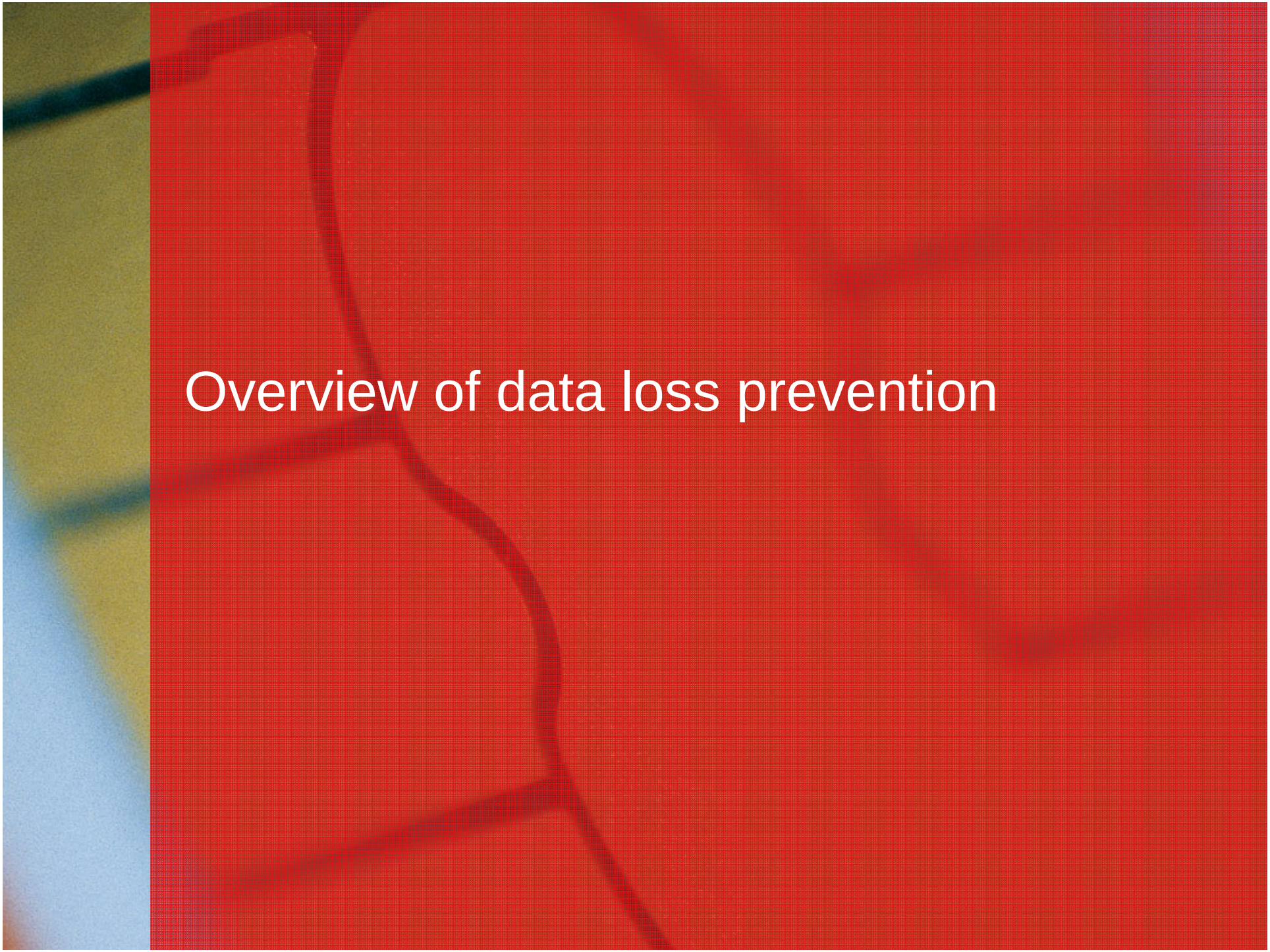
Data Loss Prevention

Edmund Tsui

Technology Consultant

Agenda

- Overview of data loss prevention
- Embarking on a data loss prevention project
- RSA Data Loss Prevention Suite
- Summary


Overview of data loss prevention

Why do we need to prevent data loss?

