocols or database managers
2. Audit trails are encrypted, as are all Privacy Database security metadata.
3. Encrypted log-files are stored locally on each server and manage
4. The Audit performed by the Security Officer, not the DBA .
5. Privacy Database provides column level access auditing for franchise database data