Pragmatic Data Security

Rich Mogull
Securosis

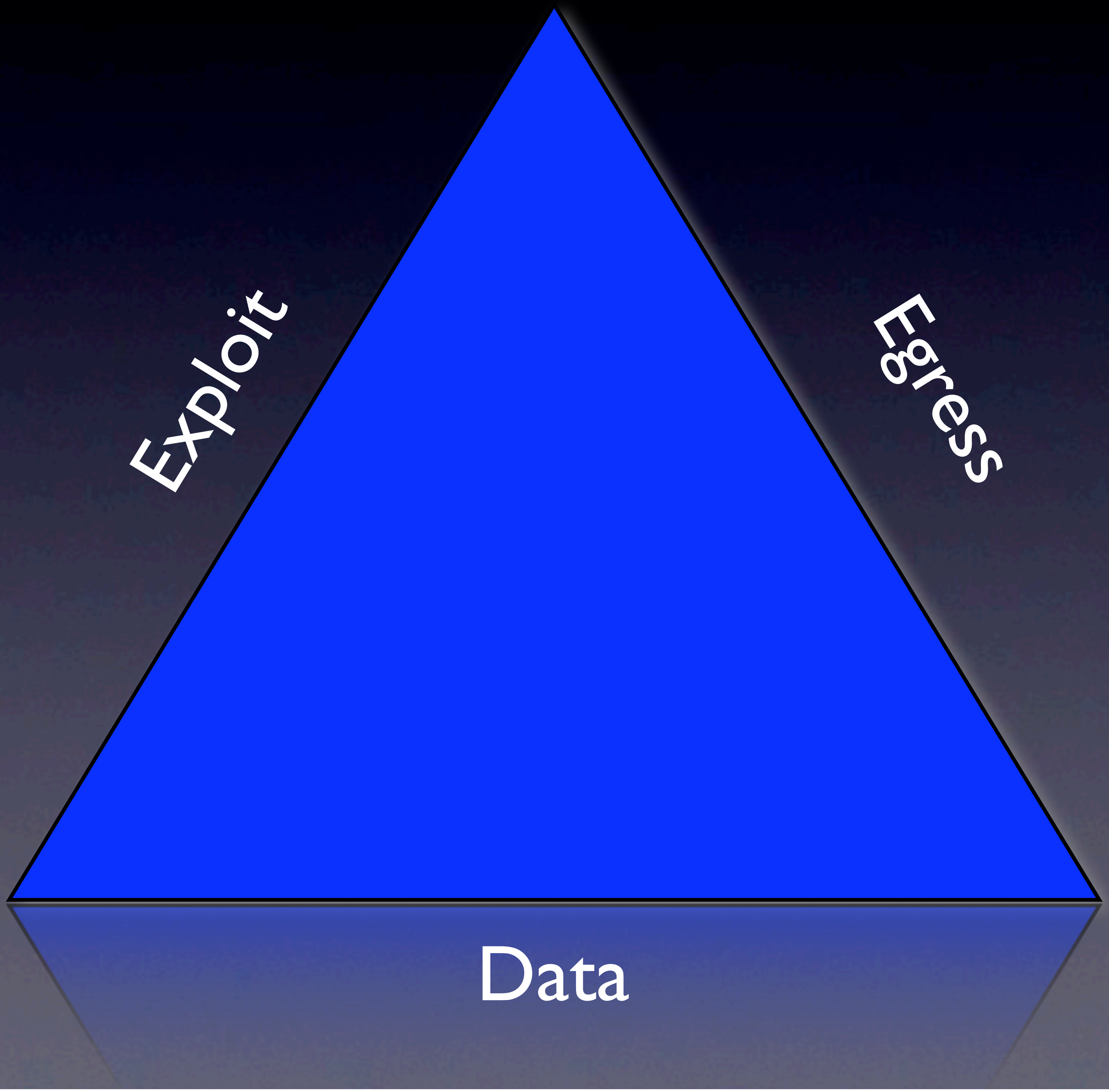
Do you feel the pain?

- No standards
- No architectures
- No money
- Many products
  - None of which work together
  - All of which make the same claims, despite conflicting features.

The Pragmatic Philosophy

- Keep it simple
- Keep it practical
- Start small
- Grow iteratively
- Eat the elephant
- Document everything

