INFORMATION SECURITY
SearchSecurity.com
INFORMATION SECURITY DECISIONS

The Information-Centric Security Lifecycle

Adrian Lane

Securosis, L.L.C.

NETWORK

Mainframe

Jail

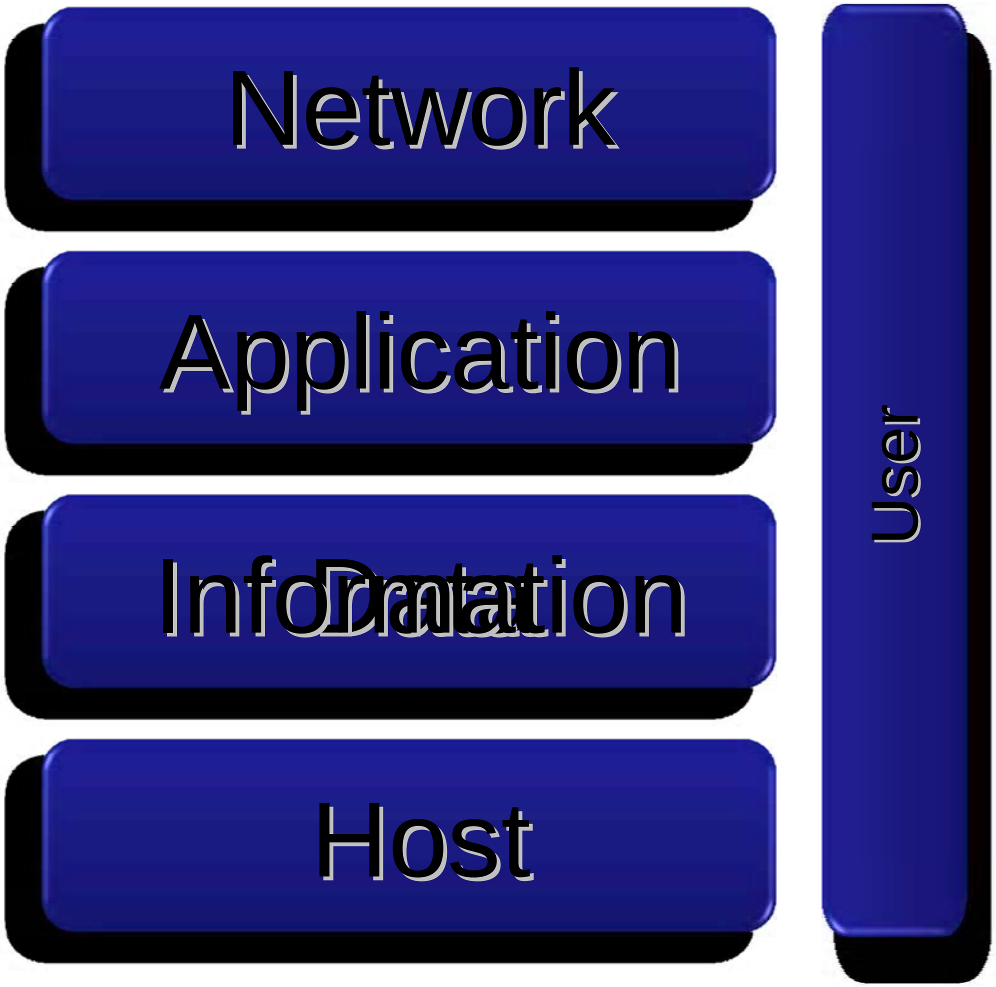
Internet I

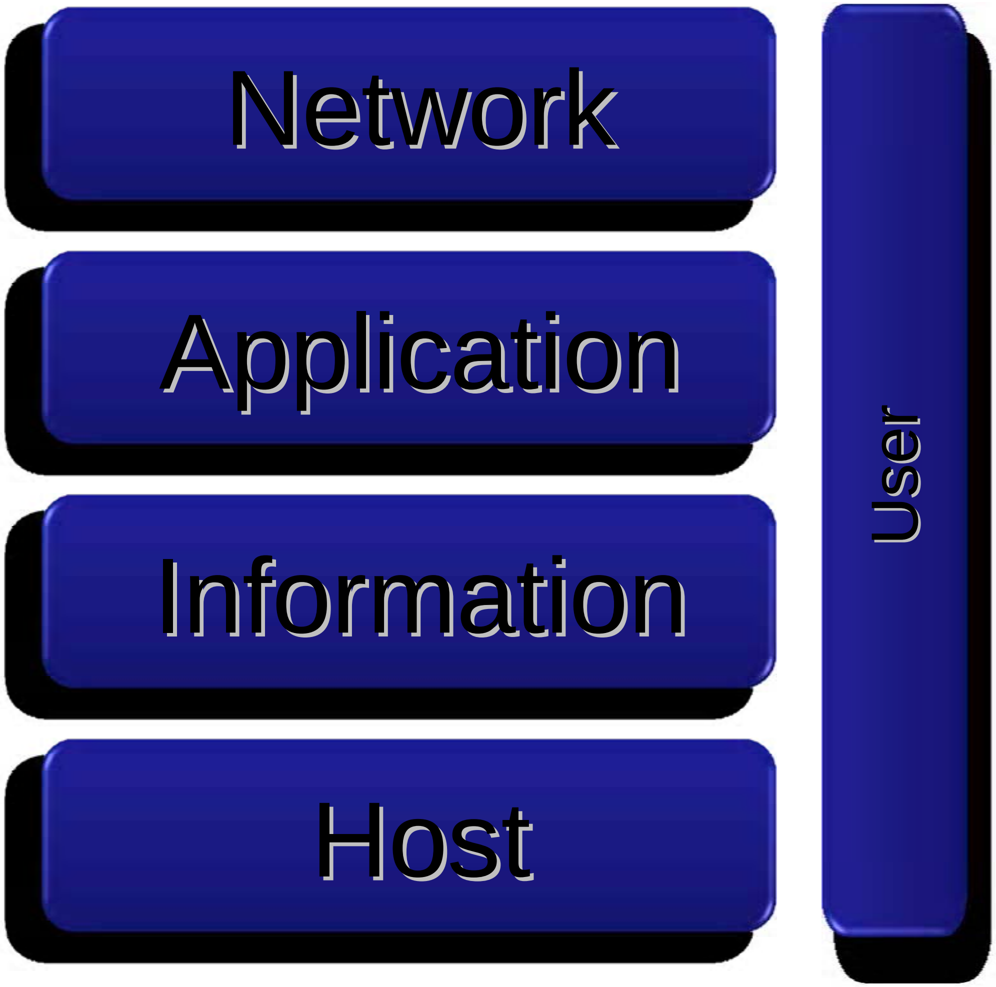
Fortress

Internet II

Zone

But what about the information?


