



# Agenda

1. Defining the data protection challenge
2. Inside Data Loss Prevention Solutions
3. Best Practices for data protection
4. Recommendations on next steps



# The Economics of Data Loss

The Financial Services Authority (FSA) has fined Nationwide Building Society (Nationwide) £980,000 for failing to have effective security controls. ChoicePoint to pay \$15 million over data breach. DuPont Employee Walked Away With \$400 Million In Trade Secrets. The former Company scientist downloaded 2,000 sensitive documents and laptop accessed 16,000 e-mails as he sought a job with a competitor ... will

... for a Regulated industry the cost per data record leaked is from \$90 to \$305 ...

Forrester Research

TJX says 4% of sales were compromised. cost per \$1 billion ...

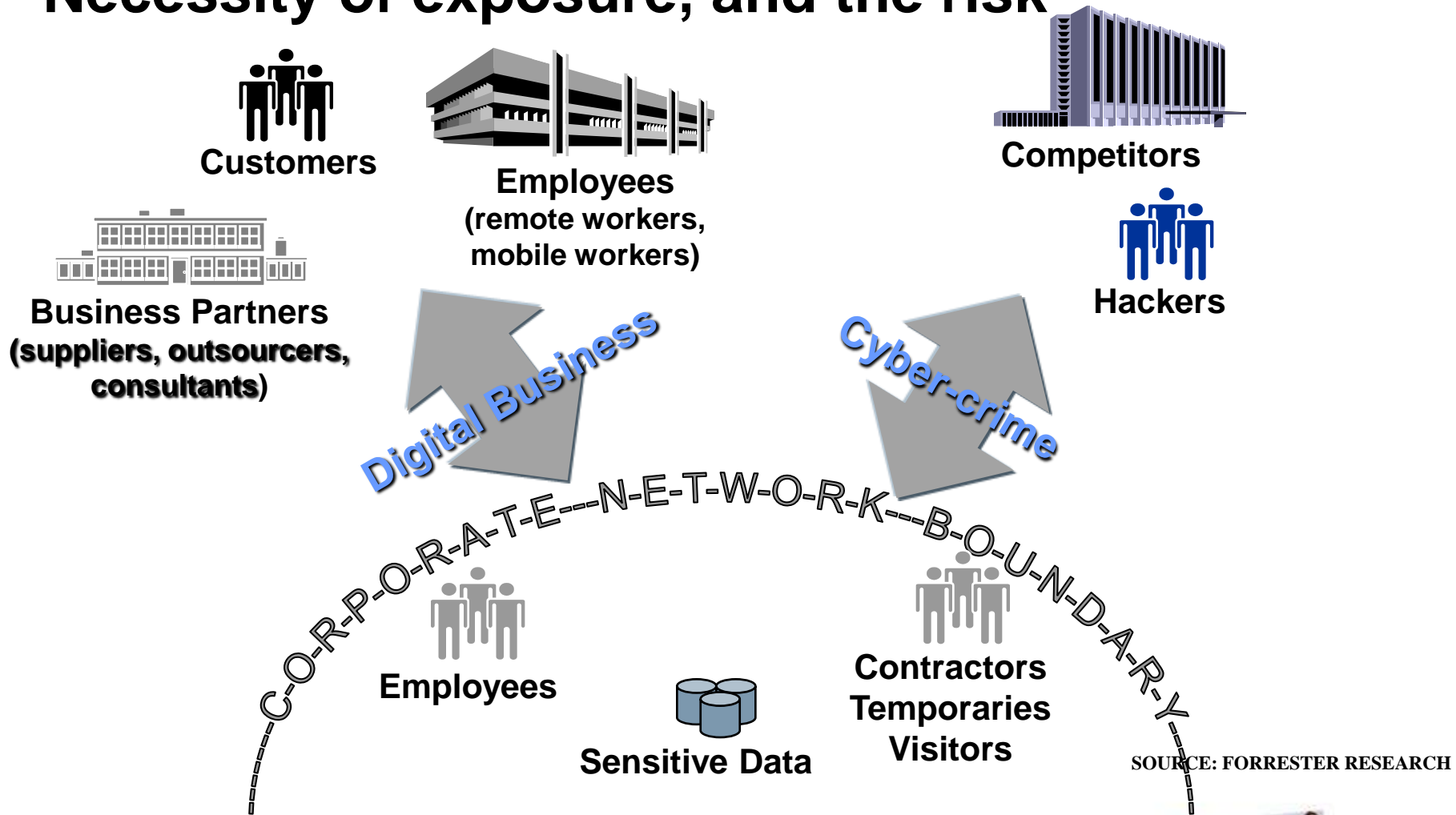
**McAfee**



Protect what you value.