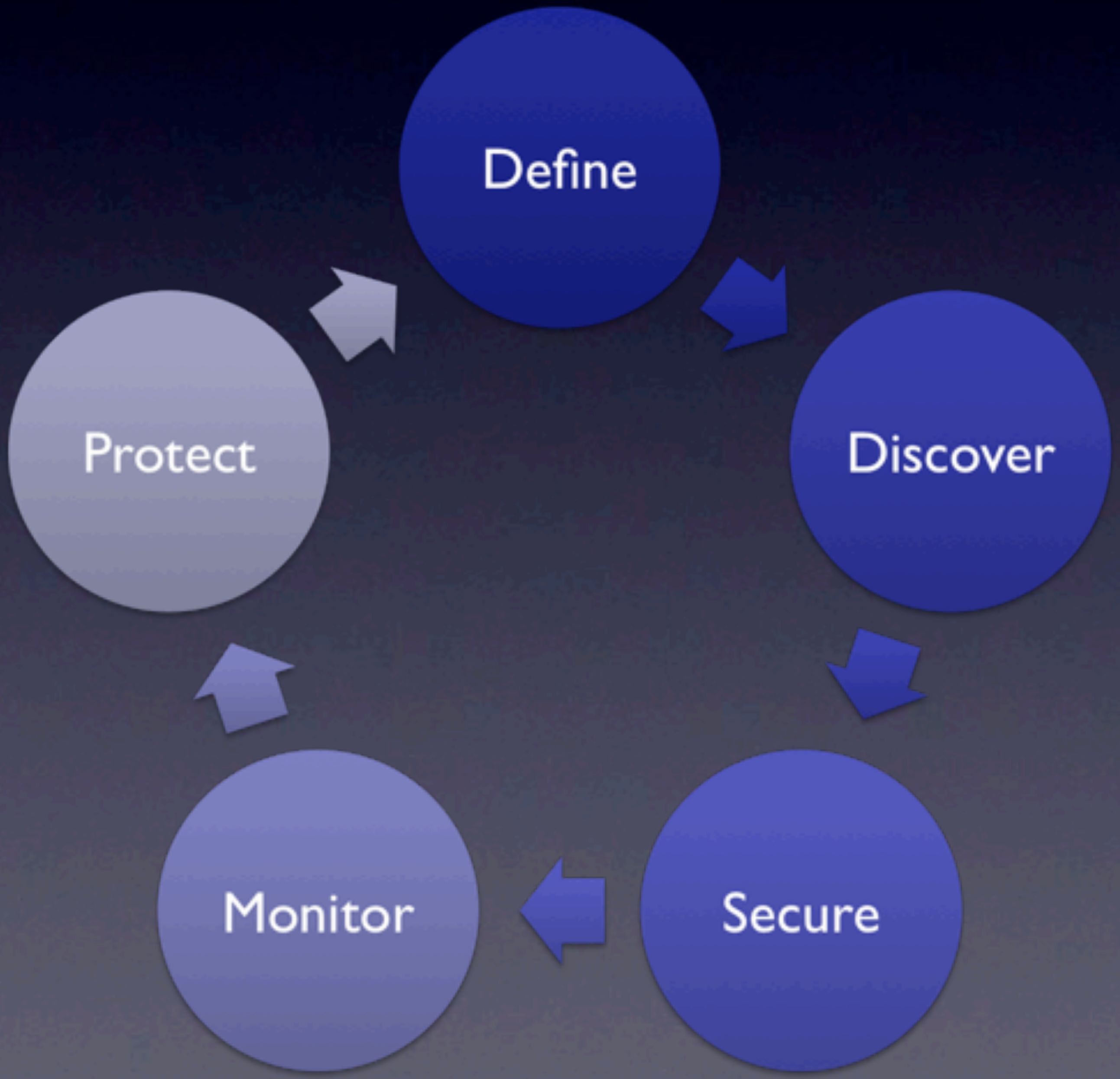
Data Breach Triangle



Securosis

BASIC

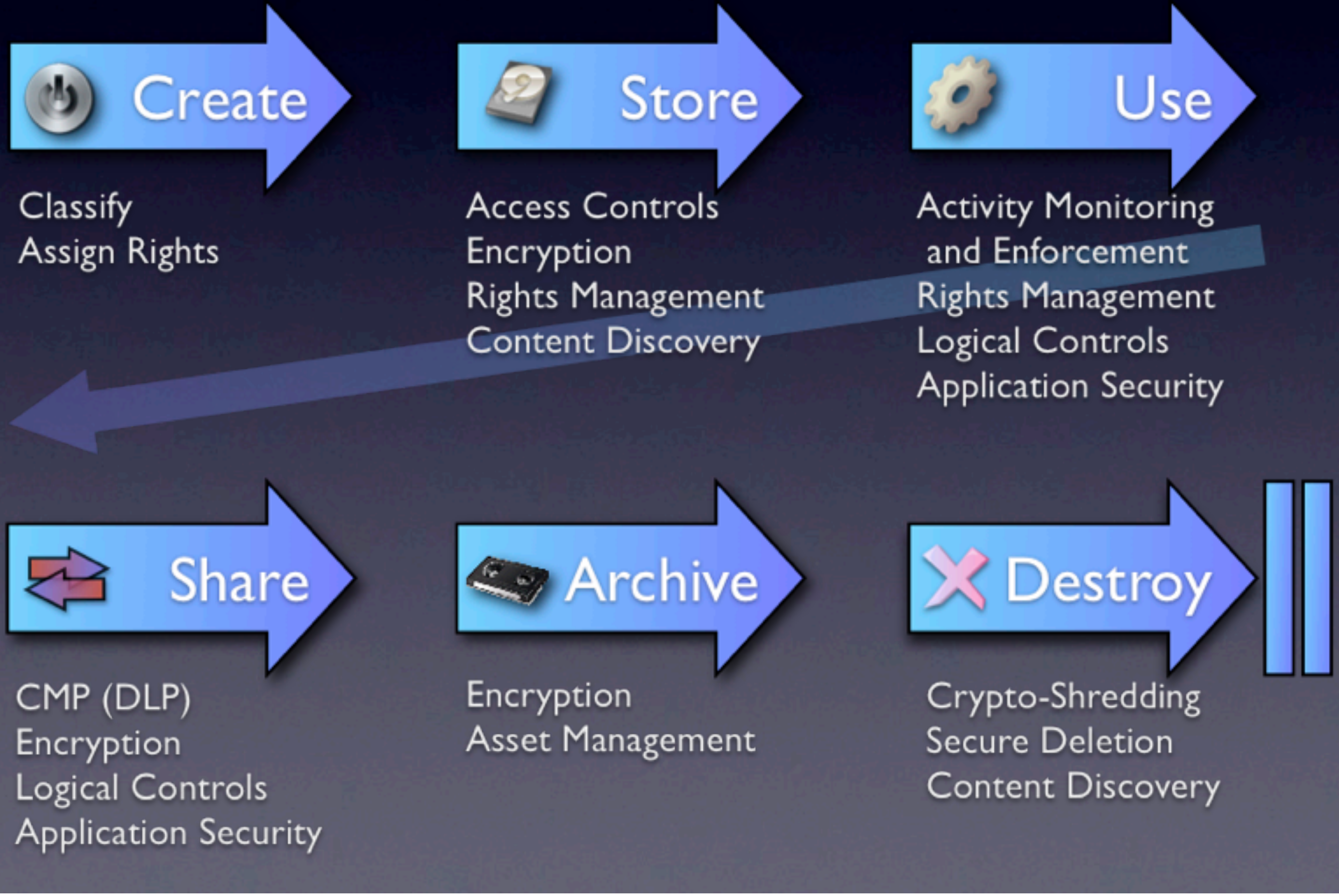
Pragmatic Data Security Cycle



Securosis

Advanced

The Information-Centric Security Lifecycle



Create

Classify
Assign Rights

Store

Access Controls
Encryption
Rights Management
Content Discovery

Use

Activity Monitoring
and Enforcement
Rights Management
Logical Controls
Application Security

Share

CMP (DLP)
Encryption
Logical Controls
Application Security

Archive

Encryption
Asset Management

Destroy

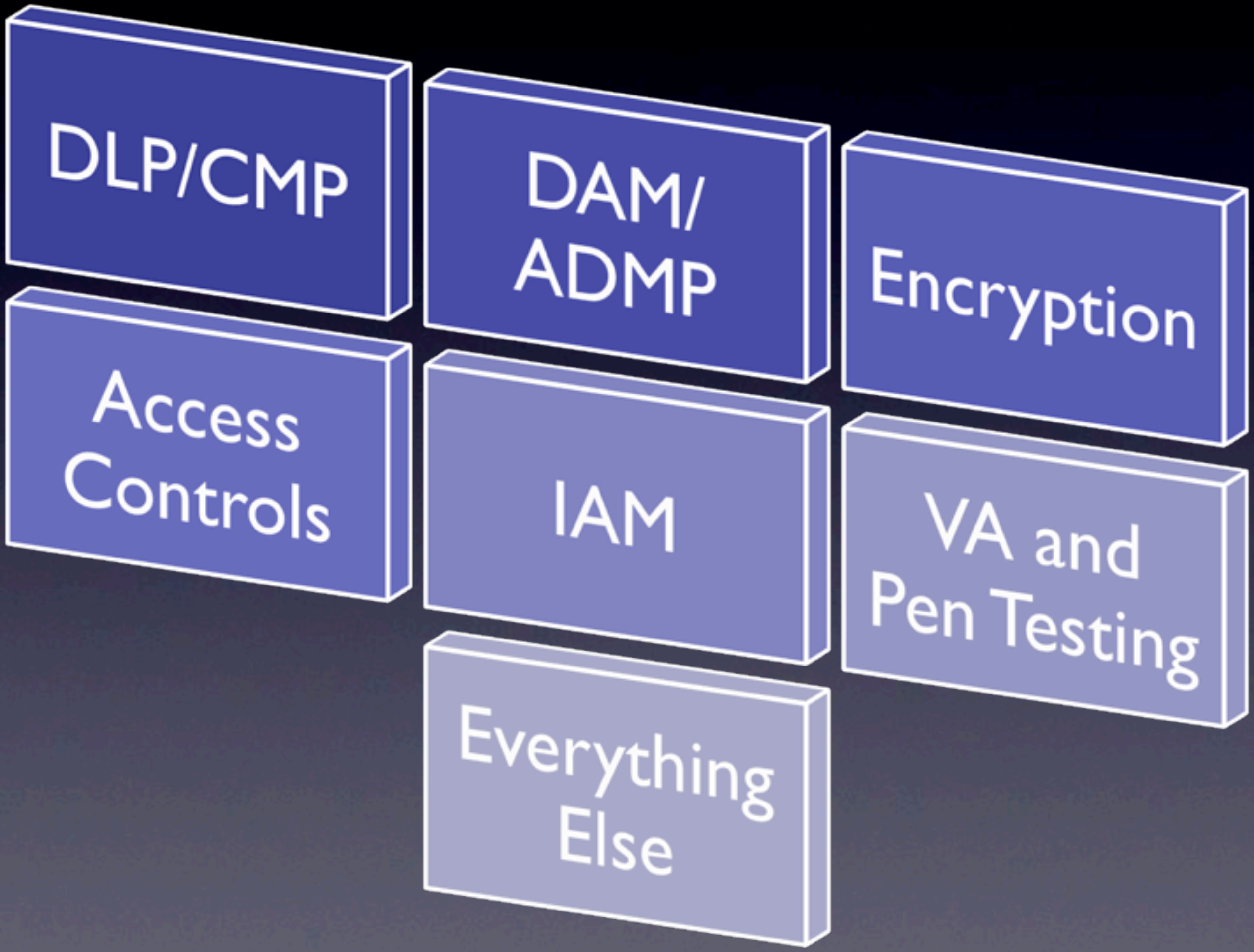
Crypto-Shredding
Secure Deletion
Content Discovery

