Protecting Data and Transactions with Encryption and Tokenization

Rich Mogull
Securosis

What We'll Cover

- Encryption and Tokenization for the financial services data center.
- How the technologies work.
- How to pick the right one for your project.

Securosis

Access Controls

Encryption

DRM

Securosis

The Three Laws of Encryption

If Data Moves Physically or Virtually

For Separation of Duties

Mandated Encryption

Securosis

Where to Encrypt

Separation of Duties	Movement/Media Protection
• Database Fields • Workstation File/Folder • Server • NAS • Applications	• Tape • SAN • Laptops/FDE • Email • Portable Media

Encryption Options

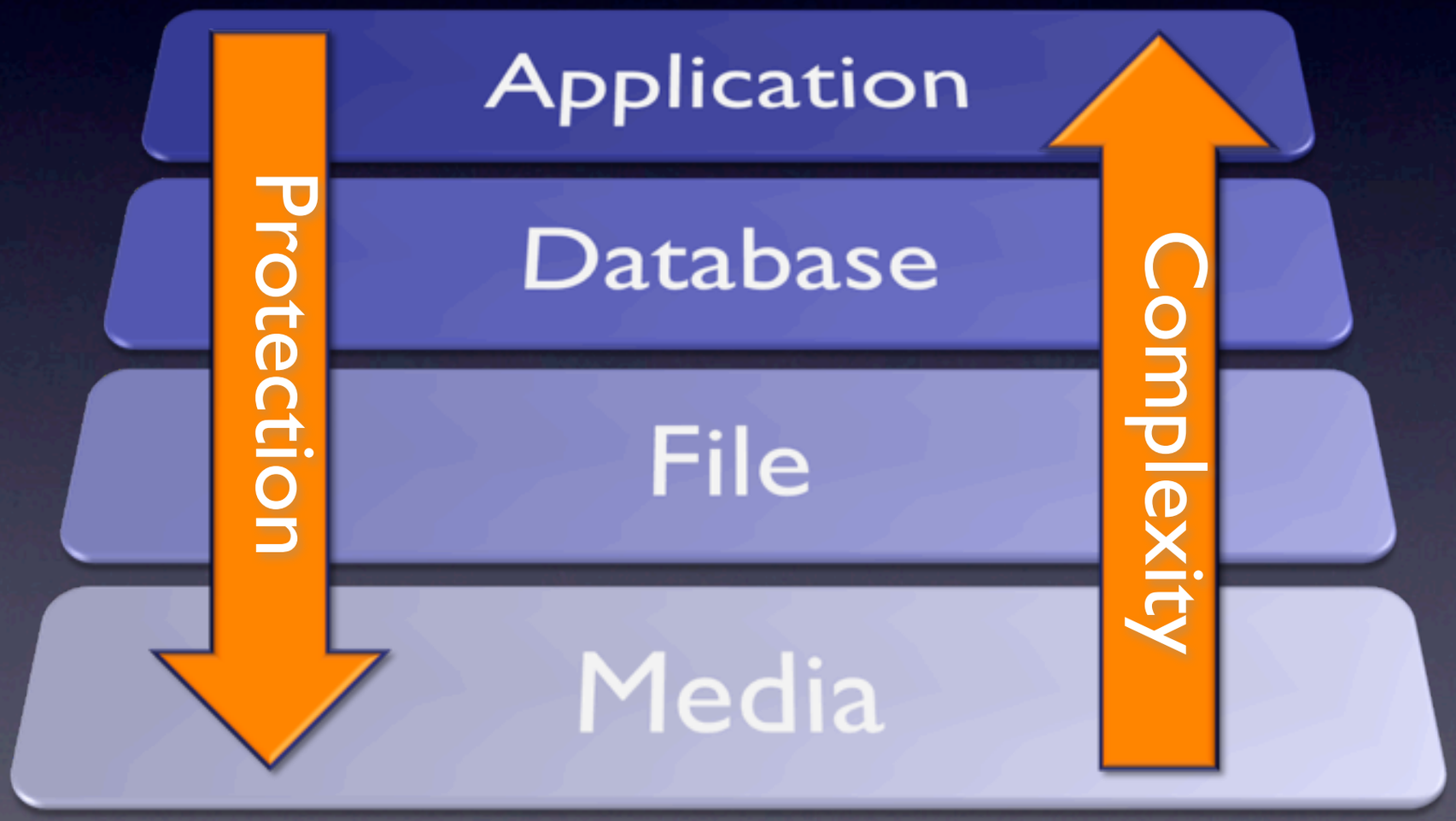
File/Folder

Application/
Database

Media

Securosis

Encryption Layers



Securosis

Location

Management

Operations

Key

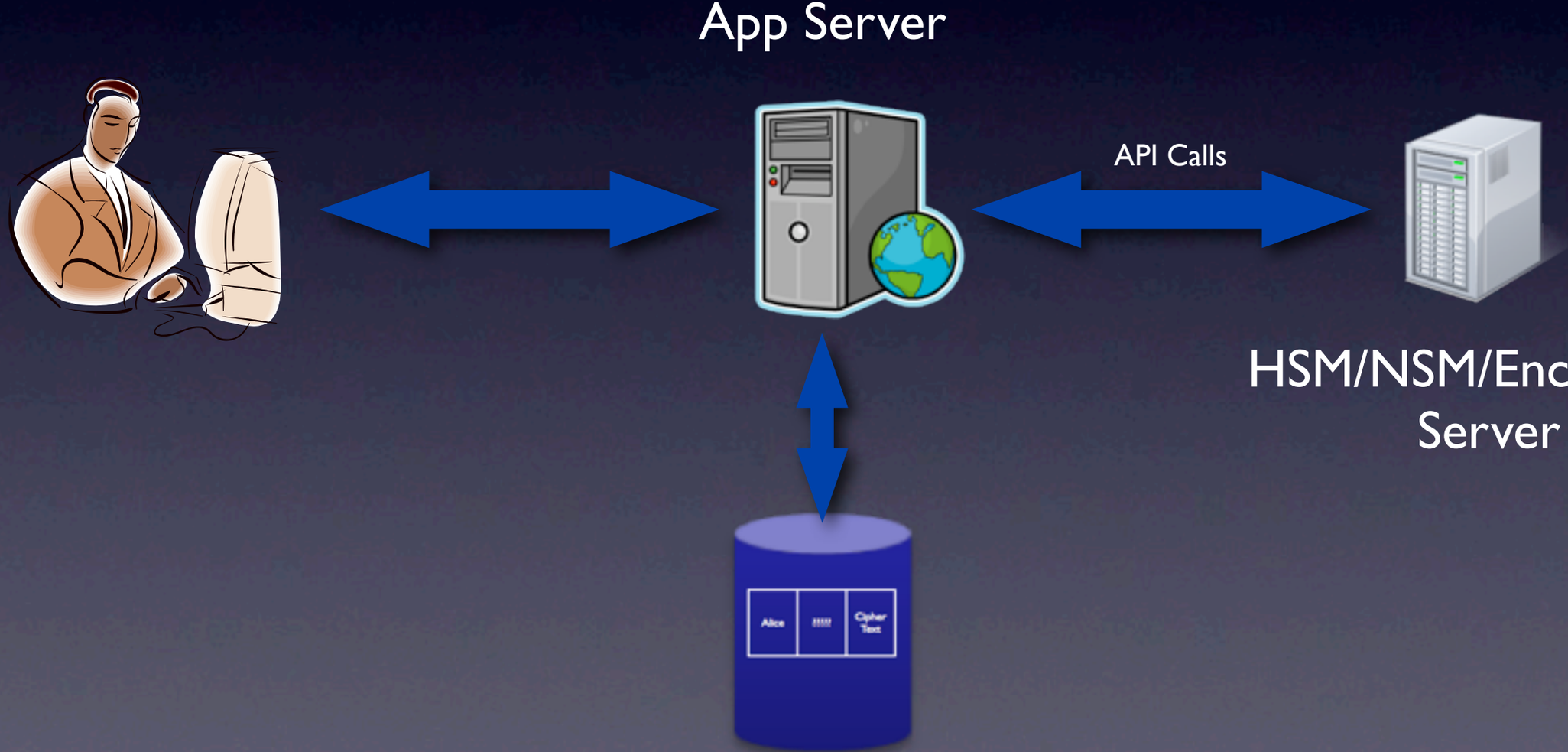
Securosis

Rules for Application Encryption

- Use toolkits.
- Use external key management.
- Rely on experts.
- Keep it simple.
- Keep it narrow.
- Have an expert evaluate it.

