



# Consequences for loss of Sensitive Data

- ▶ \$5 million to recover lost or stolen corporate data

Ponemon Institute 2007

- ▶ \$330,000 is the average value of information held on a laptop

FGI Research April 2007

- ▶ 53% of organisations would never know what data was lost

Ponemon Institute 2007

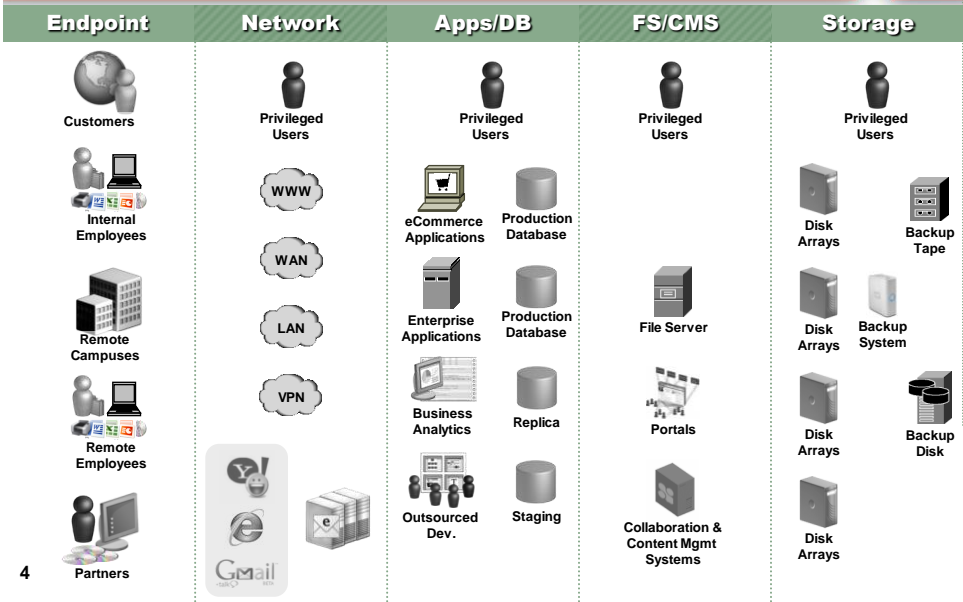
- ▶ 98% of data leaks are due to accidental breach or stupidity

