Putting the "Information" Back in Information Security

Rich Mogull
Securosis

Mainframe

Internet I

NETWORK

Internet II

Jail

Fortress

Zone

Securosis

But what about the information?

Security architectures over the next ten years will focus on information, mobility, ubiquitousness, transparency, collaboration, and openness.

Data

Application

Host

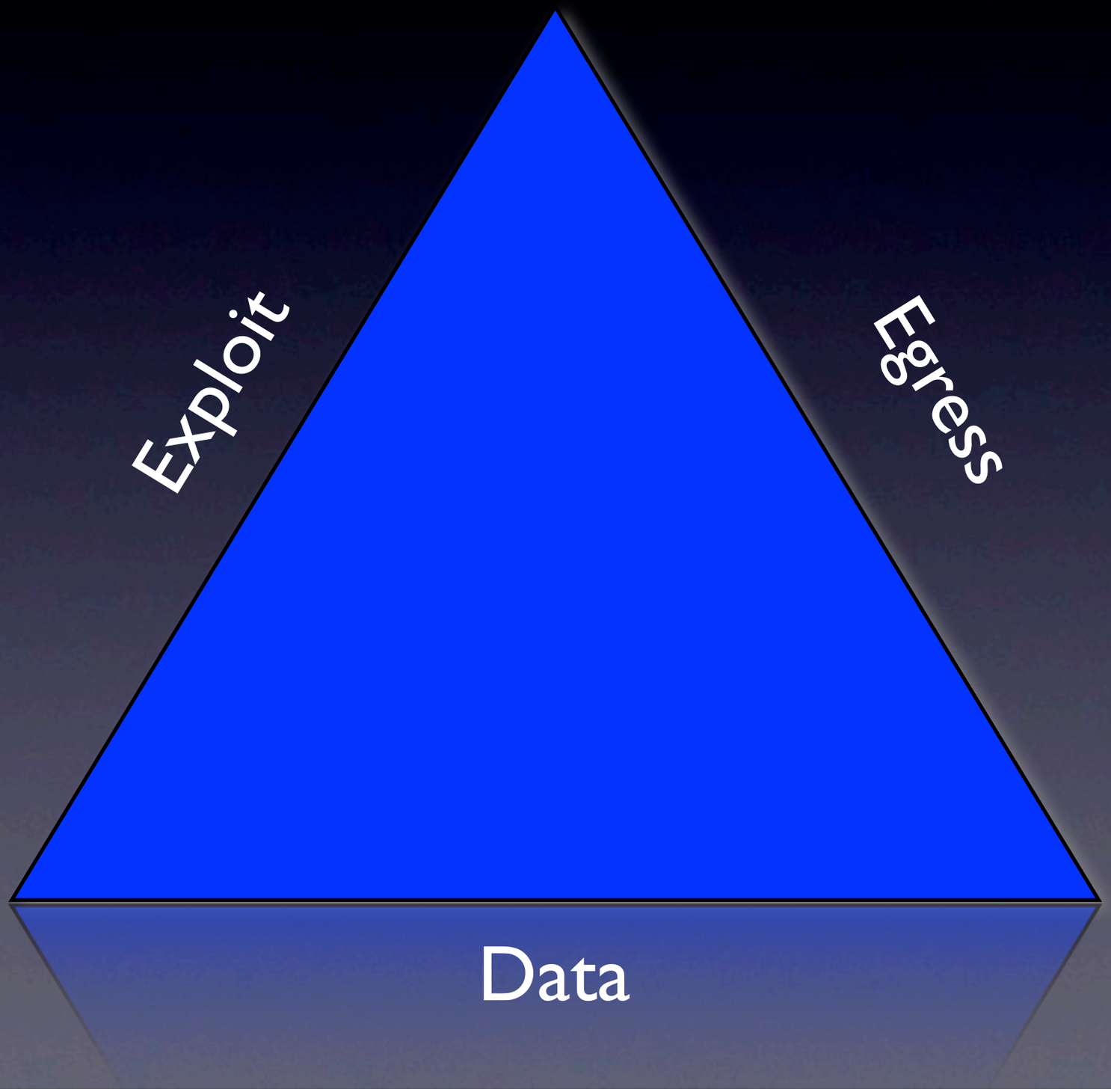
Network

User

Securosis

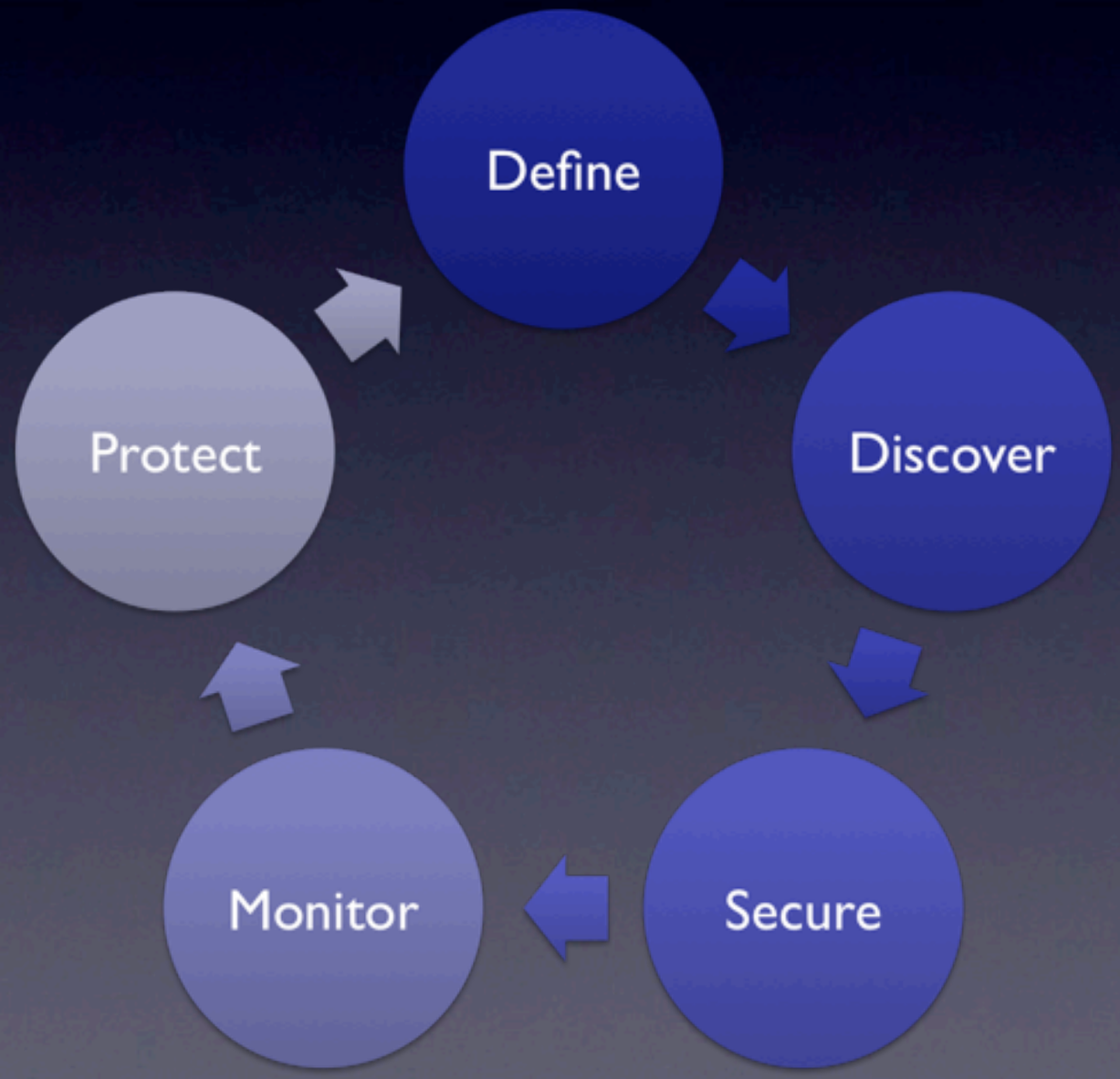
Information-Centric Security