Securosis

Application Encryption Architecture



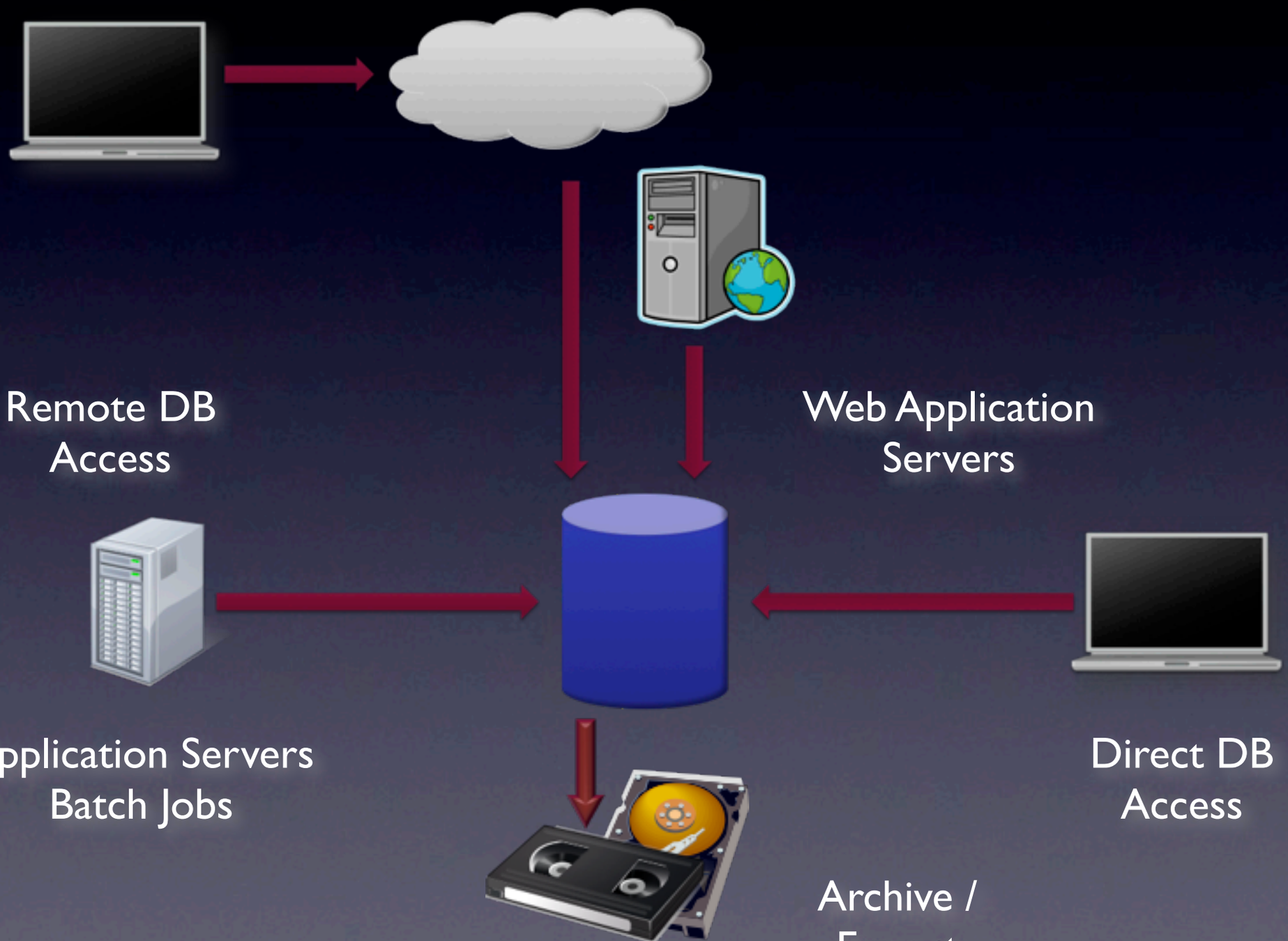
Securosis

Application Level Encryption

- Granular application of encryption
- Completely external or App/DB hybrid
- Protects data from ad-hoc queries
- Protects data on media
- Keys (potentially) secure from IT and DBAs
- Keys (potentially) not tied to credentials
- Very expensive to retrofit applications/databases