Network
Application
Information
Data
Host
User



Network

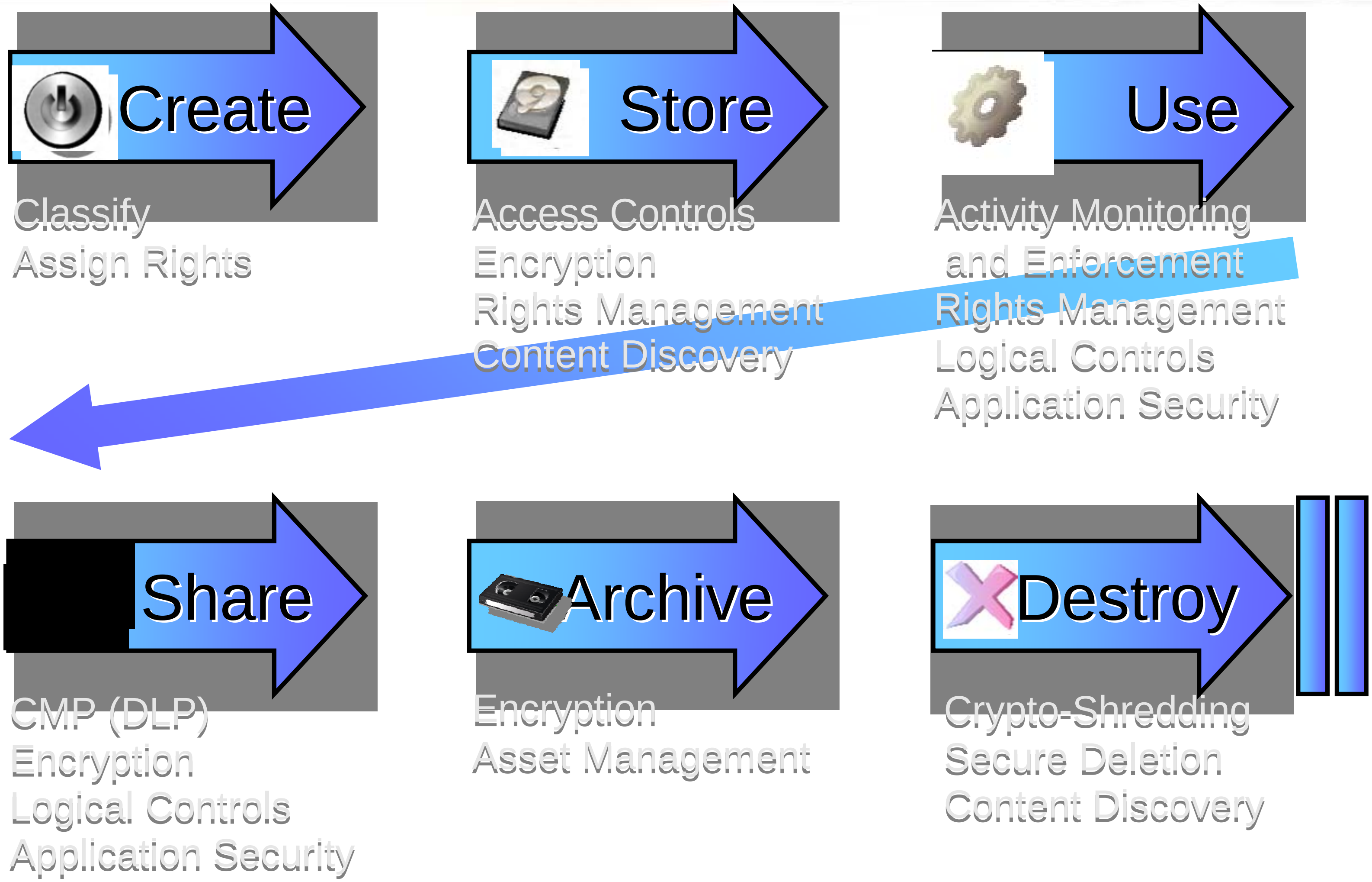
Application

Information

Host

User

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

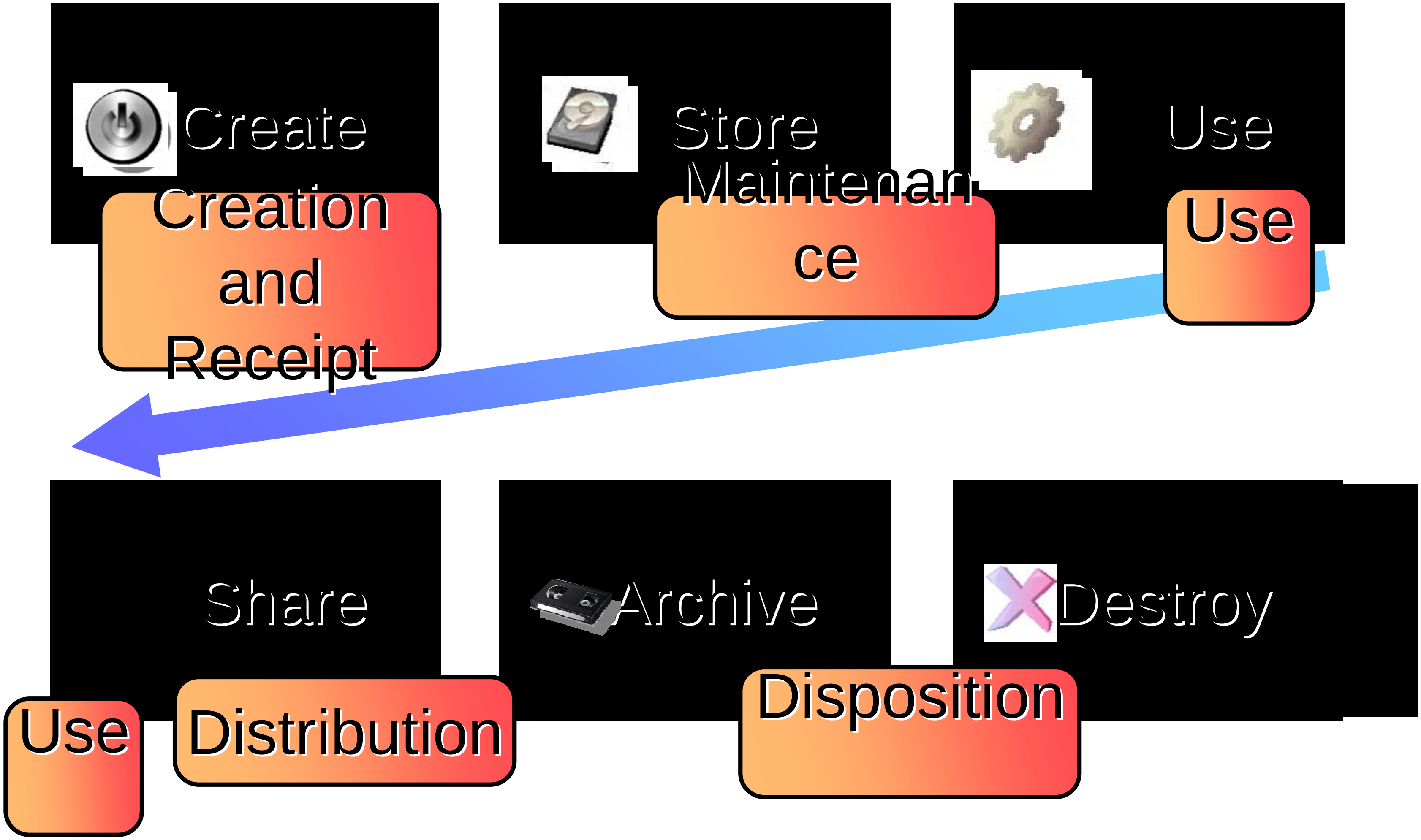
Archive

Encryption
Asset Management

Destroy

Crypto-Shredding
Secure Deletion
Content Discovery

ILM and Security



Create

Store

Use

Creation and Receipt

Maintenance

Use

Share

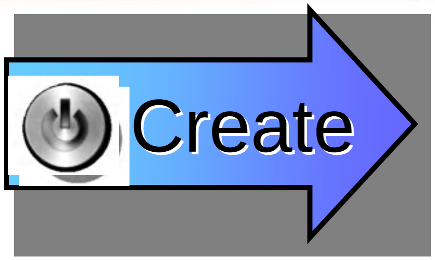
Archive

Destroy

Use

Distribution

Disposition



Create

- Content is classified as it’s created through content analysis or based on labeling of data elements.
- Rights are assigned, based on central policies.
- Mandatory and discretionary policies.