# Data Security and Compliance

## Necessity of exposure, and the risk



**McAfee**

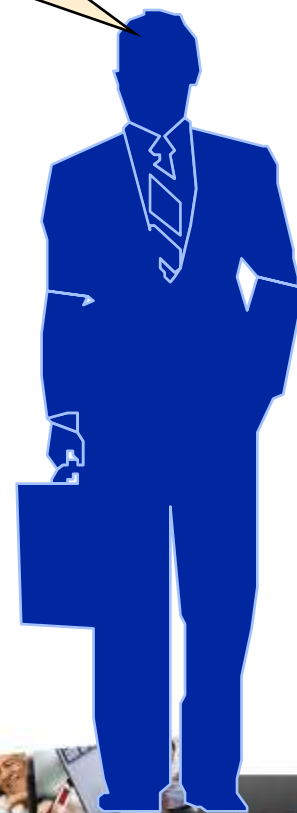


Protect what you value.

# Executive Directive ...

“Protect My Sensitive Data!  
...and don't interfere with the business!”

- Simple to say but complex to deliver
  - What data?
  - From whom?
  - Where is the data?



**McAfee**



Protect what you value.

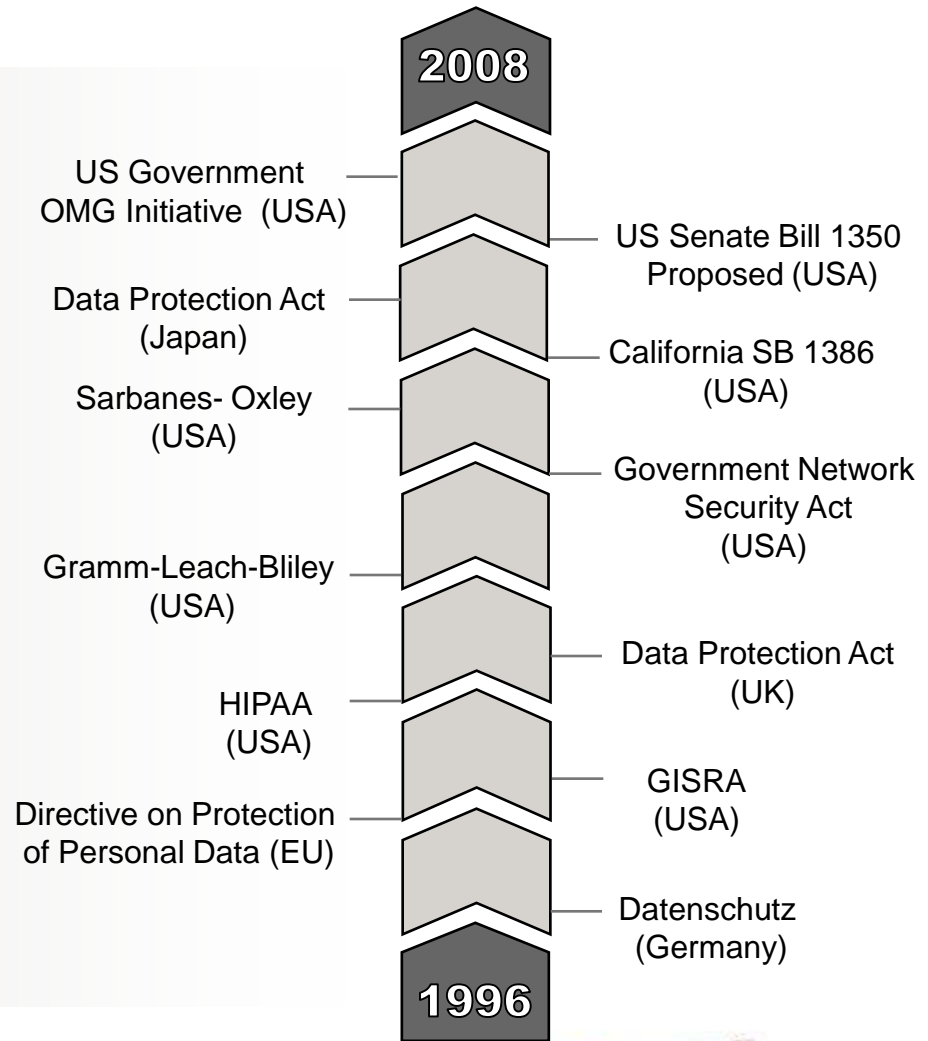
# Where to Start

- Focus on the risk drivers specific to your organization
  - Compliance, Intellectual Property, eDiscovery
- Focus on the domain
  - Define what vectors are most critical first
    - Removable Media
    - Locating where it is
    - Protecting it as leave your organization .....
  - People and Processes are key
    - Data protection is far more than a technology problem
- Determine the functional stakeholders needs
  - Interview the stakeholders like legal, human resources, compliance etc
  - Define their needs and requirements



# If driver is Regulation define linkage clearly

- Growing in number and complexity
- Public disclosure is required in the event of theft

