

Information-Centric Security: Do You Know Where Your Data Is?

Mike Wolfe, Vice President of Technology,
Vontu, Inc.

INTEROP[®]
LAS VEGAS | MAY 20-25, 2007



Agenda

- Learn about confidential data loss and its impact on organizations
- Discover how to manage the risk of the insider threat
- Explore technology solutions for preventing data loss

Trends in the Workplace

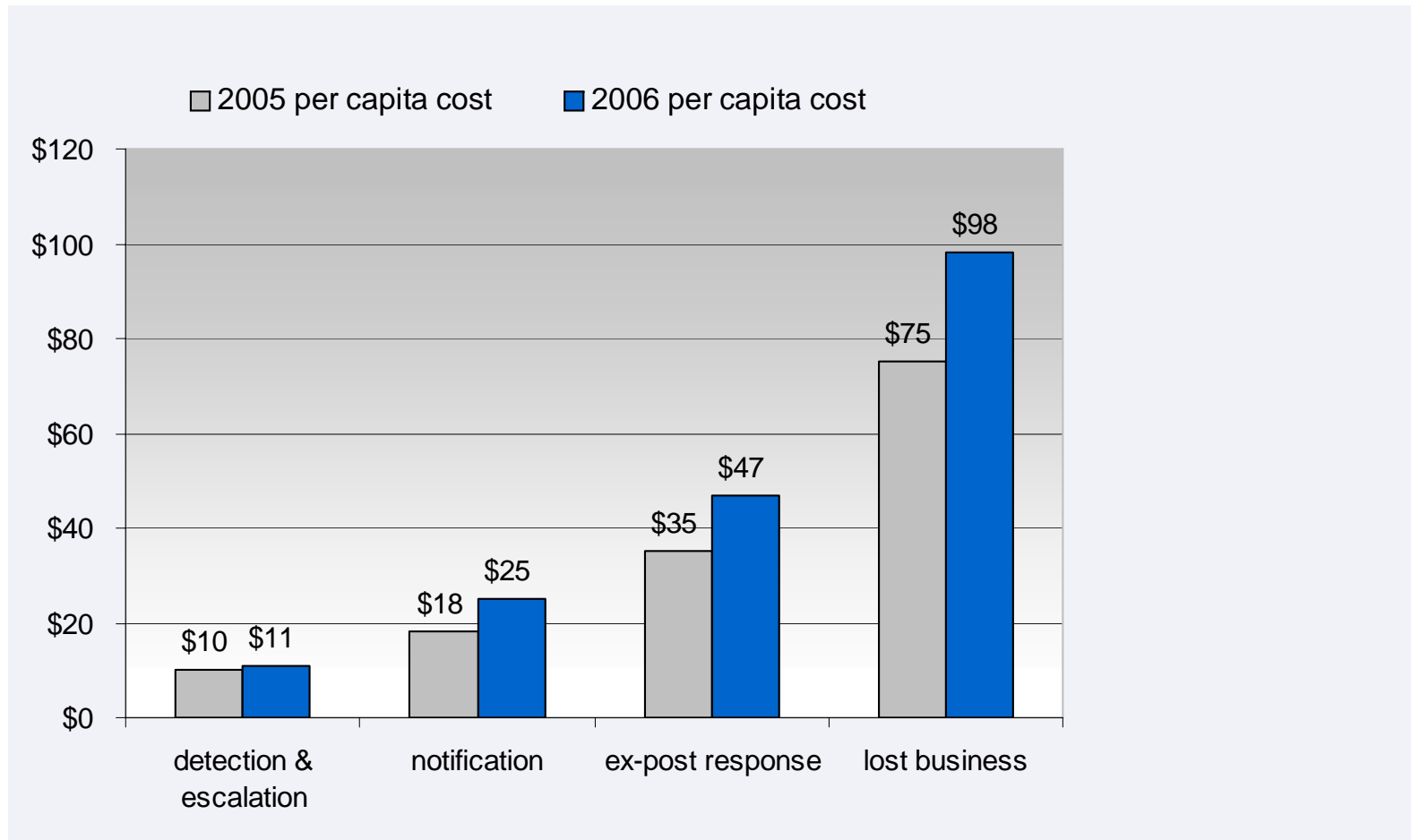
- Globalization
 - › Outsourcing, off-shoring
- Mobile Workforce
 - › Laptops, PDAs
- Internet Access
 - › VPN
- Regulations and Compliance
 - › CA SB1386
 - › GLBA
 - › HIPPA
 - › PCI
 - › eDiscovery