CSI/FBI Computer Crime 2007

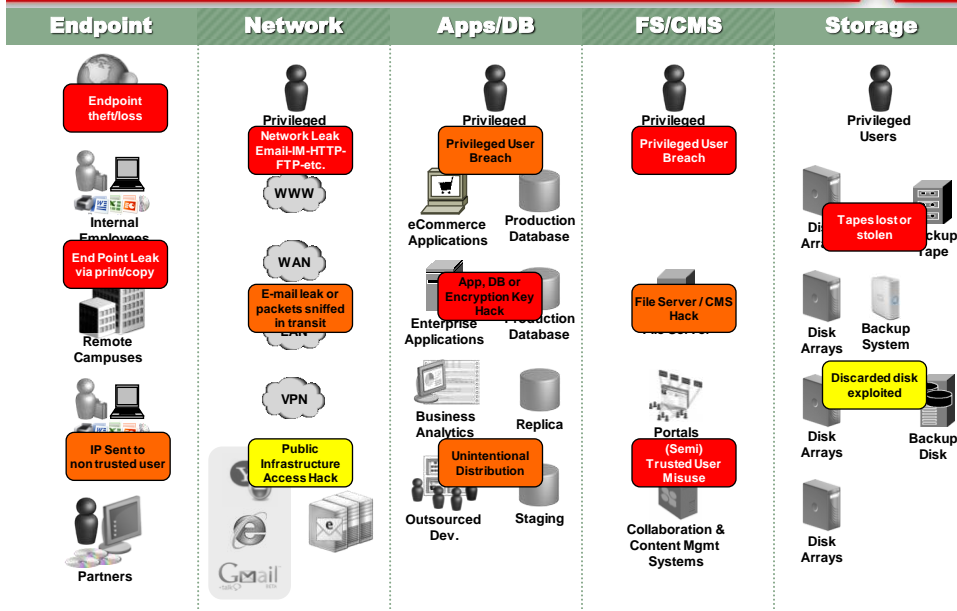


# Why is Information Security So Difficult?

...because sensitive information is always moving and transforming

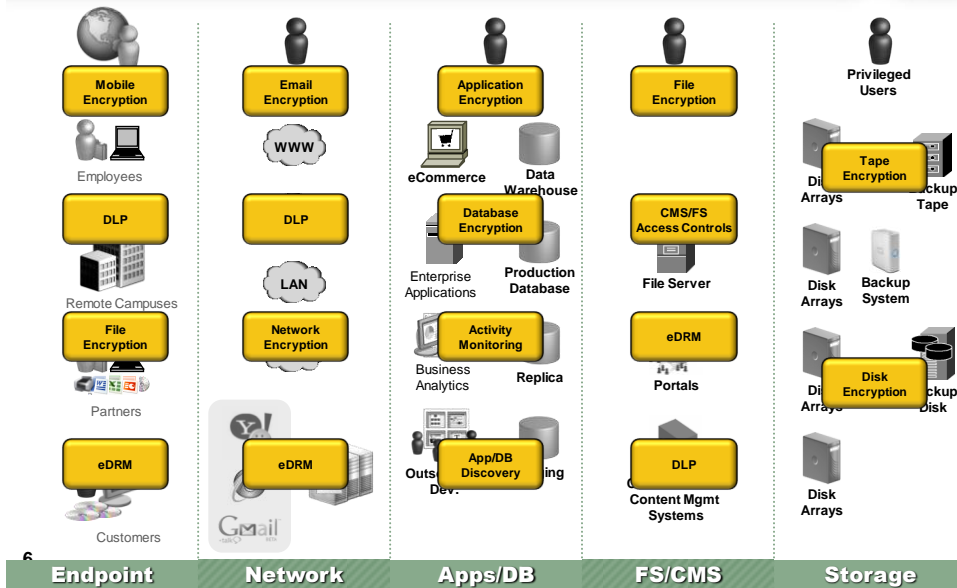


# We Are Exposed At Every Point



# A Landscape of Point Tools

...at each of these points of infrastructure



# The Cost To Our Businesses

Immediate Financial Impact		Strategic Impact	
<ul style="list-style-type: none"> <li>• Notification costs</li> <li>• Leakage investigation costs</li> <li>• Crisis management costs</li> <li>• Customer credit monitoring costs</li> </ul>		<ul style="list-style-type: none"> <li>• Loss of brand equity</li> <li>• Loss of customer loyalty</li> <li>• Probable loss of revenue</li> <li>• Potential law suits and fines</li> </ul>	
Statistics on Reported Data Leakage Incidents in the US		% of Data Leakage Incidents by Industry between 2004-2007	
<b>245.303 Million</b>	Number of records leaked in US since Jan 2005	35%	Retail
<b>\$231</b>	Average cost per record lost	22%	Food & Beverage and hospitality
<b>66%</b>	The victim did not know the data was on the system	19%	Tech Services & Manufacturing
		3%	Education
		21%	Other

7 Source: Privacy Rights Clearing House, Gartner, Verizon 2008 Breach Investigations Report, RSA Research & Analysis



# How Can DLP Solutions Help?

Endpoint	Network	Apps/DB	FS/CMS	Storage
Customers Internal Employees Remote Campus Employees Partners	Privileged Users VPN	Privileged Users eCommerce Applications Production Database Business Applications Dev.	Privileged Users Production Database Collaboration & Content Mgmt Systems	Privileged Users Disk Arrays Backup Tape Arrays System Disk Arrays Backup Disk Disk Arrays
<ul style="list-style-type: none"> <li>• Monitor and protect egress points (network, endpoints, removable media)</li> <li>• Identify and address sources of risk</li> <li>• Monitor information security policies to assure corporate compliance</li> <li>• Identify broken business processes</li> <li>• Educate employees on policy and risk</li> </ul>				

# The Business Case for DLP

Reduce Risk | Minimize Cost | Avoid Disruption

## Reduce Risk

1. What can you find? Where is it?
2. What can you do about it?
3. Time to Value

## Minimize Cost

1. Product
2. People
  - a) Setup/Maintain
  - b) Investigations
  - c) Remediation
3. Infrastructure

## Avoid Disruption

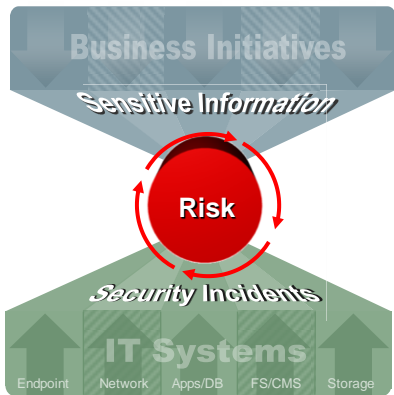
1. Consider the “who” not just “what”
2. Make controls transparent to users
3. Involve the data owners