- Protect information from accidental disclosure
- Protect information from malicious intent
- Meet regulatory compliance requirements

RSA
The Security Division of EMC

Consequences of data loss

- Company reputation
- Lost of customer confidence = business lost
- Legal prosecution
- Costs
- Employee productivity & morale
- Job

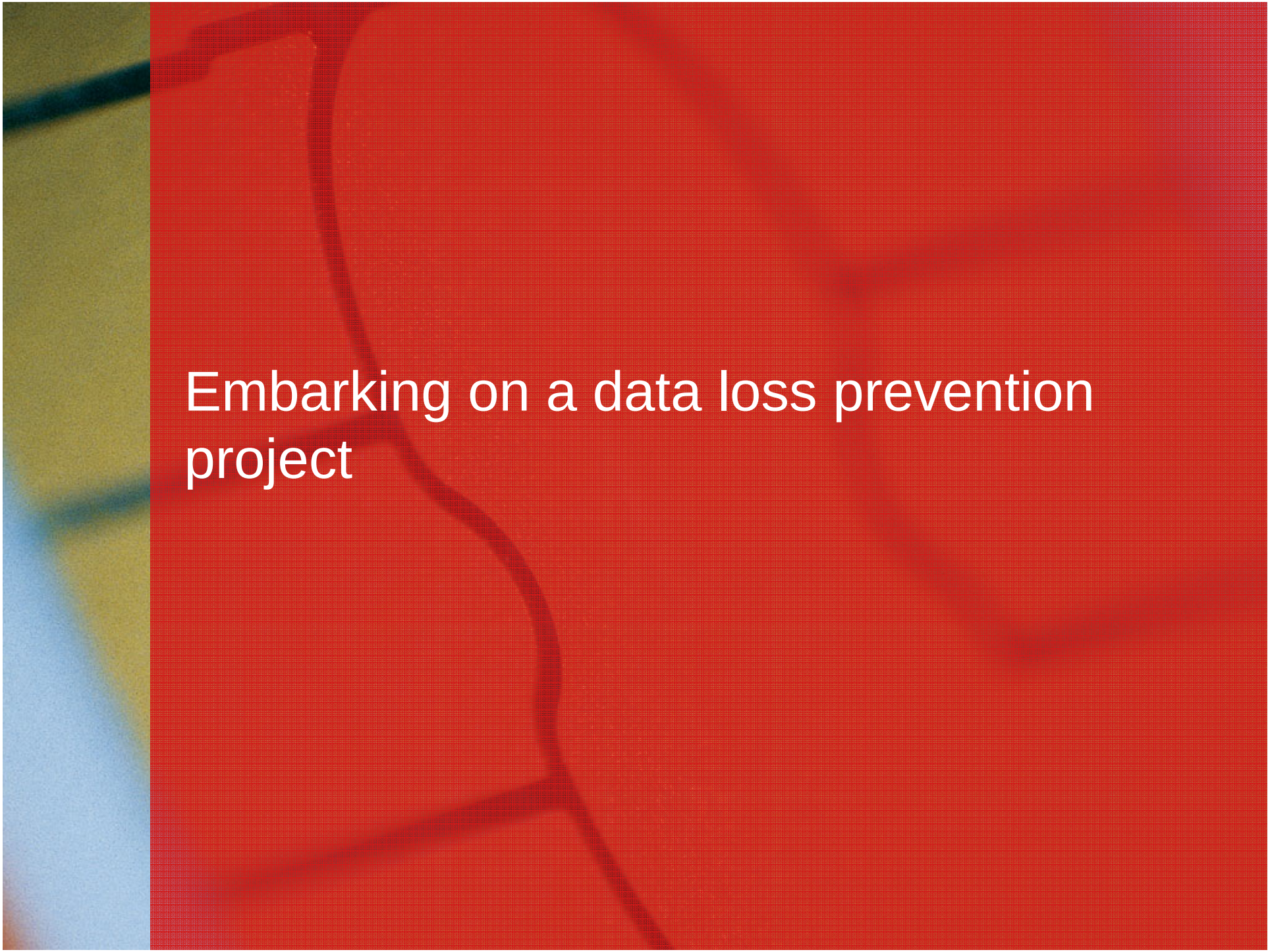
Cost of Data Loss

- Study conducted by Ponemon Institute
- Average cost of data loss is $197 per customer record in 2007
- Lost data translates to lost business opportunity
- Other costs include:
  - Customer support costs such as information hotlines
  - Reputation management
  - Productivity
  - Legal

Source: The Cost of Data Loss article from InformationWeek dated 28 Nov, 2007.

