

McAfee Data Protection



Five Steps to 99% Data Security

Todd Mayo

McAfee

May 18, 2009



AGENDA:



- Data Protection Challenges
- Common Threat Vectors for Data Loss
- 5 Steps to Implementing Data Protection
- Q&A

Data Breach - The escalation of a serious threat



“TJX’s **\$1 billion** data breach”

Super 25 rankings unveiled



The FSA has fined Nationwide **£980.000** for a stolen laptop

FINANCIAL TIMES

“DuPont scientist downloaded **22,000** sensitive documents as he got ready to take a job with a competitor...”



Marks & Spencer was sued for over **\$2mill**

THE WALL STREET JOURNAL.

“ChoicePoint to pay **\$15 million** over data breach—Data broker sold information on 163,000 people

Data Breach - The escalation of a serious threat



1500 Laptops, **2500** PDA's, **62000** Mobile Phones simply left behind in the taxi

During US election laptop stolen out of McCain's election office with sensitive data

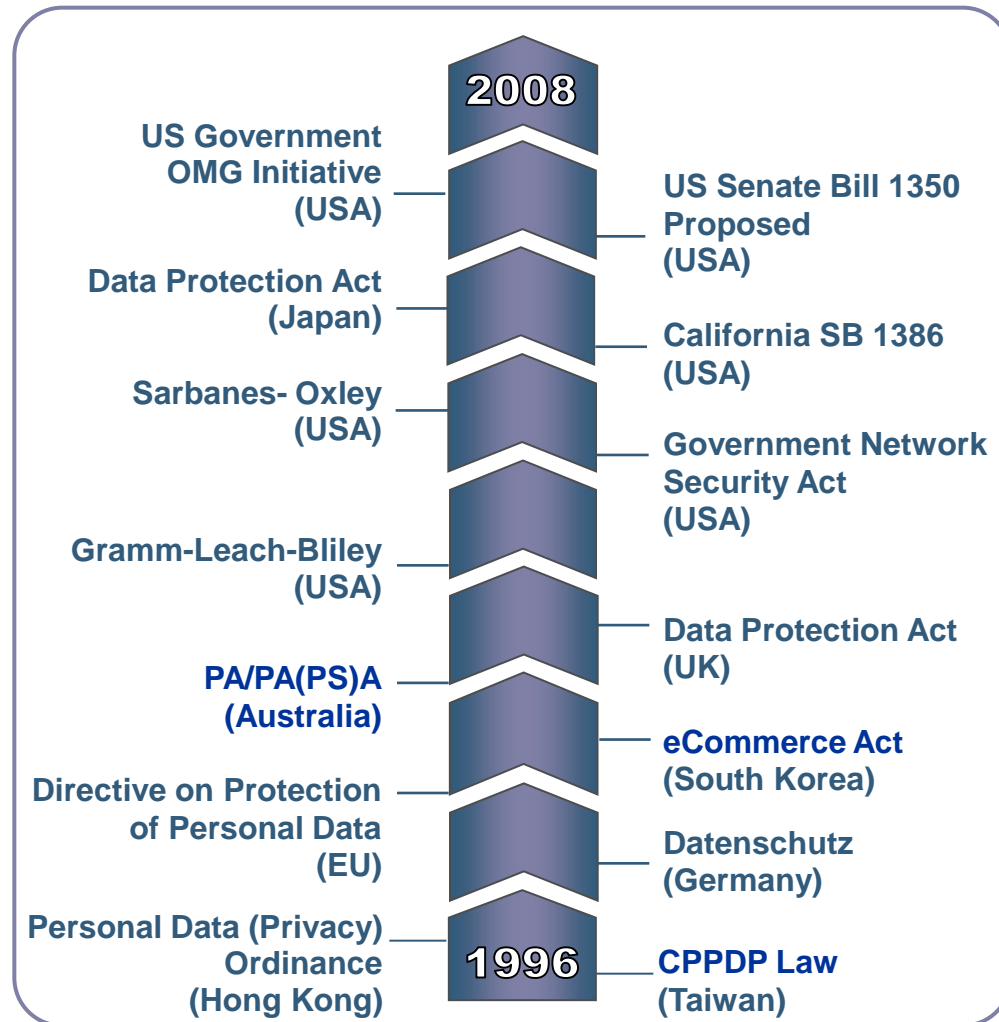
Credit Card institute lost **1 Million** credit card numbers on a CD-Rom

German Ministry lost in 2 years 189 Desktops and 326 Laptops incl. **VPN dial in details**

Data Privacy, Regulatory Compliance and You



- Increasing regulatory frameworks
 - Growing in number, complexity, responsibility on your behalf
- Designed to protect an individuals right to privacy with respect to personal data
- Hong Kong Monetary Authority
 - Examinations on Controls over Customer Data Protection
 - All USB device must be encrypted with file transfer log
 - Location of the customer data



Information - The new age currency



\$2-\$10
Credit card number



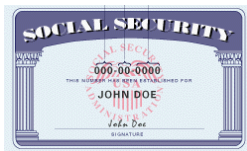
\$200-\$300
Credit Card Number with PIN



\$50-\$100
Birth certificate



\$5
PayPal account logon and password



\$100
Social Security card



\$30
Driver's license



\$500-\$1,000
Trojan to steal account information

Data Breach - The escalation of a serious threat



300 Million
USB Sticks

300-400 Million
handhelds

380 Million
corporate
desktops

300 Million
corporate
laptops

2.1 Billion
CD/DVD's

In 2008



Over 250 privacy laws
mandate Data Protection



"TJX's \$1 billion
data breach"



"ChoicePoint to pay \$15 million over
data breach—Data broker sold
information on 163,000 people"



"DuPont scientist downloaded 22,000
sensitive documents as he got ready to
take a job with a competitor..."