Impact of Data Loss

- Cost of Recent Breaches
 - › U.S. Department of Veterans Affairs
 - » Stolen VA laptop containing PII of 28.6 million veterans
 - » \$7 million – Cost of printing and mailing notices to affected veterans
 - » \$160 million – Cost to pay for one year's worth of credit monitoring for those affected
- Additional Impact Due to Lost Customers
 - › 19% of consumers terminated relationships post breach
 - › 67% likely or very likely to stop shopping online
- Average Cost to Notify
 - › \$182 per customer
- Damage to Reputation
 - › Significant...

Cost of a Data Breach

Cost Center increase in 2005 to 2006: On a per-period basis, all these costs increased from the 2006 survey

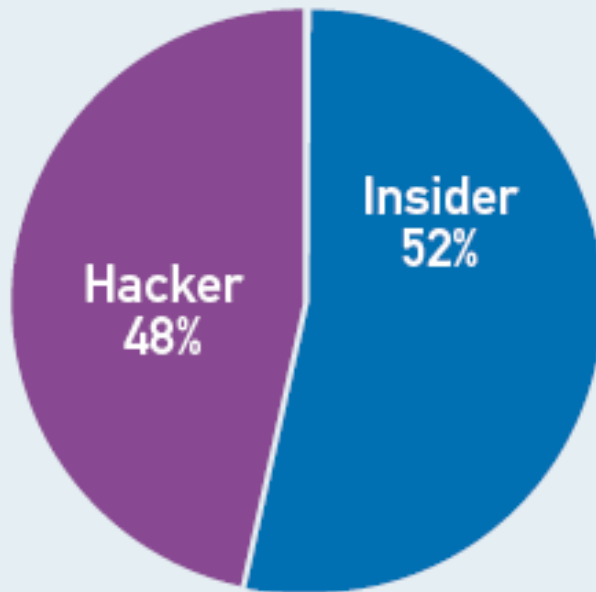


Ponemon Institute, Vontu and PGP, "2006 Annual Study: Cost of a Data Breach" (Ponemon Institute, October 2006)

The Insider Threat

Insider vs. The Hacker

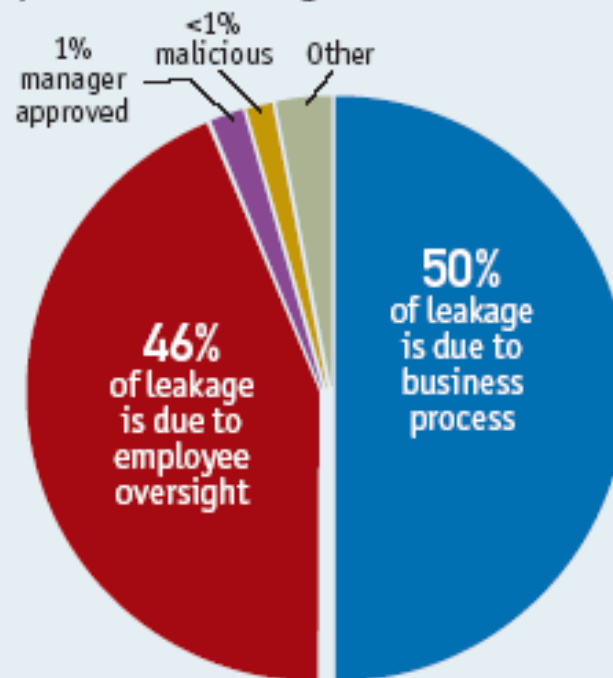
2005 Data Security Breaches



Data compiled from industry sources including EPIC.org and PerkinsCoie.com.

Inadvertent vs. Malicious

96% of leaks are due to faulty processes or oversight



Source: Vontu risk assessment findings.

Data Loss Prevention Priorities



Where is my confidential data exposed?



Where is my confidential data being copied?



Where is my confidential data being sent?



How do I enforce my data loss policies?