Data Breach Triangle



Securosis

Pragmatic Data Security Cycle



Securosis

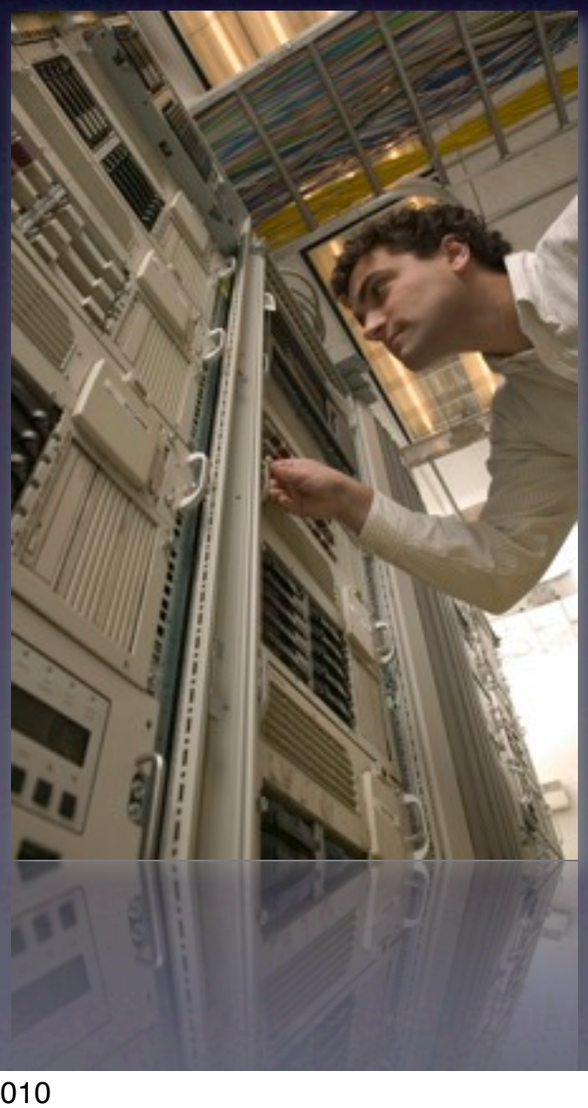
The Pragmatic Philosophy

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

Securosis

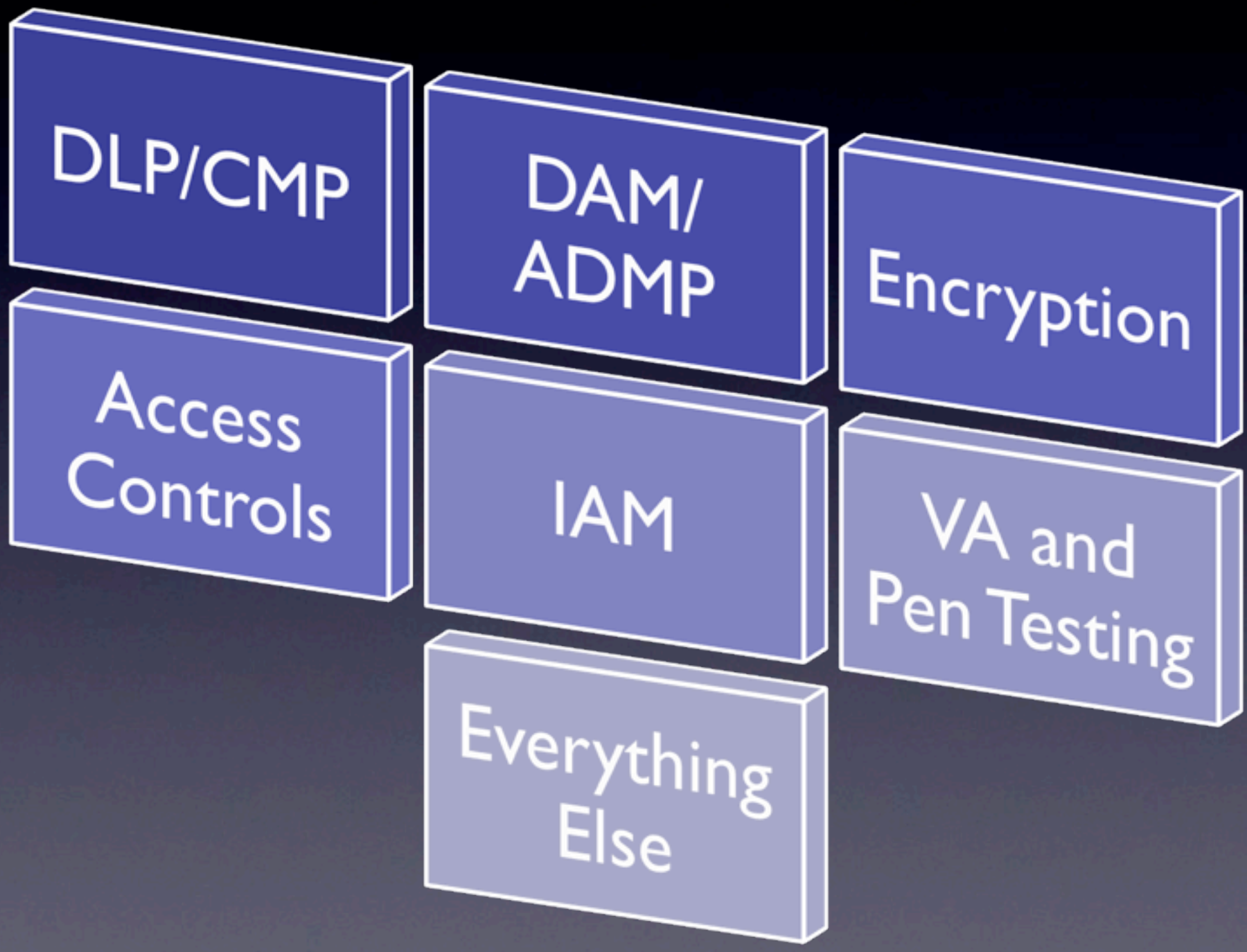
The Two Sides of Data

Data Center



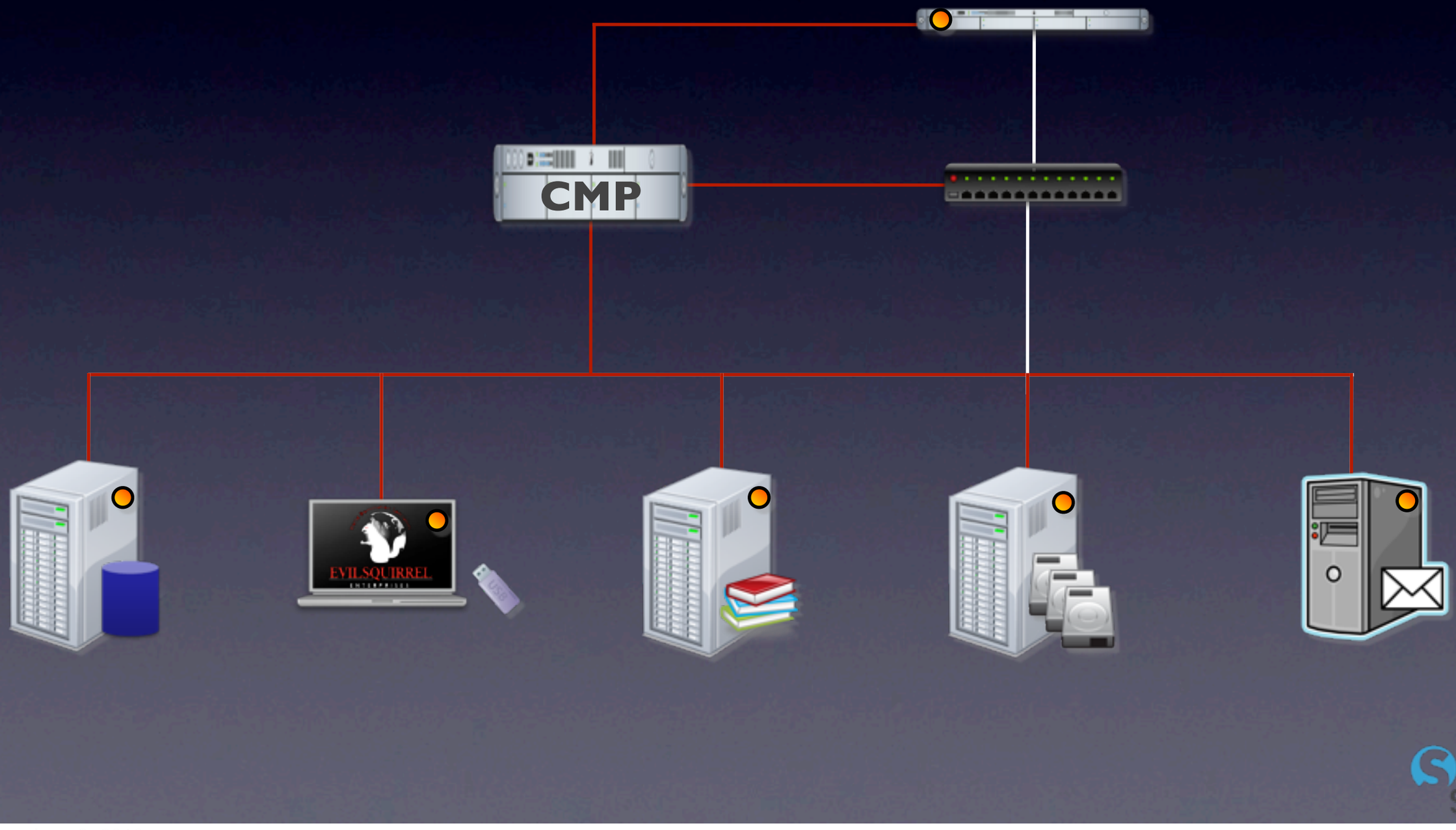
Productivity

Your Arsenal

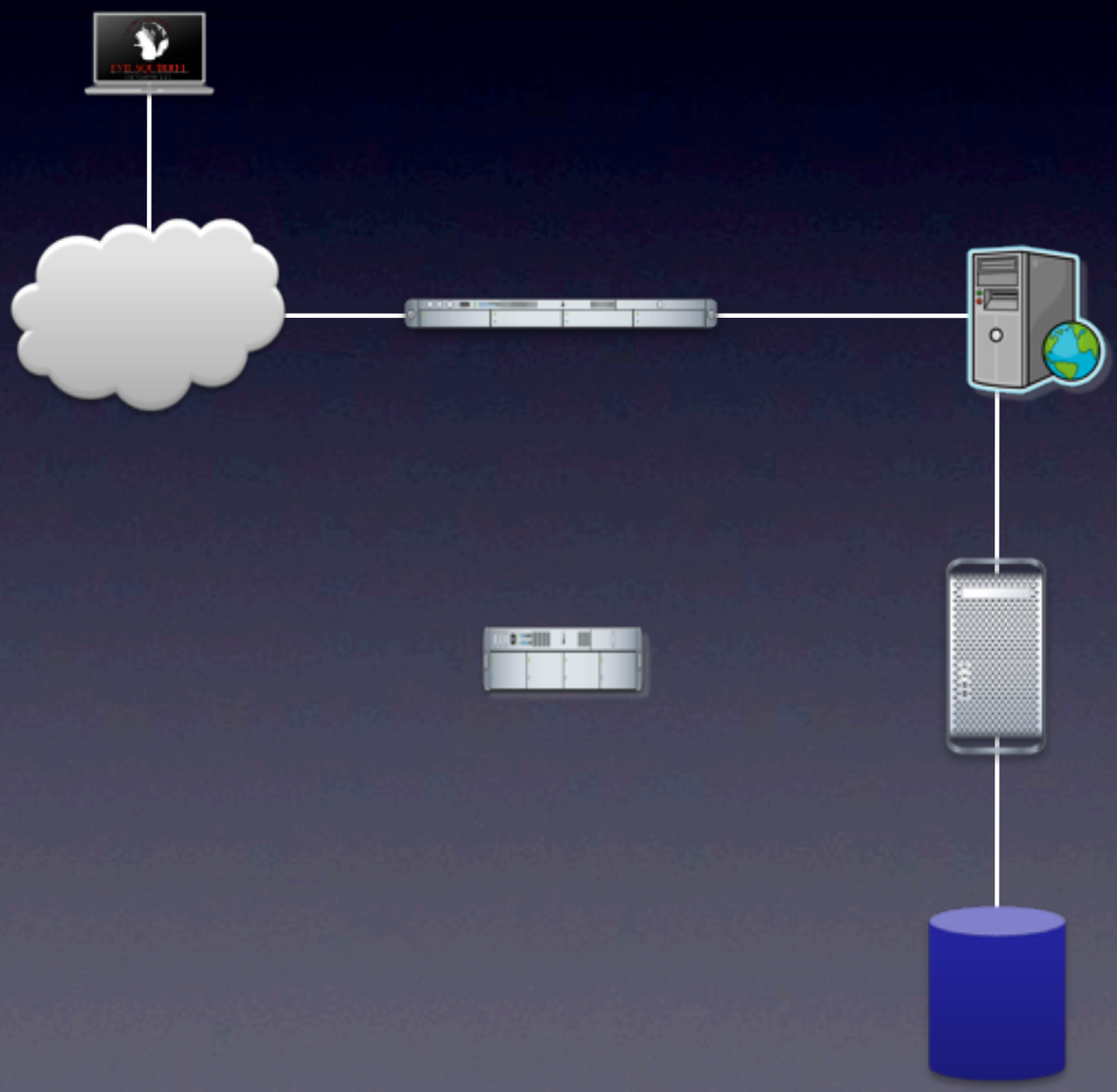


Securosis

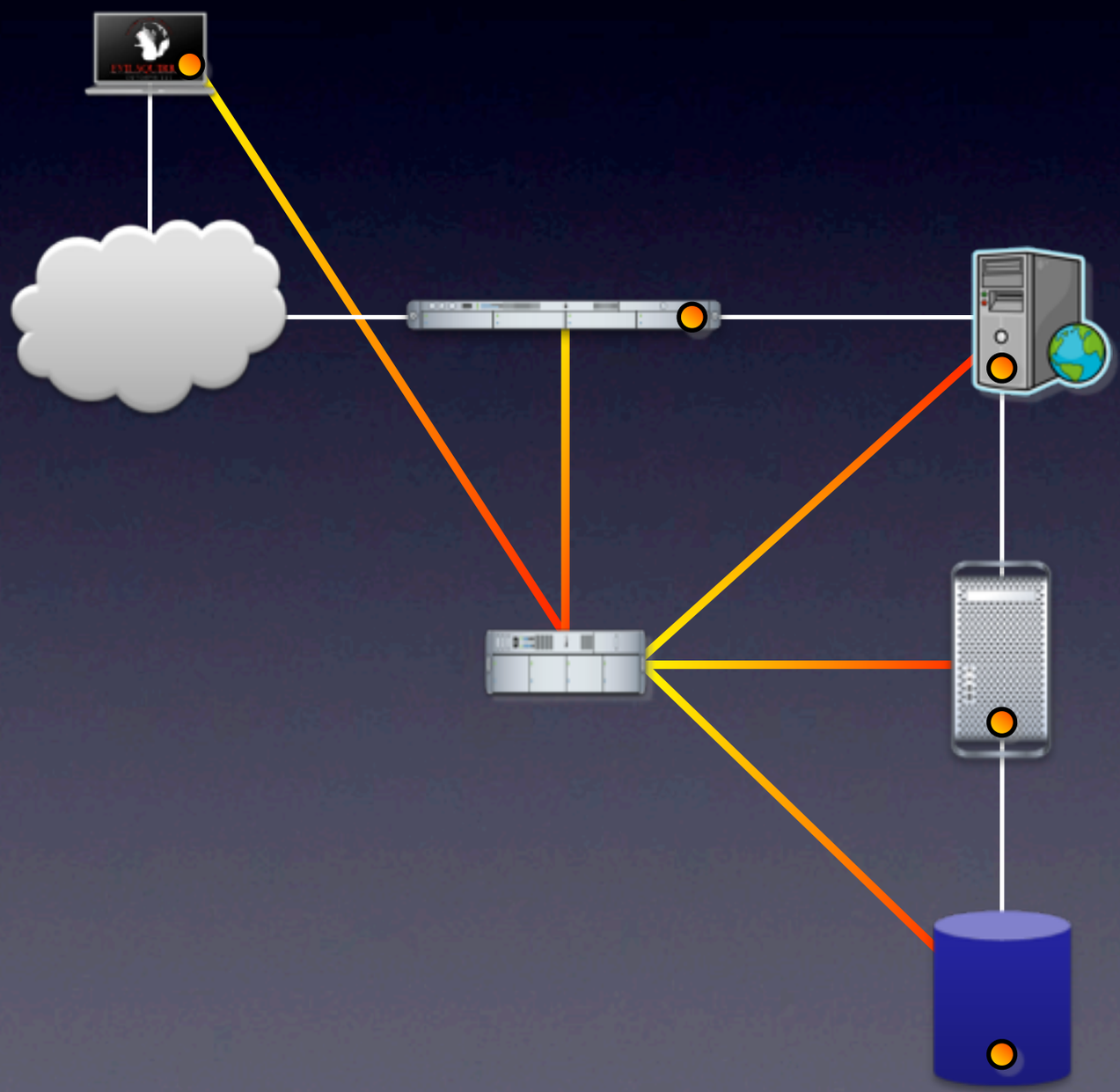
DLP/CMP



ADMP (WAF + DAM)



ADMP (WAF + DAM)