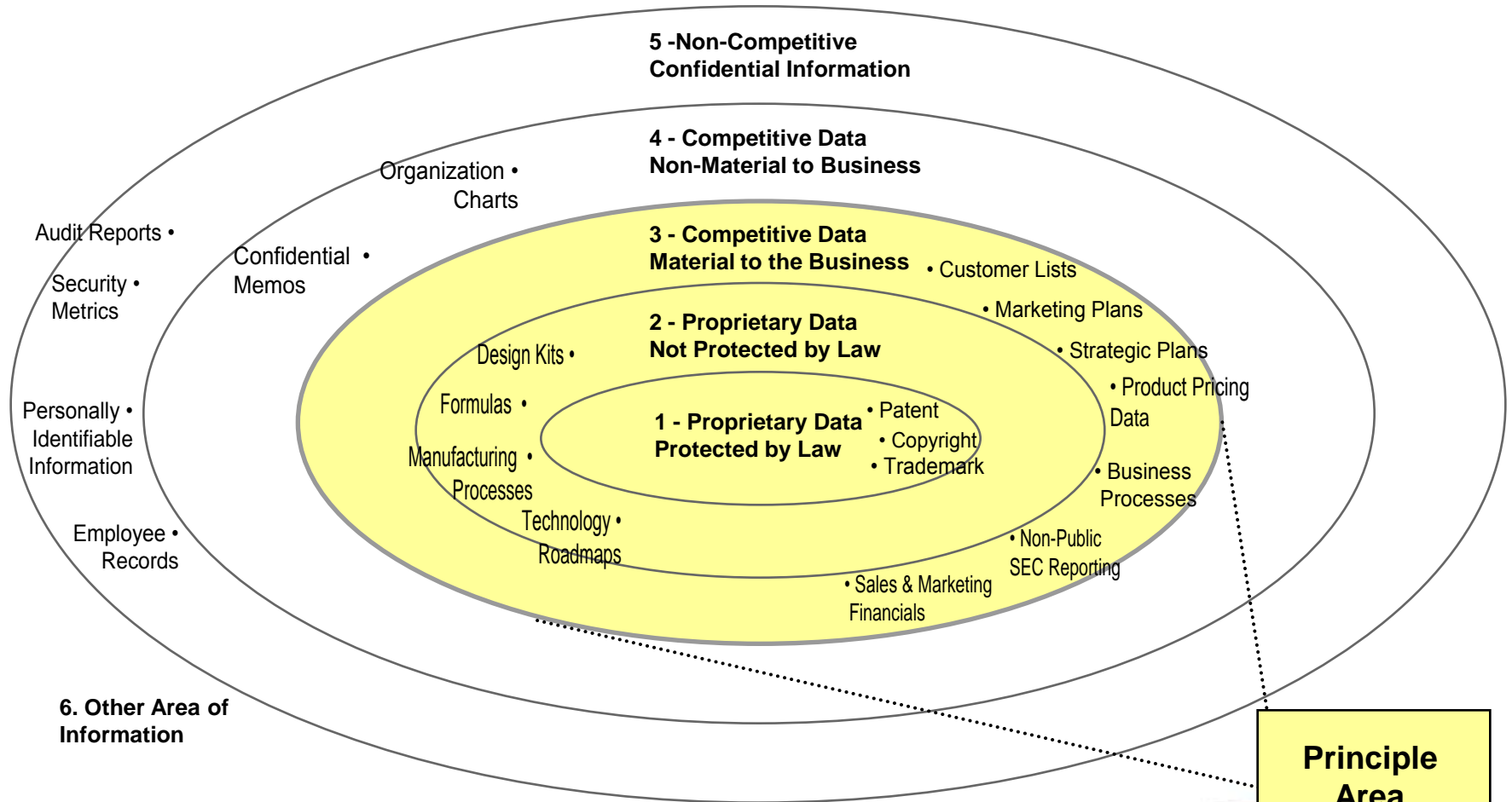


**McAfee**



Protect what you value.

# Define IP that needs Protection



# Create Risk Priority Framework

Risk Rating (Risk x Likelihood) 5=High	Means of Access, Attack, or Loss to Intellectual Property	Mitigation Techniques to Protect IP				Degree of Difficulty 3=High	Assumed Cost (Degrees)
		User Education	Policies & Standards	Process Controls	Technology Controls		
5	Users Bypass Controls	D				2	\$\$
5	Using IP data in Test & Development					3	\$\$
5	Unsecured Blackberries w/ IP	E	C,E			2	\$\$
5	Unclassified / misclassified documents	D	C			2	\$\$
4	Unintended Disclosure by Users	D				1	\$
4	Misconfigurations leads to IP insecurity		C			1	\$
4	Unsecured, weak or shared passwords					2	\$

Data Protection MUST be an organization imperative otherwise it will become additive to InfoSec workload