9



# Information Risk Management

a strategy for protecting your most critical assets



### Information-centric

Clarifies business context and reveals potential vulnerabilities

### Risk-based

Establishes a clear priority for making security investments

### Repeatable

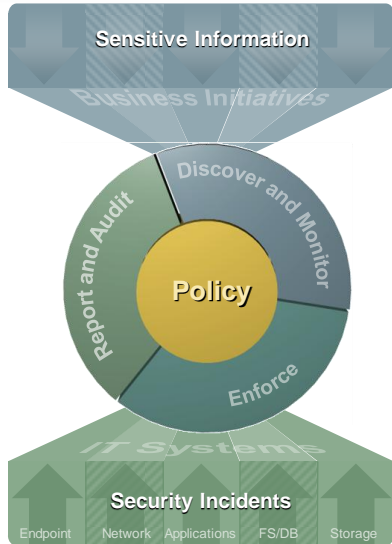
Based on foundation of broadly applicable best practices and standard frameworks

Reveals where to invest, why to invest, and how security investments map to critical business objectives

10



## Six Best Practices for Enterprise Data Protection



- ▶ Understand what data is most sensitive to your business
- ▶ Know where you most sensitive data resides
- ▶ Understand origin and nature of risk
- ▶ Select appropriate controls based on policy, risk and location of data
- ▶ Manage security centrally
- ▶ Audit security constantly