The FSA has fined Nationwide
£980,000 for a stolen laptop



Marks&Spencer was sued for over \$2mill

Over 80% of the Global 5000 have no data security in place

The perfect storm has arrived – but – most companies are still not prepared

- **Data Security is incident driven ...**
- **Insider steal information ?**
- **Data Security is complex !**
“Where do I begin ?”

Securing your information can be done ...

... in a matter of weeks – not years or months

... 2-12 weeks to value

Your five „steps“ to 99% Data Protection...

1. Understand the Risk
2. Fix Data Encryption
3. Manage Removable Media
4. Define Confidential Data
5. Deploy Data Loss Prevention



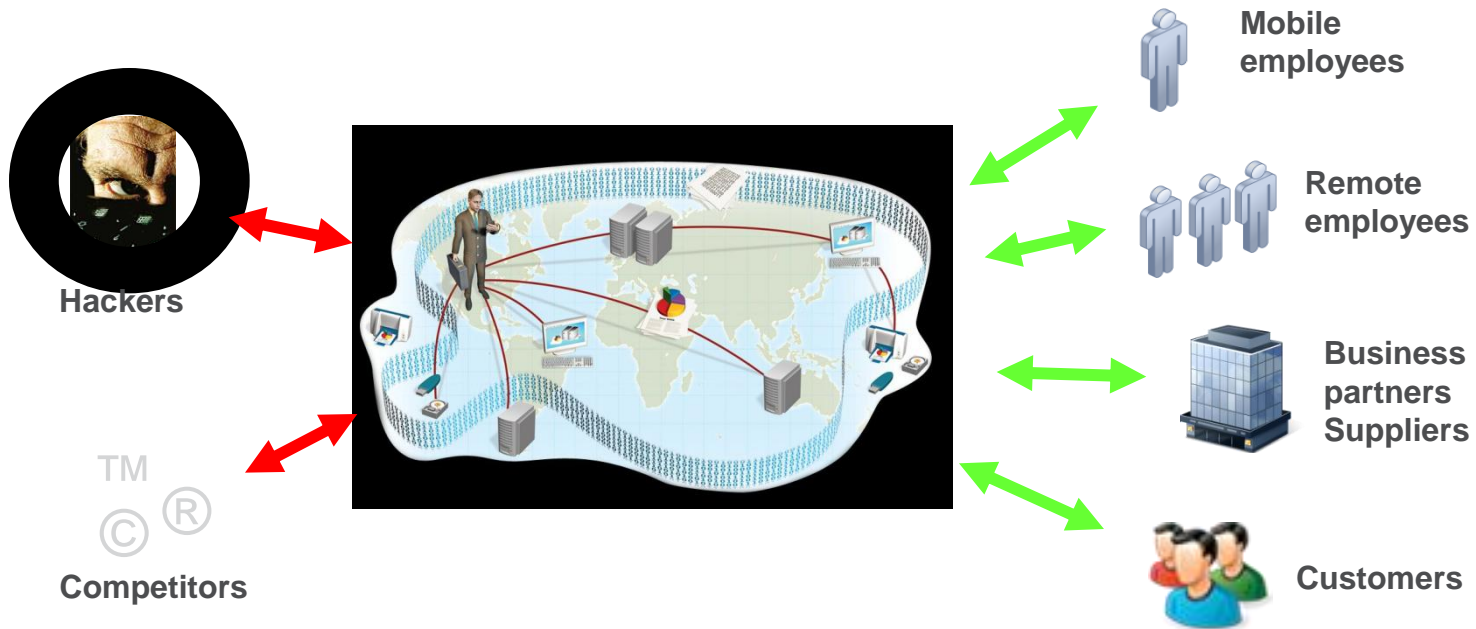
The path to protecting your vital information

