

DLP: Old wine in new barrels, or opening Pandora's box?



Wednesday, February 10, 2010

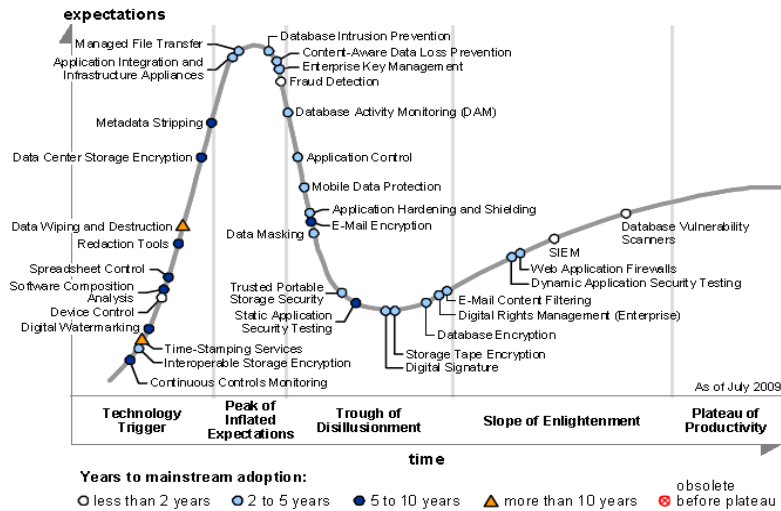


Menu

The hype - we're all part of it



Figure 1. Hype Cycle for Data and Application Security, 2009



Source: Gartner (July 2009)

The hype - based on real incidents and consequences



Information Commissioner takes action against Highland Council after two laptops are stolen

Twitter suffers from hacking incident as documents are downloaded and published across the internet

Details of over 14,000 people lost after security-protected laptop is stolen from council offices

What was predicted around Data Security in 2009? And what happened ...



- Employees laying off workers will clamor for data protection tools
- Enterprise rights management (ERM) won't go mainstream in 2009
- Full disk encryption would be deployed in the majority of corporations
- Despite interest in DLP, most deployments would fail to move beyond pilots
- Headlines will transform entitlement management into a CEO-level concern
- Client virtualisation will be adopted by many more enterprises



Source: Forrester

5

© Copyright Dimension Data 2010

10 February 2010

What is predicted around Data Security in 2010?



Data Security budgets in 2010 will flat-line

Enterprises will strike better deals on DLP – it's a buyers' market

Cloud data concerns will begin to dissipate

Full Disk Encryption will continue its slow and steady march

Source: Forrester

6

© Copyright Dimension Data 2010

10 February 2010

Data Loss Prevention is a priority



2010 Security technology project priorities (n = 308)

Security project portfolio placement (listed in "Top 5" priorities)

1	Intrusion prevention	47.5%
2	Patch management	46.1%
3	Data loss prevention	44.5%
4	Antivirus	41.1%
5	Identity management	41.1%
6	Firewalls	37.4%
7	Vulnerability assessment	37.4%
8	Network access control	35.5%
9	Security information and event management	35.5%
10	Remote-access or site-to-site VPN	31.2%

92% of organisations claim they either currently use or plan to adopt DLP models within the next 12 months

PC theft/loss is the major perceived threat across most vertical segments, business size categories and regions

Non-intentional data incidents are a real concern for organisations because of the threat of reputation damage

Source: IDC Global Security Survey, 2009

Source: Gartner IT Key Metrics Data 2010 (December 2009)

7

© Copyright Dimension Data 2010

10 February 2010

What is DLP?