Data Loss Prevention Drivers

Confidential Data Types

Customer Data
Social Security Numbers
Credit Card Numbers
Protected Health Info

Corporate Data
Financials
Mergers and Acquisitions
Employee Data

Intellectual Property
Source Code
Design Documents
Pricing

The Risk

1:400 messages contain confidential data

1:50 network files are wrongly exposed

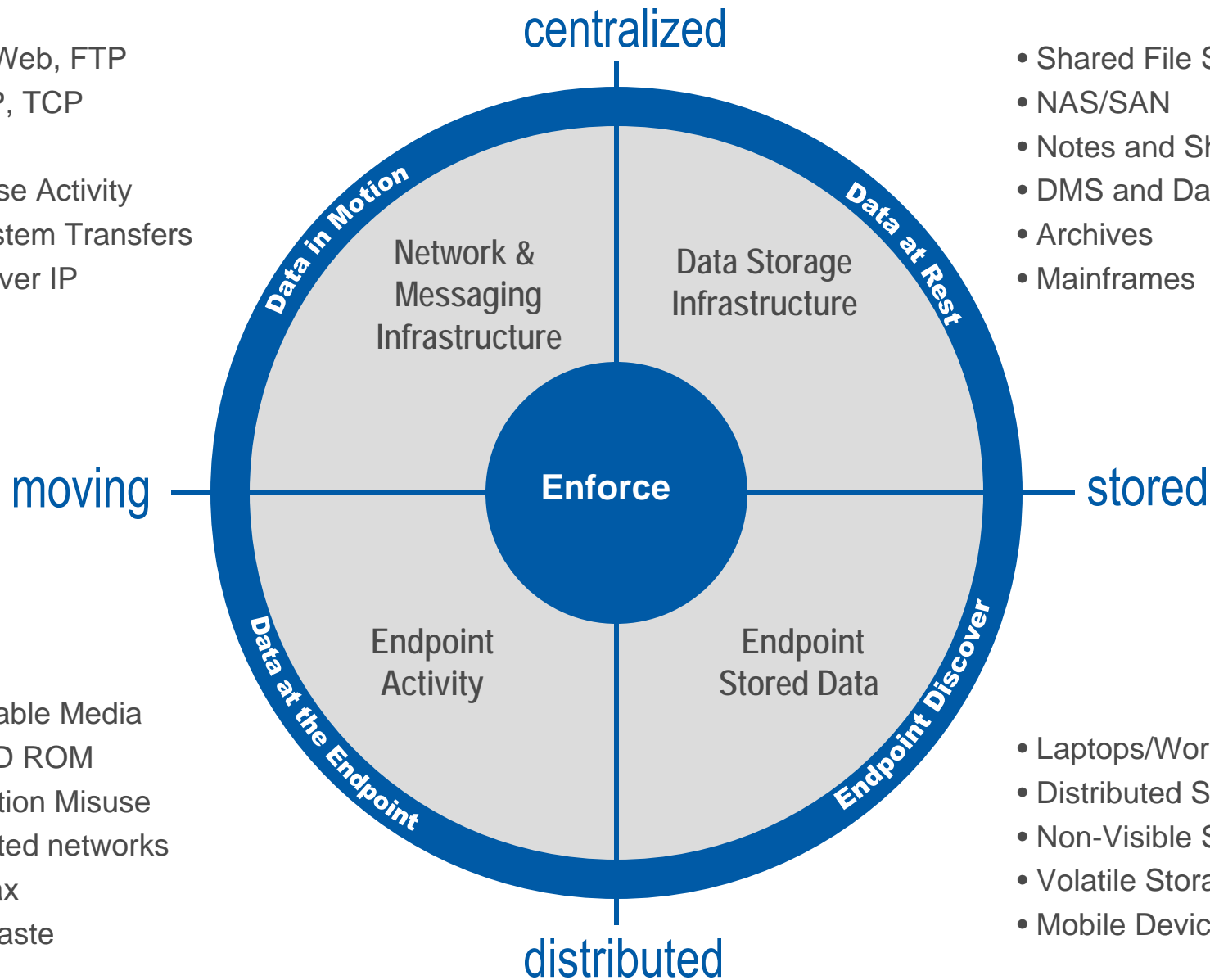
1:10 laptops are stolen

1:2 USBs contain confidential information

Data Loss Prevention: Holistic View

- Email, Web, FTP
- IM, P2P, TCP
- UDP
- Database Activity
- File System Transfers
- Voice over IP

- Shared File Servers
- NAS/SAN
- Notes and Sharepoint
- DMS and Databases
- Archives
- Mainframes



- Removable Media
- CD/DVD ROM
- Application Misuse
- Un-trusted networks
- Print/Fax
- Copy/Paste