4	Outsourcing or Partner Misuse of IP					3	\$\$\$
4	Unsecured aggregated data					3	\$\$\$
3	Network (wireless/wired) Sniffing	C,D				1	\$\$
3	Use of Hacking Tools					2	\$
3	Targeted Attacks (phishing, bots)	D				2	\$\$
3	Use of Boot Disks, Virtual Machines	C				2	\$\$
3	Blogs, Postings (Internal/External)	C,D				3	\$\$
3	Unprotected or Lost tapes and Backups		C		B,E	3	\$\$
3	Collusion & Internal Espionage	D				3	\$\$
3	Lost Devices (blackberry, USB, laptop)	D	C		B	3	\$\$
	A = Email/IM Scanning Project						
	B = Adhoc Email & File Encryption Project						
	C = Enhance Standards & Policies						
	D = Awareness Training						
	E = Require Blackberry Passwords						
	F = Read Only Drives on Certain Devices						

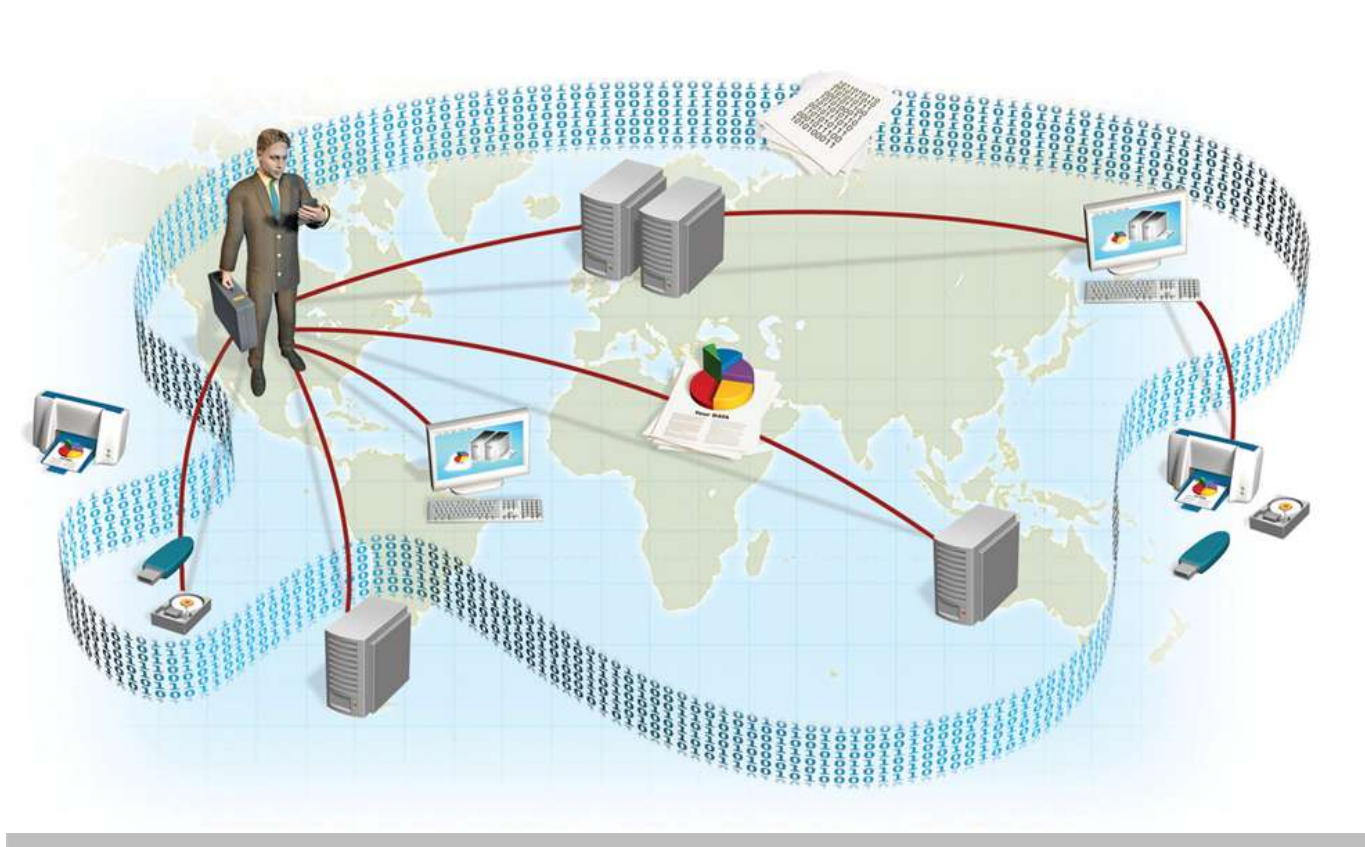


# To Summarize: The first step

- Protecting Data requires information security to become tightly woven into the business
  - An opportunity to gain wide and broad visibility
  - A partner to enabling the growth (proactive vs. reactive)
- Technology is not the hard part
  - Aligning the business stakeholder is key
  - Getting them involved early ensures that data protection is not just an InfoSec initiative
  - Raises the visibility of the solution (hence importance and drive)
- Data protection is not a static decision
  - Information is constantly changing
  - Partners are changing, solutions need to evolve and change