Create Technologies

Create

Control	Structured	Unstructured
Classify	None*	None*
Assign Rights	Label Security	Enterprise DRM

Note- Classification is expected to emerge from DLP/CMP

Label Security

Column

ID	Last	First	SSN
1111	Mogull	Richard	🟥
1112	Smith	John	🟥

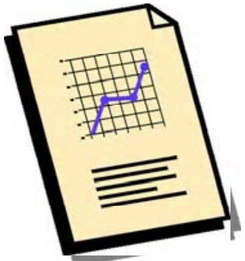
Row

ID	Last	First	Region	Label
1111	Mogull	Richard	US	Public
🟥	🟥	🟥	🟥	🟥

Content Analysis

Partial Document Matching

Database Fingerprinting



Statistical

Exact File Matching

Categories

Conceptual

Rules

- We use access controls, encryption, and rights management to protect data in storage.
- Content Discovery helps find unprotected sensitive data that slipped through the gaps.

Store Technologies

Store

Control	Structured	Unstructured
Access Controls	DBMS Access Controls Administrator Separation of Duties	File System Access Controls Document Management System Access Controls
Encryption	Field Level Encryption Application Level Encryption File / Media Encryption*	Media Encryption File Encryption Distributed Encryption
Rights Management	Label / Row Level Security	Enterprise DRM
Content Discovery	Database-Specific Discovery Tools	DLP / CMF Content Discovery Storage / Data Classification Tools

Access Controls

Encryption

DRM

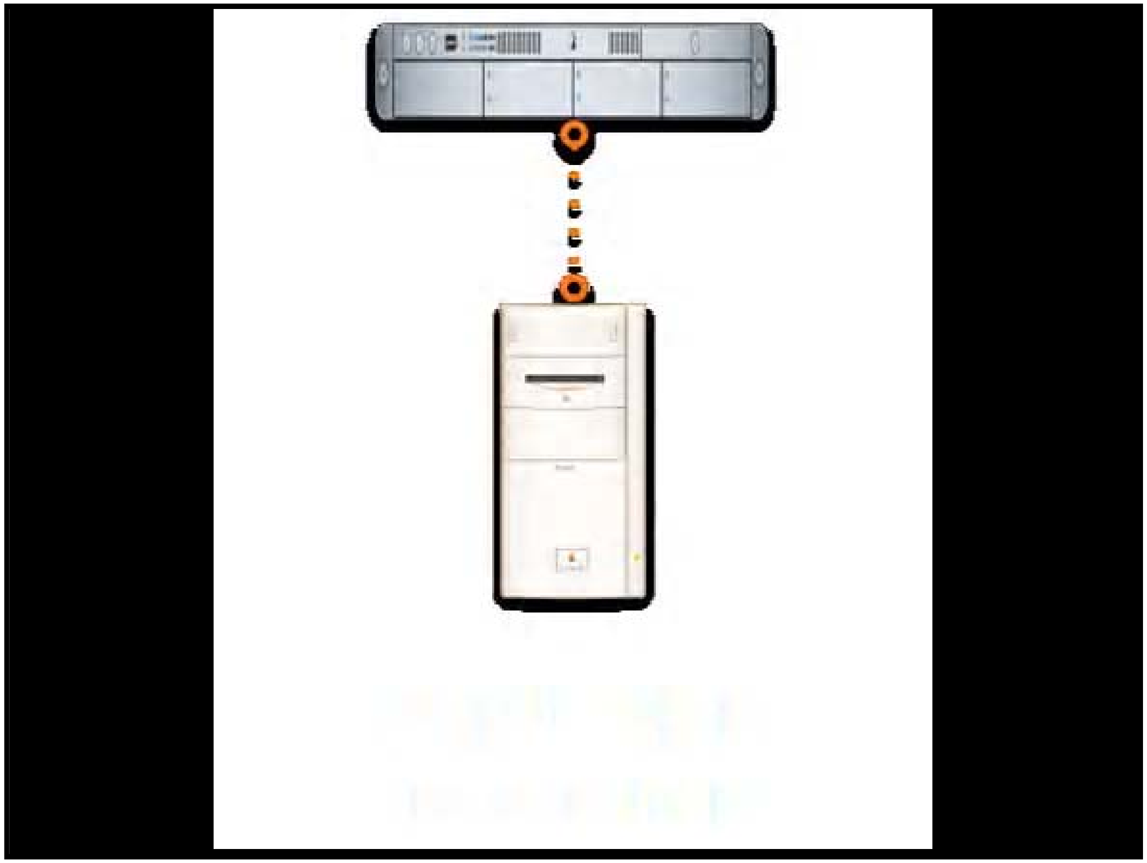
Encryption Options

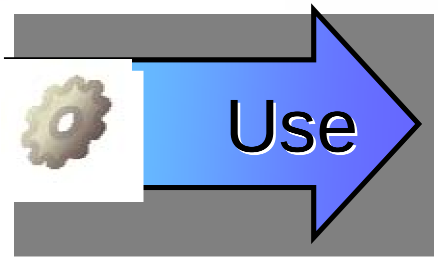
File/Folder

Application/ Database

Media

Content Discovery





Use

- Monitor and protect information during use.
- Includes business applications and productivity applications.
- Heavy use of content-aware technologies.