McAfee®

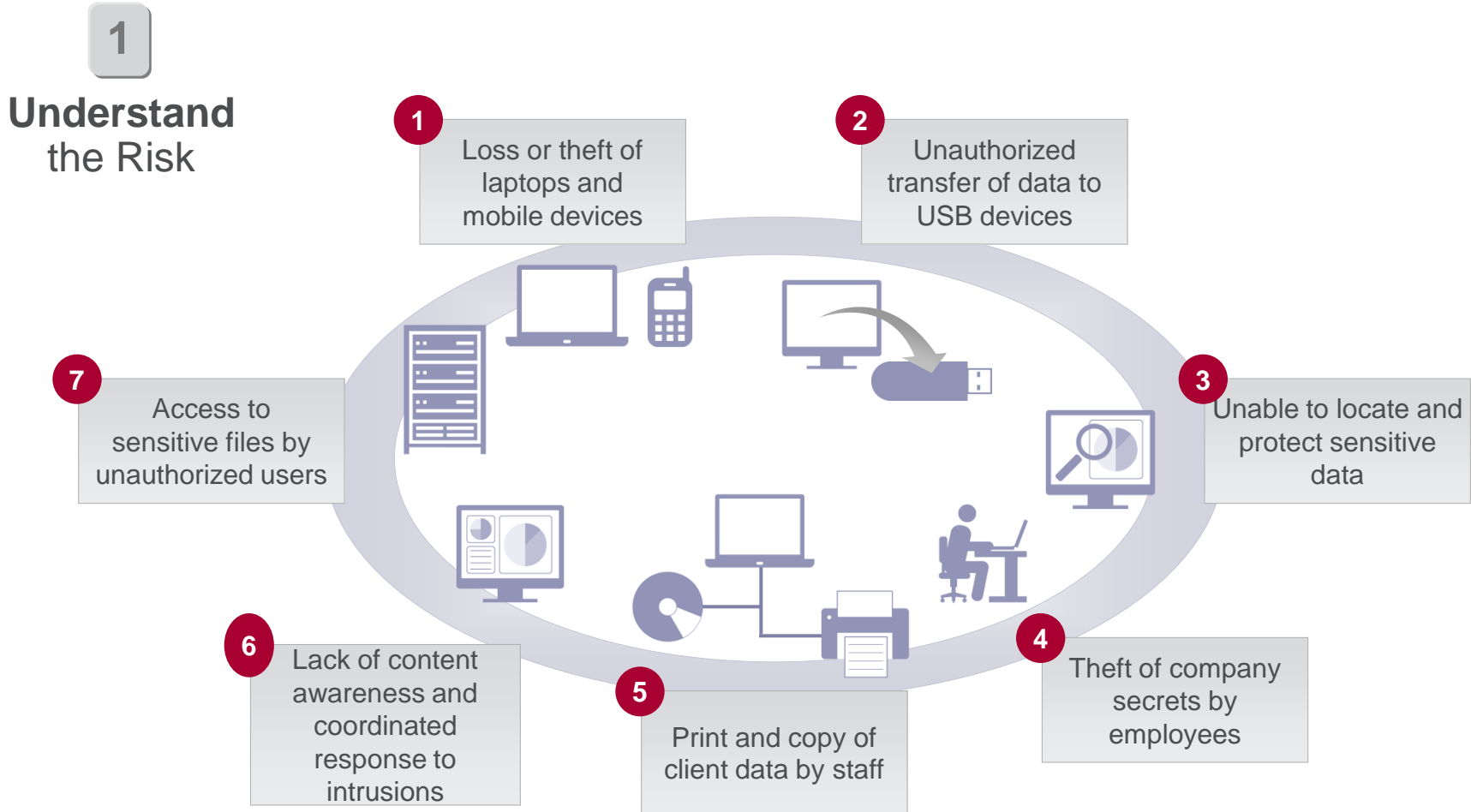
1

Understand
the Risk

**Data is not static,
so security cannot be static**



Threats magnify the problem



Data Security needs to take place anywhere...



360° Protection wherever the data travels!

1

**Understand
the Risk**

Data at **REST**

Desktops
Notebooks
Databases
Mail Archives
File Shares
Doc Mgmt Sys



Data in **MOTION**

eMail
Webmail
IM/Chat
Blogs
File Shares
FTP



Data in **USE**

USB Sticks
CD / DVD
iPod
Ext. Hard drives
Printouts



**0%
Secure**

1

Understand the Risk

To Summarize: The First Step!

Data Protection needs to be tightly woven into the business

- ⇒ Sensitive and confidential information can be lost anywhere
- ⇒ The threat comes from the inside AND the outside

Technology is NOT the hard part

- ⇒ Aligning the business stakeholder is key
- ⇒ Raise the awareness level for the threat

Data protection is not a static decision

- ⇒ Information is constantly changing & travelling
- ⇒ Partners are changing, so solutions need to evolve

1

Understand
the Risk

2

Fix
Data Encryption

Challenge !

- ⇒ Laptop is lost / stolen! What information was on it?
- ⇒ Non encrypted data is always considered “stolen” or “exposed”
- ⇒ Data privacy laws / regulatory compliance / corp. governance

How to fix the problem ?