- Laptops/Workstations
- Distributed Servers
- Non-Visible Storage
- Volatile Storage
- Mobile Devices

Data Loss Prevention Approach

DLP Foundation:

- Detection
- Coverage
- Enforcement

Detection

Protected Data



Personal Data (PII)



Intellectual Property



Corporate Data



Classified Data

Detection Challenges

Context

Format

Languages

Obfuscation

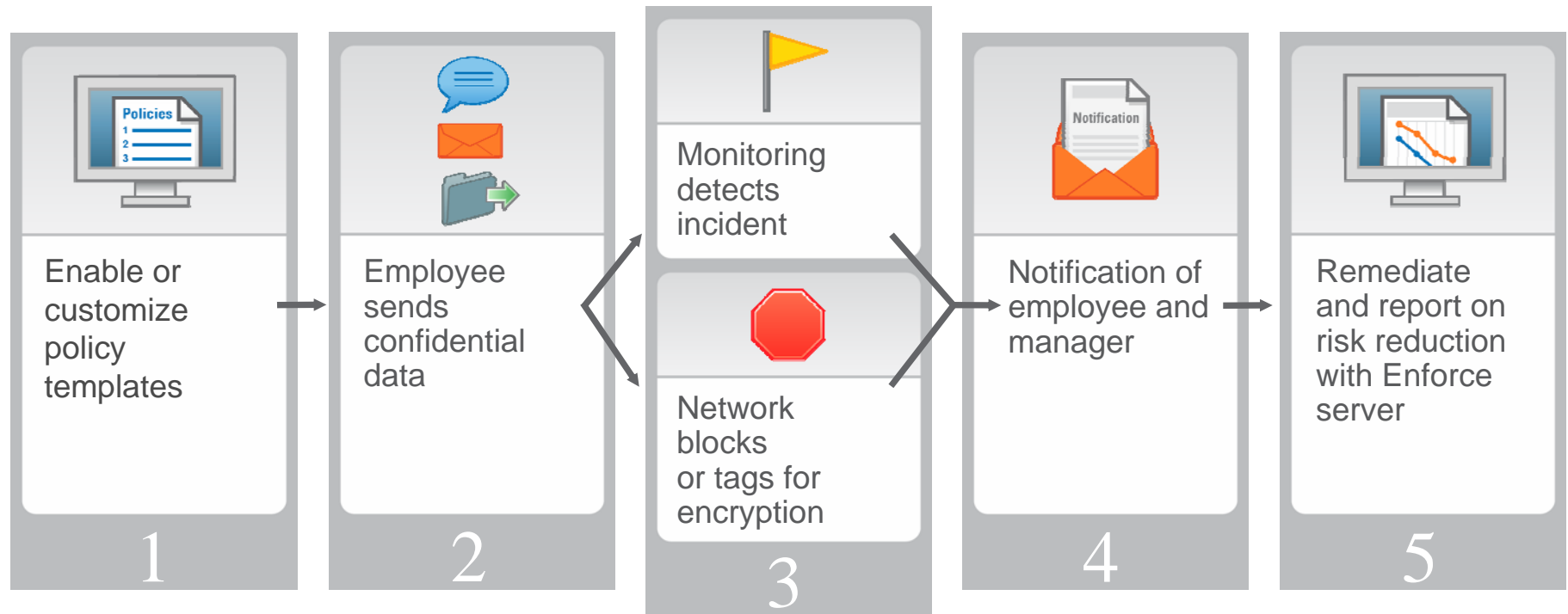
Media

Possibilities

Imagine an IT environment where:

- a data security worker creates a single policy that is automatically enforced across every network and endpoint
- employees right-click documents, emails or web pages and immediately see what actions are allowed
- data classification, storage management, and access control are based on the nature of content rather than the documents that contain it
- malicious activity is correlated and forensically captured across all network, endpoint, and storage channels
- every employee can easily maintain a state of continuous compliance

How it Works : Data in Motion



Key Data in Motion Use Cases

1. Control of Rogue Business Processes

“I do not know what confidential data is being sent to where by whom.”

2. Regulatory Compliance

“I have no way to implement or enforce my data loss compliance obligations.”

3. Encryption

“How do I automate the process of encrypting emails that require it?”

4. Conditional Blocking or Quarantine

“There are some communications that are so sensitive that I would prefer to block them.”