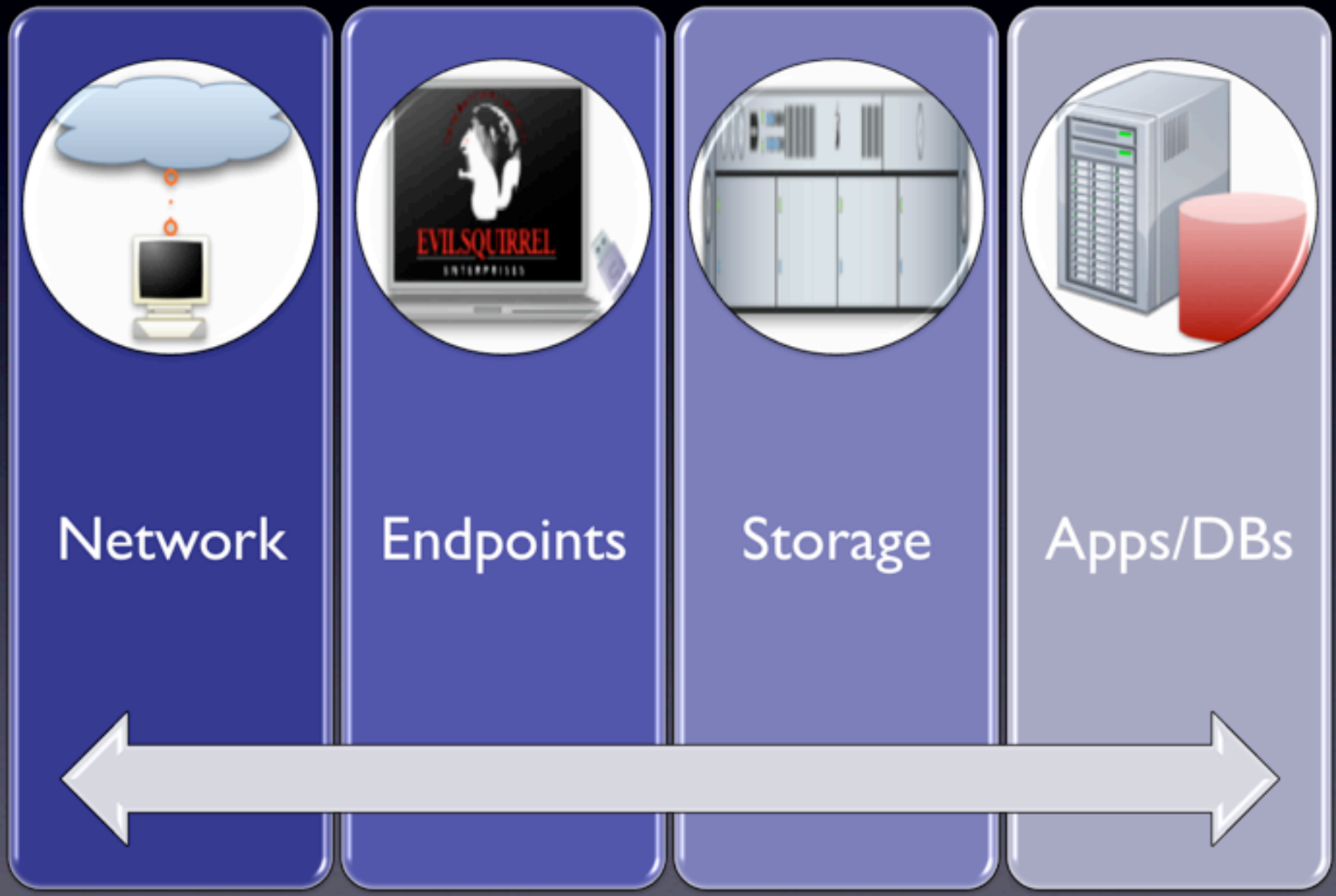


Getting Started

Discover

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

Securosis

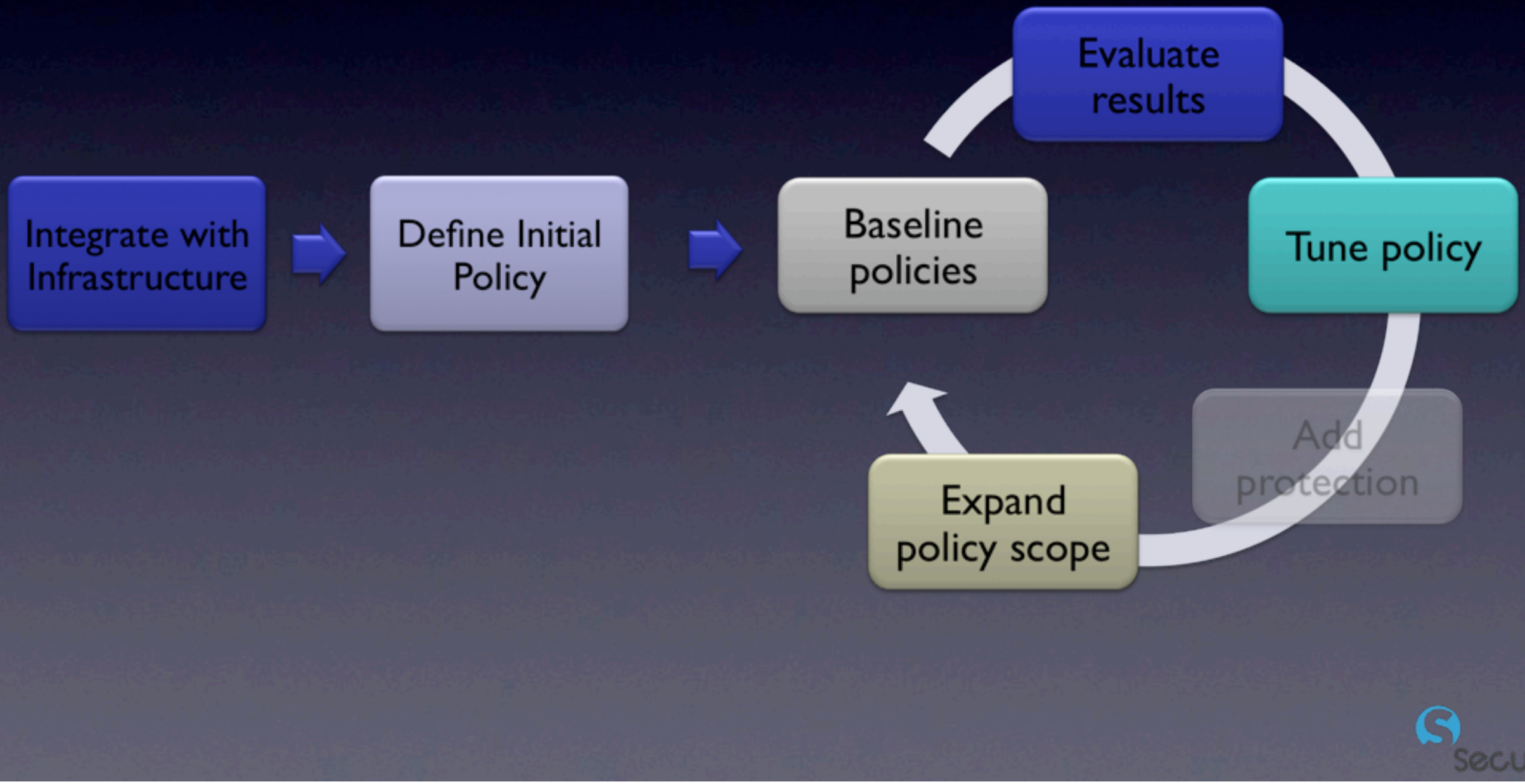

EVILSQUIRREL
ENTERPRISES
Network
Endpoints
Storage
Apps/DBs

Securosis

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

Securosis


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

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.