The Two Sides of Data

Data Center

Productivity

Your Arsenal



DLP/CMP

DAM/ ADMP

Encryption

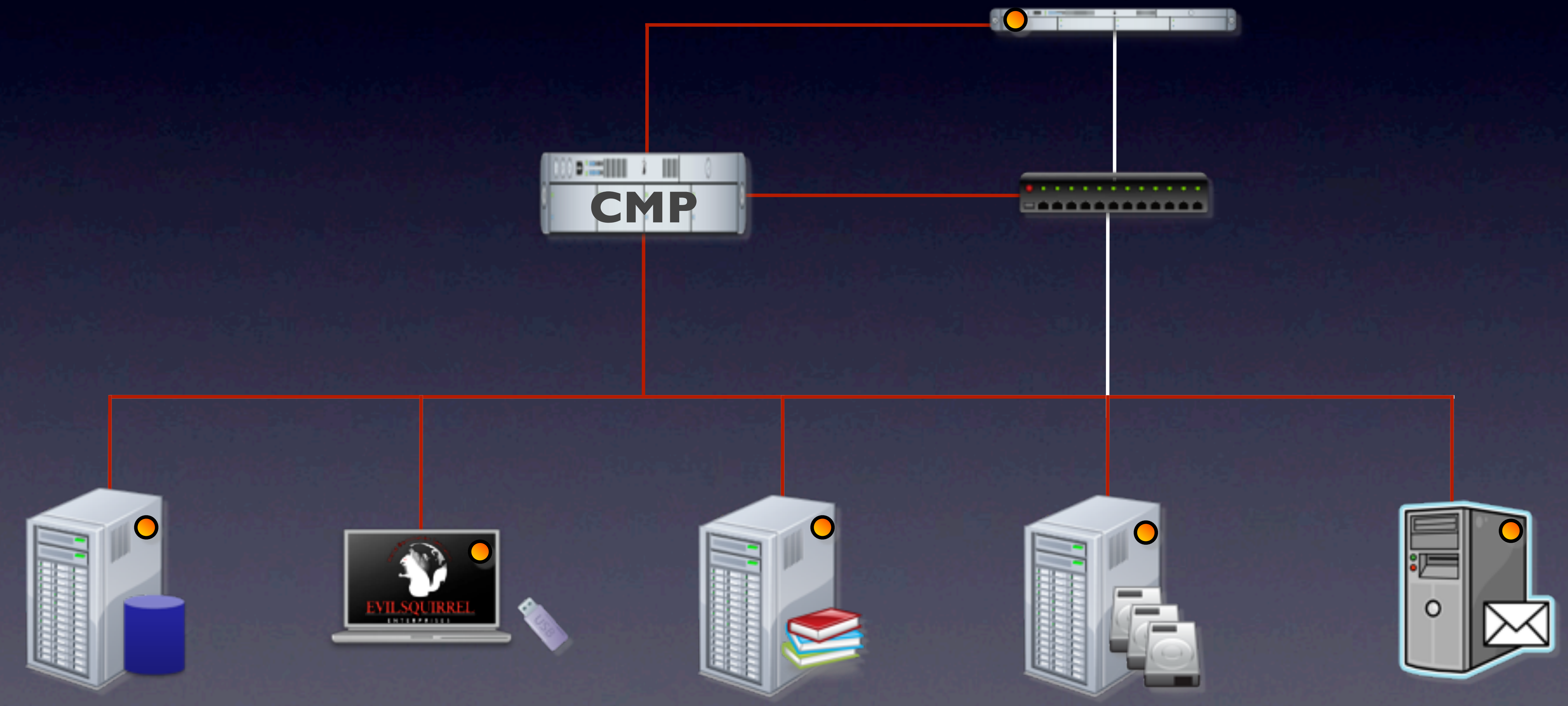
Access Controls

IAM

VA and Pen Testing

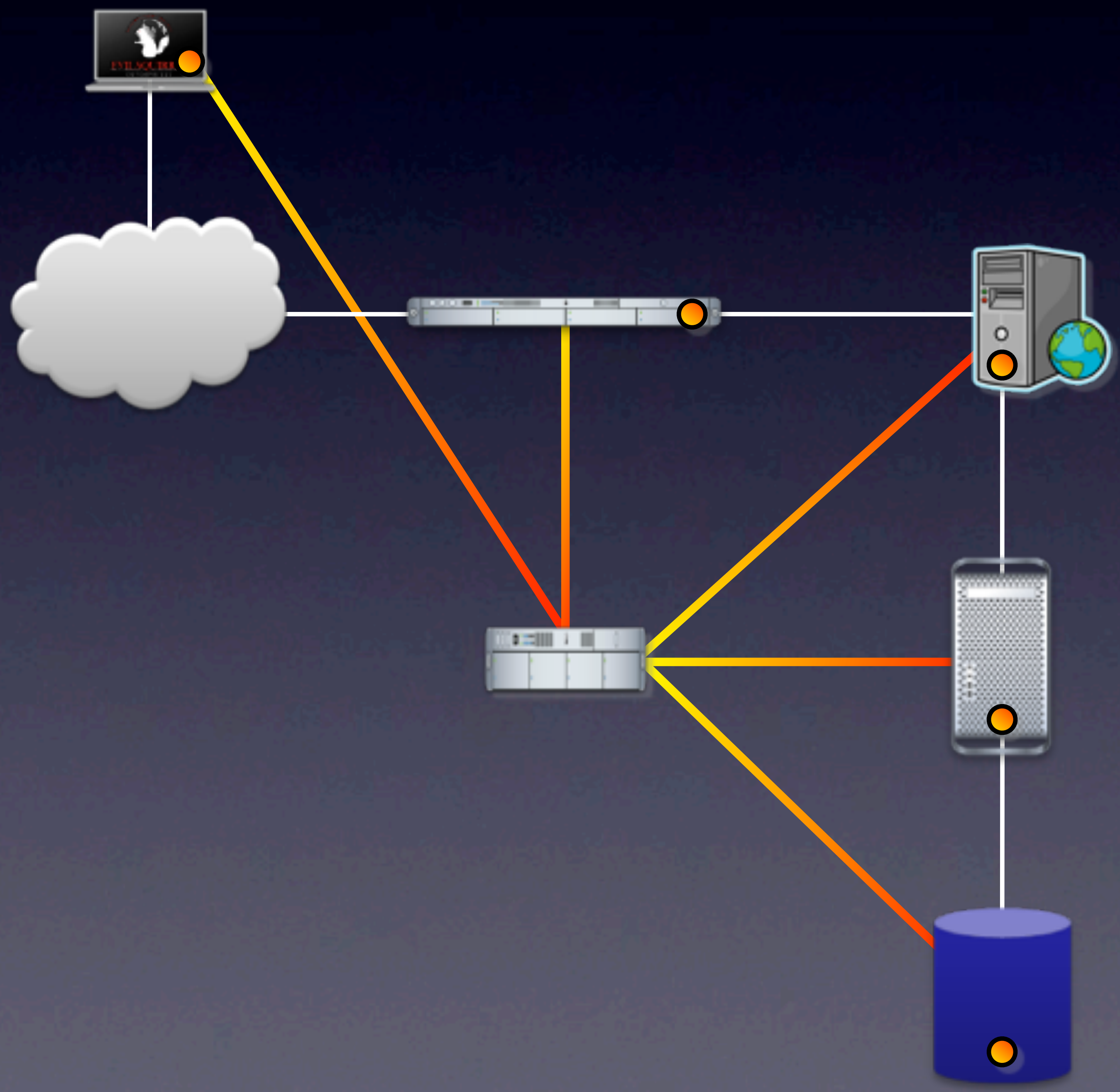
Everything Else

CMP



Securosis

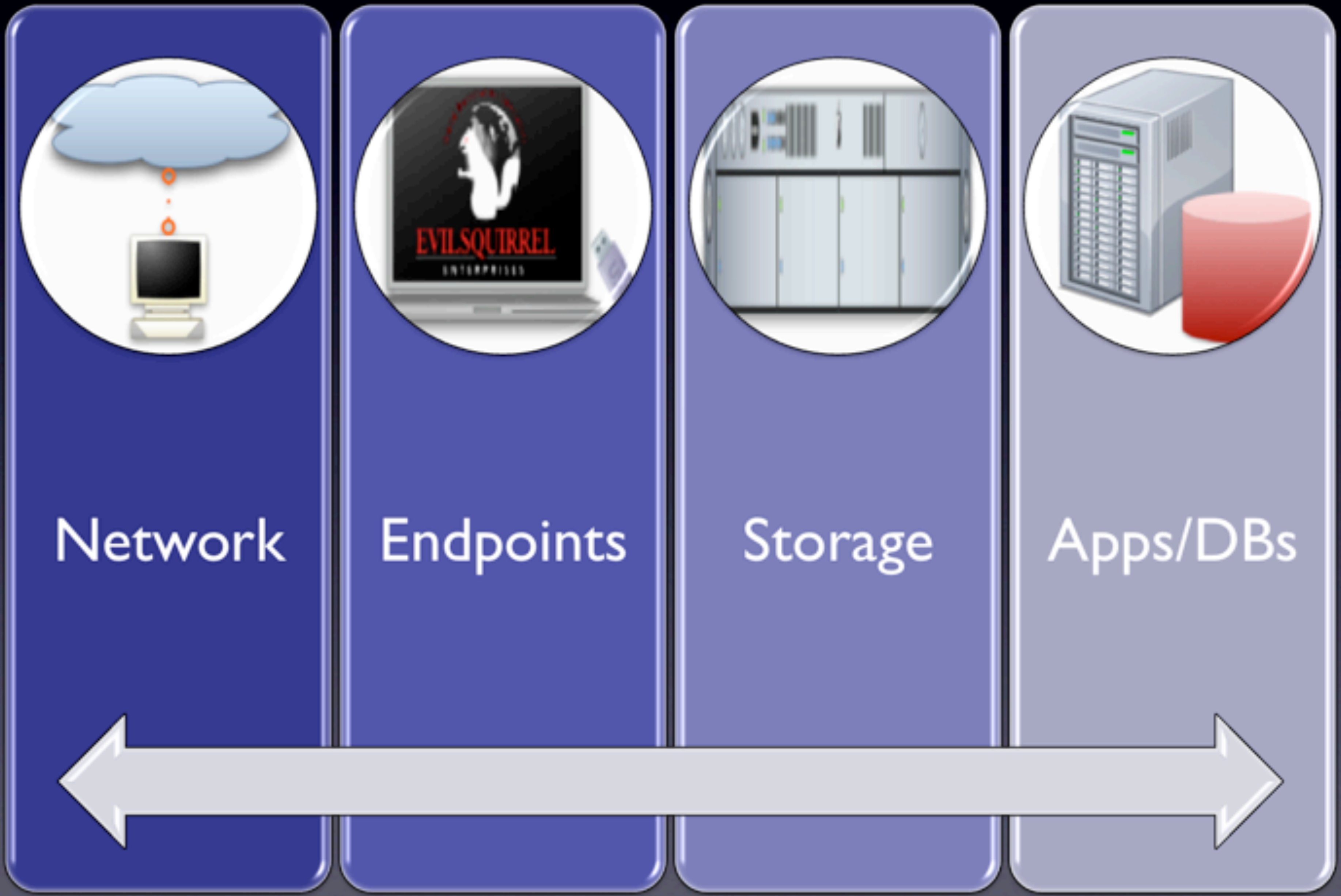
ADMP



Getting Started

Discover

1. Define sensitive data.
2. Find it.
3. Correlate back to users.
4. Assess vulnerabilities and penetration test.



Network

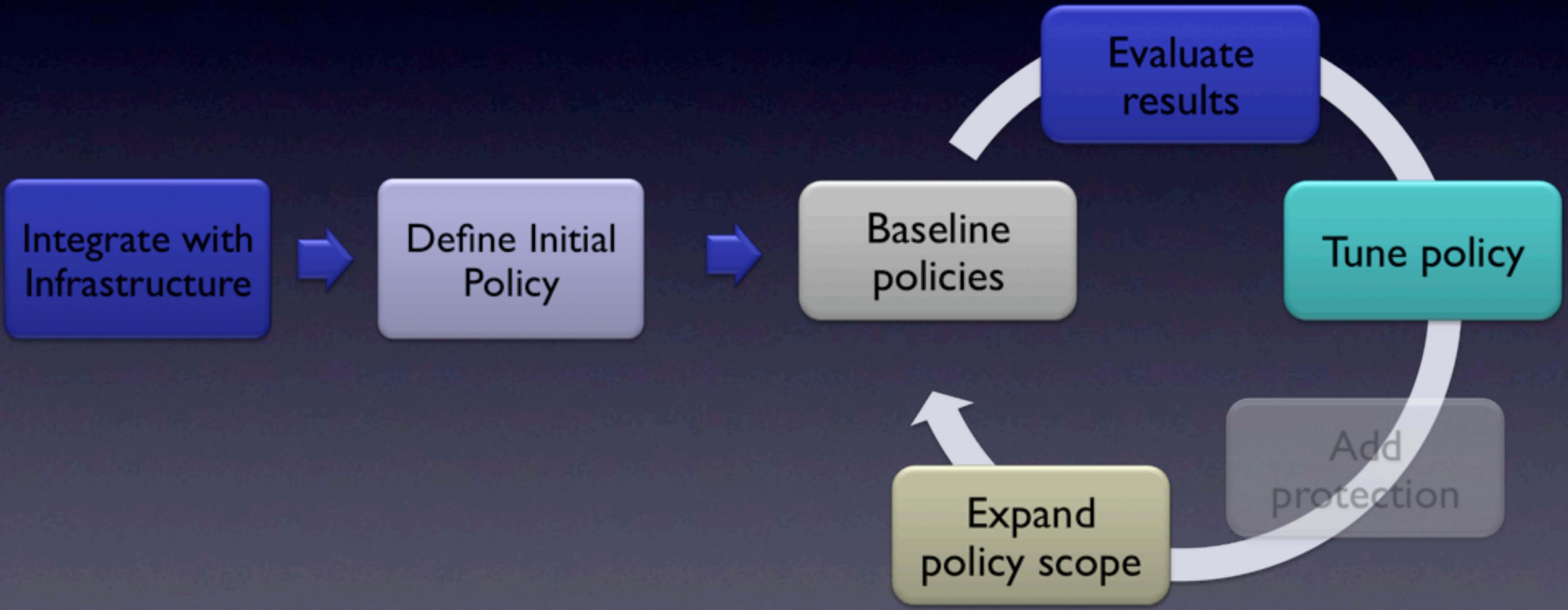
Endpoints

Storage

Apps/DBs

Techniques

DLP	DAM	Network Tools	eDiscovery/ Classification	FOSS
• Network monitoring • Server/ endpoint discovery • Some DB discovery	• DB only • Not all tools support	• WAF/UTM/ IPS/etc. • Many now include RegEx monitoring • Extremely limited	• Servers/ storage • Limited analysis	• Network and storage • Basic RegEx • Some file cracking