Securosis

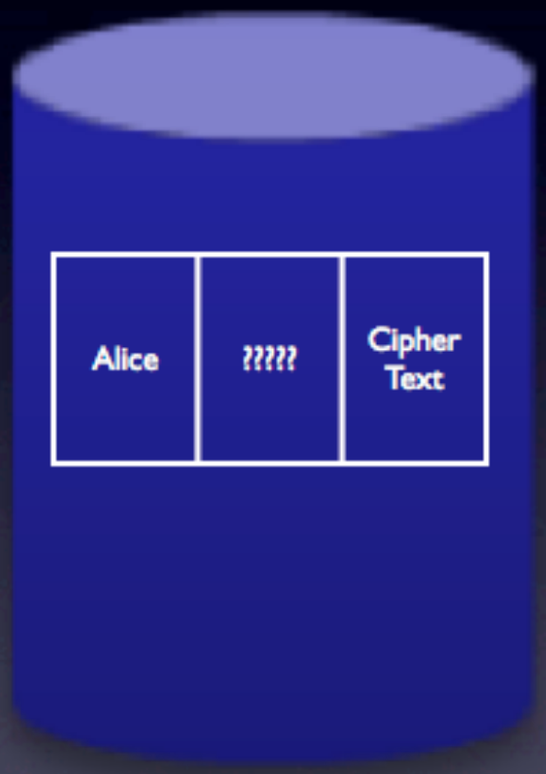
Database <> Not Data at Rest



Database Encryption Options

- Inside the Database
  - User/Object
  - Transparent
- Outside the Database
  - Application
  - OS/File
  - Media

Database Object Encryption



- Tablespace
- Table
- Column
- Row

Database Object Encryption

- Granular application of encryption
- Embeddable within queries/procedures
- Protects data from ad-hoc queries
- Protects media
- Keys secure from IT personnel
- Expensive to retrofit existing databases

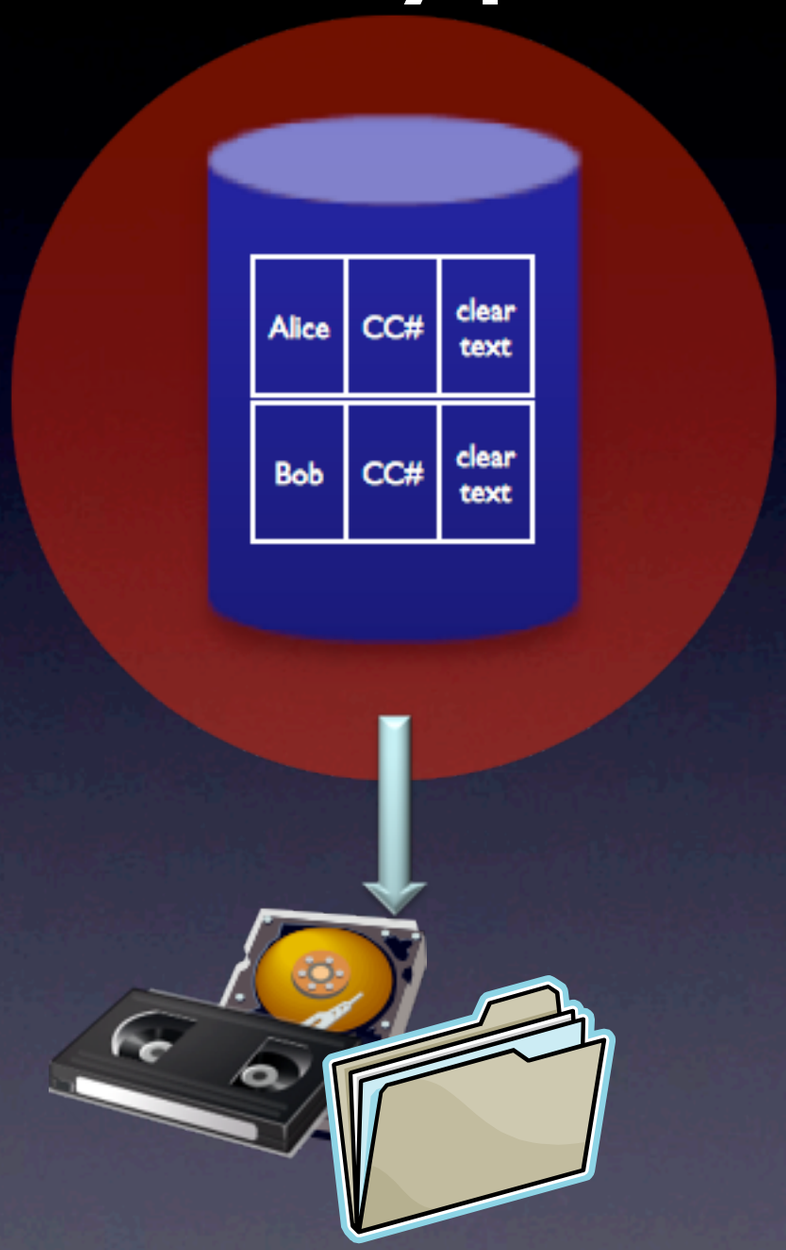
Securosis

Transparent Database Encryption

Transparent Tablespace

Data Writer

Log Writer



Transparent Column

Securosis

Transparent Database Encryption

- Options for DB, schema, tables and columns
- Protects data on media
- No disruption to IT operations
- No modifications to application or database
- Keys secure from IT; options for HSM
- Incredibly easy to implement

