Data Loss Prevention at the INL

Jonathan Homer
Idaho National Labratory

What we will cover today...

- What is Data Loss Prevention
- Why we need DLP
- Where (in the infastructure) is the right place for DLP
- "Navigating the Land Mines"
- Critical Partnerships

What Is DLP?

- Prevents Data Leakage
- Identifies and/or tracks Sensitive Data
- Monitors, Notifies, and/or Actively Prevents Data Loss

Well Duh!

What Is DLP?

- Prevents Data Leakage Well Duh!
- Identifies and/or tracks Sensitive Data
- Monitors, Notifies, and/or Actively Prevents Data Loss

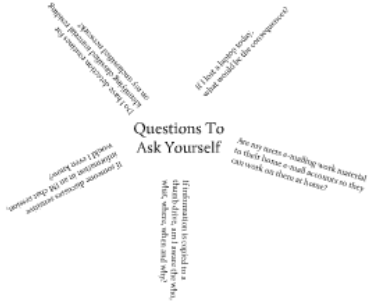
What is the need for DLP?

- 85% of commercial companies have experienced some form of data loss in the past 24 months.

- Average cost:
  $4.8 million (Ponemon Institute)
  $1.8 million (Forrester Research)

- Of all Data Breaches:
  12% due to malicious intent
  88% due ot unintended consequence

- Industry Examples:
  Veterans Affairs
  TJ Maxx



Questions To Ask Yourself

Are my

to their

can work

Do I have

identifi

on

If someo

inform

would

If I lost a laptop today,
what would be the consequences?

Are my users e-mailing work material to their home e-mail accounts so they can work on them at home?

Are my users e-mailing work material to their home e-mail accounts so they can work on them at home?

If someone discusses sensitive information in an IM chat session, would I even know?

Do I have detection routines for identifying classified material residing on my unclassified network?

4 Primary Platforms

Network DLP

- Dedicated appliance listening to network traffic
- Located at:
  - WAN Gateway
  - Critical network transveral points
  - Enclave Firewalls
- Must either act as proxy/gateway or integrate with existing infrastructure to do more than just monitor
- Allows complete coverage of network (no agent required)
- Unable to evaluate encrypted traffic (unless integrated with certificate management system)

Desktop DLP

- Agent based implementation
- Controlled by a centralized network appliance
- Monitors:
  - File Read/Write
  - Keyboard Entry
  - Clipboards
  - Web Traffic (http and SSL)
  - IM Clients
  - Print Queues
- The only (feasible) way to protect encrypted traffic

Data Crawlers

- Dedicated appliance OR set of installed agents (on servers)
- Uses centralized credentials
- Scheduled tasks to evaulate all accessible data stores
- Builds invetory of known data
- Dependent upon rule set developed by admistrators

Mobile DLP

- Least mature area of DLP
- Specialty software from unique vendors
- General Areas of Interest:
  - Blackberry/iPhone/Android
  - iPad and Tablets
  - VPN clients

Network DLP

- Dedicated appliance listening to network traffic
- Located at:
  WAN Gateway
  Critical network transveral points
  Enclave Firewalls
- Must either act as proxy/gateway or integrate with existing infrastructure to do more than just monitor
- Allows complete coverage of network (no agent required)
- Unable to evaluate encrypted traffic
  (unless integrated with certificate management system)

Desktop DLP

- Agent based implementation
- Controlled by a centralized network appliance
- Monitors:
  File Read/Write
  Keyboard Entry
  Clipboards
  Web Traffic (http and SSL)
  IM Clients
  Print Queues
- The only (feasible) way to protect encrypted traffic

Data Crawlers

- Dedicated appliance OR set of installed agents (on servers)
- Uses centralized credentials
- Scheduled tasks to evaulate all accessible data stores
- Builds invetory of known data
- Dependent upon rule set developed by admistrators

Mobile DLP

- Least mature area of DLP
- Specialty software from unique vendors
- General Areas of Interest:
  Blackberry/iPhone/Android
  iPad and Tablets
  VPN clients