1. Deploy hard drive encryption on all laptops & desktops
2. Monitor your inventory / run audit reports

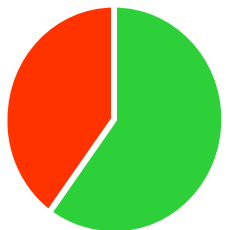
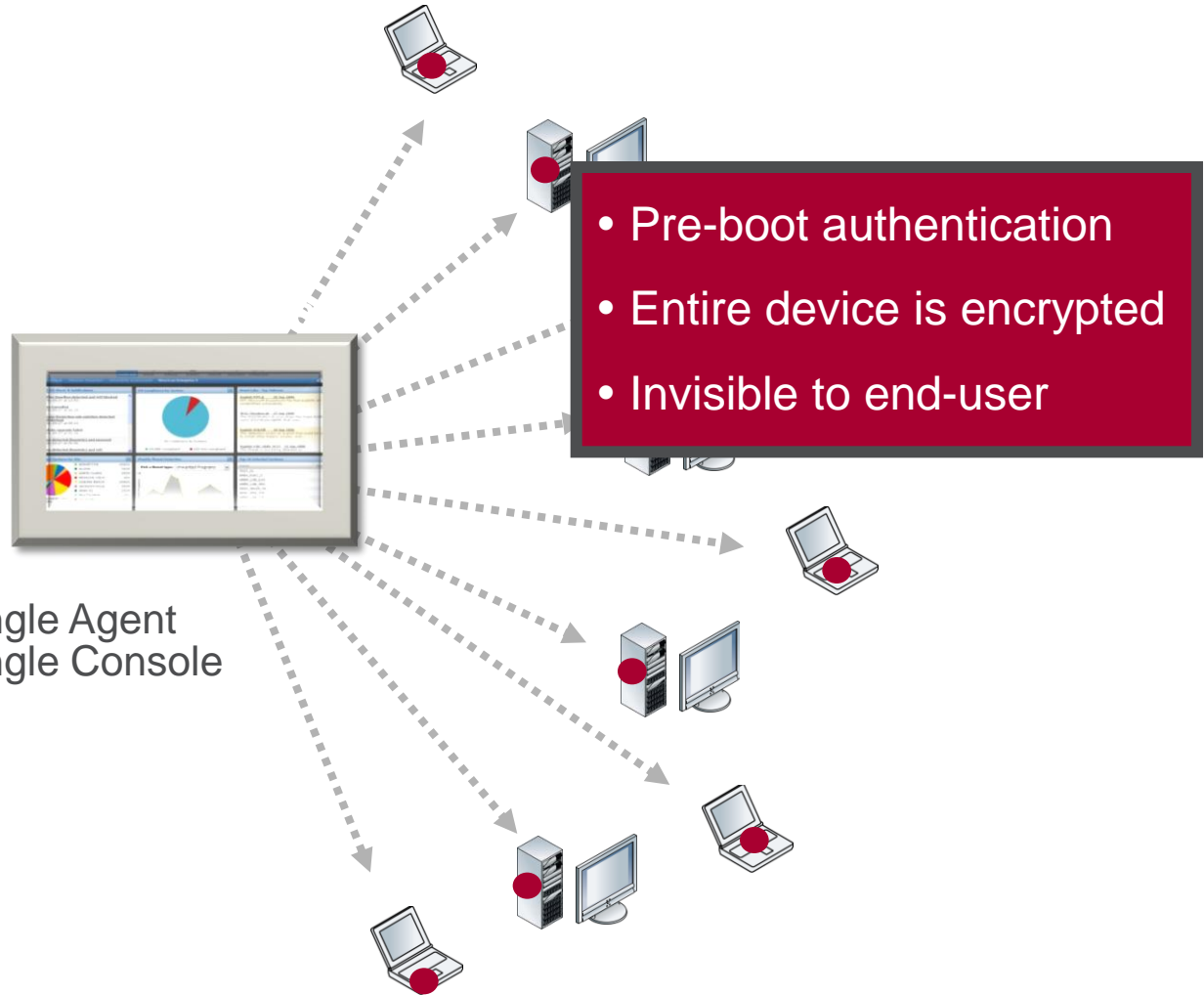
The path to protecting your vital information

1

Understand
the Risk

2

Fix
Data Encryption



60%
Secure

The path to protecting your vital information



1

Understand
the Risk

2

Fix
Data Encryption

Challenge !

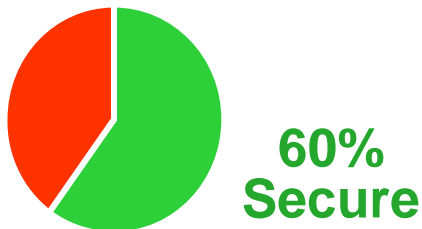
- ⇒ Laptop is lost / stolen! What information was on it?
- ⇒ If data was encrypted then it is not considered compromised
- ⇒ Data privacy laws / regulatory compliance / corp. governance

How to fix the problem ?

1. Deploy hard drive encryption on all laptops & PCs
2. Monitor your inventory / run audit reports

Time ?

- ⇒ Planning / design / policy: 1-3 weeks
- ⇒ Deployment: 2-4 weeks



1

Understand
the Risk

2

Fix
Data Encryption

3

Manage
Removable Media

Challenge !

- ⇒ Information is transferred IN and OUT
- ⇒ Can be bought anywhere for \$20



How to fix the problem ?

1. Use only encrypted USB sticks
2. Install DEVICE CONTROL software
3. Set policy to use only encrypted USB sticks - or - set policy to encrypt data when transferred