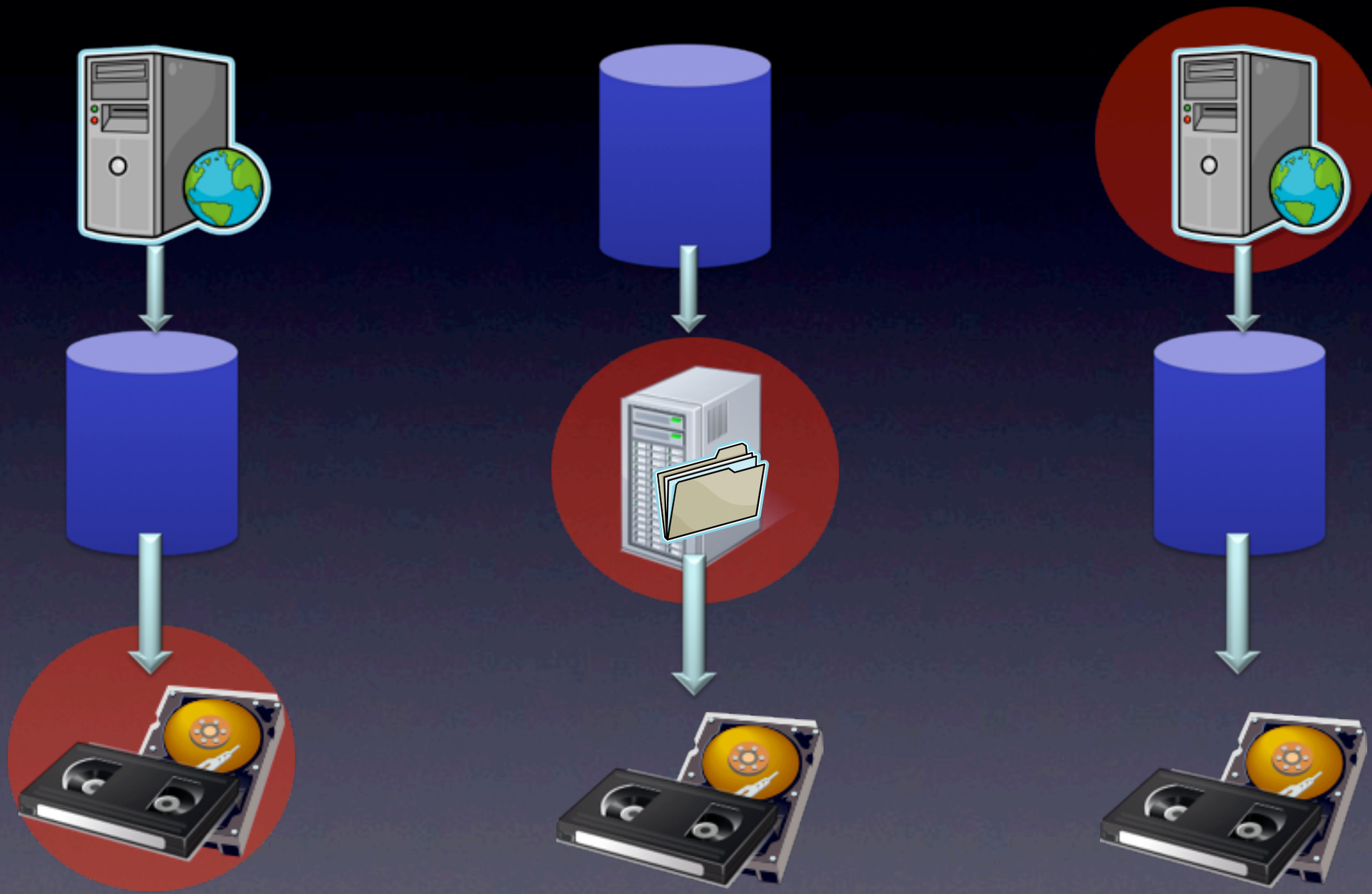
Securosis

How Easy?

```
alter table accounts
   modify (ssn encrypt using 'AES128');
```

… that easy.

