The Information-Centric Security Lifecycle

Rich Mogull
Securosis, L.L.C.

Mainframe

Jail

Internet I

Fortress

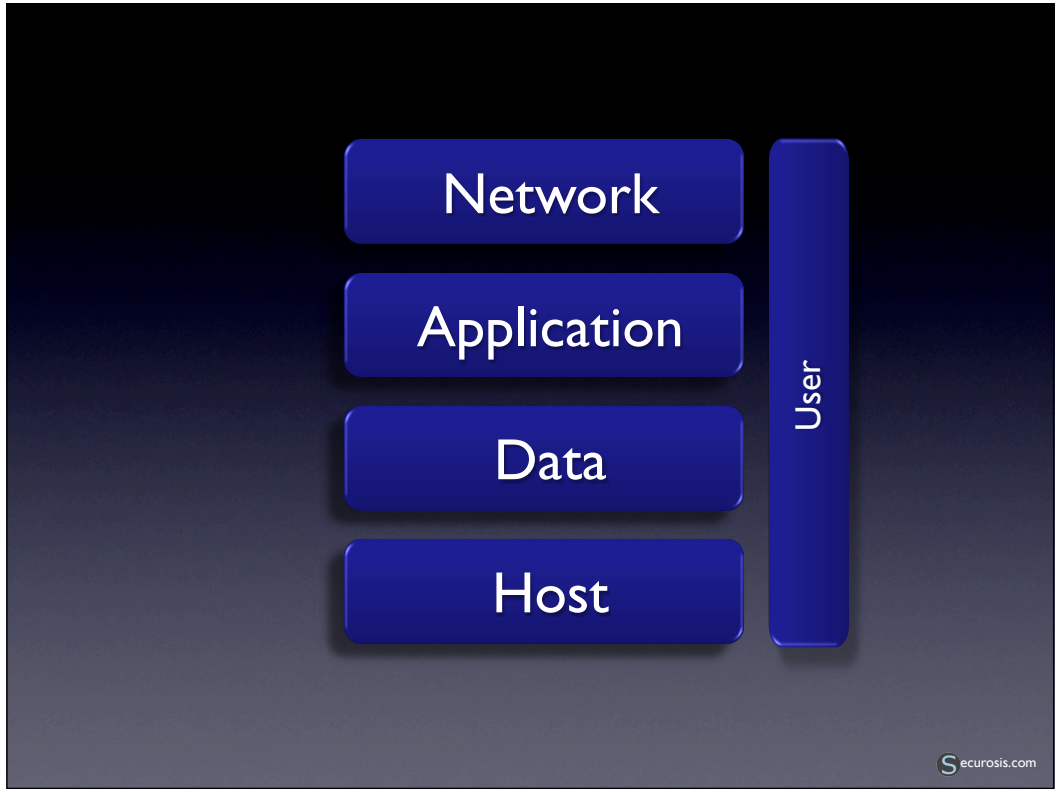