Integrate with Infrastructure
Define Initial Policy
Baseline policies
Evaluate results
Tune policy
Add protection
Expand policy scope

Securosis

VA and Pen Testing

- Find vulnerabilities
  - Focus on sensitive data stores.
  - Use specialized tools for web apps and databases.
- Penetration test
  - Validates risks.
  - Determines information exposure.

Securosis

What You Should Do

- Start with 1-3 data types.
- Use CMP/DLP to find them in storage and on endpoints.
- Use DAM/ADMP (or CMP) to find in databases.
- FOSS tools can help for basic data/PII, but not IP.

Secure

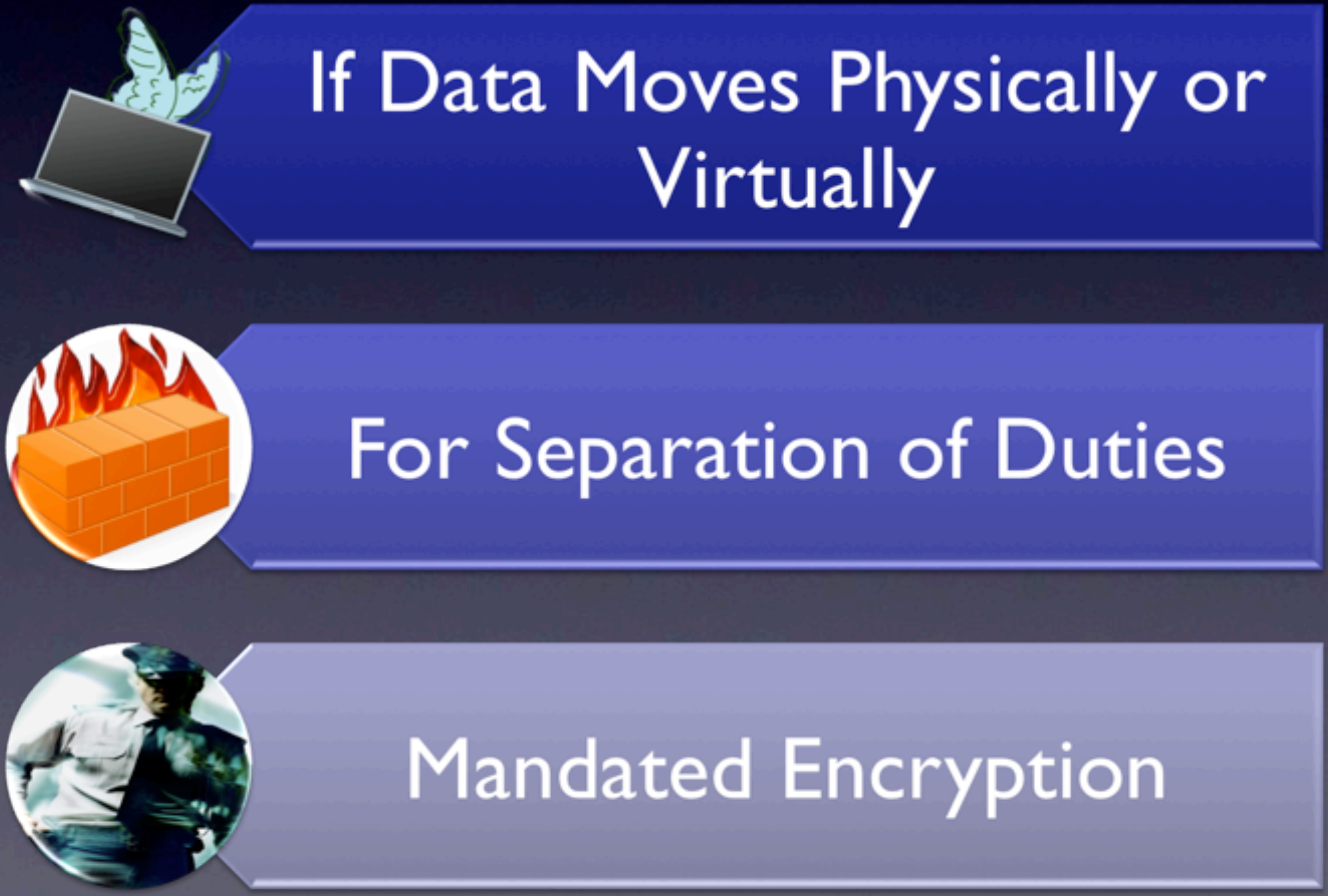
- Fix access controls.
- Remove unneeded data.
- Lock down access channels.
- (Maybe) encrypt