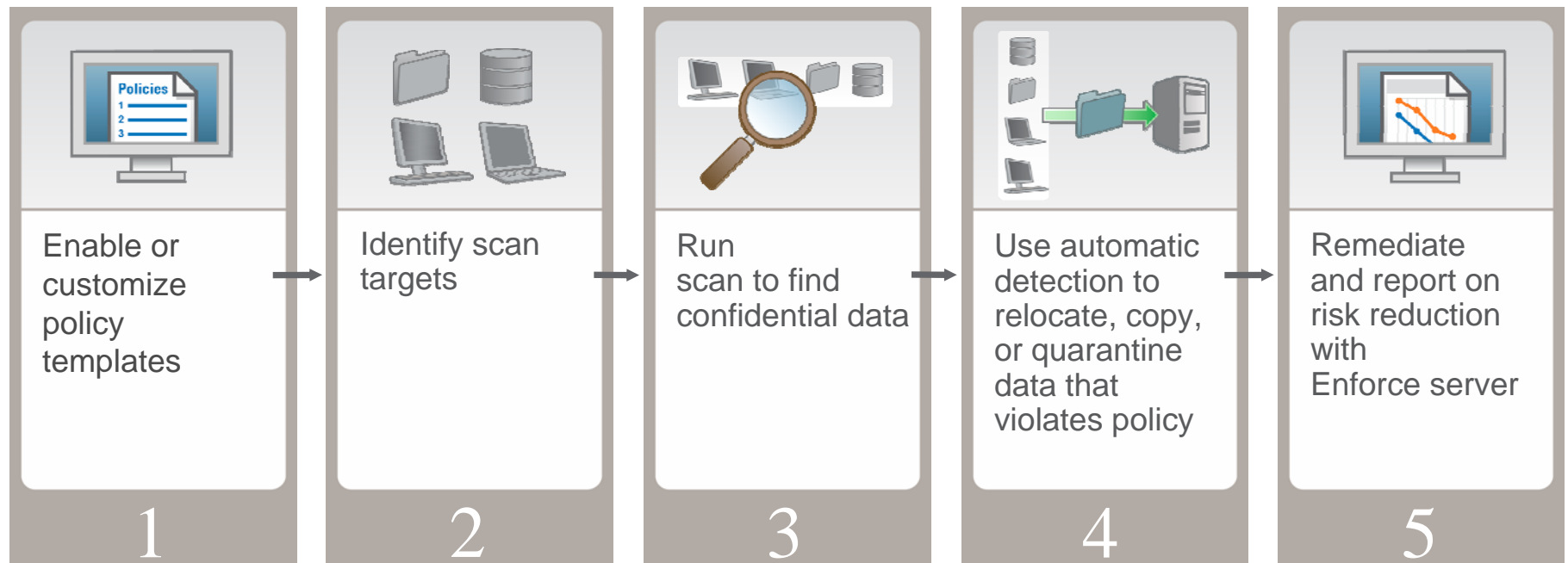
5. Monitor and/or Block SSL Channels

“I have no visibility into SSL-encrypted web mail transmissions.”

6. Employee Education

“My employees are not complying with privacy training guidelines for email and web mail.”

How it Works : Data at Rest



Key Data at Rest Use Cases

1. Compliance (GLBA, PCI, HIPAA)

“I am responsible for reducing PCI compliance risk around exposed cardholder data.”

2. Data Cleanup

“I don’t know where my confidential data is. I need to get rid of my aged data.”

3. eDiscovery

“Our eDiscovery process is time consuming and gives inaccurate results.”

4. Data Classification

“I have no way to implement and enforce my data classification policies.”