Use Technologies

Use

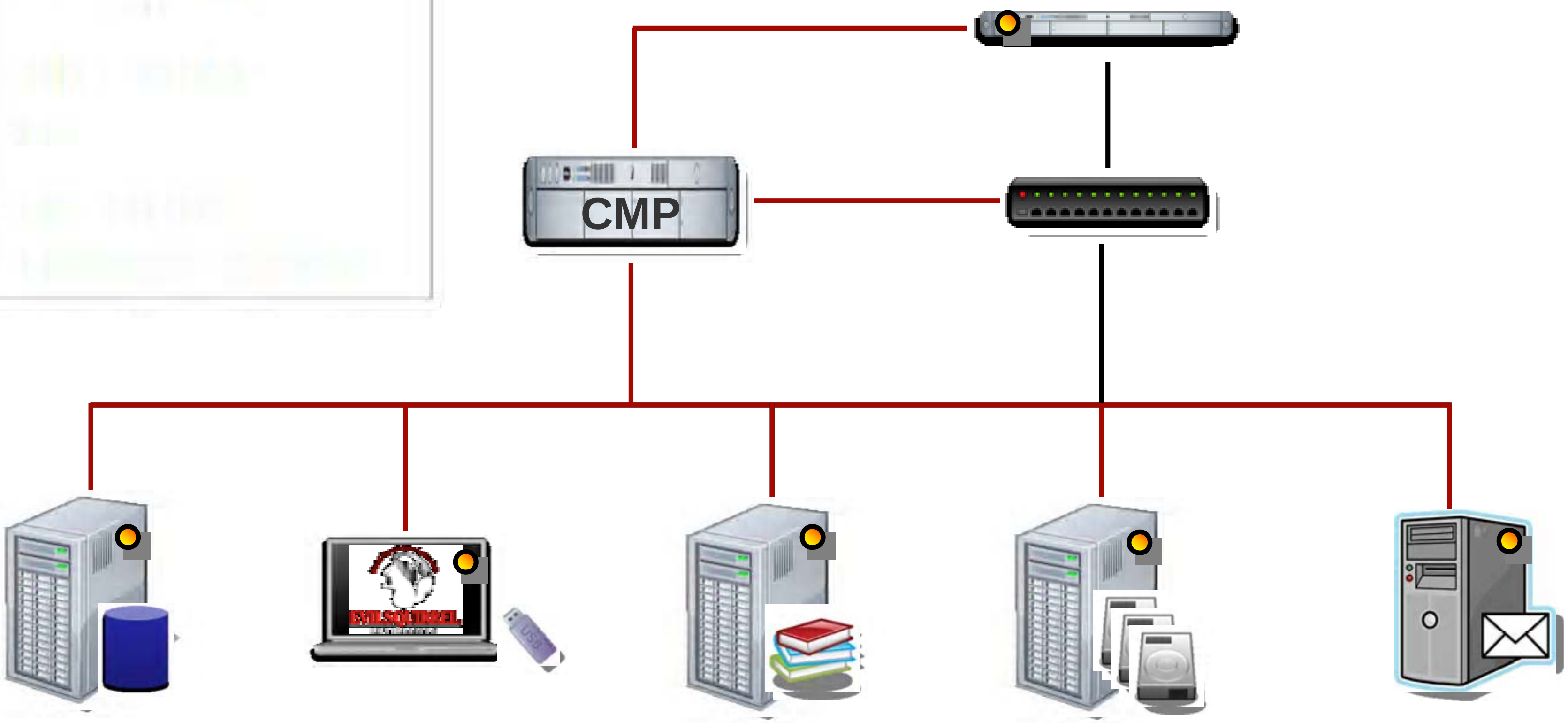
Control	Structured	Unstructured
Activity Monitoring and Enforcement	Database Activity Monitoring Application Activity Monitoring	Endpoint Activity Monitoring File Activity Monitoring Portable Device Control Endpoint DLP
Rights Management	Label Security	Enterprise DRM
Logical Controls	Object (Row) Level Security Structural Controls Application Logic	
Application Security	Implemented At Application Layer	