Securosis

Secure

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

Securosis

Access Controls

Encryption

DRM

Securosis

The Three Laws of Encryption

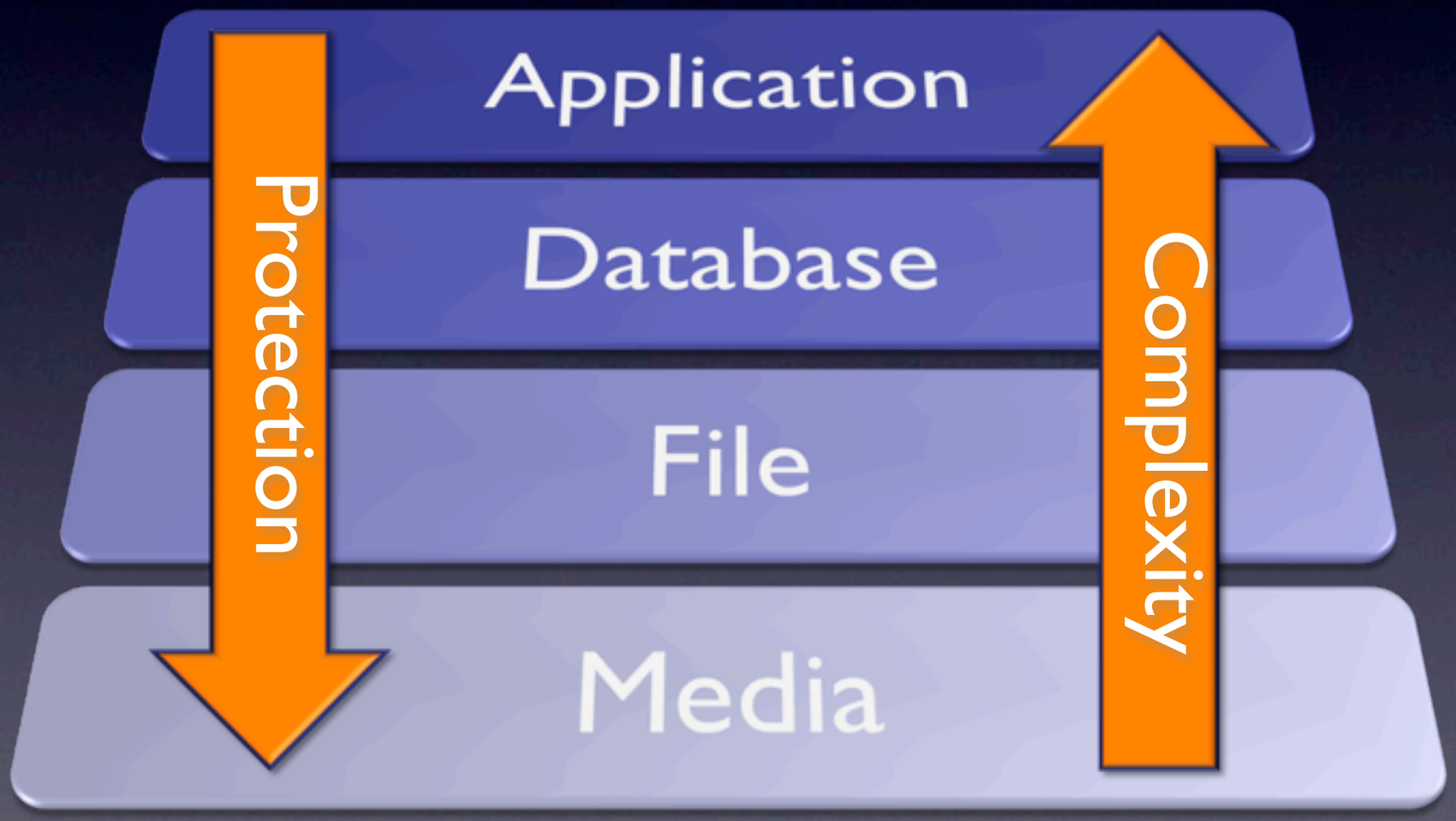
If Data Moves Physically or Virtually

For Separation of Duties

Mandated Encryption

Securosis

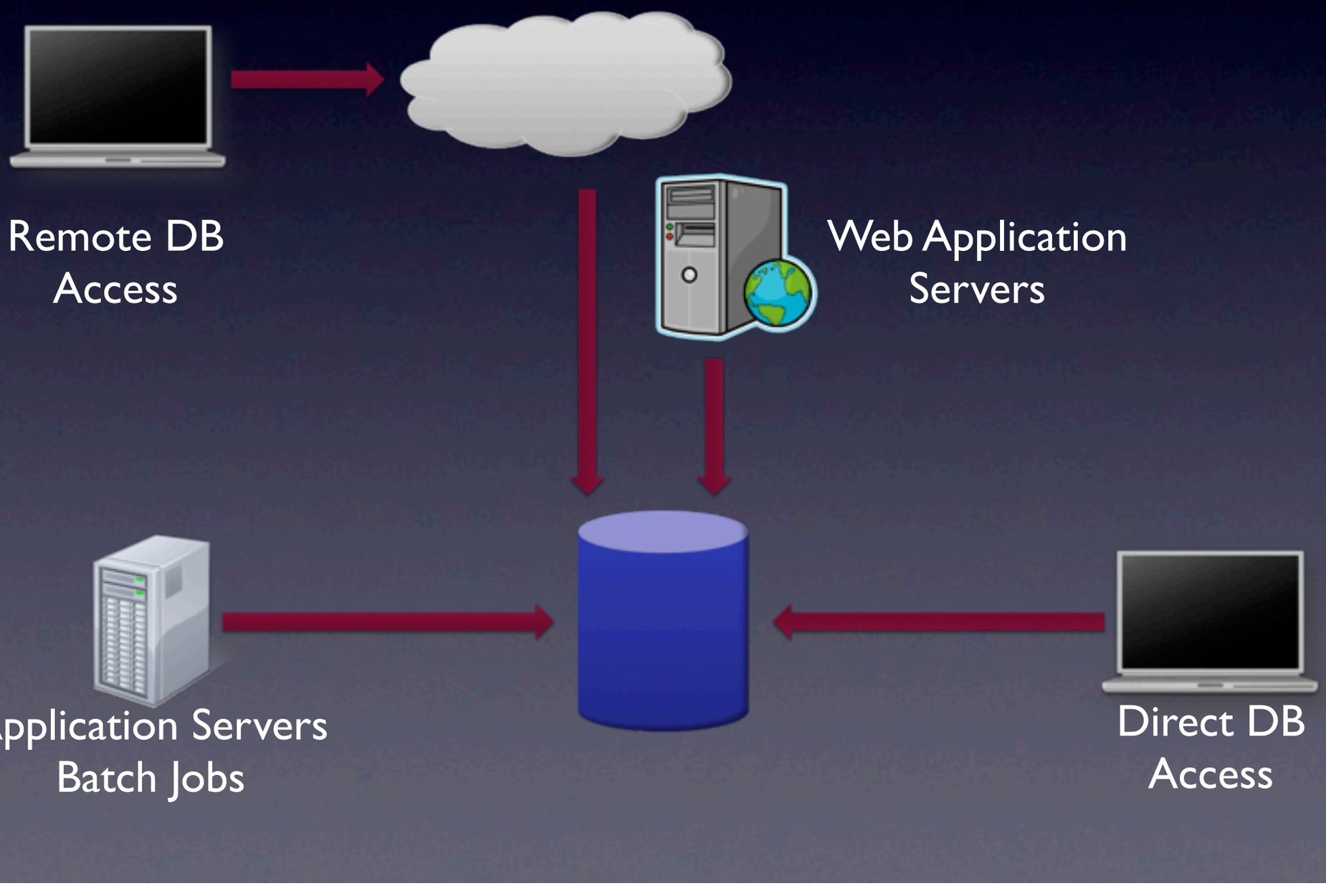
Encryption Layers



Securosis

Tokenization

Access Channels



Data Masking

Production

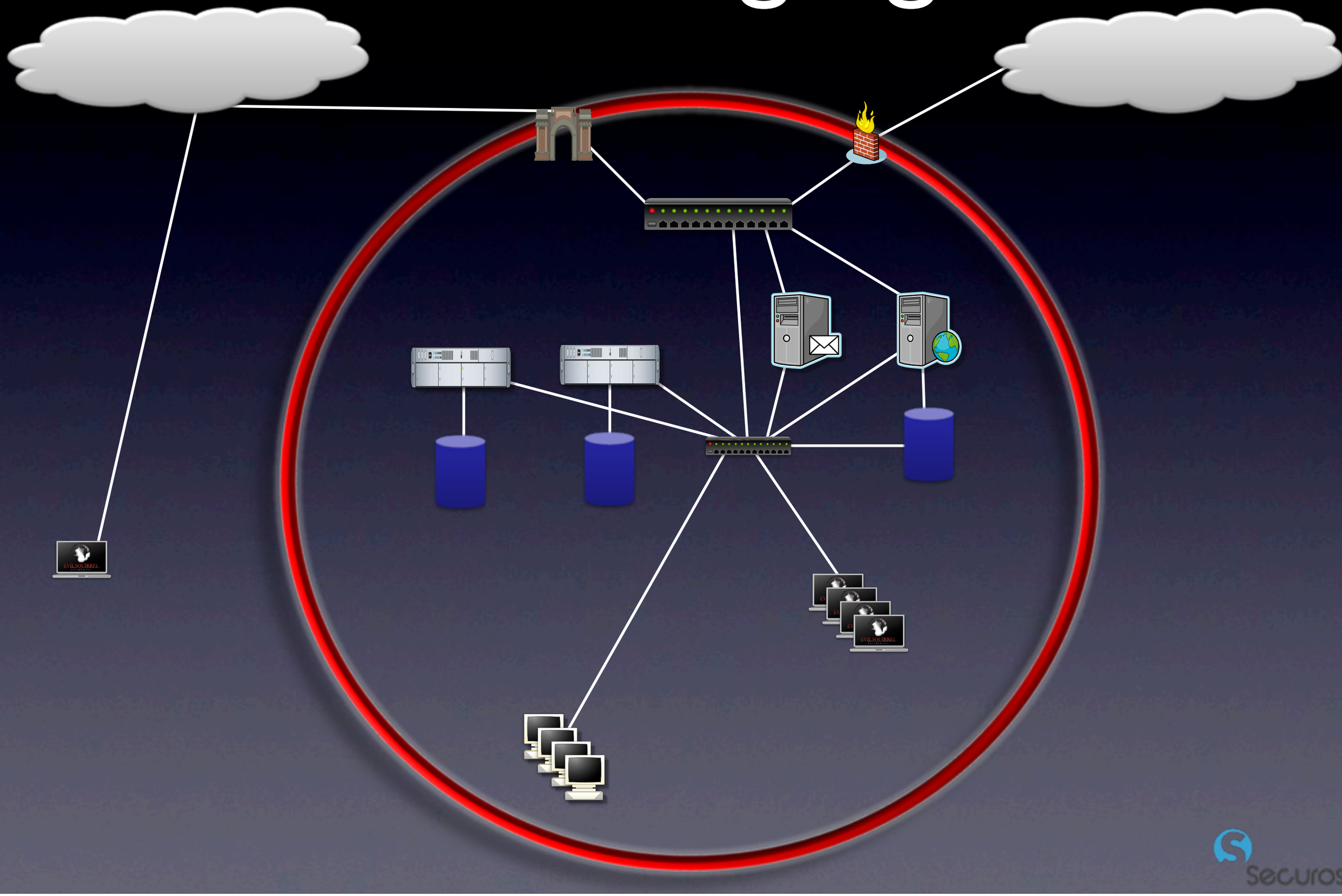
ID	Name	SSN
1	Smith	111-22-3333