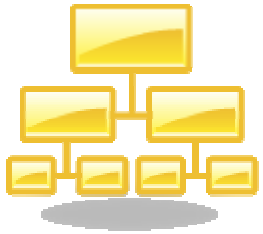
Causes of data loss

- Employees
- Outsourcing
- Contractors
- Consultants
- Partners
- Laptops
- Thumbdrives
- Mobile Devices
- Security Breaches


Embarking on a data loss prevention project

Data loss prevention project activities

- State objectives & benefits
- Get executive sponsors
- Define the project scope
- Gather resources
- Project tasks planning and allocation
- Implementation
- Tracking and reporting
- Project closure and lessons learned
- Repeat



Best Practice 1: Prioritize Data According to Governance, Risk & Compliance

- Take stock of enterprise data
- Basic guidelines for evaluating data:

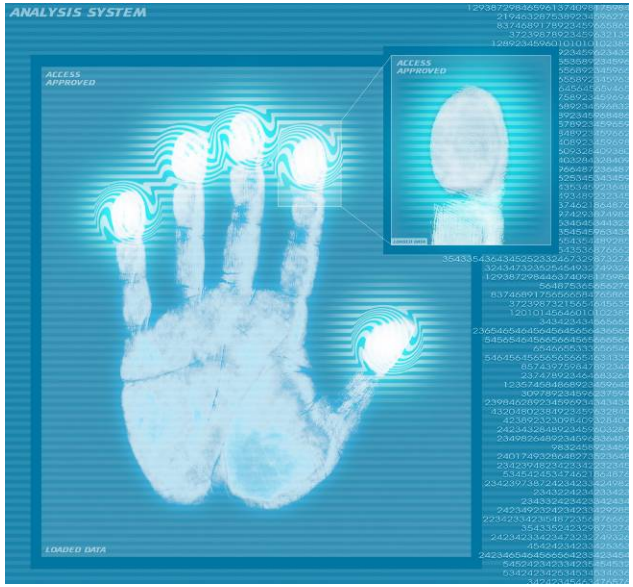
Inventories	Purpose
Types of data that are or should be classified as sensitive	Begin to understand what data requires protection
Locations where you suspect this data to reside	Outline and quantify the systems that will need to be monitored
Business functions that require access to this data	Understand how the data is currently used to keep business flowing
Individuals, by business function, that require access to this data	Learn which individuals could potentially access and expose sensitive data

Best Practice 1: Prioritize Data According to Governance, Risk & Compliance

- Understand what industry or government regulations which your organization must comply
- Evaluate the risk and impact of data breach for each type of data
- Prioritize risks and address the most serious threats first

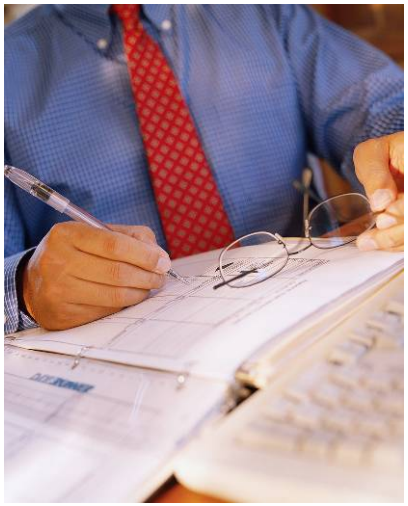
Best Practice 2: Start at the Root of the Problem

- Create an inventory of this data stored across the network
- For a start, only scan for a set of highly sensitive data instead of all the data



Best Practice 3: Build a Project Plan to Operationalize DLP

- Includes clearly defined and achievable benchmarks
- Includes steps to reach these benchmarks
- Aim of project plan is to ensure DLP solution is fully integrated with day to day operations



Best Practice 4: Leverage Cross-functional Teams

- Involve key business team members from across the organization
- Get their feedback on policies and remediation actions