Internet II

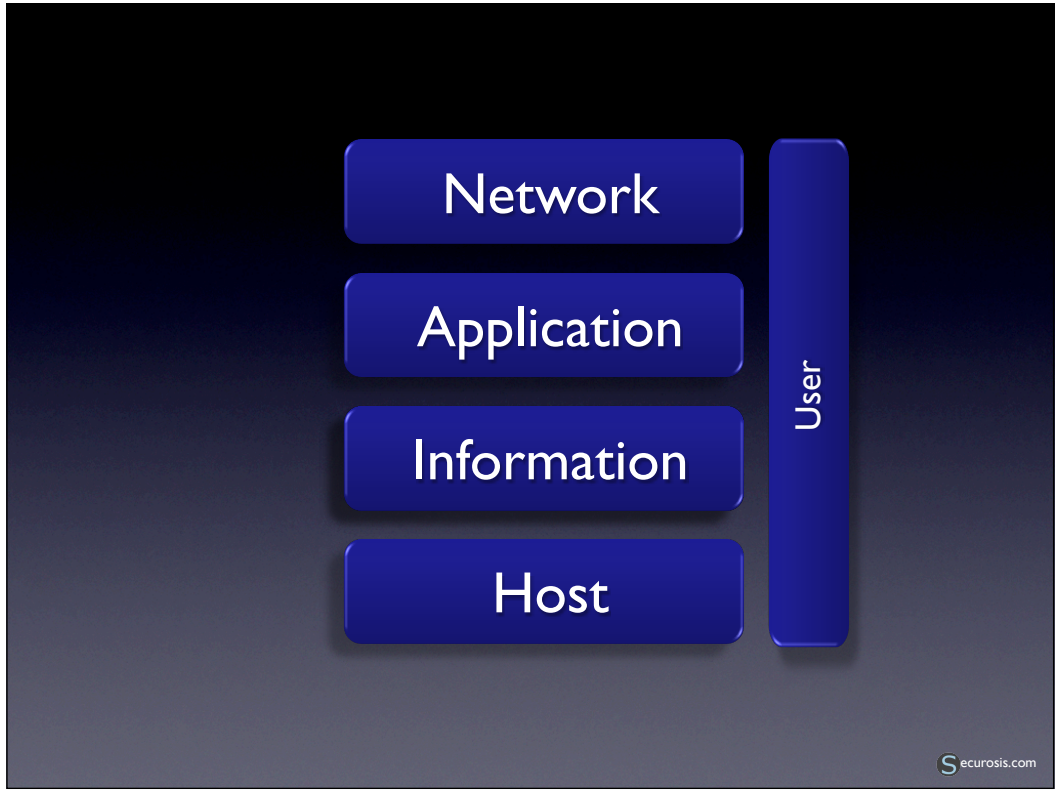
Zone

NETWORK

Securosis.com

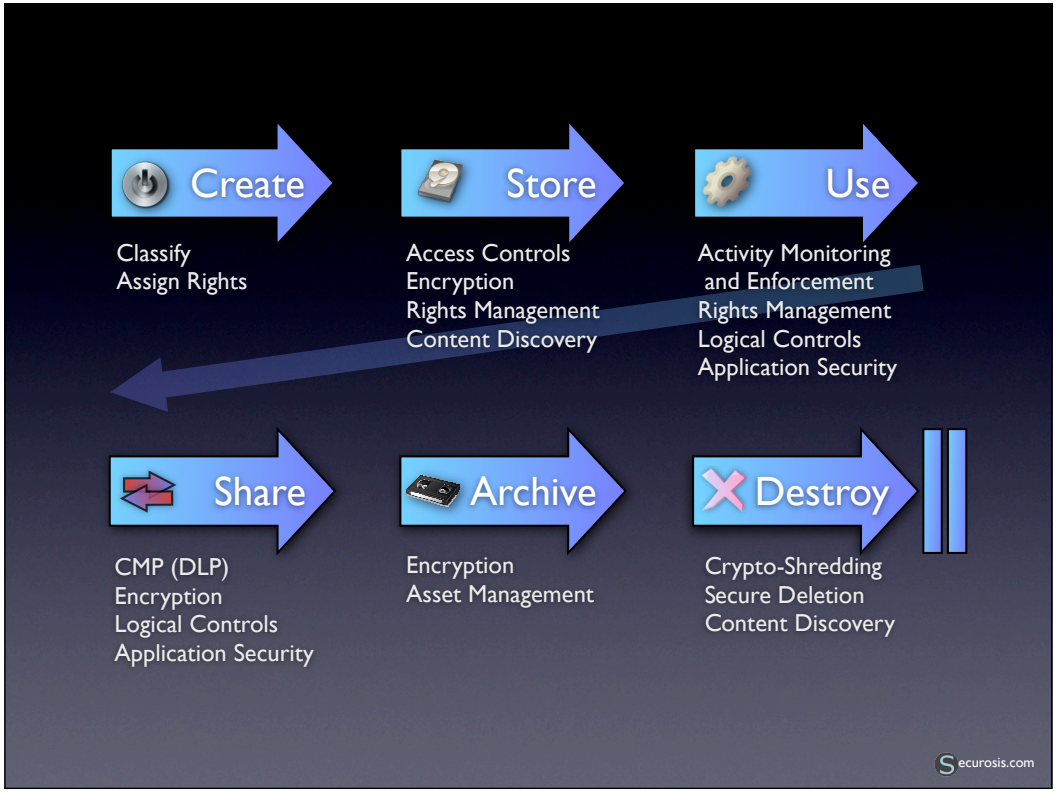
But what about the information?