2	Jones	444-55-6666
3	Doe	777-88-9999

Development

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

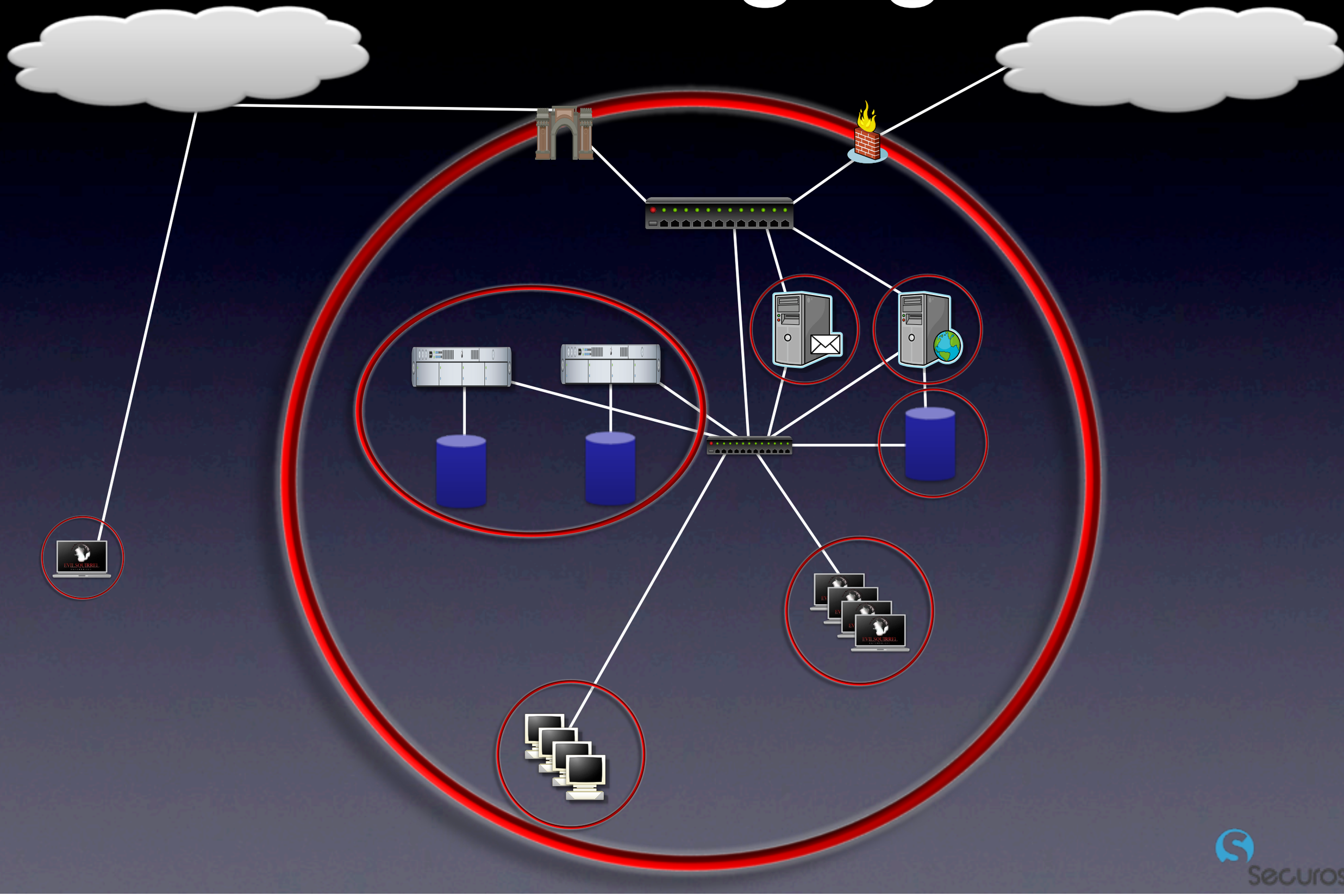
Securosis

Network Segregation



Securosis

Network Segregation



Securosis

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.

Securosis

Monitor

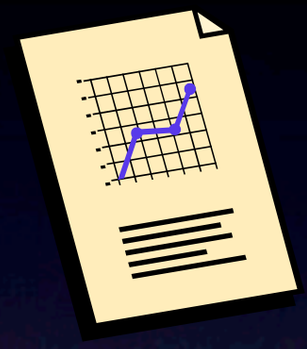
- DLP/CMP for the network, storage, and endpoints.
- DAM/ADMP for databases.
- Egress filtering.
- Other tools may help, but give a false sense of security.