It's Risk Management with a different state of mind



DLP allows organisations to set up, operate and distribute an effective security policy for information flow in order to keep control of critical information, prevent accidental breaches of compliance and confidentiality policy and support the user's ubiquity while using laptops or smaller devices

(IDC 2009)

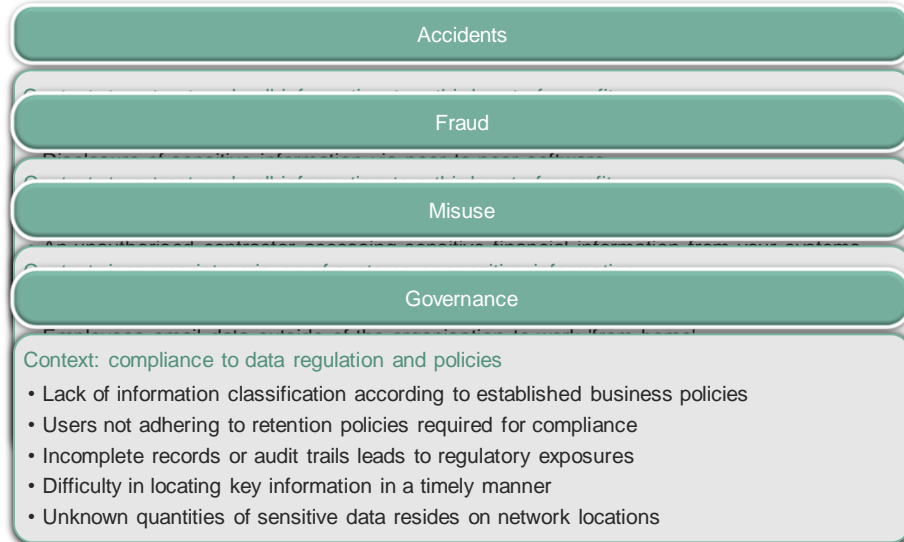


8

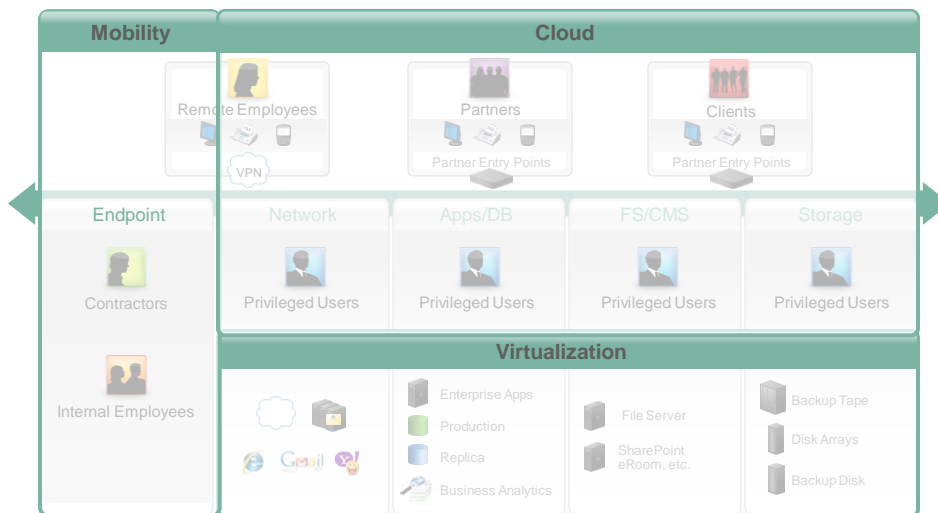
© Copyright Dimension Data 2010

10 February 2010

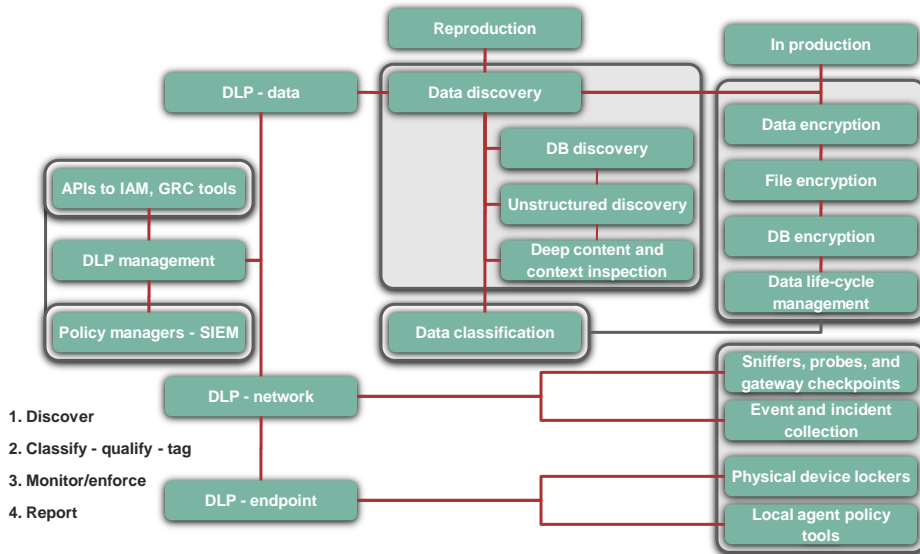
Data Loss incidents – what to look out for