Network
Application
Data
Host
User
Securosis.com

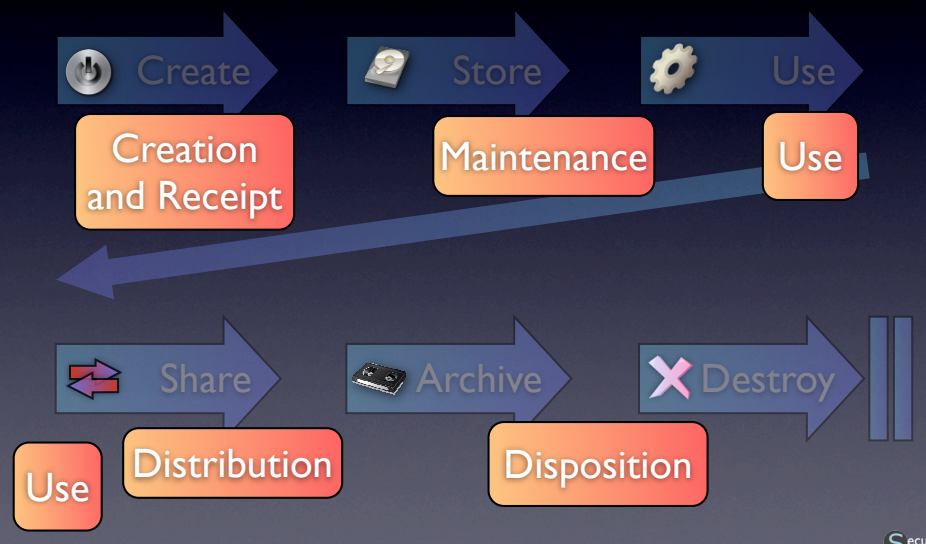

Network
Application
Information
Host
User
Securosis.com

The Information-Centric Security Lifecycle

Securosis.com


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
Securosis.com

ILM and Security



Securosis.com

- 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.

Securosis.com

Create Technologies

Create

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

Note- Classification is expected to emerge from DLP/CMP

Securosis.com

Label Security

Column

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

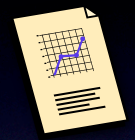
Row

ID	Last	First	Region	Label
1111	Mogull	Richard	US	Public
1112	Smith	John	EMEA	Sensitive

Content Analysis

Partial Document Matching

Database Fingerprinting



Statistical

Exact File Matching

Categories

Conceptual

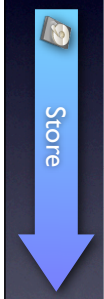
```
^(?:(?<Visa>4\d{3})|(?<Mastercard>5[1-5]\d{2})|(?<Discover>6011)|(?
<DinersClub>(?:3[68]\d{2})|(?:30[0-5]\d))|(?
<AmericanExpress>3[47]\d{2}))([ -]?)(?(DinersClub)(?:\d{6}\1\d{4})|(?
(AmericanExpress)(?:\d{6}\1\d{5})|(?:\d{4}\1\d{4}\1\d{4})))$
```

Rules

Securosis.com

- 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.