The Security Division of EMC

## RSA Data Loss Prevention Solutions

The Challenge

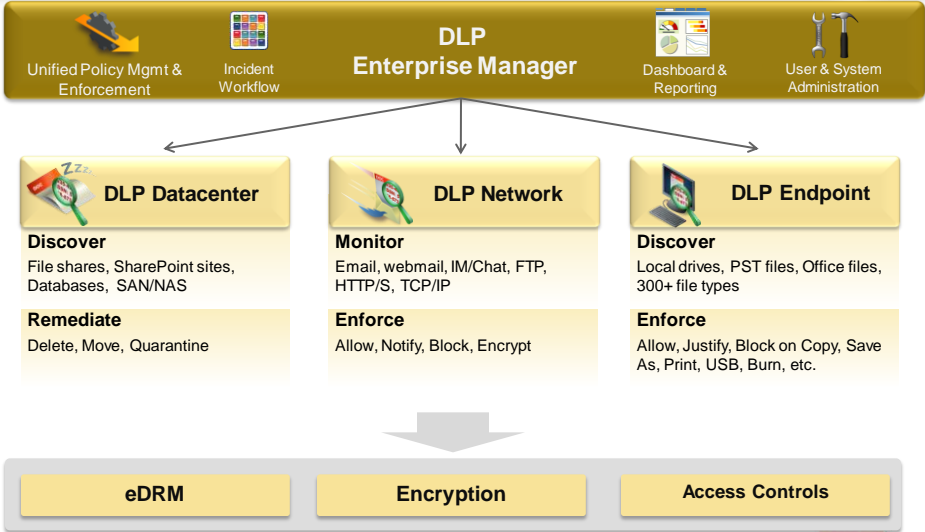
The Solution

Top 5 Success Factors

Case Studies

How RSA Can Help

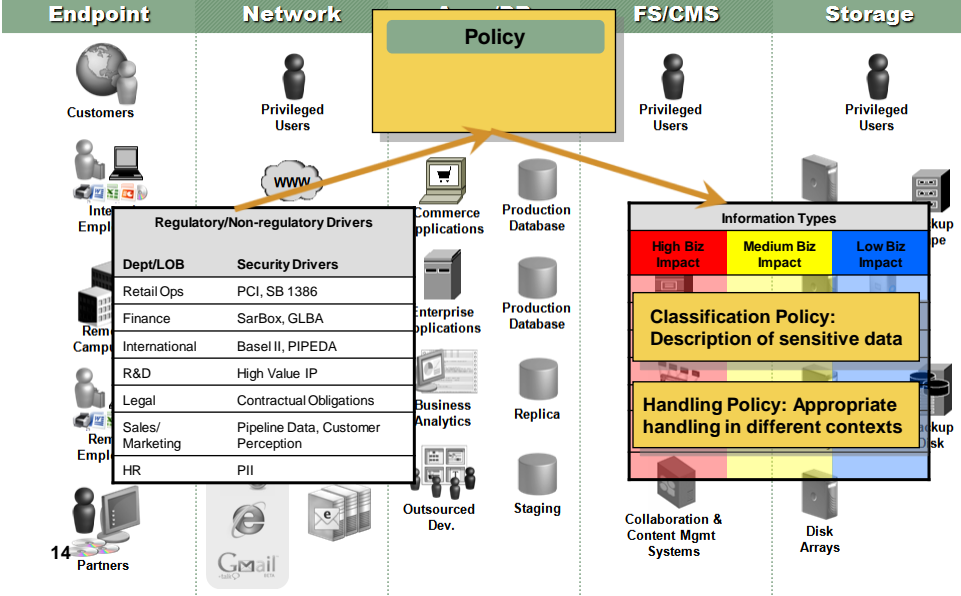
# RSA Data Loss Prevention Suite



13

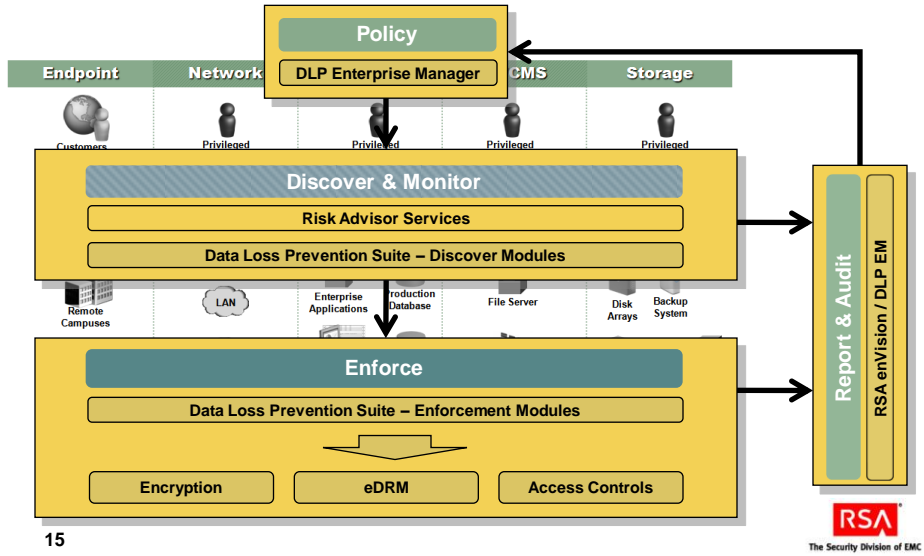


# DLP: Enabling Information-Centric Policy



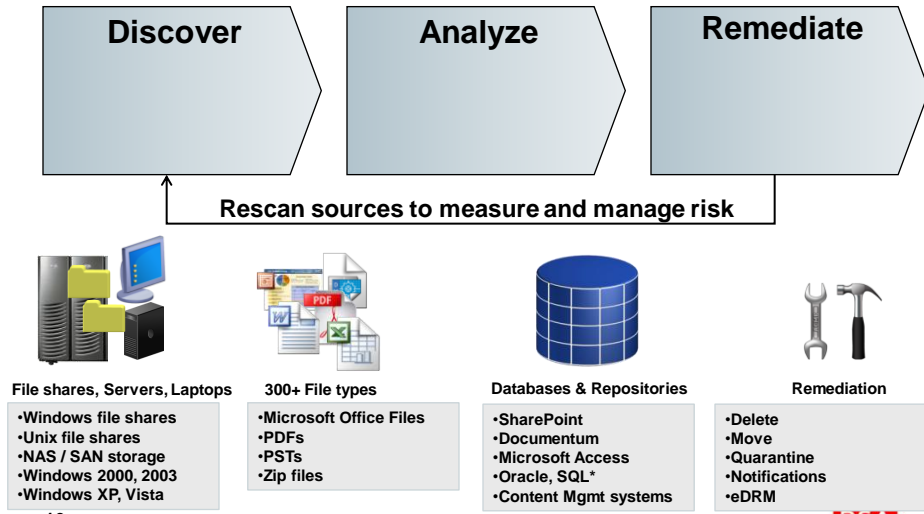
14

# DLP: Part of a Holistic Information Security Process



15

# Reducing Your Sources of Risk: Data at Rest



16

\*Roadmap features expected in 1H 09

# Protecting Data in the Network: Data in Motion



Email

- SMTP email
- Exchange, Lotus, etc.
- Webmail
- Text and attachments



Instant Messages

- Yahoo IM
- MSN Messenger
- AOL Messenger



Web Traffic

- FTP
- HTTP
- HTTPS
- TCP/IP



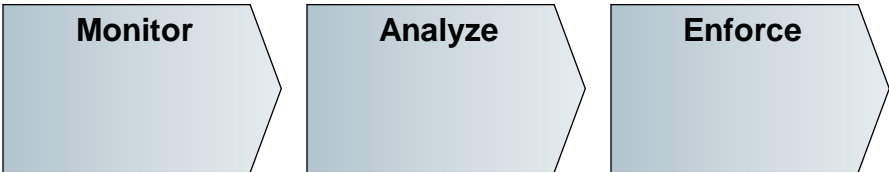
Remediation

- Audit
- Block
- Encrypt
- Log

17



# Protecting Data at the Endpoint: Data in Use



Print & Burn

- Local printers
- Network printers
- Burn to CDs/DVDs



USB

- External hard drives
- Memory sticks
- Removable media



Copy and Save As

- Copy to Network shares
- Copy to external drives
- Save As to external drives



Actions & Controls

- Allow
- Justify
- Block
- Audit & Log

18



**RSA**  
**Data Loss Prevention Solutions**

- The Challenge
- The Solution
- Top 5 Success Factors**
- Case Studies
- How RSA Can Help

**1 Policy + Classification**

<b>Critical Factors</b>	<ul style="list-style-type: none"> <li>• Effort involved in building policies, content types &amp; classifying data</li> <li>• Ability to look for and correlate combinations of content</li> <li>• Resulting accuracy of the overall solution</li> </ul>
<b>Solution</b>	<ul style="list-style-type: none"> <li>• Policy Research Team provides finely-tuned policies, content types and classification libraries -- yield highest accuracy ratings in the industry</li> <li>• Content correlation allows you look for and correlate combinations of data</li> </ul>
<b>Value</b>	<ul style="list-style-type: none"> <li>• Faster time to value → Less to setup and tune</li> <li>• Lower TCO → Fewer false alerts to drain your people</li> </ul>

## 2 Identity Aware: Policy and Response

<b>Critical Factors</b>	<ul style="list-style-type: none"> <li>• Identity-based Policy: E.g. data x ok in the hands of group y</li> <li>• Identity-based notification: E.g. Notify the persons manager</li> <li>• Identity-based control: E.g. lock this data so only group x can open</li> </ul>