	Desktop DLP	Network DLP	Network Discovery	Mobile DLP
Monitor locally stored files	Yes	No	Some	Yes
Monitor files being written	Yes	No	No	Yes
Monitor files being stored on the network	Some	Some	Yes	No
Monitor files being sent via email (unencrypted)	Yes	Yes	No	Some
Monitor files being sent via email (encrypted)	Yes	No	No	Some
Monitor files being sent via web upload (Unencrypted)	Yes	Yes	No	Some
Monitor files being sent via web upload (encrypted)	Yes	No	No	Some
Monitor files being sent by unencrypted streaming/upload	Yes	Yes	No	Some
Monitor files being sent by encrypted streaming/upload	Some	No	No	No
Perform DLP for uncredentialed devices/users	No	Yes	No	No
Log data being accessed while local DLP is disabled	No	Yes	Some	No
Monitor files being printed	Yes	Some	No	No
Monitor IM chats	Yes	Yes	No	No
Monitor clipboard activities	Yes	No	No	No
Monitor Input/Output buffers	Yes	No	No	No
Utilize Keyword detection	Yes	Yes	Yes	Yes
Utilize Pattern Recognition	Yes	Yes	Yes	Yes
Utilize Fingerprinting	Yes	Yes	Yes	No
Monitor only mode	Yes	Yes	Yes	Yes
User Alterting Mode	Yes	Some	No	Yes
Prevention Mode	Yes	Some	No	Yes

2 Methodologies

Content Analysis

Tagging

4 Detection Mechanisms

Keyword

Pattern Recognition

Fingerprint

Tagging

Primary Vendors

Pros

Cons

Pros

Cons

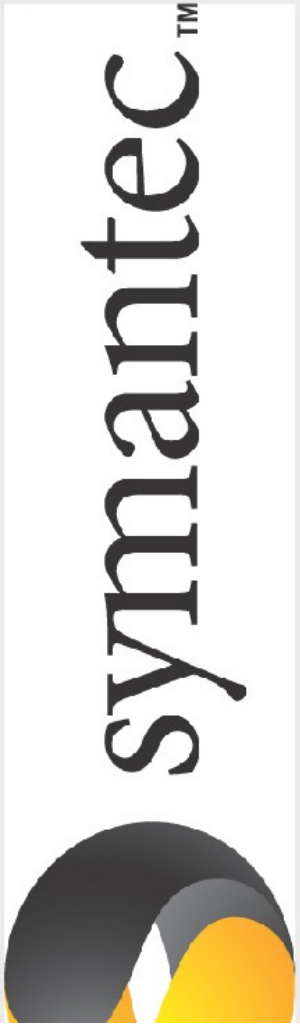
Pros

Cons

Pros

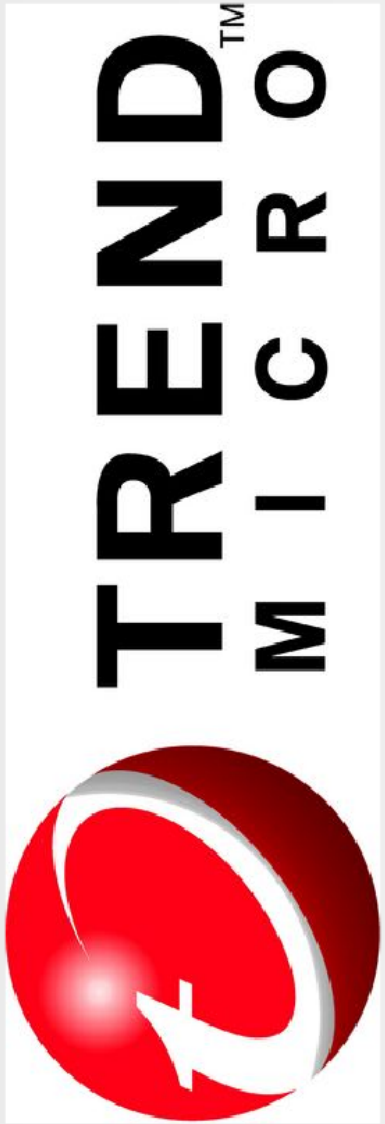
Cons

This is just the opinion of the INL, and presented here as our lessons learned only...



Pros

Cons



Pros

- Lightweight agent
- Need to finalize basic information

Cons

- Seperate agent per function
- Restricted DLP rulesets

Pros

- Integates into existing ePO structure
- Most powerful detection engine
- Works with variety of applications
- Also available:
  Network DLP
  Data Crawlers

Cons

- Weak fingerprinting technology
- Complicated rule-building interface
- no AD intergration of IAM

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Pros

- Lightweight agent
- Need to finalize basic information

Cons

- Seperate agent per function
- Restricted DLP rulesets

Where we are at....

Contact Information:

Jonathan Homer
Idaho National Lab

208-526-9660
jonathan.homer@inl.gov