# Where do DLP solutions fit in information security?



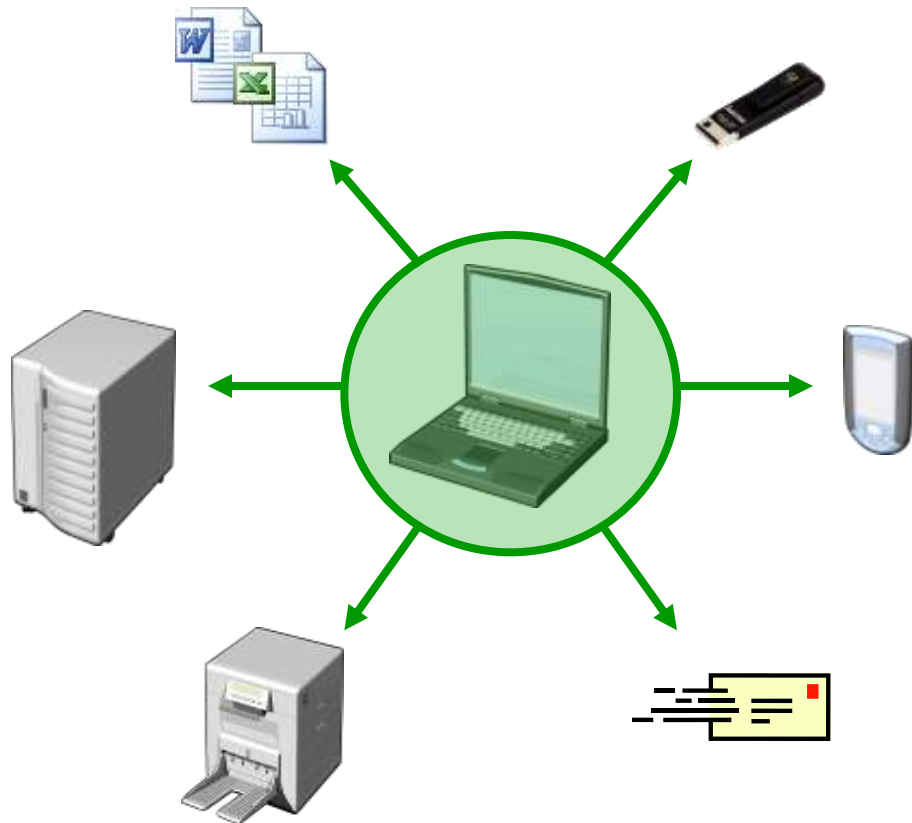
...they Secure The “Virtual Perimeter” for Data

**McAfee**



Protect what you value.

# What comprises Data Loss Prevention



- Monitor & Control every data access/transfer activity
  - File access
  - Network uploads/transfers
  - Print Operations
  - Removable media
  - Clipboard operations
  - Application field-level logging
- Enforce Risk/Classification-based policies
- Allow business operations – stop/alert for unauthorized/suspicious ones!

**McAfee**



Protect what you value.

# Data types, risk areas, and DLP approach

Data types

Risk areas

DLP approach



Forrester Research

**McAfee**



Protect what you value.