Best Practice 5: Promote a Culture of Data Protection and Awareness

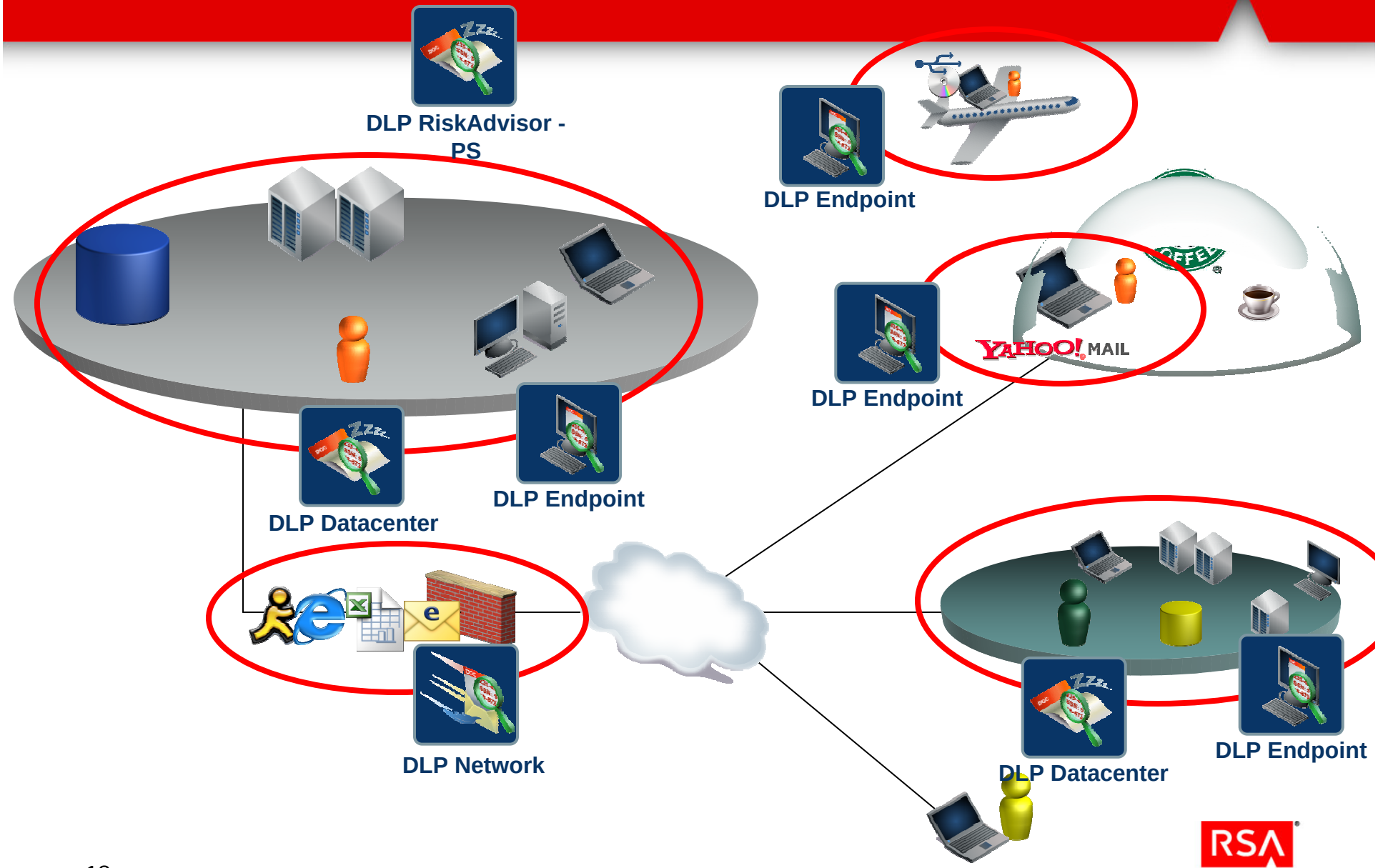
- Technology and policies alone is not sufficient
- Should continuously promote the importance of protecting sensitive data
- Provide security awareness training on an ongoing basis
- Establish ownership of data

Best Practice 6: Expand Coverage

- After discovering and protecting highly sensitive data, what next?
- Decide whether to implement additional safeguards, or
- Expand the data segments covered to medium and lower business impact segments