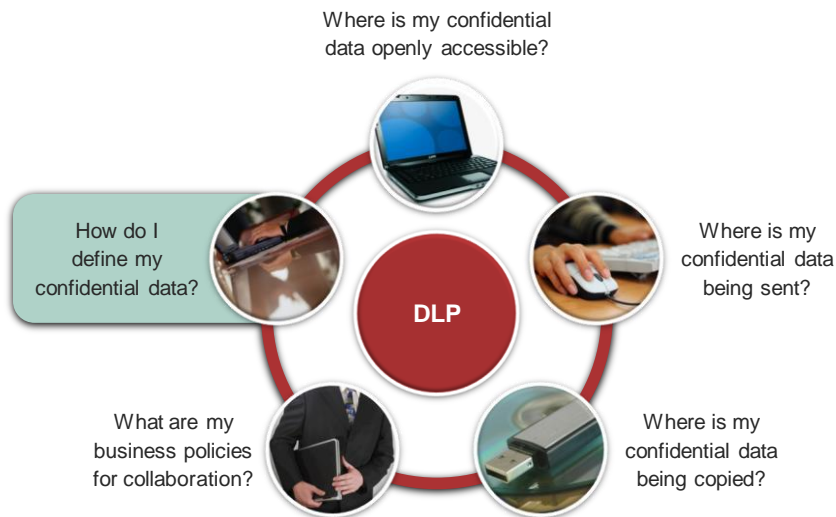
The way your infrastructure looks will determine the scope for your DLP requirements



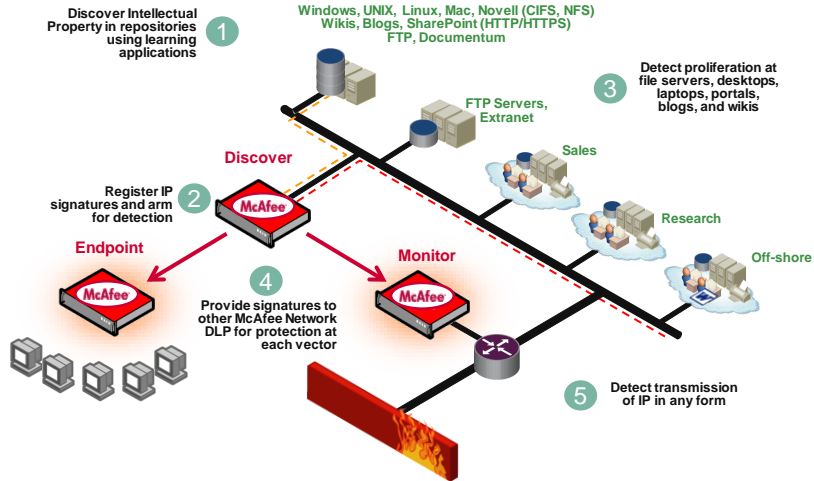
The process around DLP – according to IDC



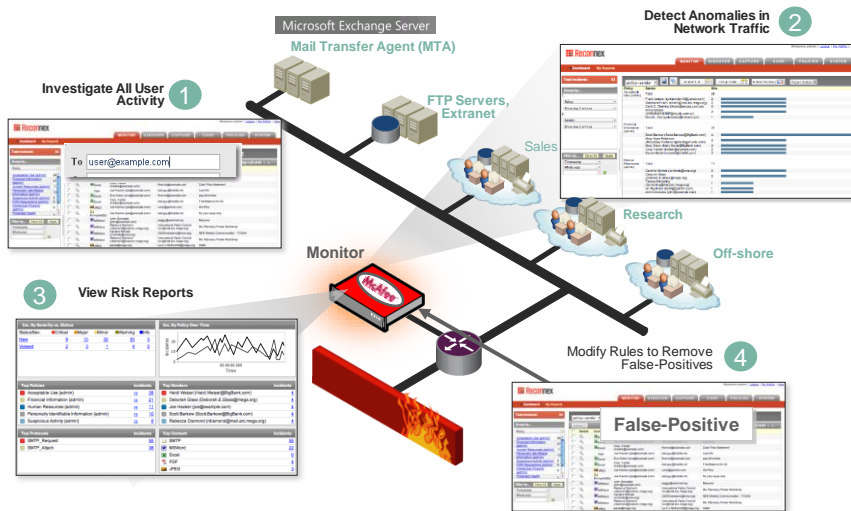
The fundamental questions to prevent data loss