Two Sides Of Information-Centric Security

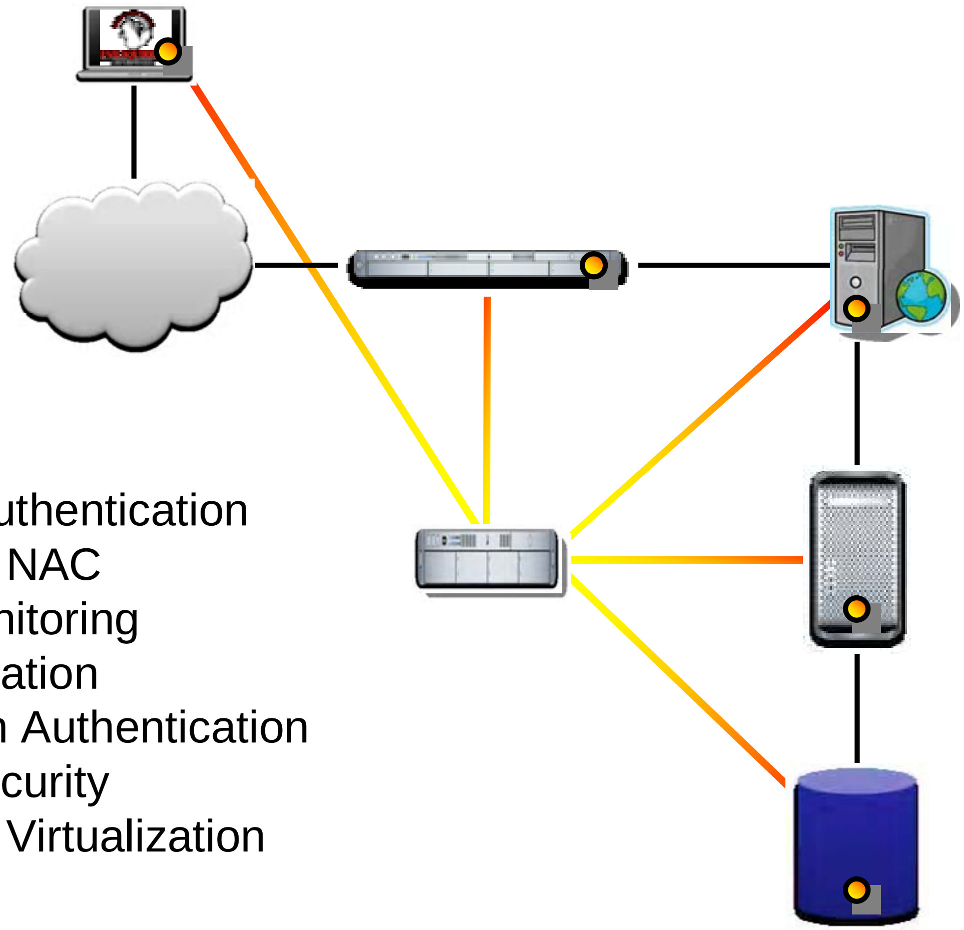
Data Center

Productivity

CMP



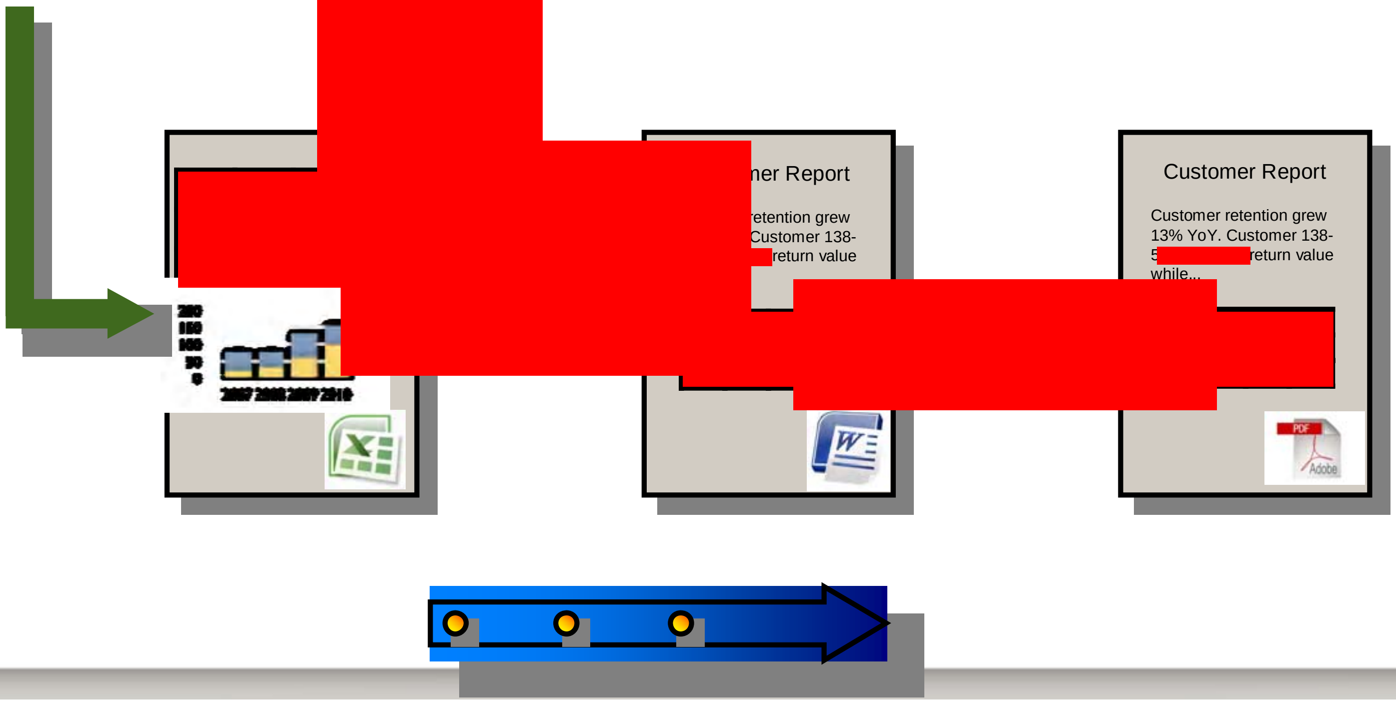
ADMP



Adaptive Authentication
Application NAC
Activity Monitoring
Anti-Exploitation
Transaction Authentication
Session Security
Application Virtualization

Cross-Domain Information Protection

ID	Last	First	SSN
1111	Mogull	Richard	[redacted]
1112	Smith	Joh	[redacted]



retention grew
Customer 138-
return value

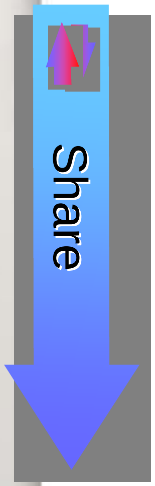
Customer Report

Customer retention grew 13% YoY. Customer 138-5[redacted]return value while...