Access Controls

Encryption

DRM

The Three Laws of Encryption



If Data Moves Physically or Virtually

For Separation of Duties

Mandated Encryption

Where to Encrypt

Separation of Duties

- Database Fields
- Workstation File/Folder
- Server
- NAS
- Applications

Movement/Media Protection

- Tape
- SAN
- Laptops/FDE
- Email
- Portable Media

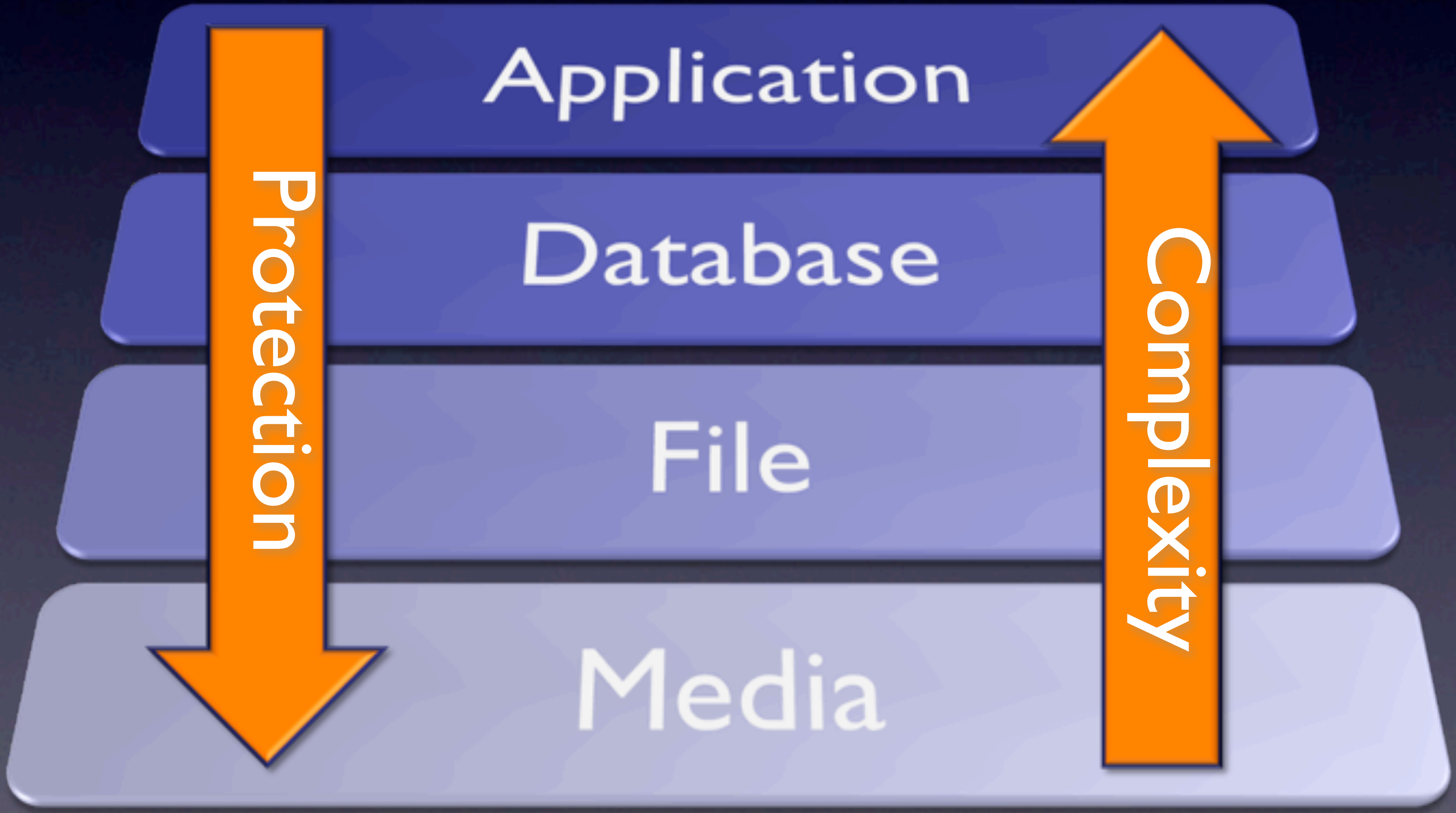
Encryption Options

File/Folder

Application/
Database

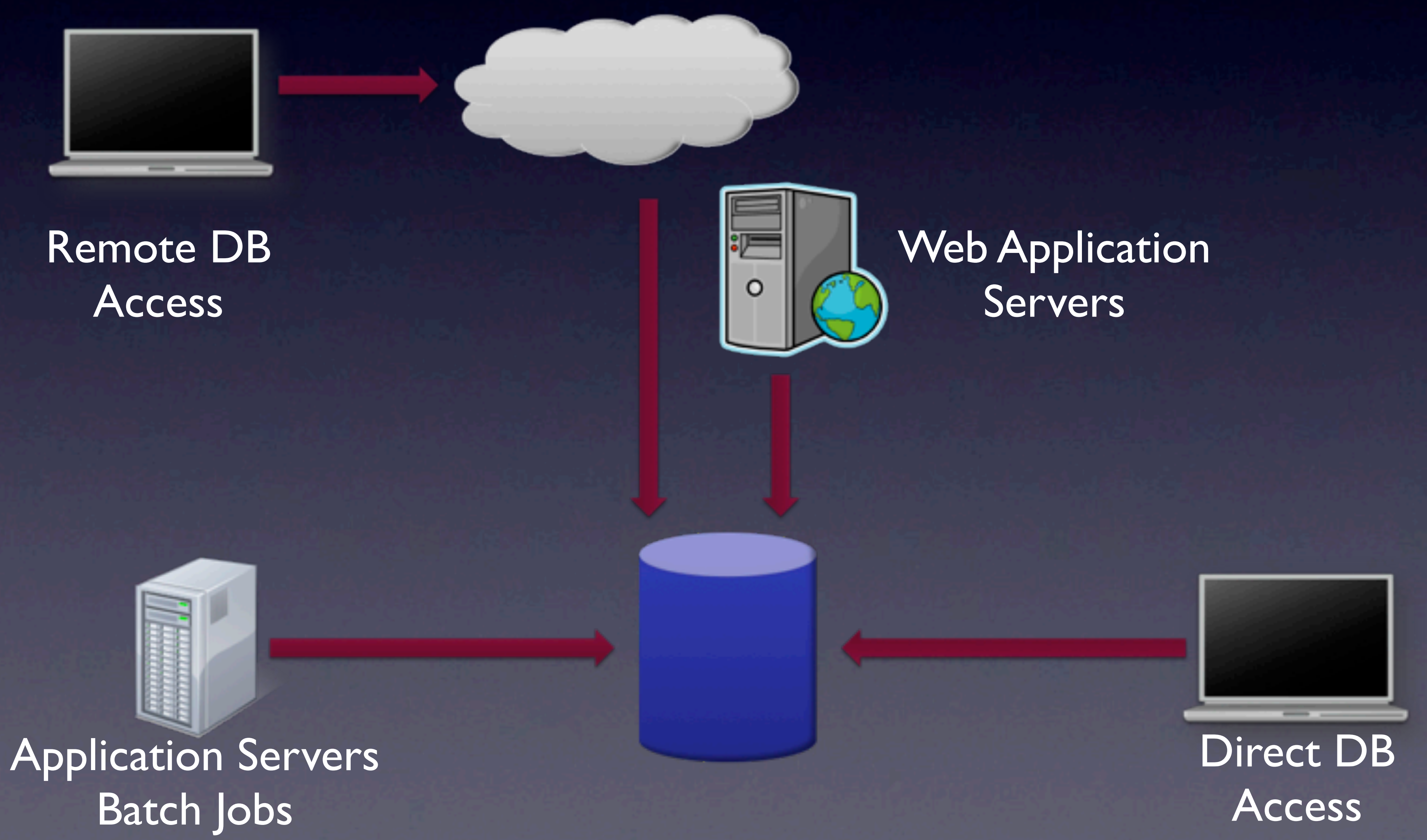
Media

Encryption Layers



Securosis

Access Channels



Remote DB Access

Web Application Servers

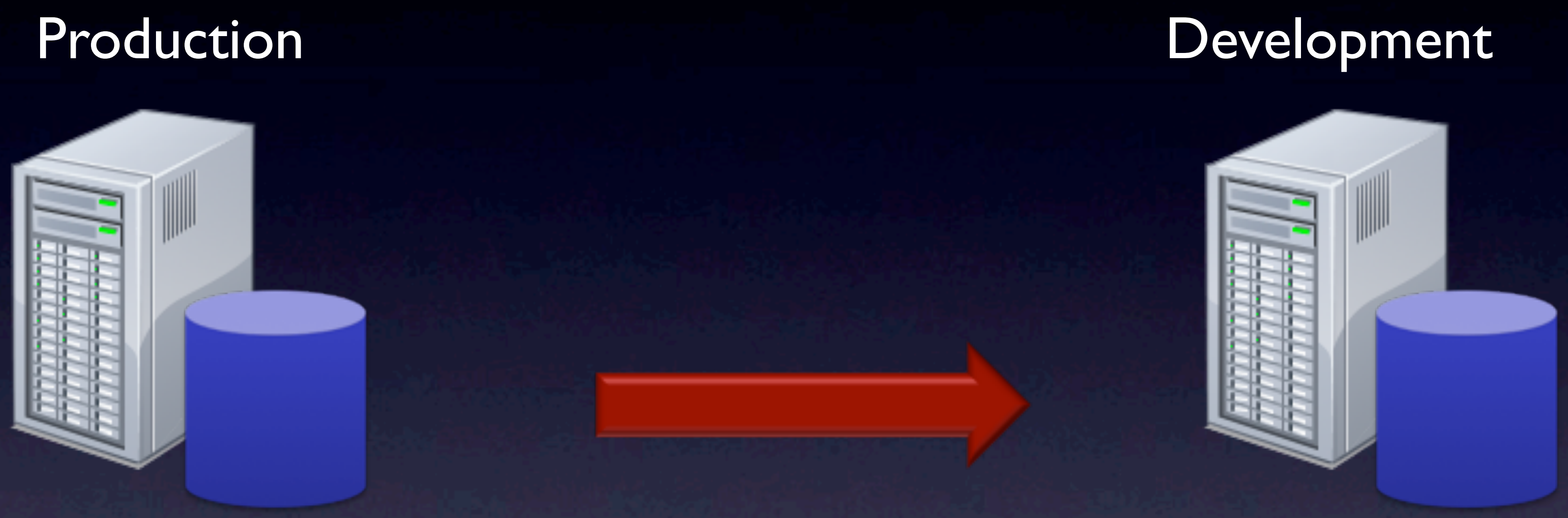
Application Servers Batch Jobs

Direct DB Access

Securosis

Data Masking

Data Masking



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

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

What You Should Do

- Remove/quarantine viral data.