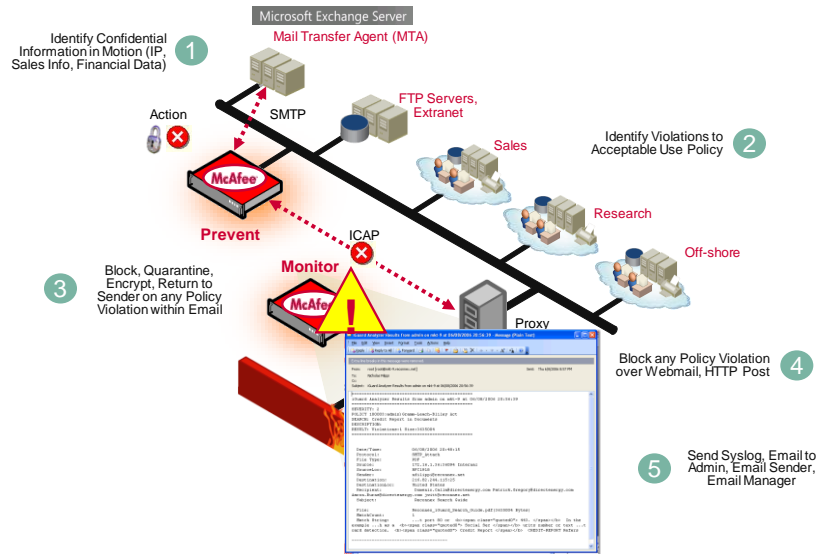
Data-at-rest: discovery and classification



Data-in-motion: monitor and capture



Data-in-motion: prevent violations



15 © Copyright Dimension Data 2010

10 February 2010

Sample standard searches:

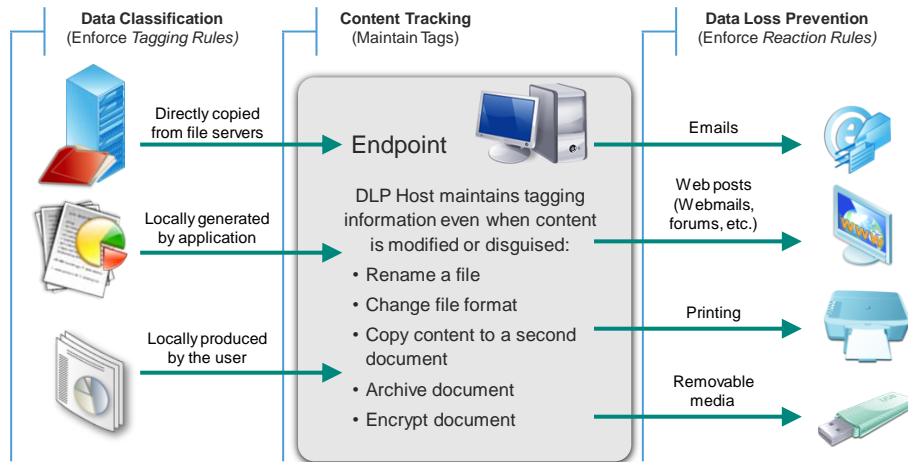


- Find covert email
- Find confidential documents
- Find FTP traffic containing source code.
- Identify disgruntled employees
- Find data leaked in the past
- Find transmission of financial information
- Find postings to social networking sites
- Find transmission of information to foreign nationals
- Tune a rule to exclude approved business practices
- Find Unencrypted User Account Information
- Scan for Sensitive Data
- Prevent Release of Privacy Information
- Find Sensitive Data Moved to Insecure Locations

16 © Copyright Dimension Data 2010

10 February 2010

H-DLP – how does it work?