Share

- Securely exchange information, inside and outside of the enterprise.
- A mixture of content-aware technologies and encryption for secure exchange.

Share Technologies



Control	Structured	Unstructured
CMP / DLP	Database Activity Monitoring (With DLP Feature)	Network / Endpoint CMP / DLP
Encryption *Only When Data Elements Not Otherwise Encrypted	Network Encryption Application Level Encryption	Email Encryption File Encryption Network Encryption
Logical Controls	Object (Row) Level Security Structural Controls	
Application Security	Implemented At Application Layer	

Inter-Organization Encryption vs. DRM

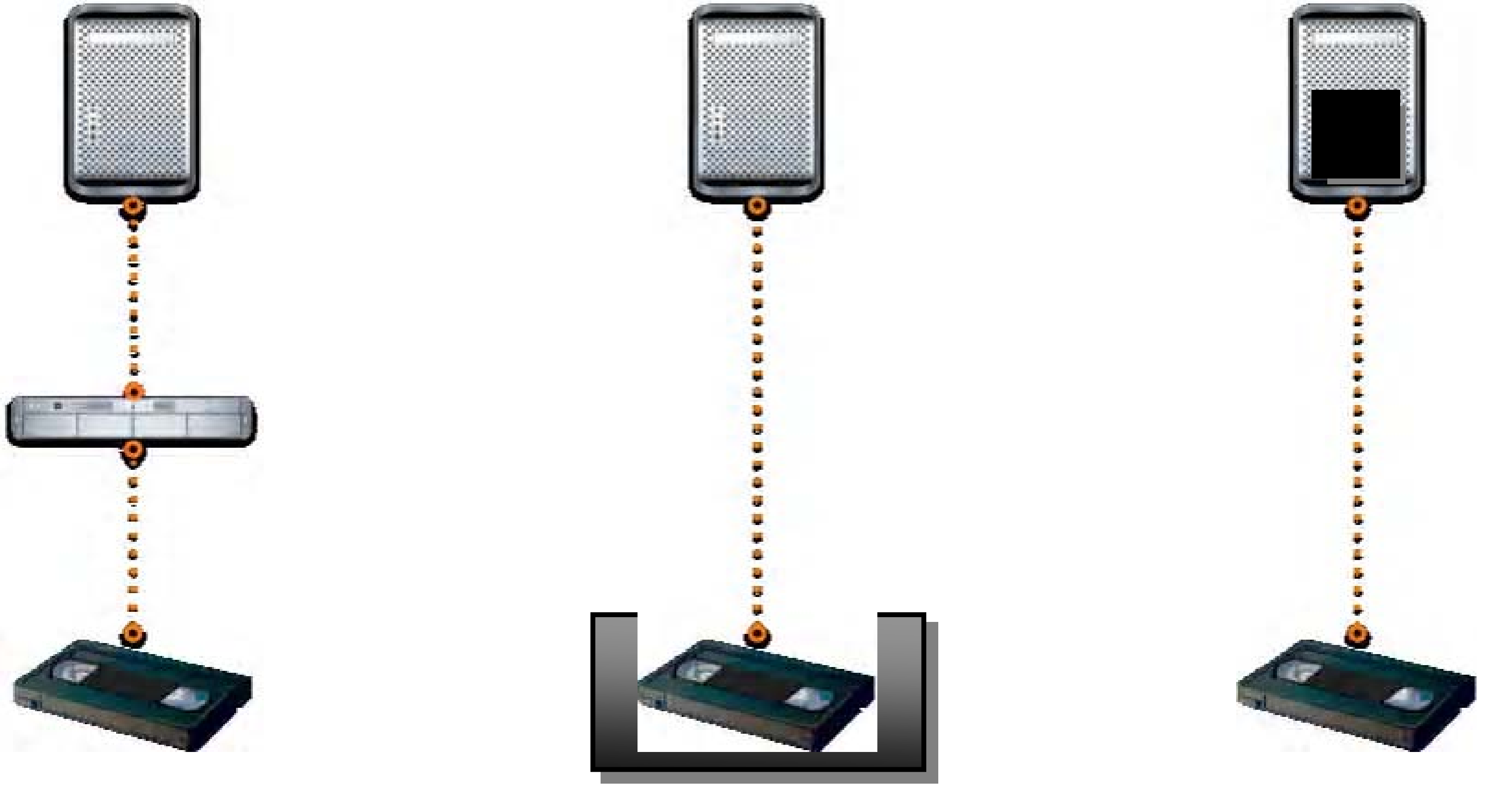
Archive

- Protect information in archival storage.
- Encryption and asset management

Archive Technologies

Control	Structured	Unstructured
Encryption	Field-Level Encryption	Tape Encryption Storage Encryption (Multiple Options)
Asset Management	Asset Management	Asset Management