The path to protecting your vital information



1

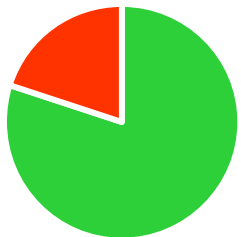
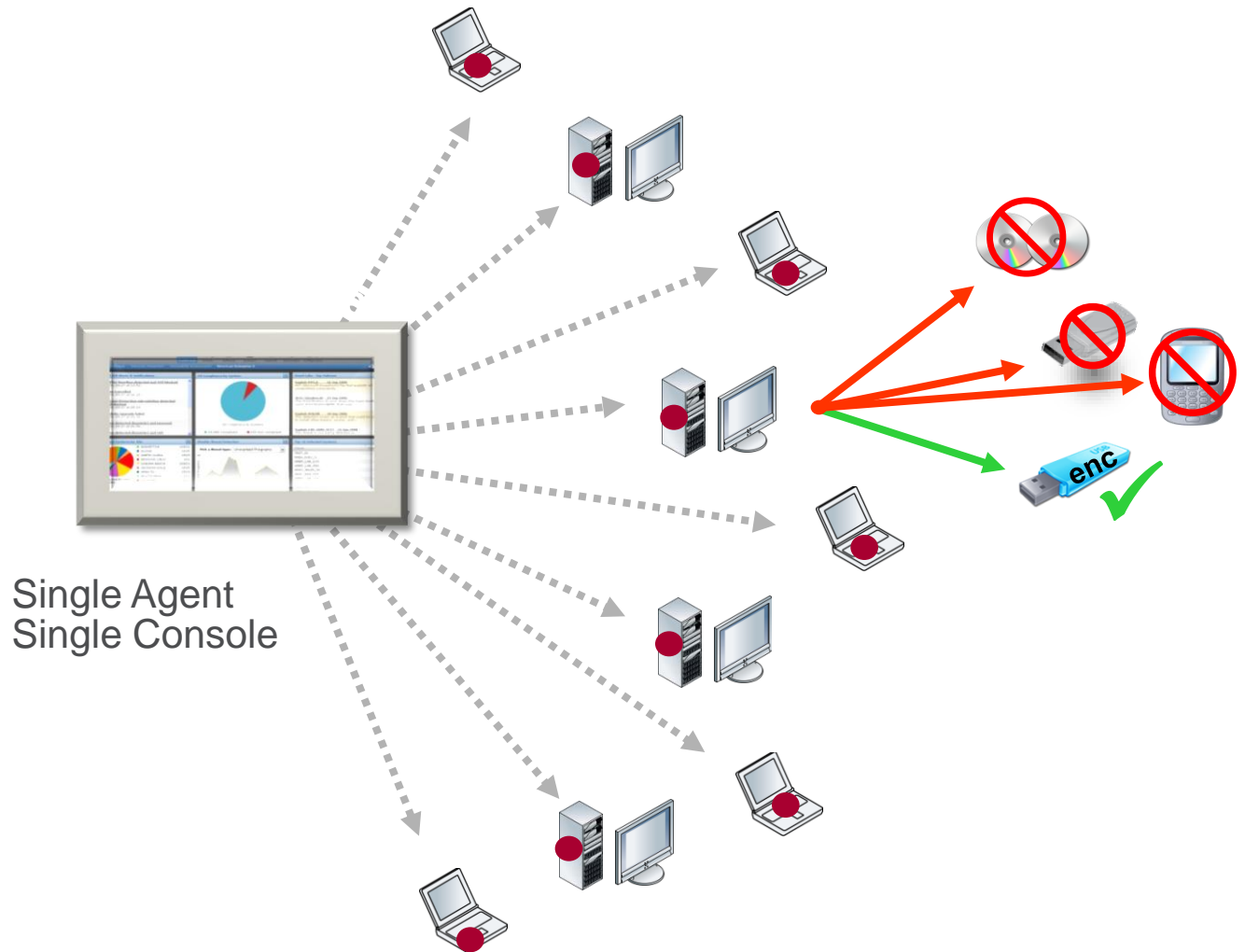
Understand
the Risk

2

Fix
Data Encryption

3

**Manage
Removable Media**



**80%
Secure**

The path to protecting your vital information



1

Understand
the Risk

2

Fix
Data Encryption

3

Manage
Removable Media

Challenge !

- ⇒ Data is transferred IN and OUT
- ⇒ Can be bought anywhere for \$20

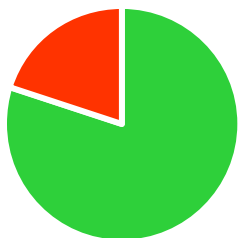


How to fix the problem ?

1. Use encrypted USB sticks
2. Install DEVICE CONTROL software
3. Set policy to use only encrypt USB sticks - or - set policy to encrypt data when transferred

Time ?

- ⇒ Encrypted USB sticks: Time to write a purchase order
- ⇒ Device Control Software: 1-3 weeks
- ⇒ Set policy for encryption: 1 week



80%
Secure

1

Understand
the Risk

2

Fix
Data Encryption

3

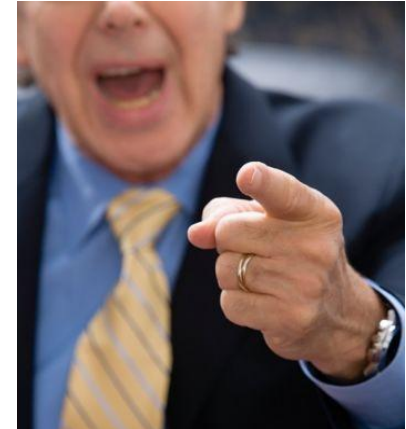
Manage
Removable Media

4

Define
Confidential Data

Executive directive ...

***“Protect my sensitive data! ...and
don’t interfere with the
business!”***



Simple to say, but ...

- ⇒ What data?
- ⇒ From whom?
- ⇒ Where is the data?

The path to protecting your vital information



1

Understand
the Risk

2

Fix
Data Encryption

3

Manage
Removable Media

4

Define
Confidential Data

1. **Focus** on risk drivers specific to your organization
 - ⇒ Compliance, Intellectual Property (IP)
 - ⇒ Business information, staff related information
 - ⇒ Legal information
 - ⇒ Customer information
2. **Define** most critical vectors
 - ⇒ Data at Rest, Data in Motion, Data in Use
 - ⇒ Location of data
 - ⇒ Focus on data that travels
3. **Determine** the functional stakeholders' needs
 - ⇒ Interview stakeholders; i.e. legal, HR, compliance, ...
 - ⇒ Define their needs & requirements

Data Protection is not static ...