<b>Solution</b>	<ul style="list-style-type: none"> <li>• We can leverage AD groups for policy and notification</li> <li>• Our integration with Microsoft RMS provides group specific controls, and enables protection beyond the boundaries of your company</li> </ul>
<b>Value</b>	<ul style="list-style-type: none"> <li>• Lower Risk → We can catch things specific to a given group</li> <li>• Lower TCO → Involve the business/data to resolve their own problems</li> <li>• Less Disruption → BU/data owners will understand impact better</li> </ul>

21



## 3 Incident Response Workflow

<b>Critical Factors</b>	<ul style="list-style-type: none"> <li>• Will you get lots of alerts for the same incident?</li> <li>• Will you get the relevant info to remediate without digging for it?</li> <li>• Can you get the alert to the right person/people in the right order?</li> </ul>
<b>Solution</b>	<ul style="list-style-type: none"> <li>• We correlate and group events so you get a single alert for an incident</li> <li>• We provide all relevant information for the event</li> <li>• We leverage AD groups for notification → get the incident to the right people</li> </ul>
<b>Value</b>	<ul style="list-style-type: none"> <li>• Less Disruption → Involving data owners and giving them the right info, results in better responses</li> <li>• Less People → Less effort on incident handling. Fewer alerts to sort through. Alert routes all pertinent info to the right person</li> </ul>

22



## 4 Scale: Distributed Environments with Large Data Stores

<b>Critical Factors</b>	<ul style="list-style-type: none"> <li>• Distributed sites: will you need dedicated h/w and setup?</li> <li>• Scan optimization: Is this manual or automated?</li> <li>• Large data stores: will this be a bottleneck with each policy change?</li> </ul>
<b>Solution</b>	<ul style="list-style-type: none"> <li>• Grid workers &amp; temporary agents → Use your existing hardware</li> <li>• Automatic scan optimization: Figures out how to leverage your hardware</li> <li>• Grid Scanning: Analyze large repositories in parallel – 10x</li> </ul>
<b>Value</b>	<ul style="list-style-type: none"> <li>• Lower TCO: Less h/w to buy. No time spent configuring/optimizing</li> <li>• Faster time to value → Get actionable results sooner</li> <li>• Less Risk → Faster scanning means smaller risk windows</li> </ul>