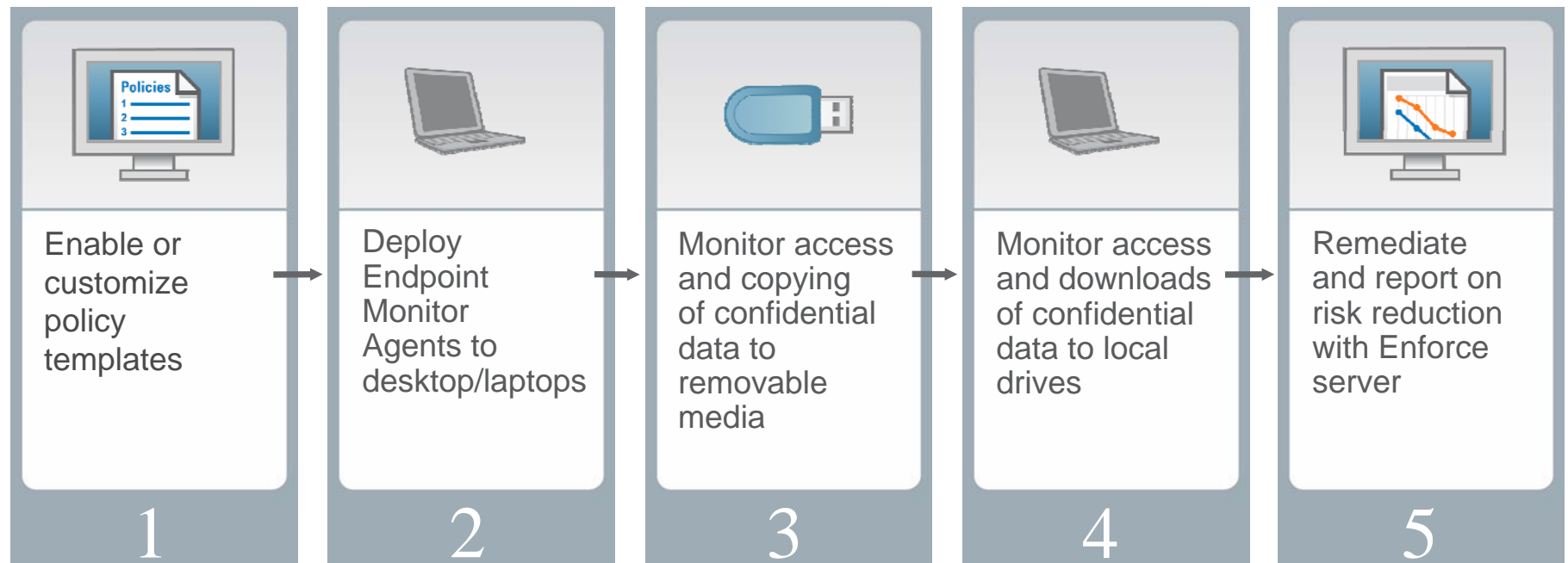
5. Data Access Audit

“Our employees still have access to data that they shouldn’t have access to.”

6. Laptop and Back-up Tape Loss

“We do not know what confidential data was on the stolen laptop.”

How it Works : Data at the Endpoint



Key Data at the Endpoint Use Cases

1. Data Flow Discovery at the Endpoint

“What sensitive data is copied from servers to local drives?”

2. Confidential Data Abuse /Theft

“What confidential data is copied to removable media?”

3. Employee Education

“How do I inform employees about policy violations occurring at the endpoint?”

Intellectual Property Case Example

- Large specialty retailer
 - › 1,000 stores
 - › 110,000 employees
- Challenge: To proactively prevent intellectual property incidents
 - › Customer data (credit card information, PCI compliance)
 - › Pricing, marketing and expansion plans
- Solution:
 - › Track and block unauthorized transmissions of confidential info
 - › Manage and measure risk over time
 - › Improve business processes and remediation workflow

Magnetic Stripe Data and PCI Compliance

- Magnetic stripe contains *nearly* complete raw credit card data
 - › Contains CVV1 used for in-person transactions
 - › Does NOT contain CVV2 for card-not-present transactions



- Storing magnetic stripe data is the cardinal sin of PCI Compliance

Regulatory Compliance Case Example

- Leading provider of investment products
 - › Fortune 100
 - › 30,000 employees
- Challenge: Protect its brand and customer trust while also meeting regulatory requirements
 - › Customer financial and private health data (SSN, HIPAA)
 - › M&A documents, network design, growth plans
- Solution:
 - › Monitor sensitive data going to removable media devices like USB flash drive
 - › Automate distributed remediation processes
 - › Improve business processes and remediation workflow