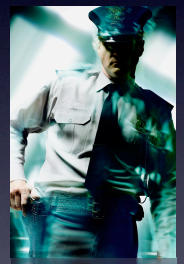
Store Technologies



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

Securosis.com

Access Controls



Encryption

DRM

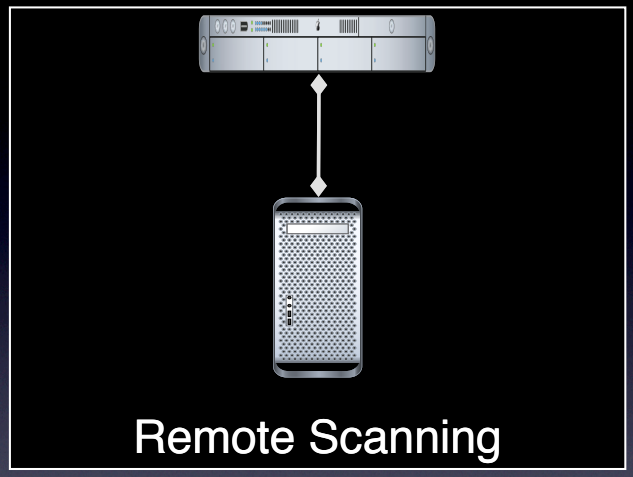
Securosis.com

Encryption Options

File/Folder

Application/
Database

Media



Content Discovery

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

Securosis.com

Use Technologies

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	

Securosis.com

Two Sides Of Information-Centric Security

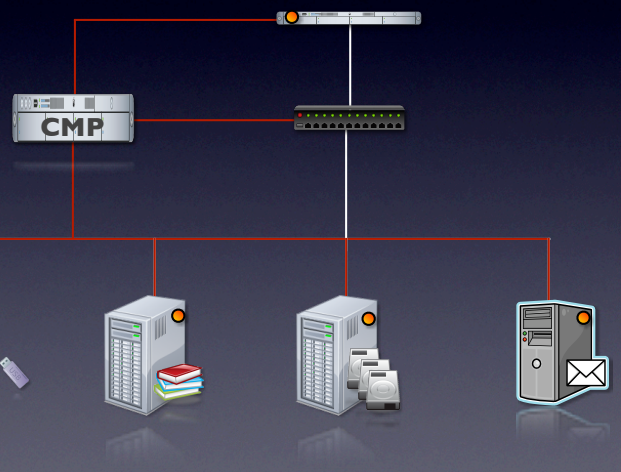
Data Center

Productivity

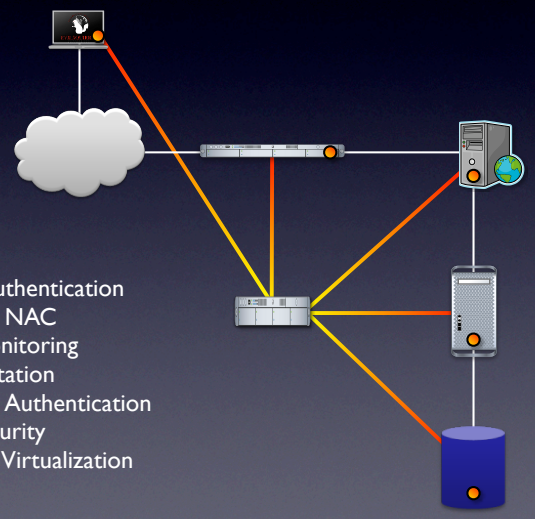
Securosis.com

CMP

- Advanced Content Analysis
- Real-Time DRM
- CMP to ADMP Bridges
- Managed and Unmanaged Systems



ADMP

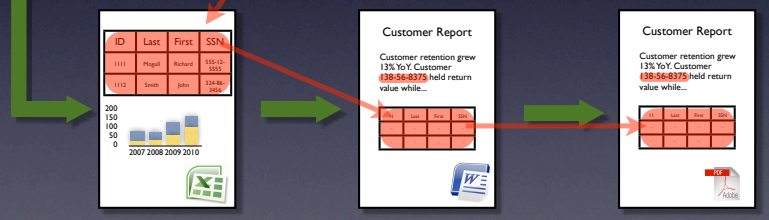


Adaptive Authentication
Application NAC
Activity Monitoring
Anti-Exploitation
Transaction Authentication
Session Security
Application Virtualization

Securosis.com

Cross-Domain Information Protection

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



Securosis.com

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

Share Technologies

Share

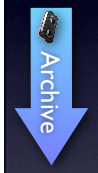
Control	Structured	Unstructured
CMP/DLP	Database Activity Monitoring (With DLP Feature)	Network/Endpoint CMP/DLP
Encryption *Only When Data Elements Not Otherwise Encrypted	Network Encryption Application Level Encryption	Email Encryption File Encryption Network Encryption
Logical Controls	Object (Row)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