Securosis

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

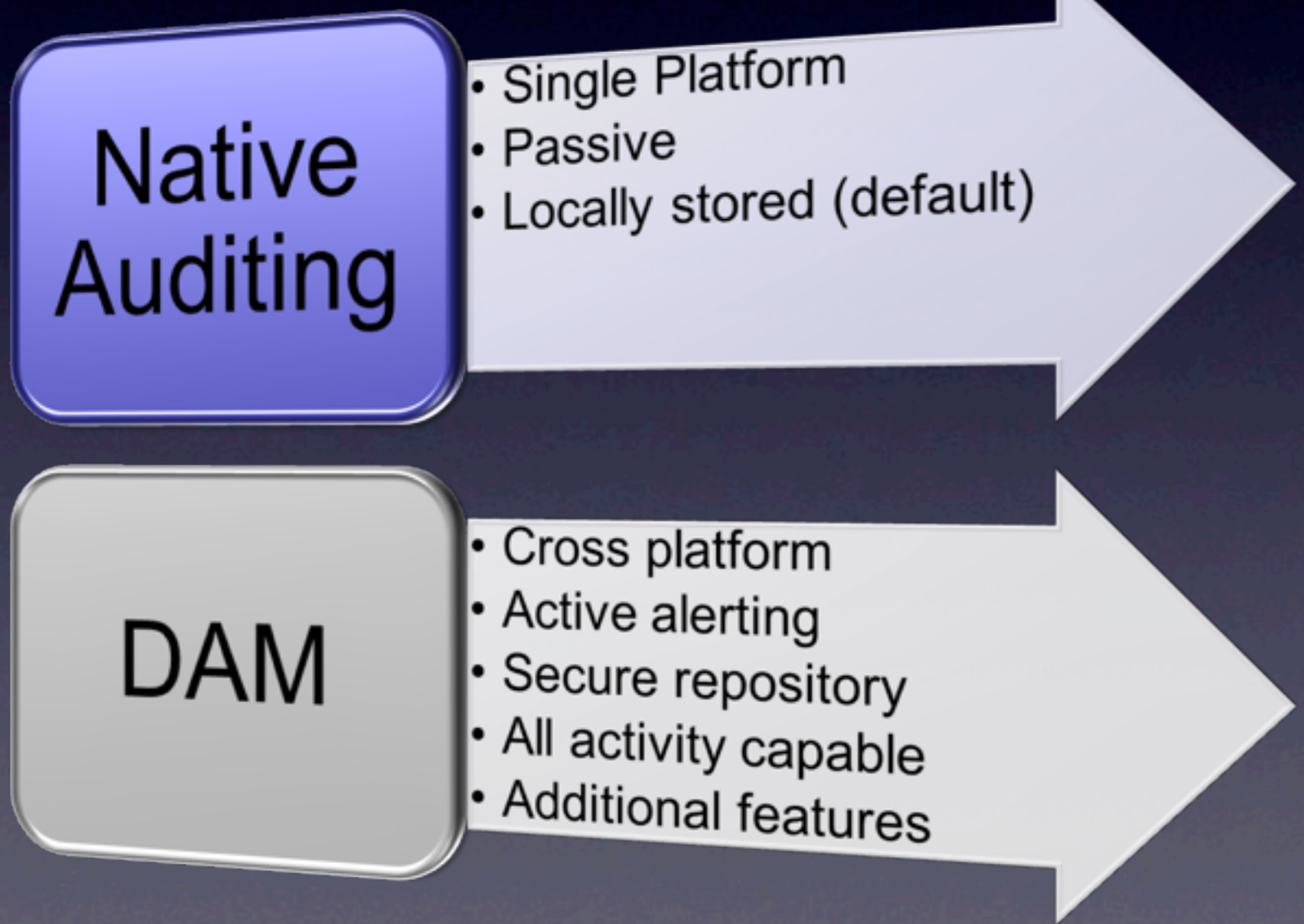
Securosis

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

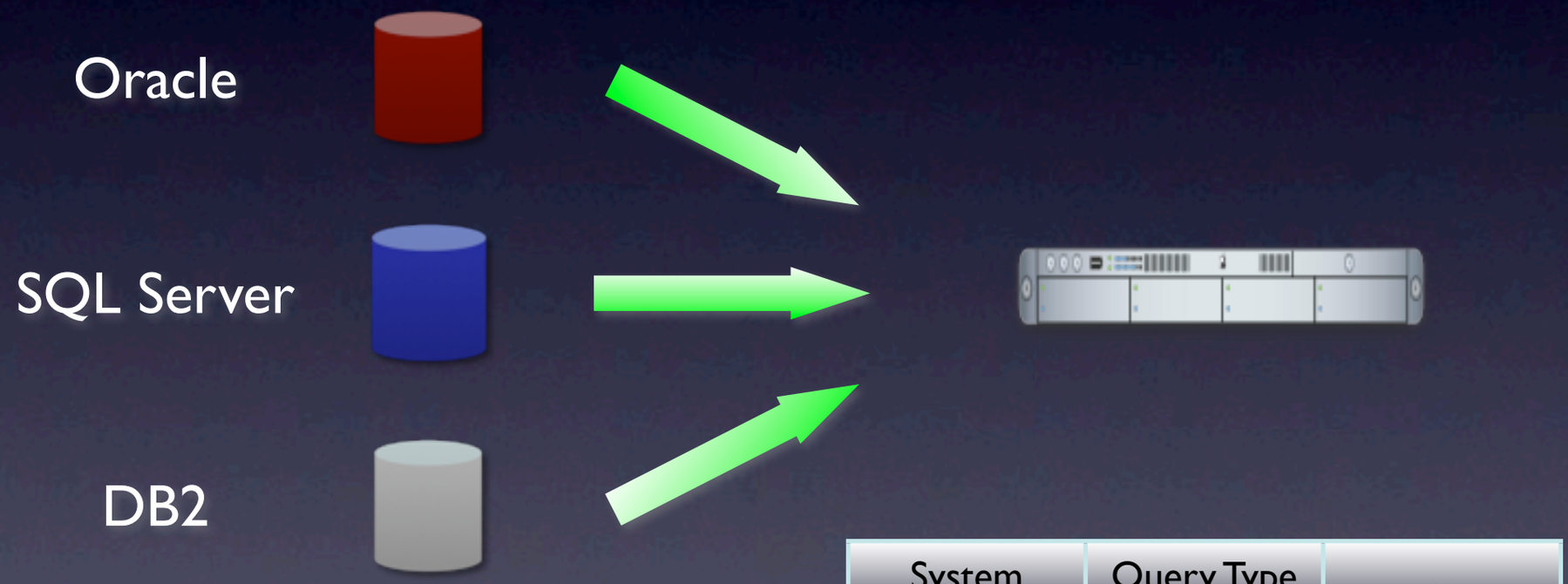
Securosis

DB Auditing vs. Activity Monitoring



Securosis

Aggregation and Correlation



System	Query Type	...
Or1	Select	
MS23	Update	

Securosis

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

Network Security Monitoring

- Network monitoring for data security is now absolutely essential for financial services.
- Deep packet inspection and egress filtering.
- *Must* have proactive alerting, especially on transaction networks.

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.

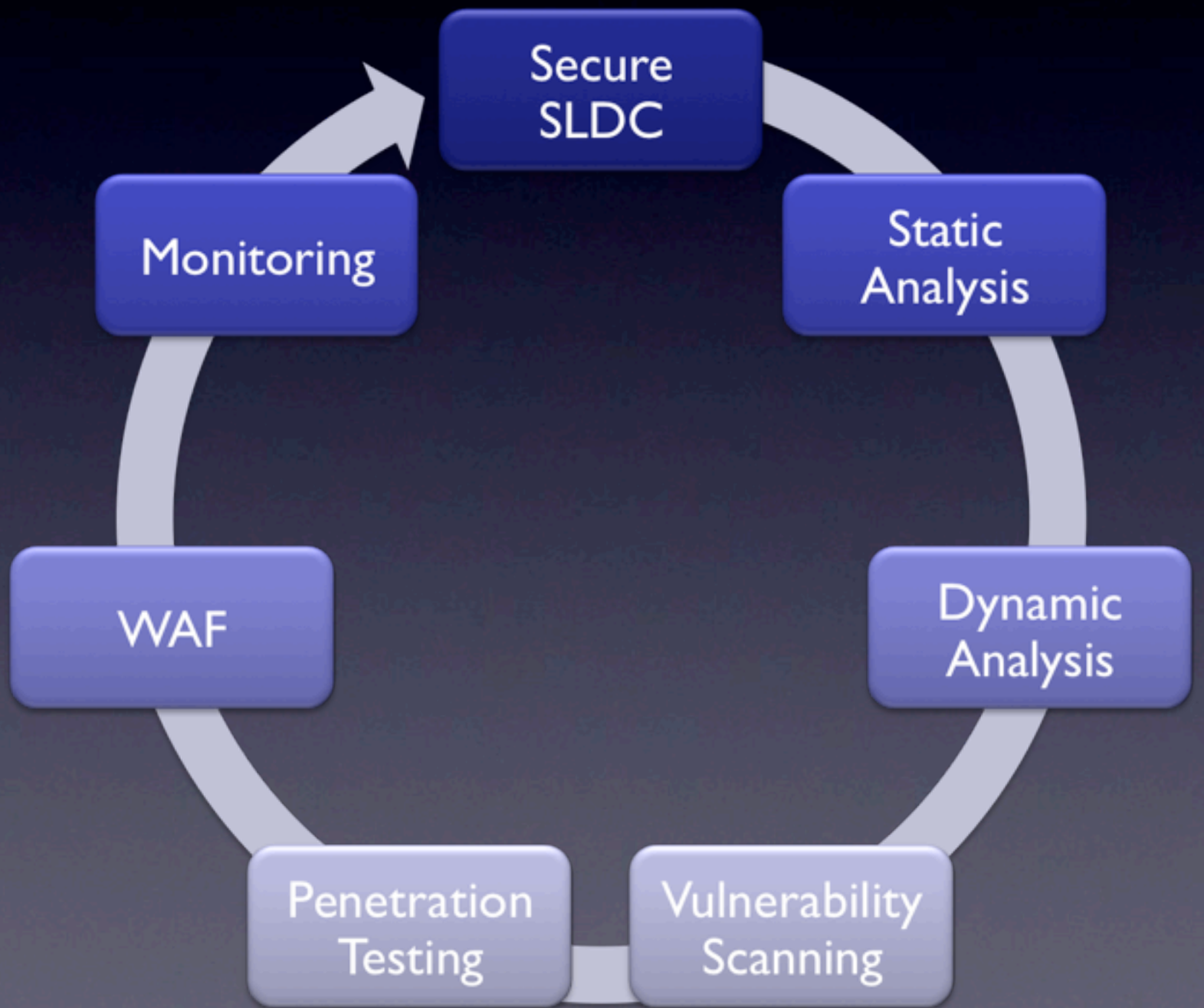
Securosis

Protect

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

Securosis

Web Application Security



Securosis

WebAppSec Priorities

- Vulnerability Assessment to find
- Web Application Firewall to shield
- Fix the code