External Database Encryption



Media Encryption

OS/File

Application

Securosis

OS/File Encryption

- Data encrypted when written to disk
- Applied to all or part of database
- Protects data on media
- No modifications to application or database
- Keys secure from DBAs; options for HSM
- Easy to implement
- Performance advantage to TDE

Securosis

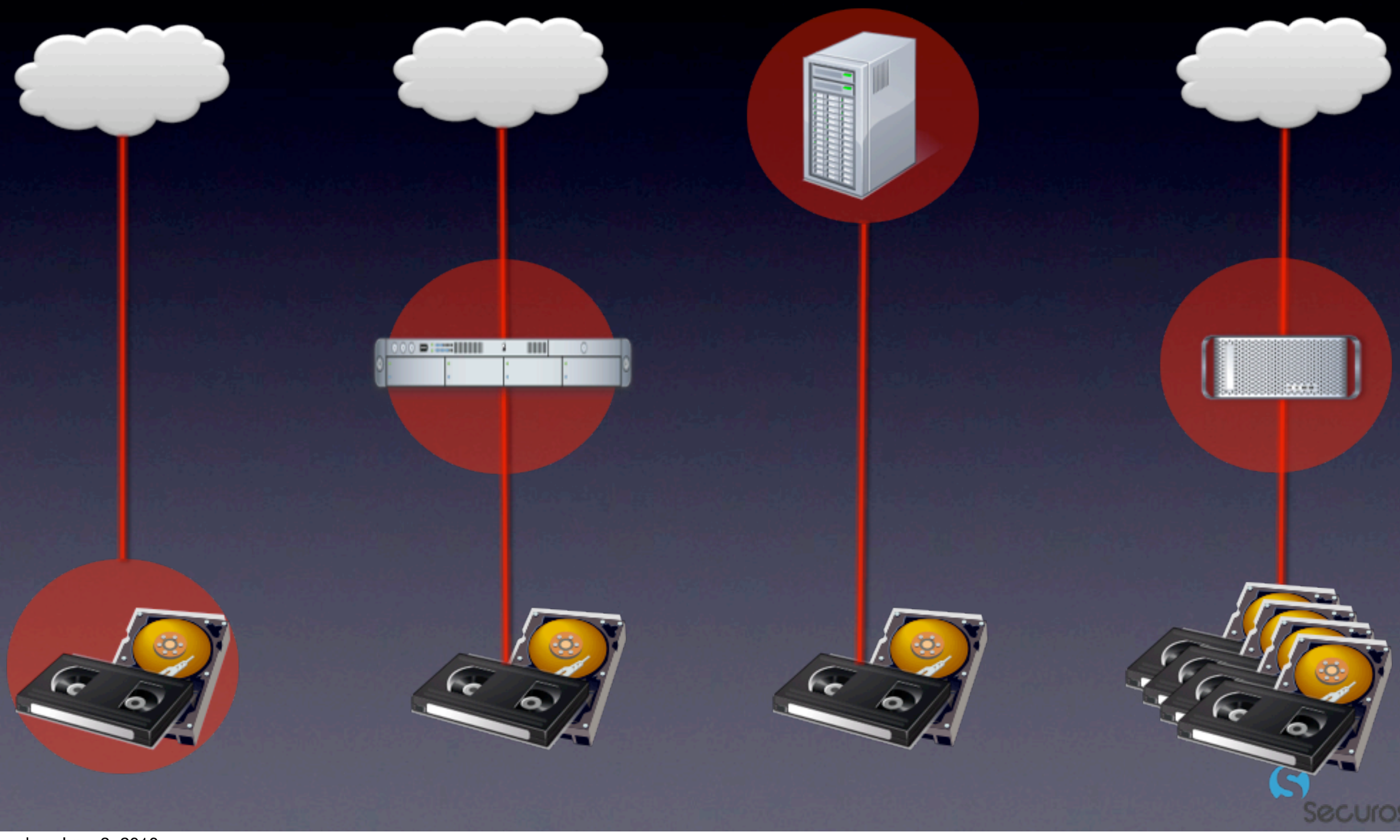
Tape/SAN Encryption Options

Drive

Inline

Server

Controller

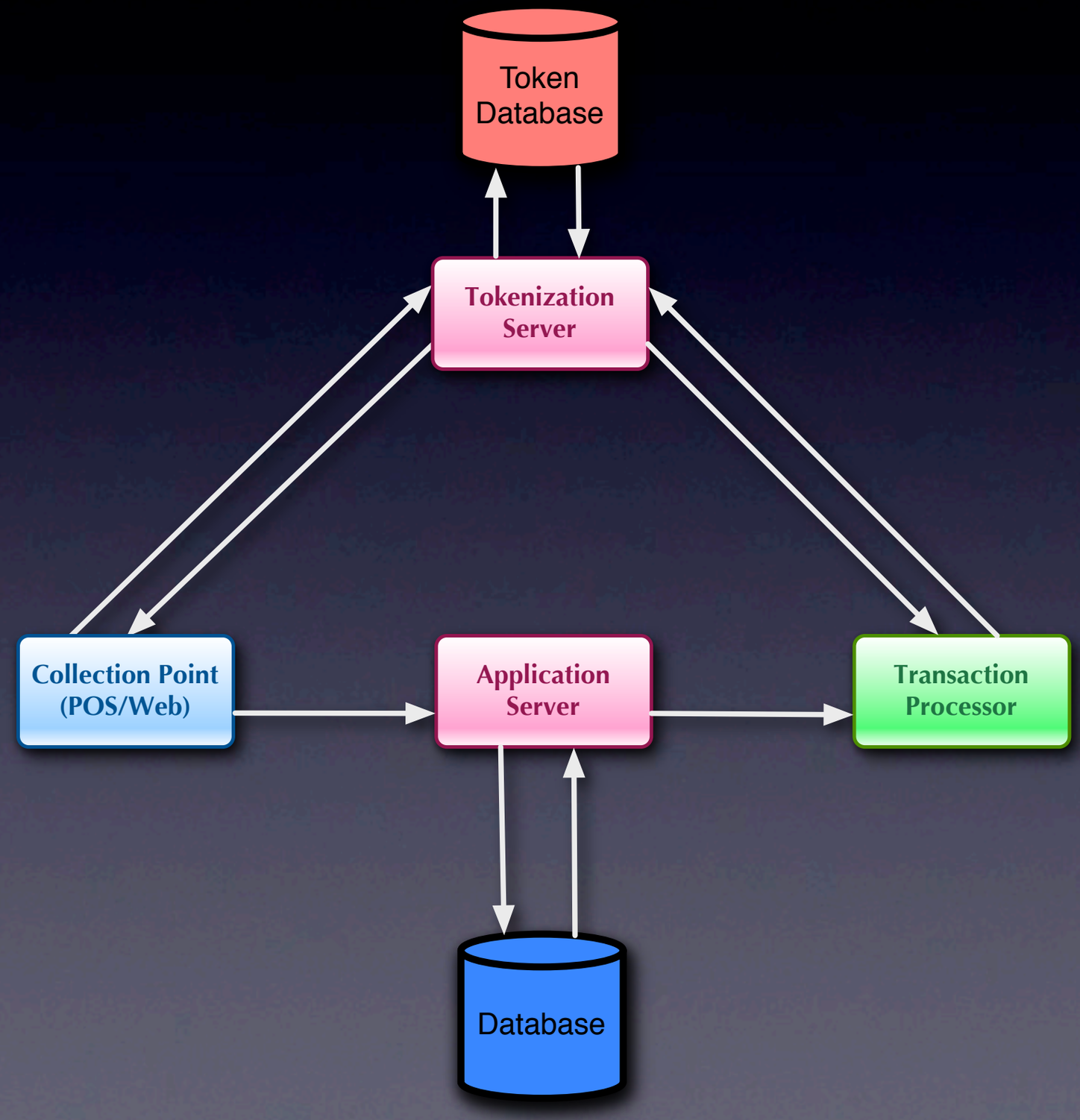


Securosis

Media Encryption

- Protects data on media
- Keys secure from DBA
- Many variants (speed, cost, flexibility)
- Cost varies widely
- Not suitable for many regulatory requirements