Securosis.com

Inter-Organization Encryption vs. DRM

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

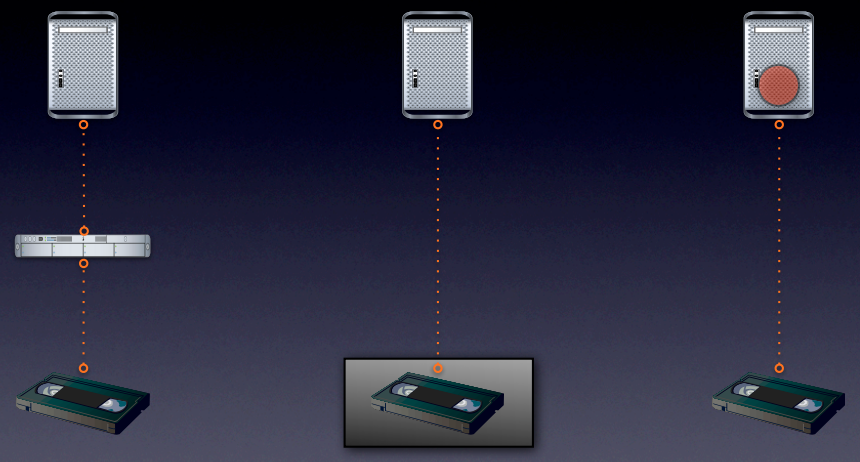
Archive Technologies



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

Securosis.com

Tape Encryption Options



In-line

Drive

Software

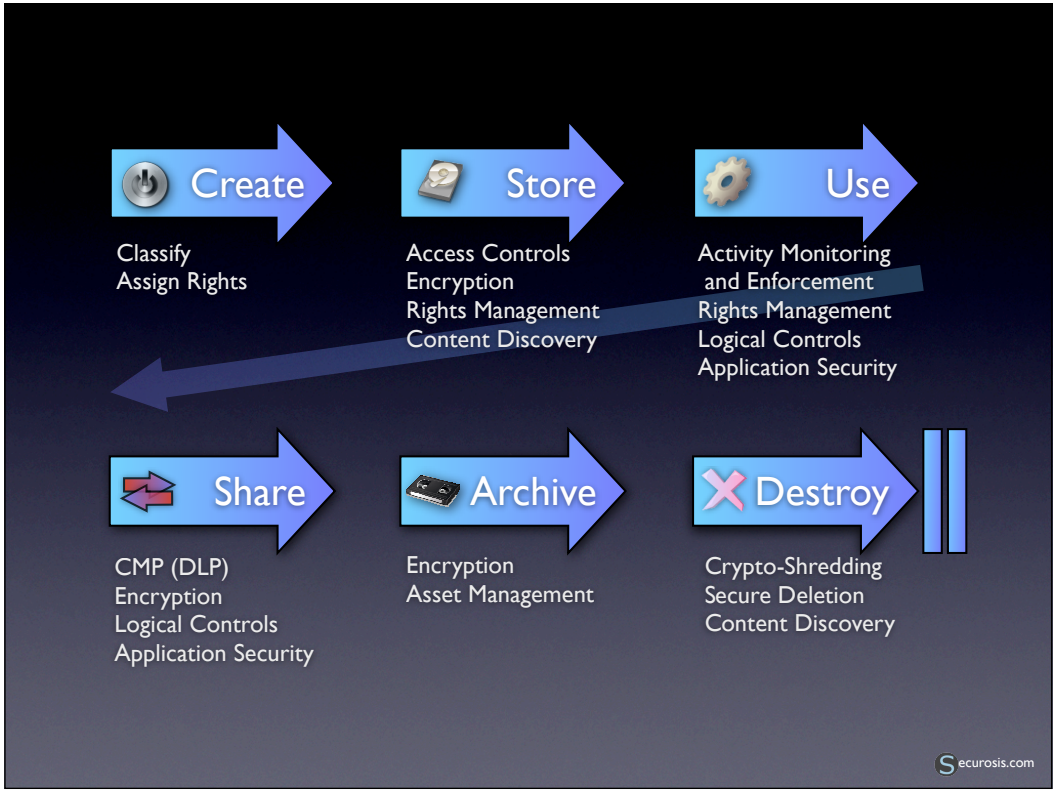
Securosis.com

- 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

Securosis.com


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
Securosis.com

Rich Mogull

Securosis, L.L.C.

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