Quick Wins with Data Loss Prevention

Rich Mogull
Securosis, LLC

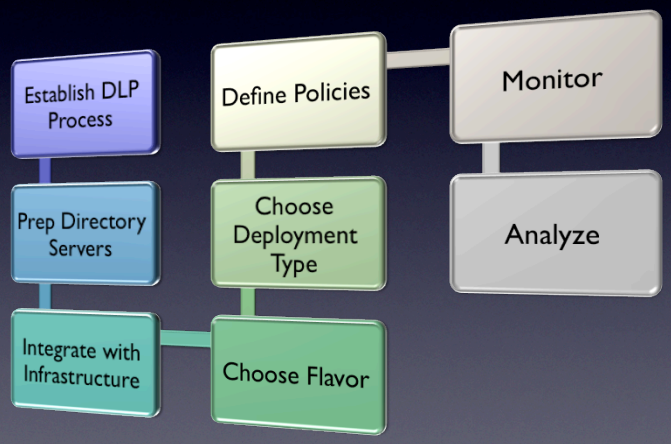
Securosis

DLP Fears

- Too complex to deploy.
- Too many false positives.

Securosis

The Quick Wins Process



Securosis

"Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use through deep content analysis."

-Rich Mogull

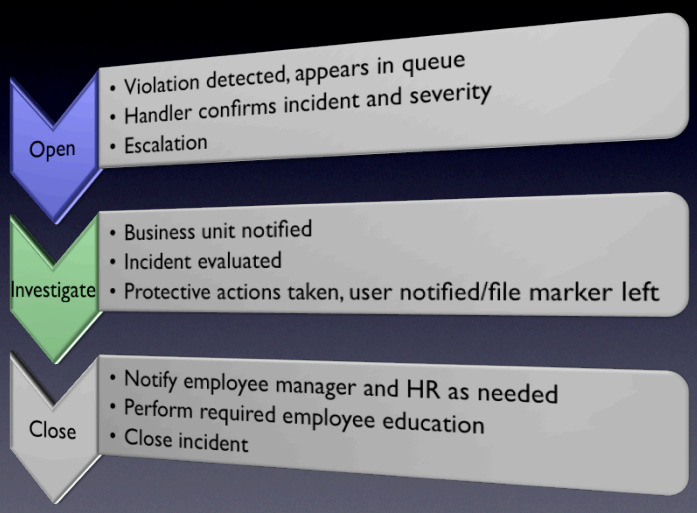
Securosis

What DLP Provides

- Helps you identify where you store sensitive information.
- Helps you understand how that information is used and moved throughout your organization.
- Proactively protects your information, while limiting impact on legitimate business processes.

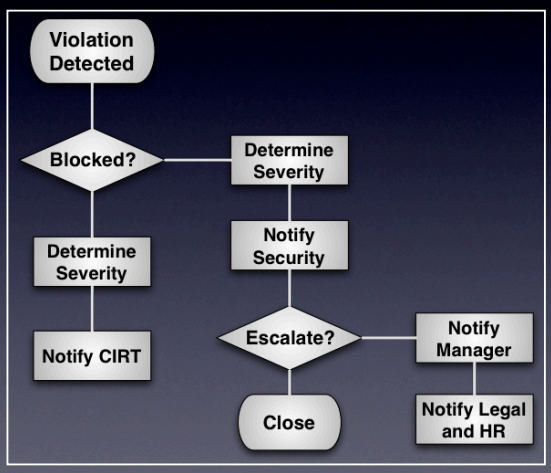
Securosis

Defining Process



Securosis

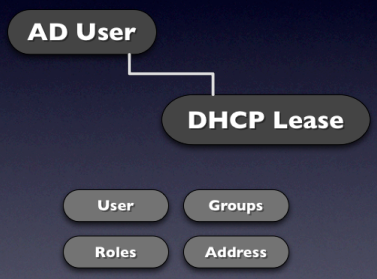
Process Workflow



Securosis

Prepare Directory Servers

- Why? DLP policies are typically user and group based.
- Need to correlate activities back to warm bodies.
- Poor directories are a leading obstacle to DLP deployments.
- Email vs. Web vs. Endpoint



Securosis

Integrate with Infrastructure

Network	Endpoint	Storage
• Passive sniffer (SPAN/ Mirror) • Email (MTA)	• Software deployment	• Admin credentials

Integration Recap

- For all deployments: Directory services (usually your Active Directory and DHCP servers).
- Network deployments: Network gateways and mail servers.
- Endpoint deployments: Software distribution tools.
- Discovery/storage deployments: File shares on the key storage repositories (you generally only need a username/password pair to connect).

Choose Flavor

Single Data Type

Information Usage

Securosis

Choose Deployment Type

Network

Storage

Endpoint

Securosis

Define Policies

Single Type

- Leverage an existing category when possible.
- Tune later.
- False positives are good!

Information Usage

- Turn on (nearly) everything.
- Collect as much as possible to identify usage patterns.

Securosis

Monitor

ID	Time	Policy	Channel	Severity	User	Action	Status
1138	1625	PII	Email	1.2 M	rmogull	Blocked	Open
1139	1632	HIPAA	IM	2	jsmith	Notified	Assigned
1140	1702	PII	HTTP	1	192.168.0.213	None	Closed
1141	1712	R&D/Product X	USB	4	bgates	Notified	Assigned
1142	1730	Financials	Storage	4	192.168.1.94	Encrypt	Escalated
1143	12/1/08	Source Code	Cut/Paste	12	sjobs	Confirm	Open

Securosis

Analyze

- Top violations by data type.
- Top violations by business unit.
- Top violations by volume.
- False positive patterns.
- Different violations from same source.
- Unusual origins.

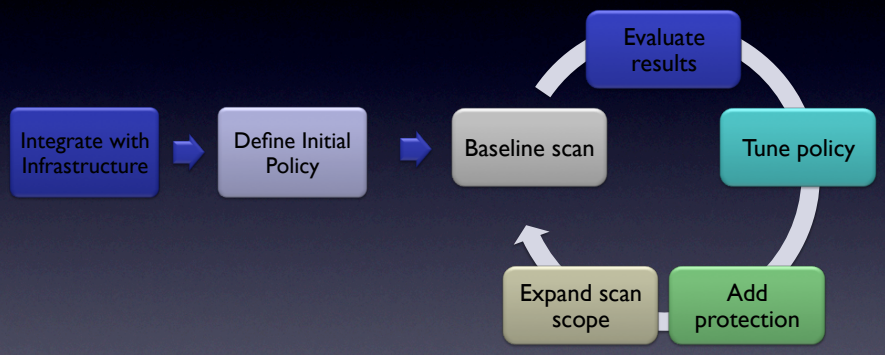
Securosis

What Did We Accomplish?

- Established a flexible incident management process.
- Integrated with major infrastructure components.
- Assessed broad information usage.
- Set foundation for later.

Securosis

Deployment Best Practices



Securosis

Rich Mogull

Securosis, L.L.C.

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

Securosis