Tokenization



Tokenization

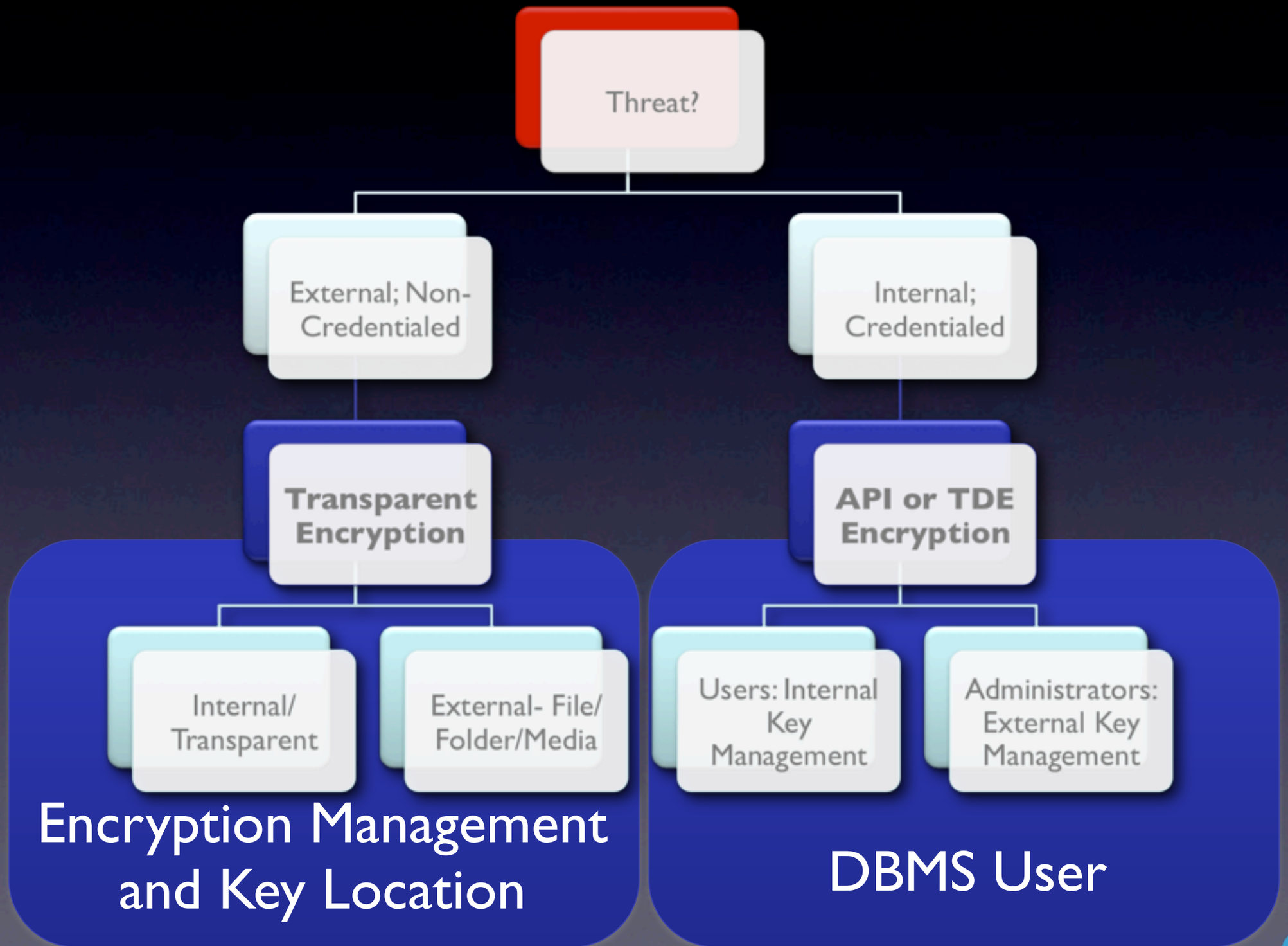
- Token values can be completely random or pattern based.
- May reduce audit scope.
- May reduce application level changes.
- How tokens generated and stored is key.

Format Preserving Encryption

Reversible
Not NIST or PCI Approved
Can be based on AES

Securosis

Encryption Selection Process



Securosis

Key Management

- Internal or external options for all variants
- Internal keys easier to use, cost effective
- External is more secure, provides SOD and offers more features
- External means more cost and complexity

Access Controls & Encryption

- Access Controls are very effective
- Encryption helps when access controls are not available
- Encryption supports access control, not a substitute
- Encryption offers secondary authentication
- Encryption with separation of duties

Data Masking

Data Masking

Production

ID	Name	SSN
1	Smith	111-22-3333
2	Jones	444-55-6666
3	Doe	777-88-9999

Development

ID	Name	SSN
1	Johns	123-45-6789
2	George	453-67-7356
3	Blike	245-12-7329

Securosis

Summary

- Transparent encryption for retrofitting applications / databases.
  - TDE is very simple, with no impact to operations
- Tokenization is an excellent option for applications.
- Beware conversion points- bad guys target encryption/ decryption locations and they study your transaction systems.
  - Memory parsing attacks on the rise.
- For financial services, application encryption with HSMs most common and best option (outside tokenization).

Securosis

Rich Mogull

Securosis, L.L.C.

rmogull@securosis.com
http://securosis.com
AIM: securosis
Skype: rmogull
Twitter: rmogull