23



## 5 Single Policy Framework for Infrastructure

<b>Critical Factors</b>	<ul style="list-style-type: none"> <li>• Create a single policy set for a given regulation or class of data, and leverage that throughout the infrastructure</li> <li>• Leverage your existing infrastructure versus adding more point tools</li> </ul>
<b>Solution</b>	<ul style="list-style-type: none"> <li>• DLP Suite uses a common policy framework for all components including integrations</li> <li>• Microsoft: Building RSA DLP into their products. AD RMS in Dec '08</li> <li>• Cisco: Integrating with Cisco products at the NW, datacenter and end point</li> <li>• EMC: Integrating with Documentum, Celerra, SourceOne, etc.</li> </ul>
<b>Value</b>	<ul style="list-style-type: none"> <li>• Less Risk → Enterprise wide coverage. Catching things anywhere</li> <li>• Less Cost → Leverage your existing infrastructure. Less things to buy, deploy and manage</li> </ul>

24



## Other Best Practices for DLP

- ▶ Don't boil the ocean: Start with top 1 - 3 policies
- ▶ Don't just focus on controls – look at the processes
  - Much of the problem stems from broken business/IT process
  - Work with BU and data owners to resolve
- ▶ Leverage DLP to educate employees on corporate policies
- ▶ Remediation
  - Involve BU and data owners
  - Automate in stages: Audit → Notify → Block
- ▶ Governance Reporting: Help management understand the value of the solution in reducing risk

25



## RSA Data Loss Prevention Solutions

The Challenge  
The Solution  
Top 5 Success Factors  
Case Studies  
How RSA Can Help

## Customers From A Wide Range of Industries

## Case Study: Technology Company

# Microsoft®

Minimized risk by discovering all HBI data from 106K users

Driver	Situation	Solution	Results
<ul style="list-style-type: none"> <li>Protect High Business Impact (HBI) Data</li> <li>PCI, PII and Intellectual Property</li> </ul>	<ul style="list-style-type: none"> <li>100 TB of data in file shares</li> <li>30,000 file shares</li> <li>120,000 SharePoint sites</li> </ul>	<ul style="list-style-type: none"> <li>DLP Datacenter with site coordinators in Redmond, &amp; India</li> <li>12 machine Grid System</li> </ul>	<ul style="list-style-type: none"> <li>Selected for scalability, performance, accuracy</li> <li>Incremental scans in ½ day</li> <li>Managed by 2 people</li> </ul>

## Case Study: Healthcare Provider



**Monitors transmissions for HIPAA and to prevent risk**

Driver	Situation	Solution	Results
<ul style="list-style-type: none"> <li>• Protect privacy of patient information</li> <li>• FDA, GLB, HIPPA, SOX, PCI</li> <li>• Proactive Approach to Data Protection</li> </ul>	<ul style="list-style-type: none"> <li>• Concerns over USB, misdirected emails, blogs, remote users, mobile workforce and webmail</li> <li>• 4K email users and 11k employees/physicians</li> </ul>	<ul style="list-style-type: none"> <li>• DLP Network: Monitor email and web traffic</li> <li>• DLP Datacenter: Discover sensitive file share data</li> <li>• DLP Endpoint: Monitor data in use on laptops</li> </ul>	<ul style="list-style-type: none"> <li>• Identified broken business processes &amp; prioritized efforts</li> <li>• Out of box Templates. Quick "go-live" after PoC.</li> </ul>

29



## Case Study: A Fortune 50 Retailer

### LARGE ★ RETAILER

**Identify and encrypt all emails containing credit card data**

Driver	Situation	Solution	Results
<ul style="list-style-type: none"> <li>• Protect credit card data</li> <li>• Payment Card Industry (PCI) Level 1 credit card processor</li> </ul>	<ul style="list-style-type: none"> <li>• Transmit 1 million plus emails per day</li> <li>• ~2,000 contain sensitive data</li> </ul>	<ul style="list-style-type: none"> <li>• DLP Network integrated with Voltage IBE for encryption</li> <li>• High availability configuration</li> <li>• Installed in-between Exchange &amp; Internet gateways</li> </ul>	<ul style="list-style-type: none"> <li>• Higher accuracy than the competition with 2-3 False Positives per day</li> <li>• No additional headcount allocated</li> </ul>