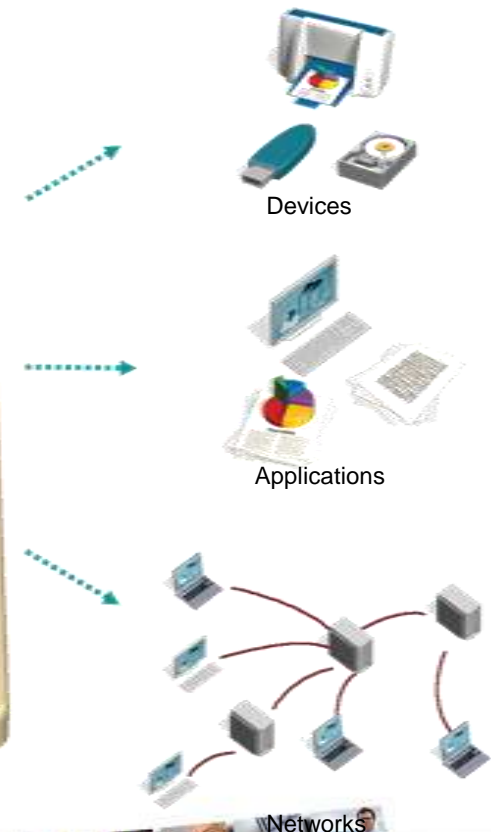
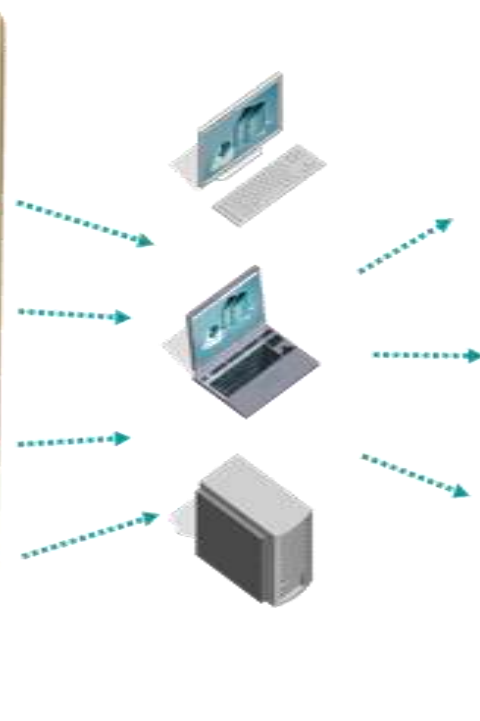
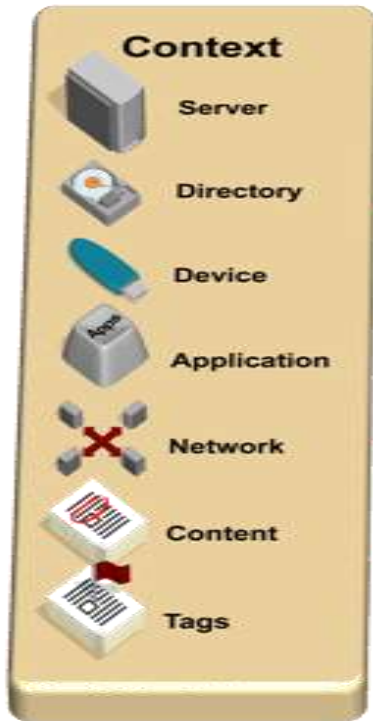
# How Does DLP work?

**1** Where Did the Data Come From?  
(What Classification?)

**2** What is the User Doing With It?  
Read, Write, Print, Move, Burn, Copy/Paste, Upload, etc.

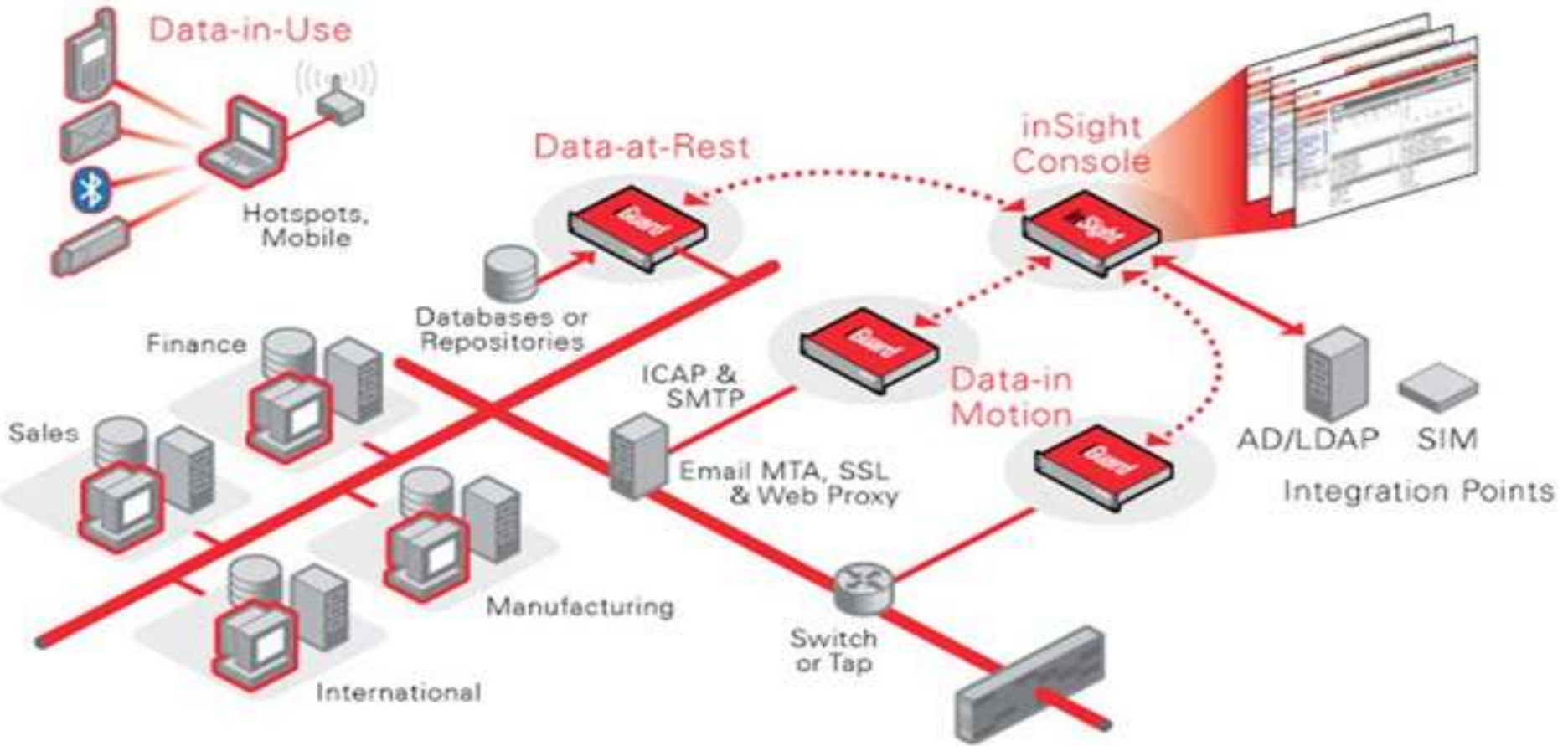
**4** What is the Policy regarding Actions to be taken?