- If you can't map access controls to users, just lock it down and manage exceptions.
- Encrypt laptops, backup tapes, and portable media.
- Lock down application and database access channels.
- Begin data masking.

Monitor

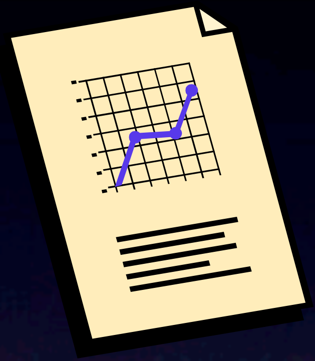
- DLP/CMP for the network, storage, and endpoints.
- DAM/ADMP for databases.
- Egress filtering.
- Other tools may help, but give a false sense of security.

Content Analysis

Content Analysis

Partial Document Matching

Database Fingerprinting



Statistical

Exact File Matching

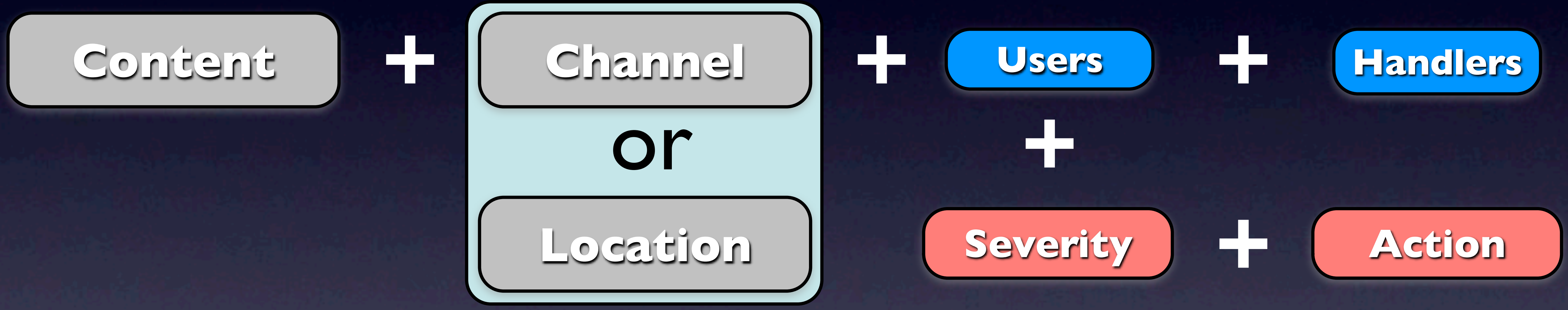
Categories

Conceptual

```
^(?:(?<Visa>4\d{3})|(?<Mastercard>5[1-5]\d{2})|(?<Discover>6011)|(?
<DinersClub>(?:3[68]\d{2})|(?:30[0-5]\d))|(?
<AmericanExpress>3[47]\d{2}))([ -]?)(?(DinersClub)(?:\d{6}\1\d{4})|(?
(AmericanExpress)(?:\d{6}\1\d{5})|(?:\d{4}\1\d{4}\1\d{4})))$
```