30



# Case Study: Financial Services



## Protection of Credit Card Data Across Distributed Environment

Driver	Situation	Solution	Results
<ul style="list-style-type: none"> <li>• Protect credit card data of online customers</li> <li>• Need to prevent fraud brought about internal "Deep Defense" project</li> <li>• Competitive pressure</li> </ul>	<ul style="list-style-type: none"> <li>• Internet banking services organization needed to assure online users that all front- and backend transactional processes are secure</li> <li>• Required monitoring across distributed computing environment</li> </ul>	<ul style="list-style-type: none"> <li>• RSA DLP Endpoint is able to execute a distributed scan across all networked computers to analyze content in place without adding a client to the machine</li> </ul>	<ul style="list-style-type: none"> <li>• DLP Endpoint located sensitive data on endpoints, providing increased visibility and stronger controls over sensitive data stored on Digital Insight's equipment</li> <li>• Remediated high risk endpoints</li> </ul>

31



# RSA

## Data Loss Prevention Solutions

- The Challenge
- The Solution
- Top 5 Success Factors
- Case Studies
- How RSA Can Help

# How Can We Help

## Your Current Status

### Gathering Information

- 1. Investigating DLP in general
- 2. Identifying business drivers
- 3. Developing a business case
- 4. Identifying a Project Sponsor

### Planning to Procure and Deploy

- 1. Have a defined DLP project
- 2. Developing a detailed DLP project
- 3. Evaluating DLP vendors

## We Can Help

### By Offering

- 1. *Risk Advisor* to discover current risk
- 2. *Free Scan* to support business case
- 3. ROI/TCO analysis for DLP
- 4. DLP workshop

### By Providing

- 1. A framework for DLP evaluation
- 2. An evaluation environment
- 3. A detailed DLP proposal
- 4. Deployment architecture

# RSA

## Data Loss Prevention Solutions

- The Challenge
- The Solution
- Top 5 Success Factors
- Case Studies
- How RSA Can Help

**RSA DLP and Microsoft**

## Microsoft and RSA Partnering to Secure Sensitive Business Data

Advancing Information Protection with a Built In Approach

**Microsoft**<sup>®</sup>



The Security Division of EMC



The Security Division of EMC

## What have Microsoft and RSA announced?

- ▶ Microsoft and RSA partnering to secure sensitive data with a “Built in vs. Bolt on” approach to protect data based on:
  - Content
  - Context
  - Identity
- ▶ Microsoft building RSA DLP classification technology directly into products to protect sensitive data throughout the infrastructure
- ▶ First step is the RSA DLP Suite’s integration with Active Directory Rights Management Services
  - Automate the application of AD RMS policies based on data sensitivity
  - Deeper integration with AD to leverage groups for identity aware policies and incident response



The Security Division of EMC

## The Business Challenge

Companies face growing risks in protecting data

- Information protection is most important security concern in the enterprise, outranking malware as top priority
- Data loss and liability are growing concern (regulatory and corporate compliance)

Data must be protected, but also be accessible

- Balance required between security and accessibility
- Information must be useable to be of value
- Increasingly need to enable use of information across company boundaries (partners, vendors, customers)

Current solutions are costly and complex

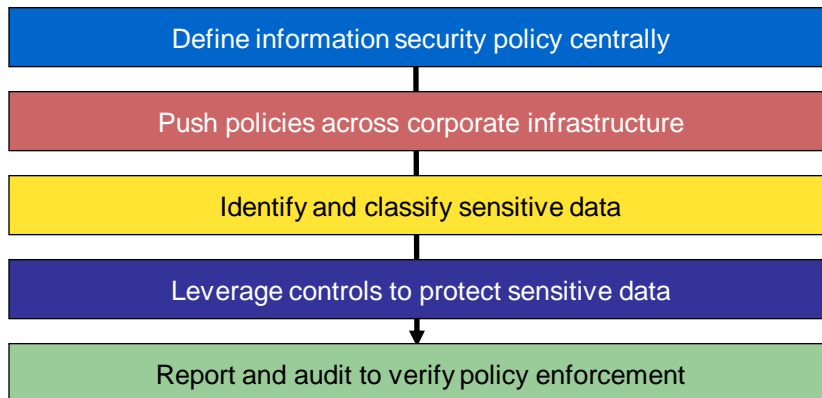
- Difficult to correctly identify and protect sensitive information across the enterprise
- Point solutions require that multiple policies and technologies be stitched together and independently managed