**3** Where Is the Data Going?



Protect what you value.

# How and Where DLP Products Fit



**McAfee**

Reconnex Confidential

Reconnex Confidential

Protect what you value.

# Understanding the Risk?



Where is my confidential data openly accessible?



Where is my confidential data being sent?



Where is my confidential data copied?



What are my business policies for collaboration?



How do I define my confidential data?



# Data at Rest:

Where is my confidential data openly accessible?



## Best Practice

- Data at Rest products crawl the organization based on taxonomy of content and can provide analysis of what servers have what content
- Based on inventory scans to answer what is available where delegation of reviews of materials can be done
  - Personally identifiable information can be given to compliance team
  - Acceptable use information to HR team
  - Source code to engineering team .... Etc
- Once the data distribution model is understood, automated remediation can be used

## Problem

Organization has SharePoint servers, central repositories and desktops and laptops that contain sensitive data. **Where is all the data?**

## Challenge

Need to find the data and categorize it to enable organizations to apply protections ***without requiring additional software installed.***

**McAfee**



Protect what you value.

# Data in Motion:

Where is my confidential data being sent?



## Problem

Large financial services organization needs to protect PII data as it leaves their network, but *who is sending what to whom?*

## Challenge

All information leaving must be analyzed, and unmanaged machines use the network hence solution must be transparent.

## Best Practice

- Network Based data in motion products passively analyze all communications Webmail, IM, Blogs, Email etc
- Pre-built rules can be run to determine what information violates policy
- Rules and Policies are mapped to business stakeholders to ensure incident review and remediation is not an information security challenge
- Mining of incidents allows for rule tuning and refinement

**McAfee**



Protect what you value.

# Data in Use:

Where is my confidential data being copied?



## Problem

Organizations have laptops, desktops with USB, WIFI, Bluetooth enabled. ***What is allowed to be copied?***

## Challenge

USB, WIFI have valid business needs and to block all devices stops business.

## Best Practice

- Identify high risk machines for sensitive information disclosure i.e. remote sales, engineers etc
- Deploy logging only capabilities to determine business need and use of removable media
- Define rules and policies by department and group requirements
- Use automated protection mechanisms i.e. automatic USB encryption, Only allow supported USB drives, User Justification to aid in education of users



# Learning: Mine the Data



## Problem

Outsourced partners need access to high business impacting information but ***how can InfoSec determine who needs access to what***

## Challenge

Lack of automation required interviews with multi-departmental stakeholder to determine who and what (takes MONTHS)