Rules

Policy Creation



Content + Channel or Location + Users + Handlers

+

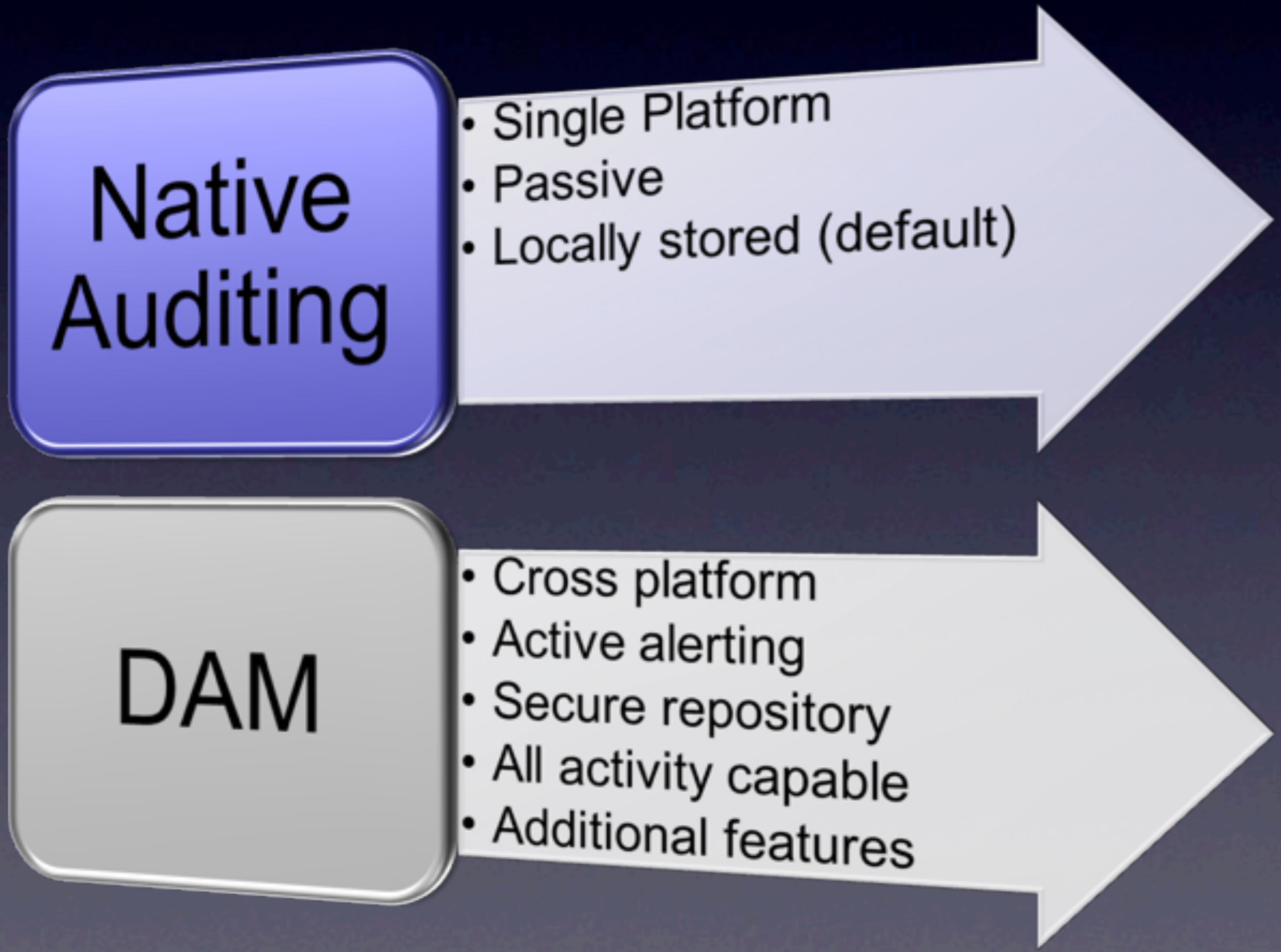
Severity + Action

Directory Integration
Application Integration
Agent Management

Incident Management

ID	Time	Policy	Channel/ Location	Severity	User	Action	Status
1138	1625	PII	/SAN1/files/	1.2 M	rmogull	Quarantine	Open
1139	1632	HIPAA	IM	2	jsmith	Notified	Assigned
1140	1702	PII	Endpoint/ HTTP	1	192.168.0.213	None	Closed
1141	1712	R&D/Product X	USB	4	bgates	Notified	Assigned
1142	1730	Financials	//sjobs/C$	4	sjobs	Quarantine	Escalated

DB Auditing vs. Activity Monitoring



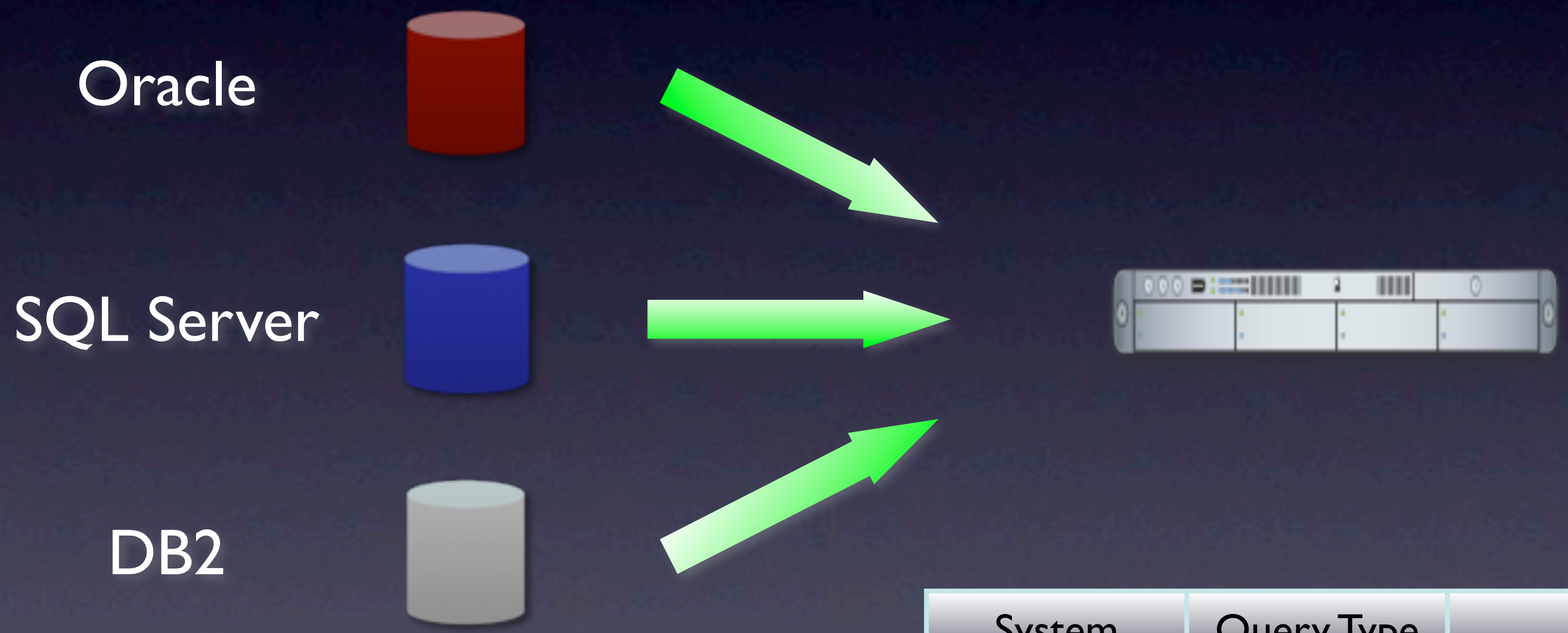
Native Auditing

- Single Platform
- Passive
- Locally stored (default)

DAM

- Cross platform
- Active alerting
- Secure repository
- All activity capable
- Additional features

Aggregation and Correlation



Oracle

SQL Server

DB2

System	Query Type	...
Or1	Select	
MS23	Update	

Alternatives/Adjuncts

- SIEM
  - Many SIEM tools now include DAM support, or can pull (some of) audit logs.
- Log Management
  - Many also now include some database support
- Triggers
  - A bad option, but free and might be good enough under some circumstances