The Security Division of EMC

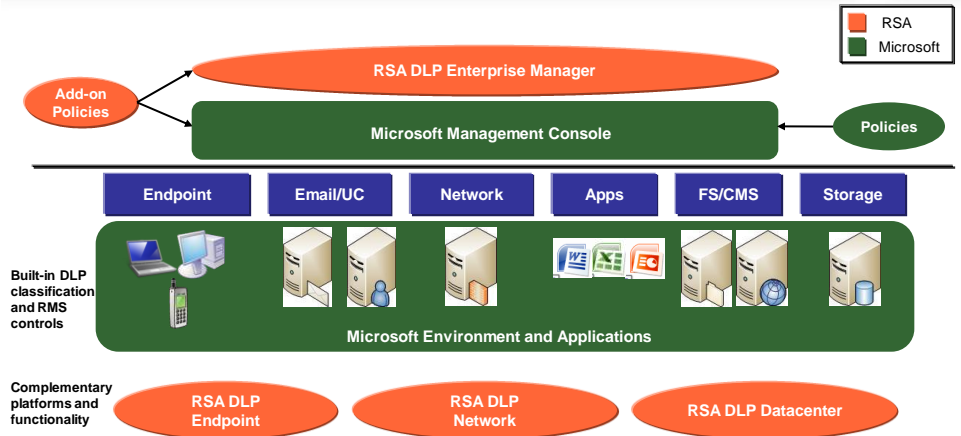
## Microsoft & RSA Developing “Built In vs. Bolt On”

*Building information protection throughout the infrastructure to enable customers to:*



The Security Division of EMC

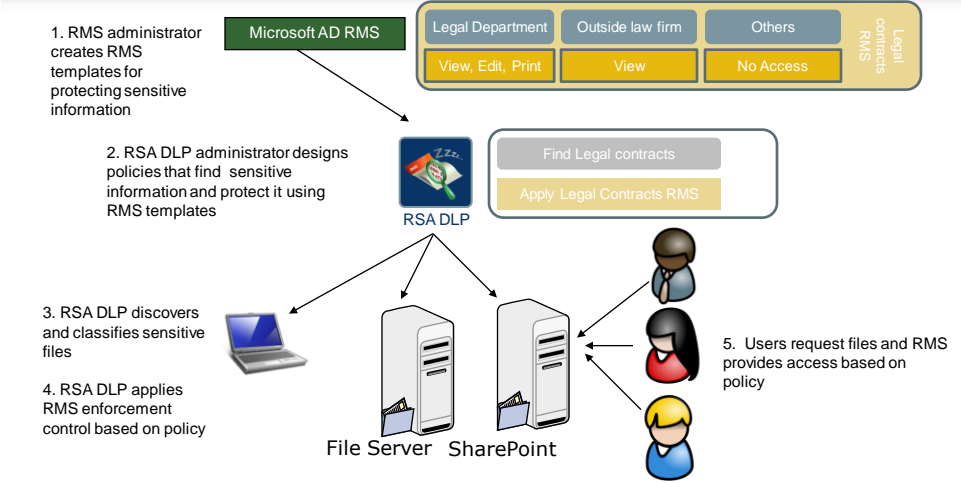
# Long term – Microsoft and RSA Building Information Protection into Infrastructure



- Common policies throughout infrastructure
- Built-in approach to protect data based on content, context, identity
- Future ready: Seamless upgrade path for current DLP customers



# First Step - RSA DLP Suite integrating with Microsoft AD RMS in DLP 6.5 Release



- Automate the application of AD RMS protection based on sensitive information identified by RSA DLP
- Ease the roll out of RMS by applying policies with group by group deployment based on AD organizational/functional groups



## Summary

- Microsoft and RSA partnering to secure sensitive data with a “Built in vs. Bolt on” approach to build protection into the infrastructure
  - Common policies and classification throughout the entire system
  - Provides security while enabling the right levels of accessibility
- Microsoft to build RSA DLP classification technology into products to provide protection based on content, context, and identity
  - Microsoft selected RSA due to its strength in the areas of correlation, policies, scalability
- First step is the RSA DLP Suite’s integration with Active Directory
  - Automate the application of AD RMS policies based on data sensitivity
  - Apply policies at the AD Group level to organizational/functional groups with the highest risk of data breaches
  - Implements persistent security policies



The Security Division of EMC