CMP Deployment Modes

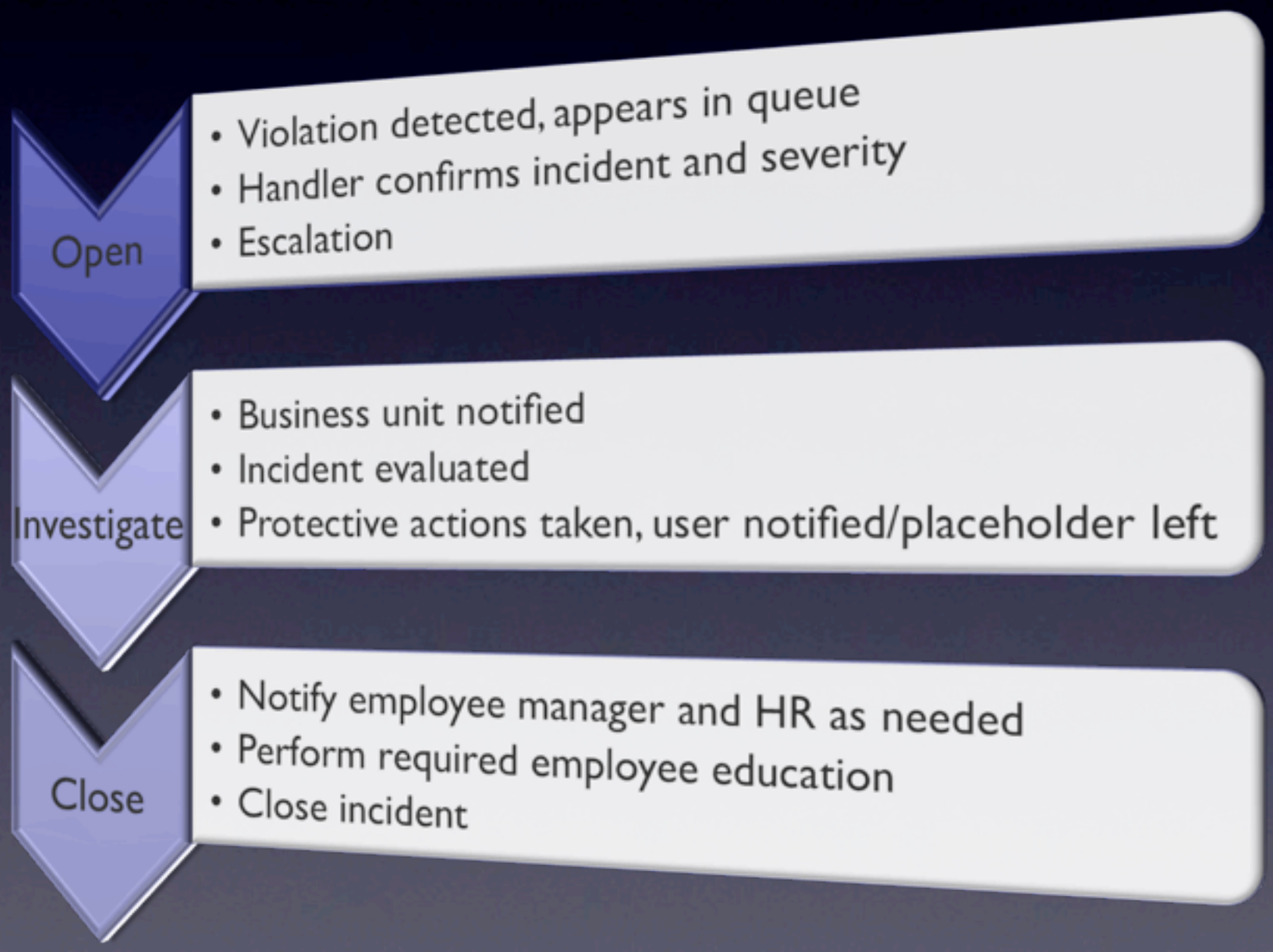
Passive	• Monitoring only
Bridge	• Block, but some data leaks
Proxy	• Full blocking • Often requires integration

Securosis

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



Securosis

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

Securosis

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).

Securosis

The Plan

- Segregate known transaction networks and enforce strict monitoring and egress controls.
- Use DLP and database discovery to find other data sources. Trust me, they are out there.
- 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 financial 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/tokenize it?

Securosis

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 Future?

Cloud Info-Centric Security Building Blocks

Labels

Securosis

Cloud Info-Centric Security Building Blocks

Encryption

Securosis

Cloud Info-Centric Security Building Blocks

EDRM

Cloud Info-Centric Security Building Blocks

DLP

Securosis

Cloud Info-Centric Security Building Blocks

IAM

Securosis

Labels are applied via context and content analysis

Create

Apply Contextual Labels

Analyze Content

Apply Mandatory and Discretionary Rights

Securosis

New Granularity in "Unstructured" Content

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:mv="urn:schemas-microsoft-com:mac:vml" xmlns:mo="http://schemas.microsoft.com/office/mac/office/2008/main" xmlns:ve="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v="urn:schemas-microsoft-com:vml" xmlns:w10="urn:schemas-microsoft-com:office:word" xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wp="http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing"><w:body><w:p w:rsidR="001333AF" w:rsidRDefault="001333AF"><w:pPr><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr></w:pPr><w:r w:rsidRPr="001333AF"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t>What Mac Users Need to Know About Security</w:t></w:r></w:p><w:p w:rsidR="001333AF" w:rsidRDefault="001333AF"><w:pPr><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t>By Rich Mogull</w:t></w:r></w:p><w:p w:rsidR="001333AF" w:rsidRDefault="001333AF"><w:pPr><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr></w:pPr></w:p><w:p w:rsidR="00B105ED" w:rsidRDefault="001333AF"><w:pPr><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr></w:pPr><w:r><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t>Few topics in the Mac community are as contentious as</w:t></w:r><w:r w:rsidR="00DB4EE1"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve"> security</w:t></w:r><w:r><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve">. </w:t></w:r><w:r w:rsidR="00DB4EE1"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t>On one side are vendors and the press; hyping every new potential threat like it's the end of the world</w:t></w:r><w:r w:rsidR="001147E2"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve"> with the hope of selling more products or getting more readers</w:t></w:r><w:r w:rsidR="00DB4EE1"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve">. On the other side are the religious zealots who consider Macs immune to security problems, and react to any discussion of potential weaknesses like a personal assault. Caught in the middle </w:t></w:r><w:r w:rsidR="002C06E3"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t>of these competing agendas is the vast sea of</w:t></w:r><w:r w:rsidR="00DB4EE1"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve"> average Mac users</w:t></w:r><w:r w:rsidR="00B105ED"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve">, who desire little more than to know what they need to do to </w:t></w:r>

Securosis

New Granularity in "Unstructured" Content

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:mv="urn:schemas-microsoft-com:mac:vml" xmlns:mo="http://schemas.microsoft.com/office/mac/office/2008/main" xmlns:ve="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o="urn:schemas-microsoft-com:office:office" xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="http://schemas.openxmlformats.org/of
xm word/
20
w: Pr></
w sers
N
w
w w:p
w Pr></
w:
w w
to tica"
w:
w:
w: reat
like it's the end of the world</w:t></w:r><w:r w:rsidR="001147E2"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve"> with the hope of selling more products or getting more readers</w:t></w:r><w:r w:rsidR="00DB4EE1"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve">. On the other side are the religious zealots who consider Macs immune to security problems, and react to any discussion of potential weaknesses like a personal assault. Caught in the middle </w:t></w:r><w:r w:rsidR="002C06E3"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t>of these competing agendas is the vast sea of</w:t></w:r><w:r w:rsidR="00DB4EE1"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve"> average Mac users</w:t></w:r><w:r w:rsidR="00B105ED"><w:rPr><w:rFonts w:ascii="Helvetica" w:hAnsi="Helvetica"/></w:rPr><w:t xml:space="preserve">, who desire little more than to know what they need to do to </w:t></w:r>

In database content we can apply labels/ rights at the row/field level.

In document-based content we can now apply at the paragraph or object level.