17

© Copyright Dimension Data 2010

10 February 2010

DLP – where to start?



Acknowledge the challenge of moving from a network-centric view on security to a data-centric approach

Engage experts on information / data lifecycle management in this process – they might not currently be part of your IT security team, but will understand, for example, data rights management

Create an overall plan and roadmap around data-centric security and DLP

Make sure that your roadmap includes point solutions to point problems, without allowing that process to make your DLP strategy reactive

18

© Copyright Dimension Data 2010

10 February 2010

Think broad AND create immediate impact



Some organisations faced important challenges when they tried to build-up complex sets of rules and generate data protection policies.

IDC believes policy work should be focused on immediate needs and kept simple in the first steps of implementation.

Interesting to notice that majority of these urgent needs are generally covered by the common compliance requirements such as privacy protection, financial and HR data protection, critical processes protection, etc.

Compliance policies could be easily implemented as most of DLP solutions provide out of the box policy templates that could be used to respond to current regulations and standards of different geographies, specifically for large organisation. These templates allow also smooth adoption of DLP technology through reusability. Advanced tuning could happen rapidly after full implementation.

(IDC 2009)

Practical steps you need to take



Conduct a DLP Assessment

DLP Assessment – baseline your maturity



Workshop

Conduct a 120 questionnaire with selected key stake holders with an interest in data security



Discovery

Implement data discovery appliance to the network and/or file repositories



Analysis

Collate and analyse the results and benchmarks from the workshop along with the results from the data discovery phase



Presentation

Write a report that details the findings and recommendation
Present the findings and recommend next steps

21

© Copyright Dimension Data 2010

10 February 2010

DLP Assessment – deliverables



A written report covering:

- Executive summary which provides a summary of the exercise process and findings, a statement of the project **scope** as well as non-technical descriptions of all **high-risk findings** along with associated technical risks
- Selected **high-impact, lowest-cost remediation measures** to be implemented across the four sections to bring the customer to “accepted posture levels”. The four sections are:
 1. Risk management
 2. People and organisation
 3. Policies and processes
 4. Technology
- **Detailed technical findings** which encompass the following areas:
 - › Most critical data security violations
 - › Data flows including traffic analysis
 - › Top 10 from emails and search terms (pre-defined and custom built)
 - › Detailed search term outcomes