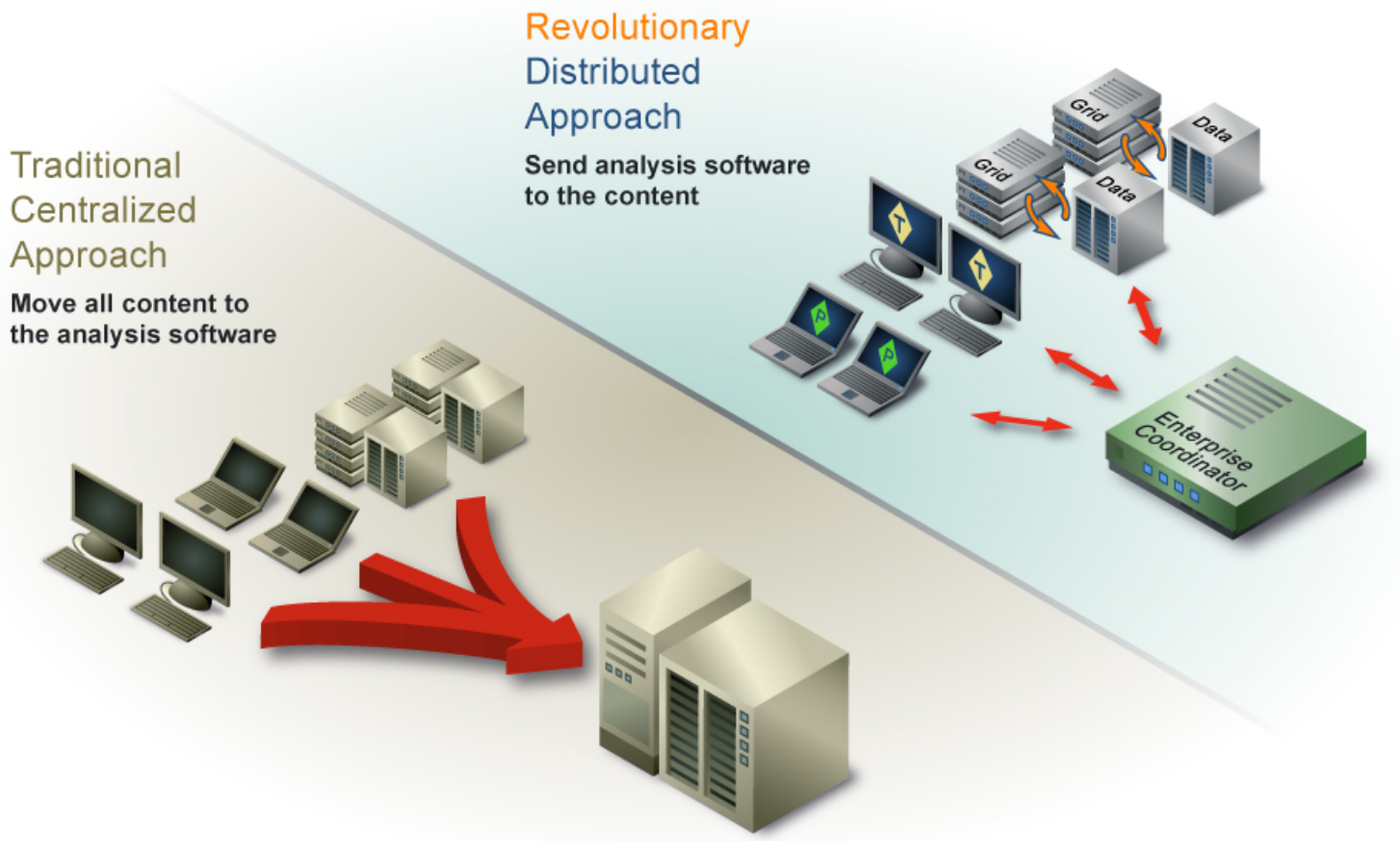
RSA Data Loss Prevention Suite

RSA Data Loss Prevention Suite



RSA
The Security Division of EMC

RSA DLP Discovery Scalability and Performance



RSA DLP Discovery technology provides unmatched performance and scalability via a unique distributed agent architecture

RSA Data Loss Prevention Suite

ENTERPRISE MANAGER

DLP Datacenter

Software (Grid or Agents)

Discover — File shares, SharePoint sites, Database files, SAN/NAS

Remediate — Delete, quarantine, move

DLP Network

Monitor Sensor — **Monitor** — Email (SMTP, IMAP), HTTP/S, FTP, P2P, IM/Chat, etc.

Enforce Interceptor ICAP Server — **Enforce** — Block, Notify, Alert, Encrypt

DLP Endpoint

Discover Software (Agents) — **Discover** — Laptops and desktops with Windows 2000 SP4 or higher OS

Enforce Software (Agents) — **Allow/Block** — Copy, print, save, USB, burn, etc.

DLP RiskAdvisor — **PS Engagement**

Microsoft uses RSA DLP Suite

*"Grid processing and incremental scanning were essential for Microsoft given the volume of data that we store. Also, RSA DLP Datacenter generates matched files with an **accuracy rate consistently at or above 98%**."*

Olav Opedal
Security Program, Microsoft

Cisco & RSA Collaboration

Cisco & RSA Collaboration

- RSA and Cisco will work closely together to develop joint solutions
- Cisco intends to integrate data-classification technology from the RSA's DLP Suite with Cisco's DLP capabilities in the network and on desktop and server endpoints
- RSA plans to take advantage of the various Cisco policy enforcement points with the RSA DLP Suite

Summary

- Technology alone is not sufficient
- Everyone in the organization must play a part
- Make data loss prevention part of organization culture
- Use a proven market solution to facilitate the data loss prevention efforts

The Security Division of EMC

Thank you!