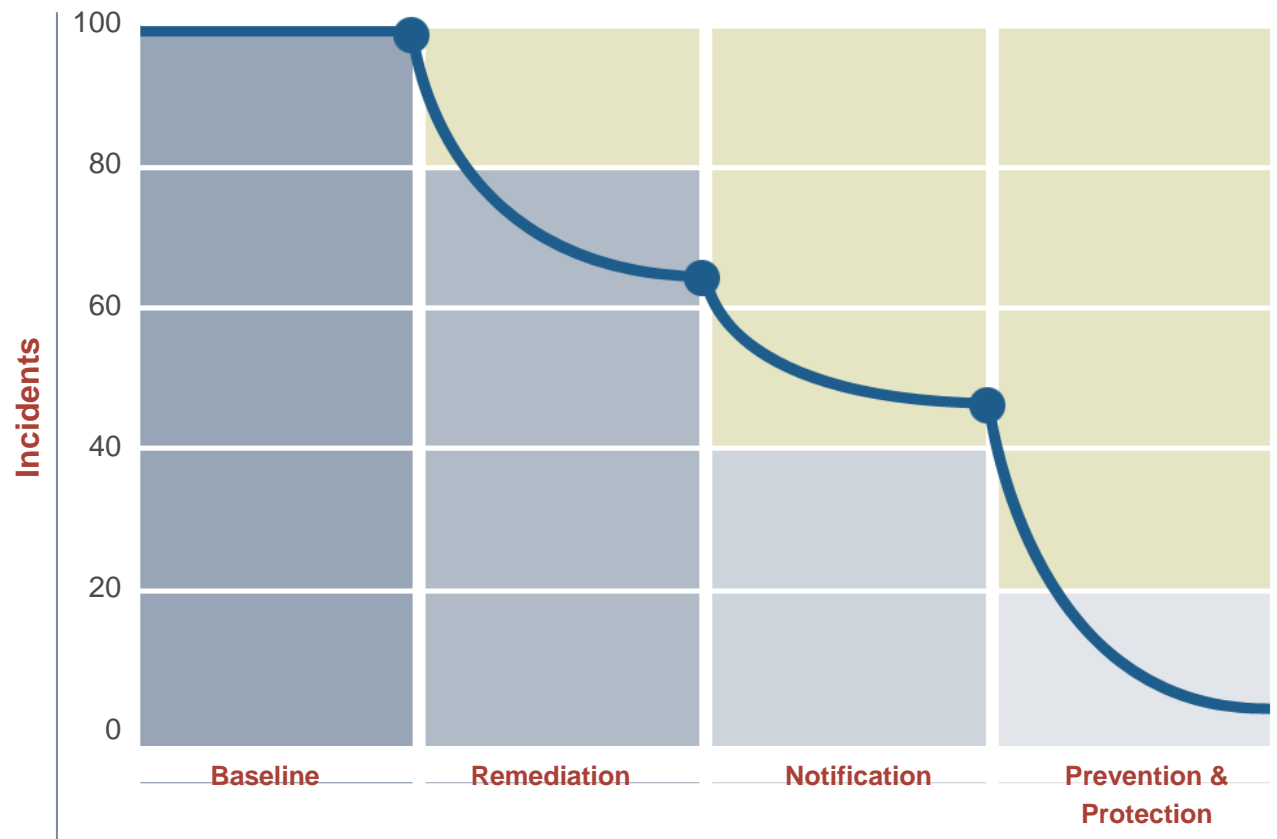
Automated Policy Enforcement and Workflow to

Enforcement Levels

1. Remediation
2. Notification
3. Prevention and Protection

How is Risk Reduced?

- › Fix broken processes
- › Educate workforce
- › Notify policy violators
- › Notify management
- › Protect files
- › Prevent incidents



Successful DLP Workflow

90% of DLP is Incident Response

- | | | |
|--------------------------|---|---------------------------------------|
| Right Automation | ▶ | Resolution, Enforcement, Notification |
| Right Person | ▶ | Route Incidents to Right Responder |
| Right Order | ▶ | High Severity of Incidents First |
| Right Information | ▶ | 5 Second Test |
| Right Action | ▶ | 1 Click Response |
| Right Metrics | ▶ | Prove Results to Execs and Auditors |

DLP Requirements

Data in Motion

- Complete network coverage
- Multi protocol blocking, including HTTPS
- Automated encryption
- Safeguard employee privacy

Data at Rest

- Target coverage: file shares, databases, Lotus Notes
- Automated data protection
- Actionable incident details including ACL's
- Scan management

Data at the Endpoint

- Content aware monitoring
- Continuous monitoring
- Reliable and manageable
- Scalable architecture for enterprise-wide deployments
- Scale

Policy Enforcement

- Detection: all data types, all languages
- Universal policy management
- Remediation: automated, prioritized, correlated
- Access and privacy controls
- Reporting: dashboards, multi-dimensional summarization

Platform

- System management
- Distributed architecture
- User & identity management
- Integration and APIs
- System security

Thank You.