Securosis

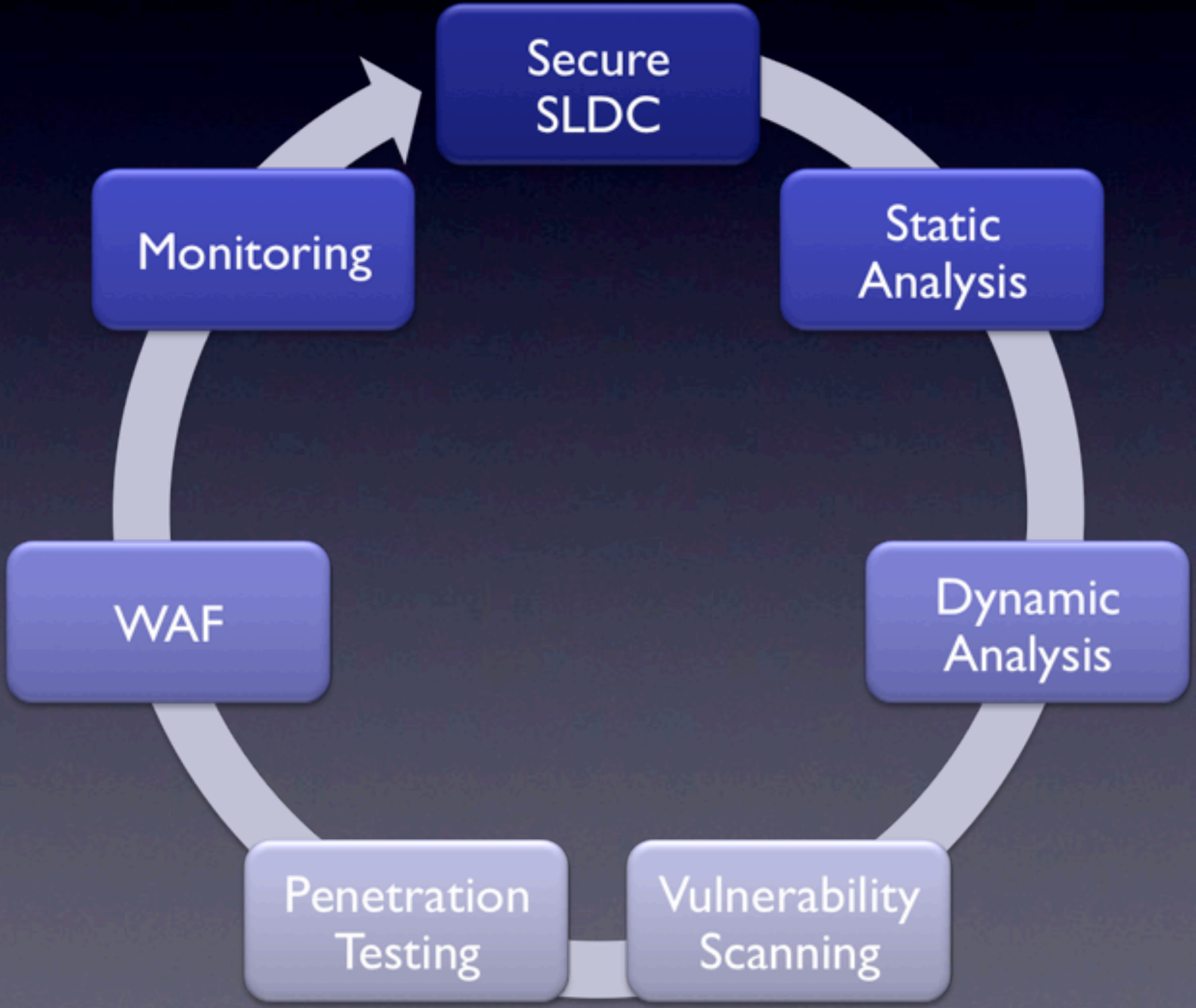
What You Should Do

- Focus network DLP/CMP on transaction areas first, since that's where the worst losses occur.
- Use DAM on priority databases, then expand.
- Other logging/monitoring can help, but is not content specific, and won't give great results.
- Monitor sensitive data on endpoints with DLP, especially portable storage transfers.

Protect

- Secure web applications.
- Validate encryption.
- Use DLP/CMP for network communications and endpoints.
- Set DAM policies for proactive alerting.

Web Application Security



Securosis

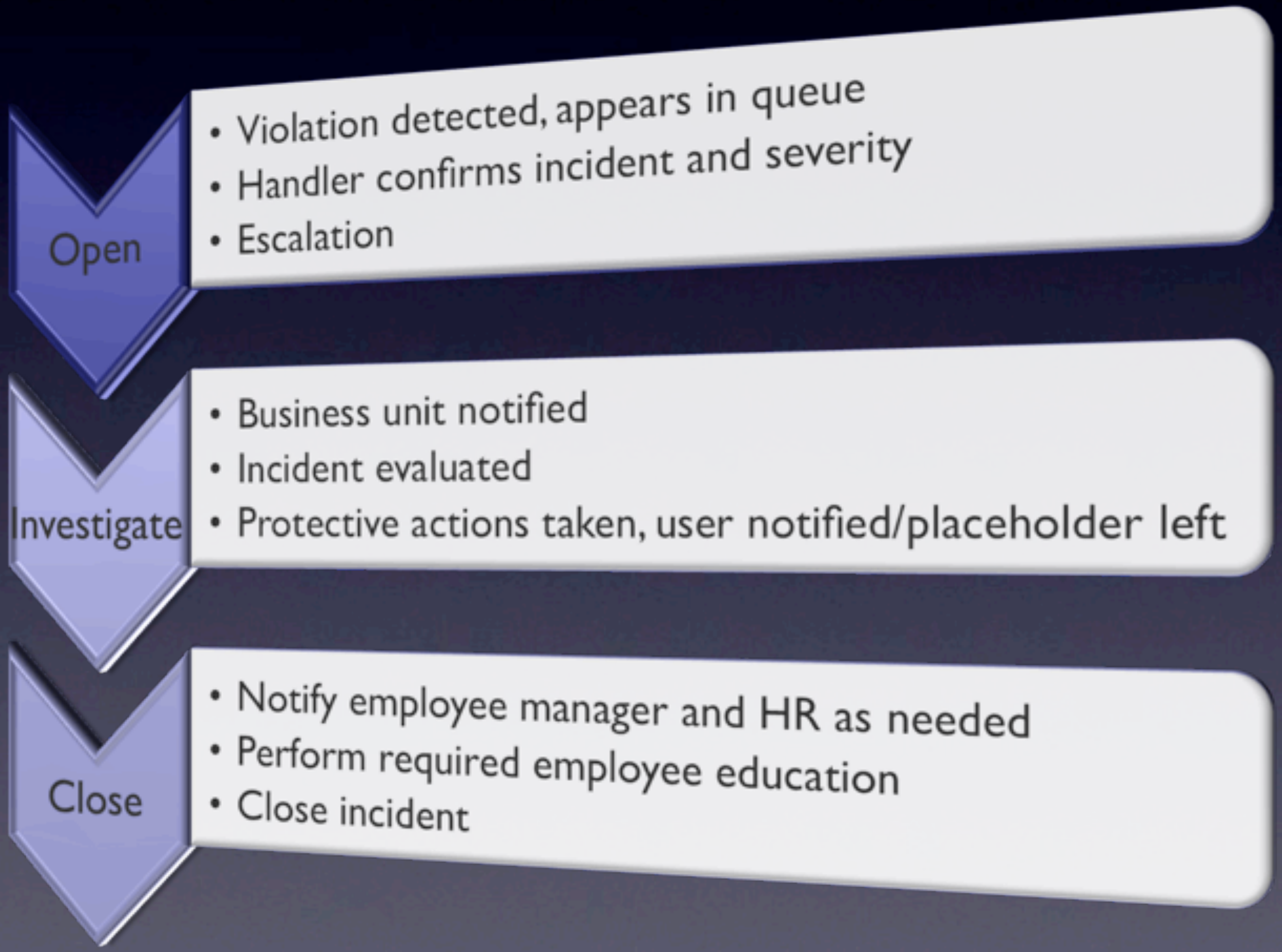
CMP Deployment Modes

Passive	• Monitoring only
Bridge	• Block, but some data leaks
Proxy	• Full blocking • Often requires integration

Endpoint Options

- DLP/CMP for content-based blocking.
- Portable device control or encryption for gross protection.
- Monitor/shadow files with CMP or PDC.

Defining Process



Open

- Violation detected, appears in queue
- Handler confirms incident and severity
- Escalation

Investigate

- Business unit notified
- Incident evaluated
- Protective actions taken, user notified/placeholder left

Close

- Notify employee manager and HR as needed
- Perform required employee education
- Close incident

Egress Filtering

- Segregate sensitive networks/transactions paths
- Lock channels with firewall/UTM
- Filter content with DLP
- Application control/next gen firewalls
- Hide behind a VPN

What You Should Do

- WAFs offer the quickest protection for web applications.
- DLP/CMP for network monitoring and blocking.
    - You may use existing email and network tools to protect PII, but it will be more difficult to manage and offer less protection.
- PDC or DLP/CMP for endpoint data protection (on top of encryption).

Data Security on the Cheap

- Focus on as few critical data types as possible.
- Use FOSS or existing tools for discovery.
- Prioritize with VA and penetration testing.
- Leverage features in existing tools.
  - Email/web filtering
  - USB blocking
  - OS-based encryption

Securosis

Your Best Options

- Start with DLP/CMP content discovery.
- Identify databases with sensitive data, and start activity monitoring (DAM).
    - Focus VA and penetration tests on these systems, especially if accessed via web applications. This is the single biggest channel for major breaches.
- Encrypt all laptops.
- Egress filter transaction networks.
- Slowly minimize use of protected data. Do you *really* need to let that many people access it? Can you consolidate it?

Rich Mogull

Securosis, L.L.C.

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