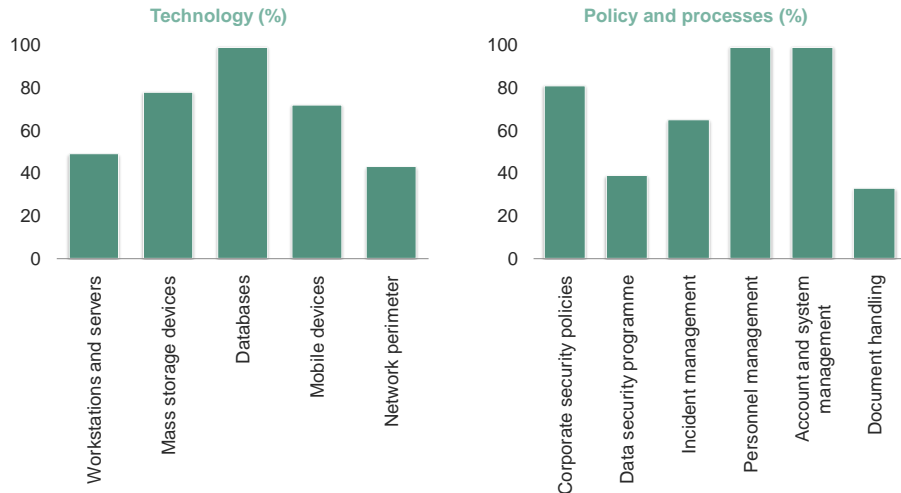


22

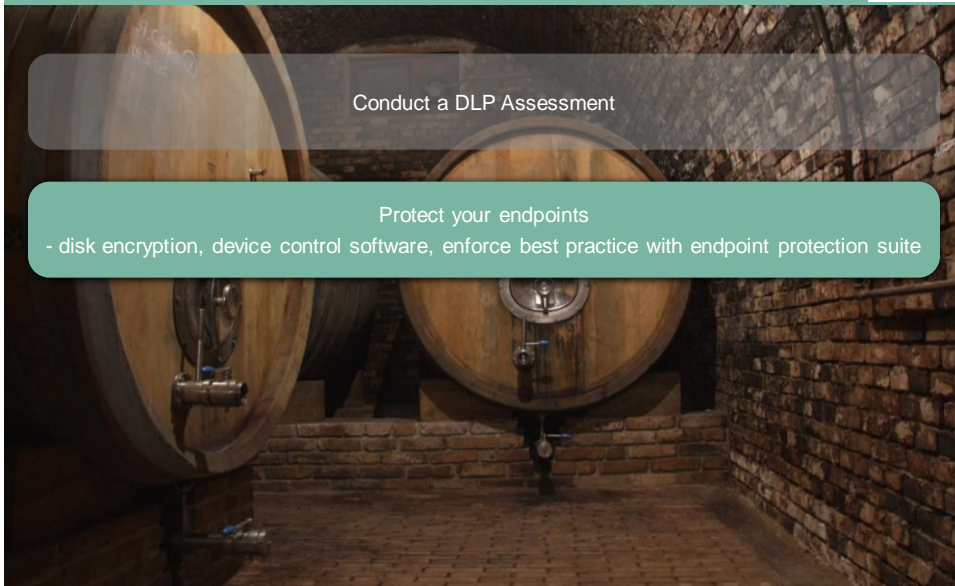
© Copyright Dimension Data 2010

10 February 2010

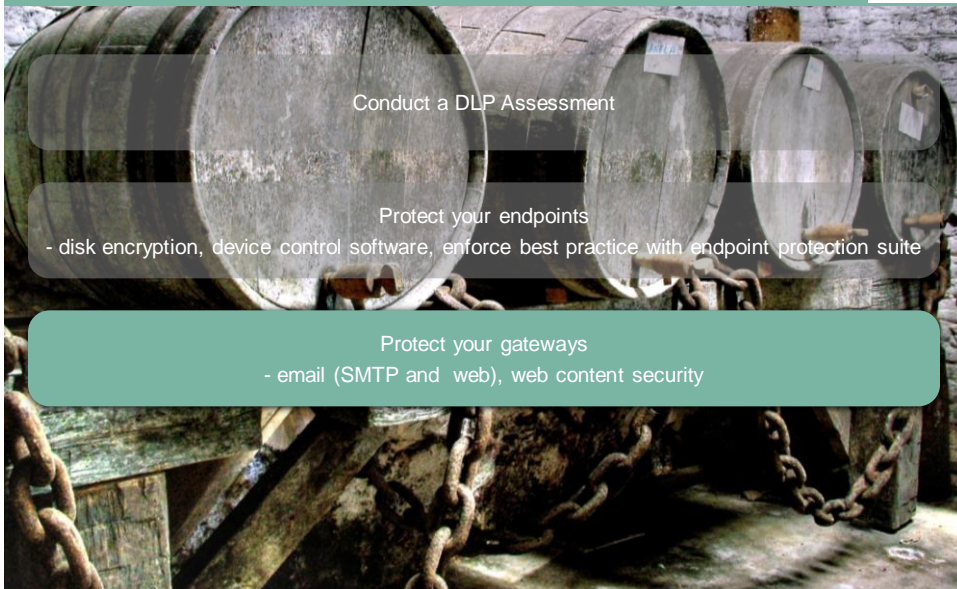
DLP Assessment – deliverables



Practical steps you need to take



Practical steps you need to take



Conduct a DLP Assessment

Protect your endpoints

- disk encryption, device control software, enforce best practice with endpoint protection suite

Protect your gateways

- email (SMTP and web), web content security

Practical steps you need to take



Conduct a DLP Assessment

Protect your endpoints

- disk encryption, device control software, enforce best practice with endpoint protection suite

Protect your gateways

- email (SMTP and web), web content security

Discover and classify your data

THANK YOU



Wednesday, February 10, 2010