## Best Practice

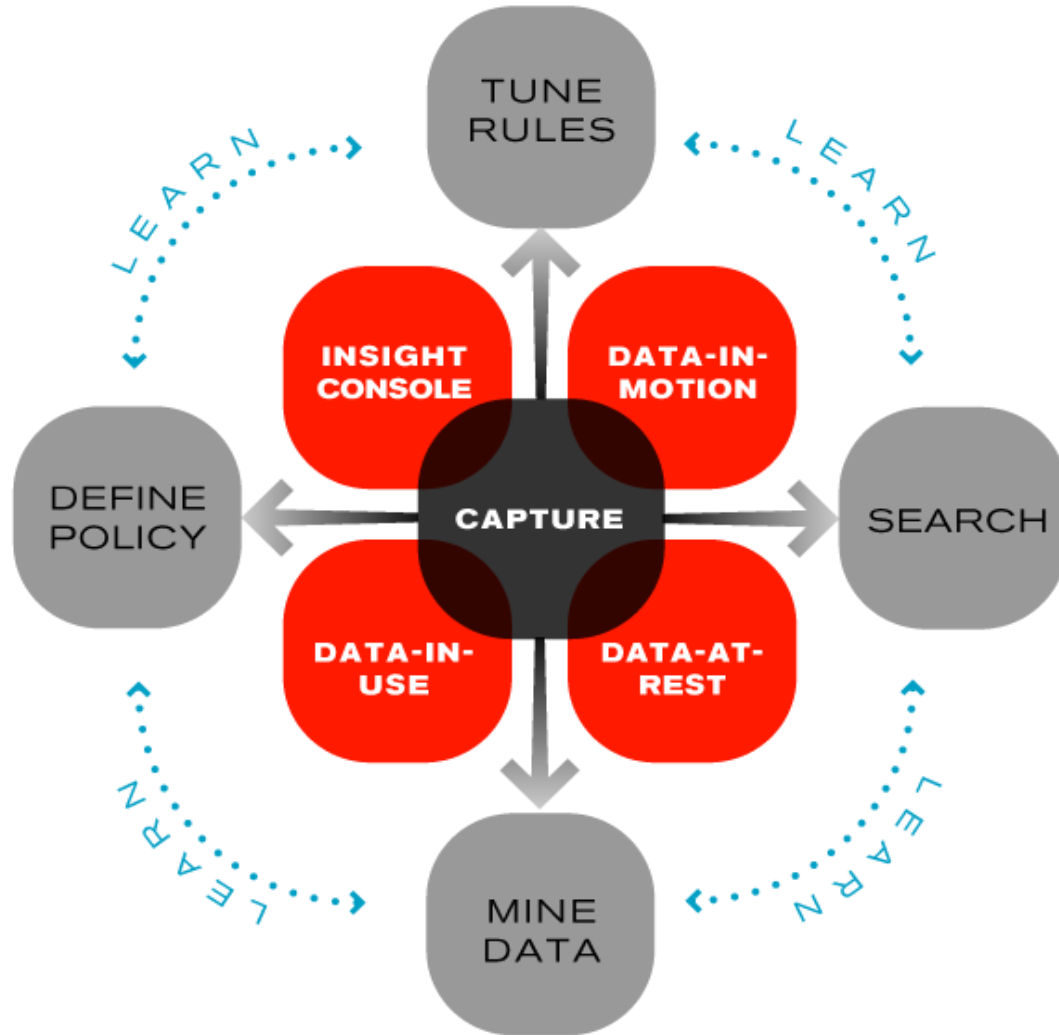
- Deploy data loss prevention solutions that classify and index all communications and information
- Index can then be queried to determine business process, information flows, stakeholders and sensitive information
- Does not require considerable upfront knowledge, rather uses your organizations communications to help you learn.

**McAfee**



Protect what you value.

# Why Reconnex?



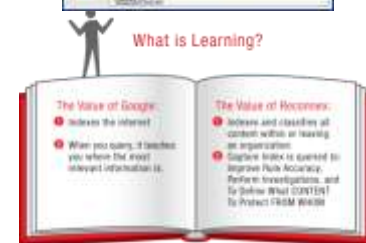
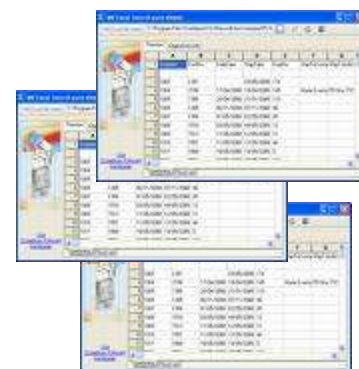
**McAfee**



Protect what you value.

# What can you do now

- Leverage vendor programs
  - Free risk assessment report to qualified prospects
  - Involve stakeholders into the reporting process to allow them to gain visibility into risks
- Multi-stakeholder requirements analysis
  - Vendors/3<sup>rd</sup> Parties can provide requirements methodology to allow you to gain input from ALL your stakeholders
  - Customized demonstrations for different parts of your organization
- Deploy a full data loss prevention solution as POC
  - Not just a report of risk, rather a deployment of a solution to help your team gauge the use of the solution



**McAfee**



Protect what you value.

# In Conclusion

- Data loss prevention is not just a technology problem, rather a business driver
  - Business stakeholder involvement is key
  - Allows information security to move from reactive to proactively engaging with the business
- Key drivers for data protection usually exist
  - Compliance, IP protection, eDiscovery are top of mind and budgeted
  - Info Sec needs to move into the business arena to aid
- Products are robust, deployments are now wide
  - More than 50% of Fortune 500 companies have data loss prevention solutions in place
  - Key to success is understanding what and from whom?
- Key to fast time to value is FOCUS and Partnership



**McAfee**



Protect what you value.

# Data Loss Prevention Best Practices

Thank You

Faizel Lakhani (faizel@reconnex.net)

Vice President Products-Reconnex