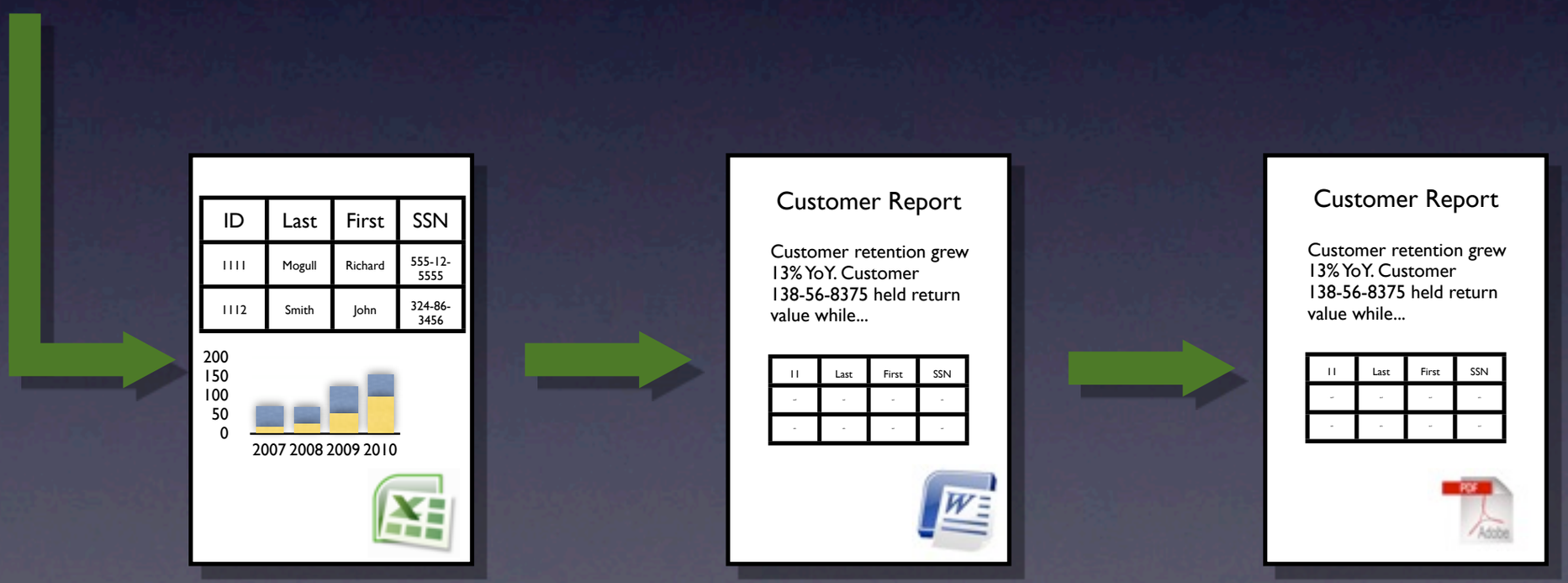
Securosis

Cross-Domain Information Protection

ID	Last	First	SSN
1111	Mogull	Richard	555-12-5555
1112	Smith	John	324-86-3456

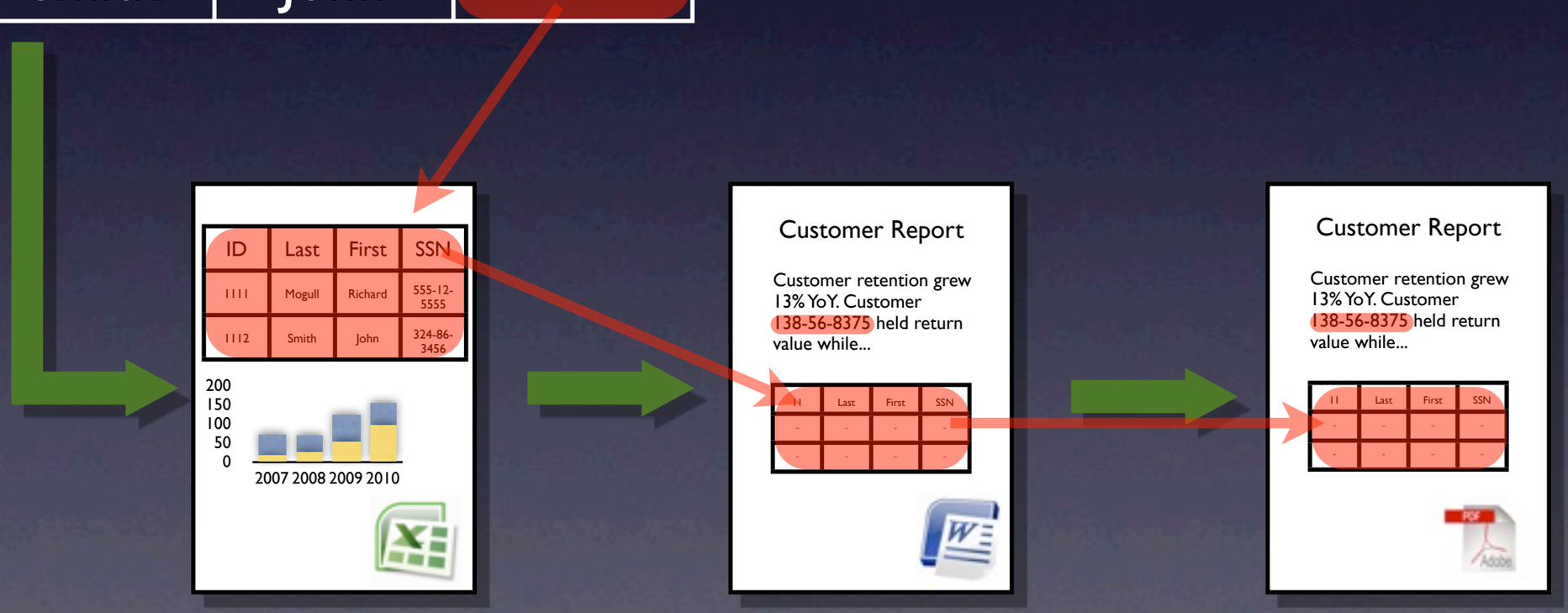
Cross-Domain Information Protection

ID	Last	First	SSN
1111	Mogull	Richard	555-12-5555
1112	Smith	John	324-86-3456



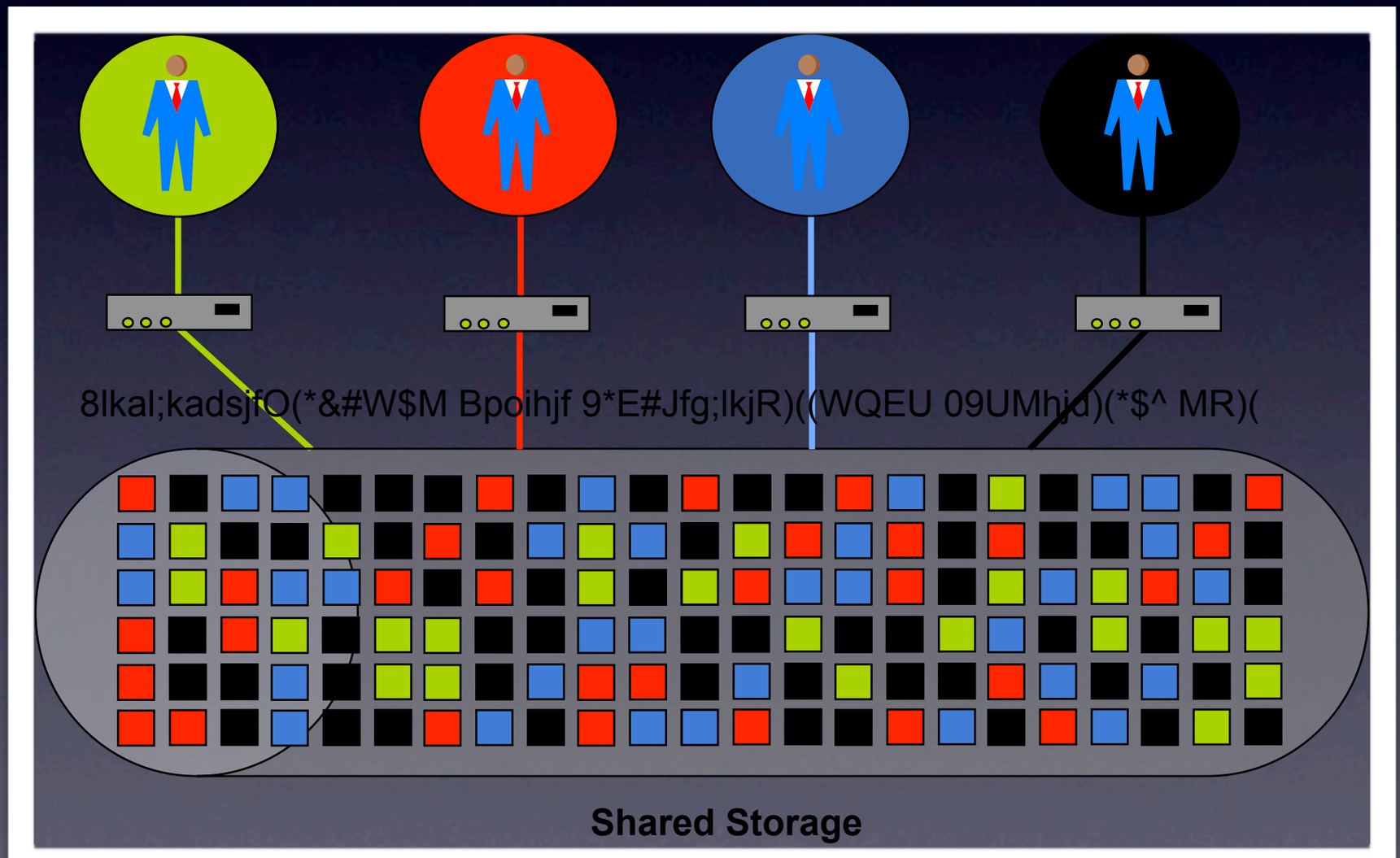
Cross-Domain Information Protection

ID	Last	First	SSN
1111	Mogull	Richard	555-12-5555
1112	Smith	John	324-86-3456



Securosis

Data Dispersion
Data-In-Motion/Rest



Securosis

Where This Take Us

- Content analysis fully integrated into both productivity and transaction applications.
- Rights (and thus encryption) applied at the point of creation, at the data-element level.
- Choke points between on-premise, off-premise, and between cloud services enforce policies at the data level, enforced by encryption/DRM.
- Rights transfer and are maintained between state changes.

Securosis

Rich Mogull

Securosis, L.L.C.

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