The path to protecting your vital information



1

Understand
the Risk

2

Fix
Data Encryption

3

Manage
Removable Media

4

Define
Confidential Data

5

Deploy
Data Loss
Prevention

First Step



- ⇒ Mine Data
- ⇒ Capture Data Transfers
similar to Google Indexing

Time ?
1 week

Second Step

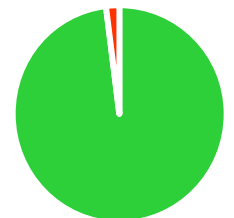


- ⇒ Define DLP Policy
- ⇒ Run report

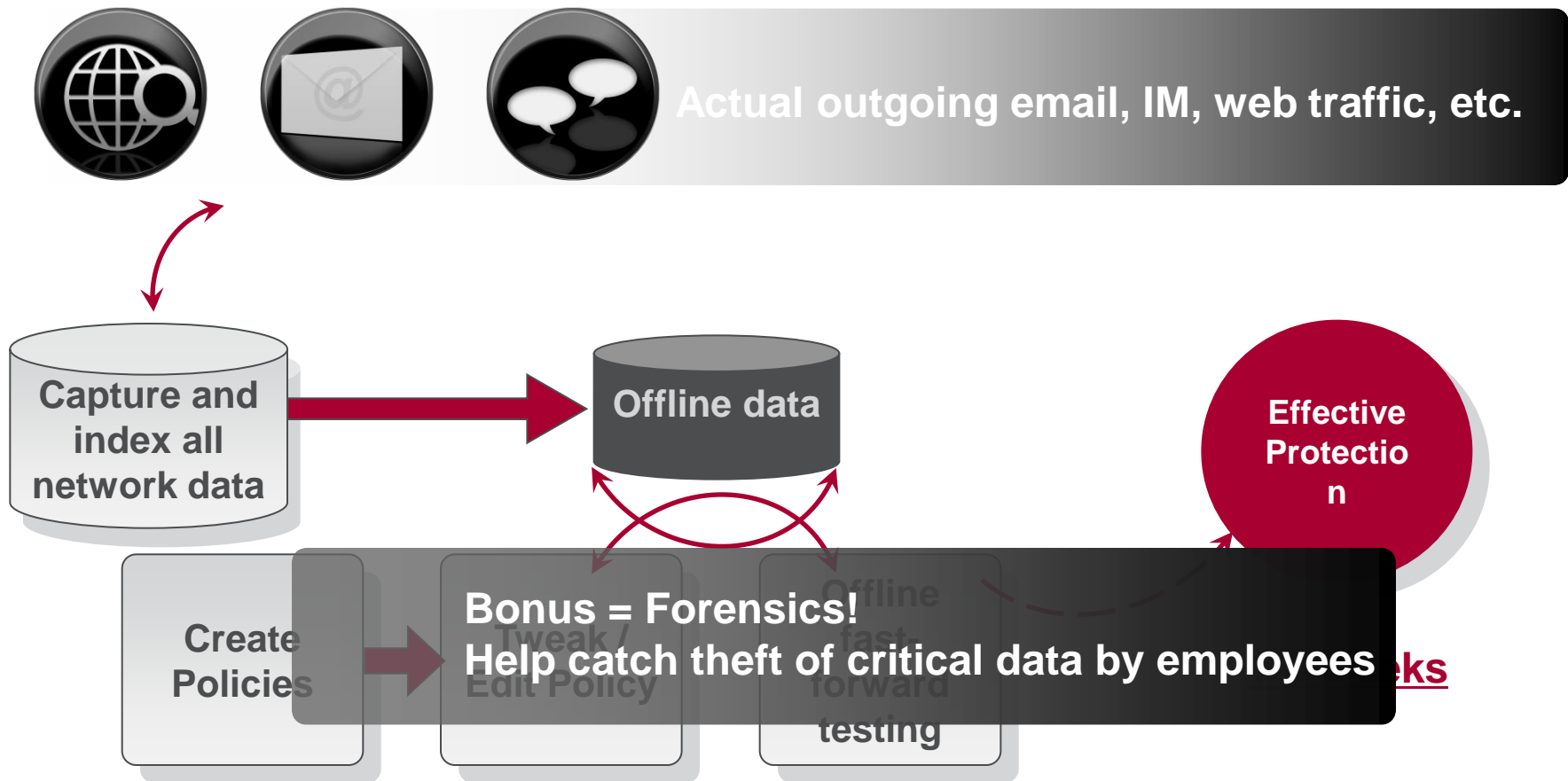


Time ?
1-2 weeks

98-99%
Secure



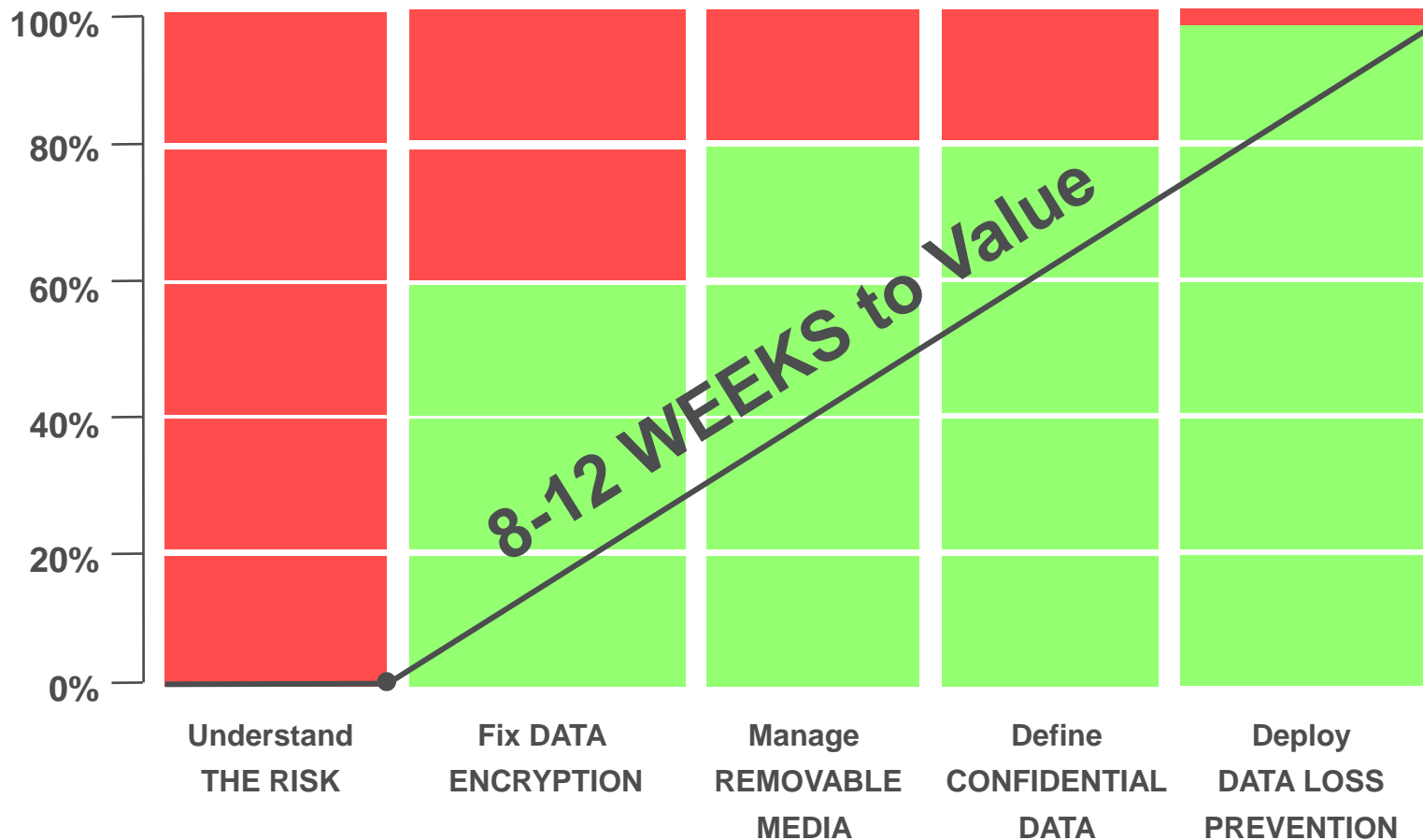
DLP policy creation with "Capture"