Tape Encryption Options



In-line

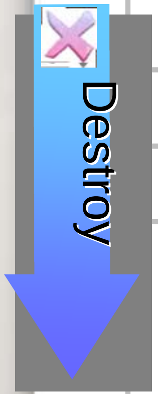
Drive

Software

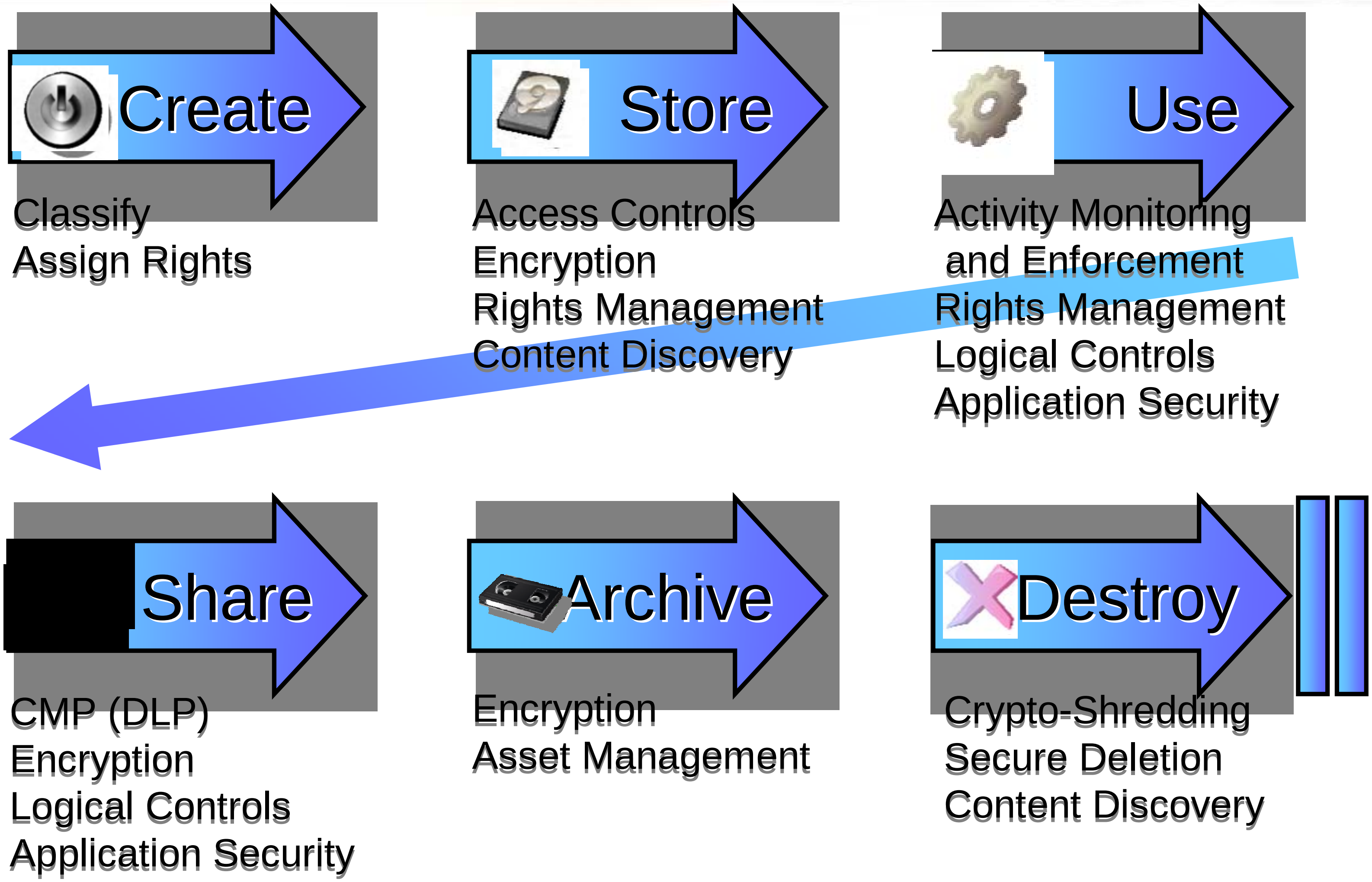
Destroy

- Ensure data is not recoverable at end of life
- Content discovery to ensure dangerous data isn’t hiding where it shouldn’t be.

Destroy Technologies



Control	Structured	Unstructured
Crypto-Shredding	Enterprise Key Management	Enterprise Key Management
Secure Deletion	Disk / Free Space Wiping	Disk / Free Space Wiping
Physical Destruction	Physical Destruction	Physical Destruction
Content Discovery	Database-Specific Discovery Tools	DLP / CMF Content Discovery Storage / Data Classification Tools Enterprise Search E-Discovery



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

Adrian Lane

Securosis, L.L.C.

- alane@securosis.com
- http://securosis.com
- AIM: whoisadrianlane
- Skype: whoisadrianlane