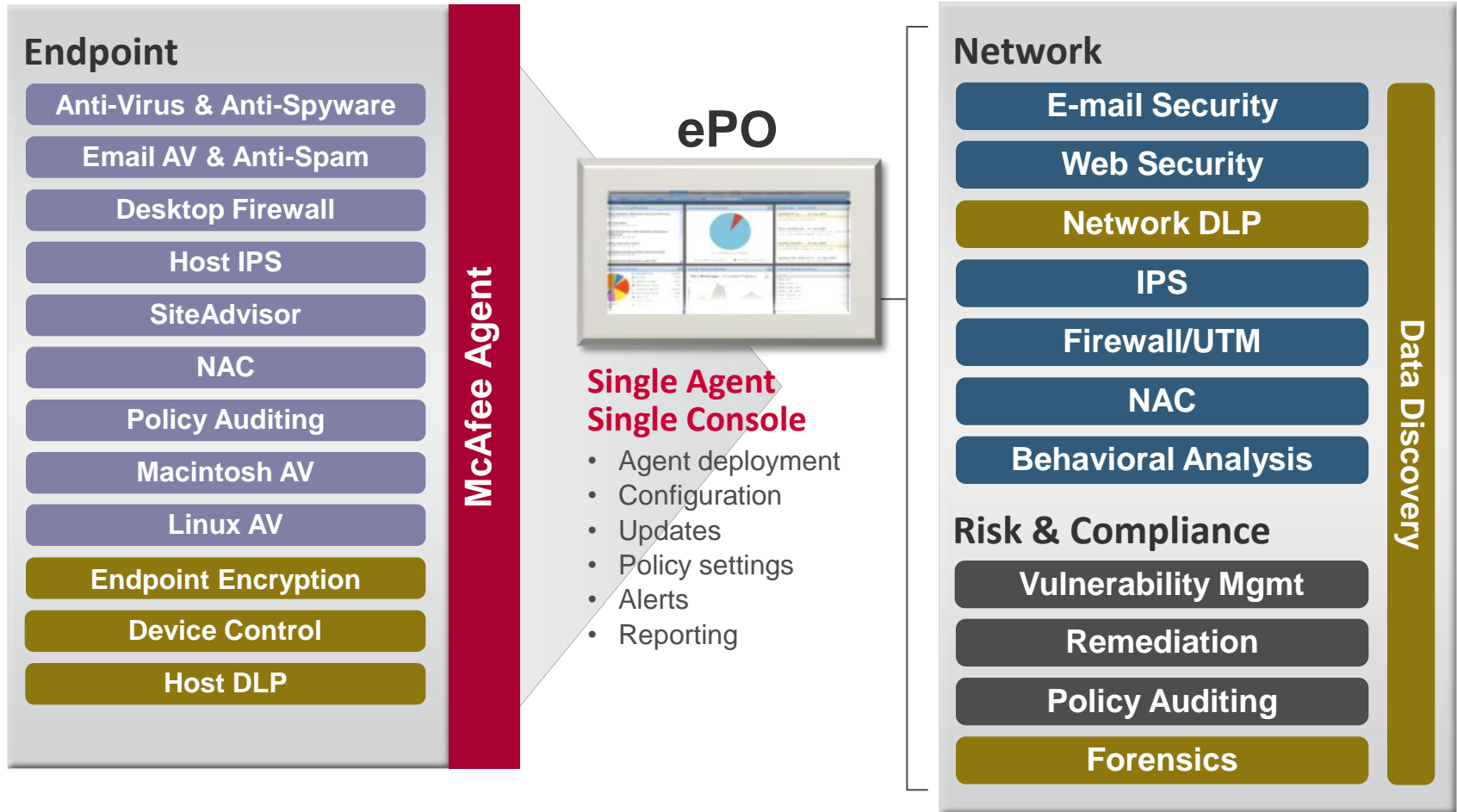


The path to protecting your vital information



Data Security





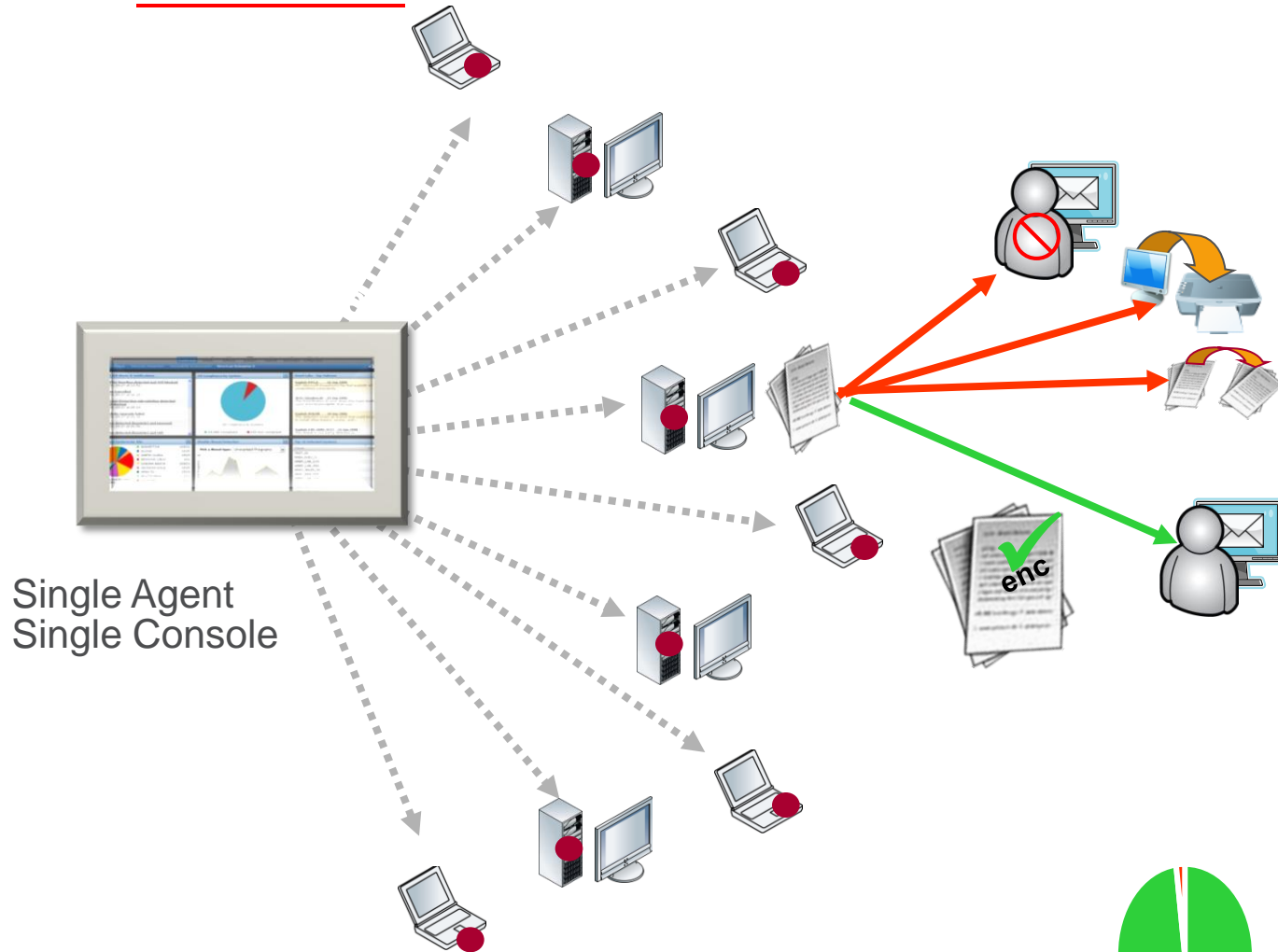
THANK YOU!!

The path to protecting your vital information

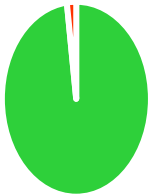
McAfee®

Host DLP

- 1 Understand the Risk
- 2 "Fix" Data Encryption
- 3 Manage Removable Media
- 4 Define Confidential Data
- 5 **Deploy Data Loss Prevention**



98-99%
Secure



McAfee Data Protection

McAfee[®]

May 18, 2009



The path to protecting your vital information



Network DLP

1

Understand
the Risk

2

“Fix”
Data Encryption

3

Manage
Removable Media

4

Define
Confidential Data

5

Deploy
Data Loss
Prevention

First Step



- ⇒ Mine Data
- ⇒ Capture Data Transfers
similar to Google Indexing

Time ?
1 week

Second Step



- ⇒ Define DLP Policy
- ⇒ Run report



Time ?
1-2 weeks

98-99%
Secure

