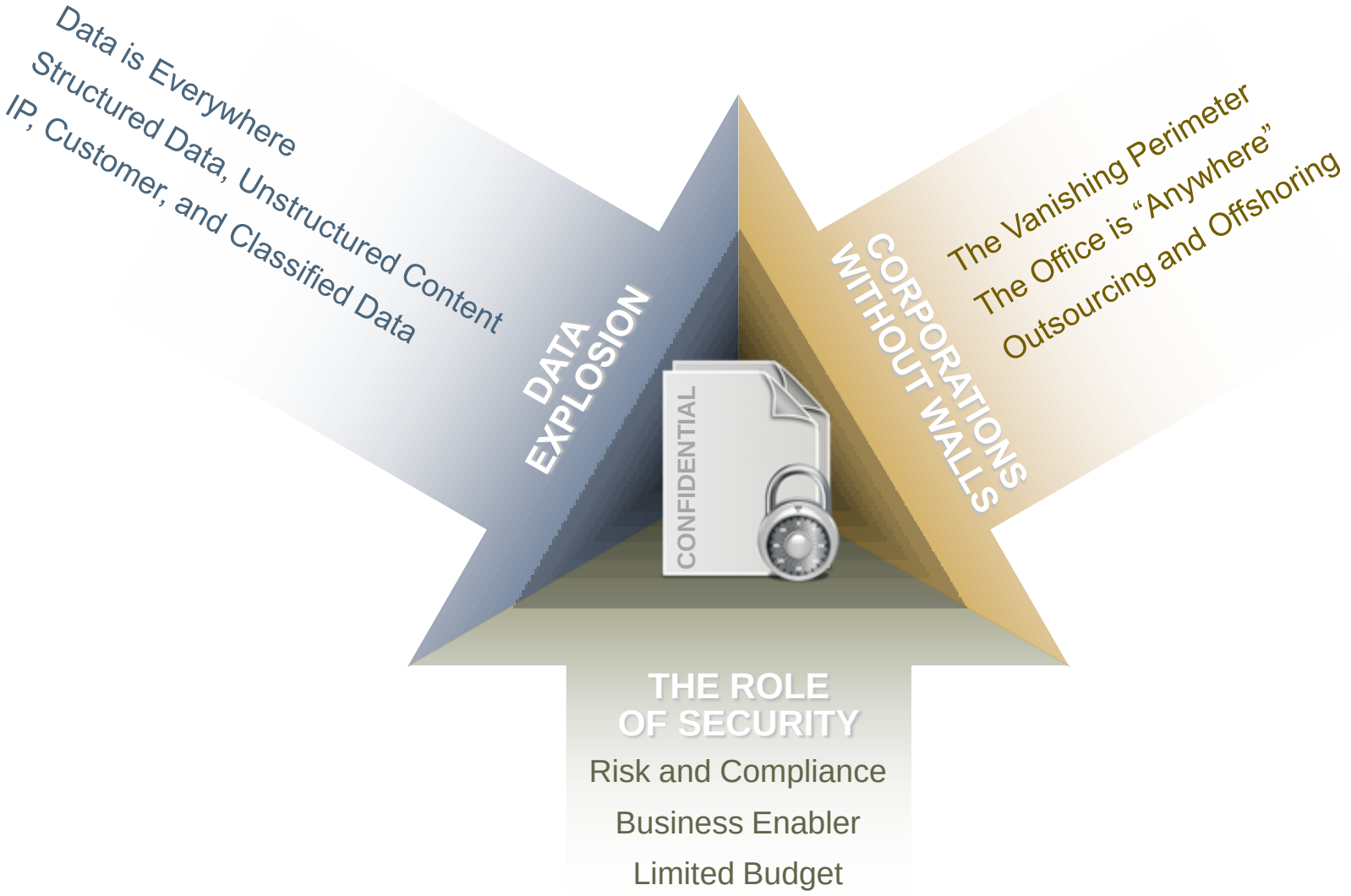
Data Loss Prevention

South Florida Security Mgmt & Compliance User Group

May 7, 2009

Security for a Wide Open World



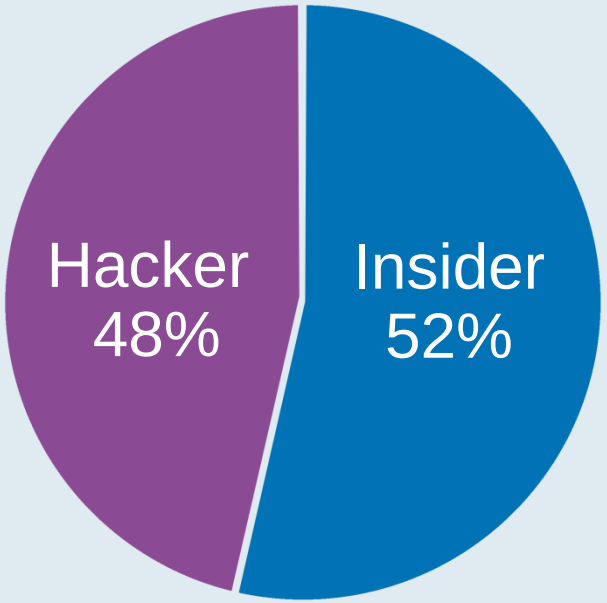
Data Loss Prevention Drivers

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** contains confidential data
	1:50 network files is wrongly exposed
	4:5 companies lost data on **laptops**
	1:2 companies lost data on **USB drives**

The Shift in Data Security Threat

Insider vs. The Hacker

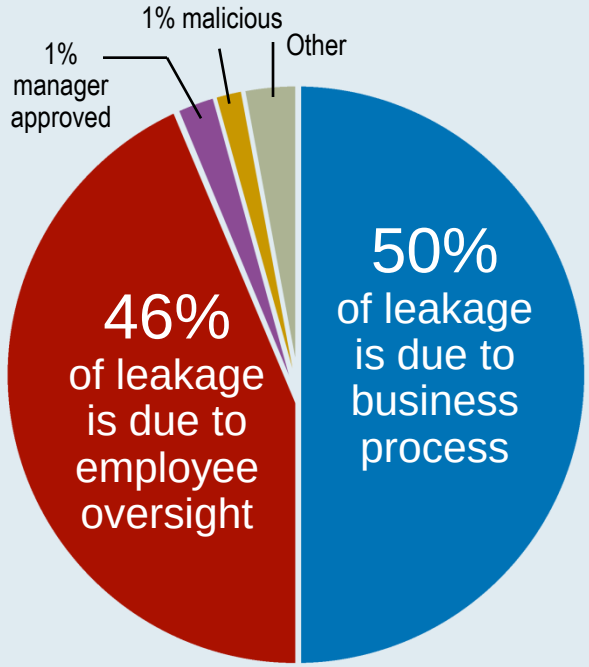
Breaches since 2005:
1380 and counting
> 318M records



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: Symantec Data Loss Prevention Risk Assessment findings.

Key Data Security Regulations

Regulation	Overview	Amendments	Fines and Penalties
GLBA	Mandates financial institutions to enact board-approved security policy that supports privacy and protection of **NPPI**	•Financial Privacy Rule, 16 CFR 313 •Safeguards Rule, 16 CFR 314 •Pre-texting Rule, 15 USC 6821	•$500K for a felony •$200K for Class A misdemeanor •$10K for Class B or C misdemeanor •$10K for an infraction
PCI	Requires all members, merchants, and service providers that store, process and transmit **cardholder data** to keep that data secure	•v1.1 revised in Sept .2006 •v1.2 revised in Oct. 2008	•Violation of any one of 12 requirements will trigger overall PCI non-compliance
HIPAA	Requires any organization entrusted with **PHI** to safeguard that data against misuse or disclosure	•In effect since 2003 •Supplemental regulations around ePHI took effect in 2005	•$50K and/or imprisonment for wrongful disclosure •$100K and/or imprisonment for offense under false pretenses •$250K and/or imprisonment for offense with intent to sell information
State Data Privacy	Requires agency, person, or business to notify state residents if there was a **PII** security breach	•CA 1386 went into effect in July 2003 •To-date, 43 states have enacted security breach notification laws	•Varies depending on state •Civil fines •Injunctions and notice requirements •Damages
MA. Chapter 93H	Authorizes state to set and enforce standards for processing / destruction of **PII**	•In effect since 2007 •Executive Order to take into effect on Jan.1, 2009	•Civil penalty of $5K per violation •Civil fine of $100 per data subject for wrongful disposal up to $50K per incident

What is Data Loss Prevention?

Where is your confidential data?

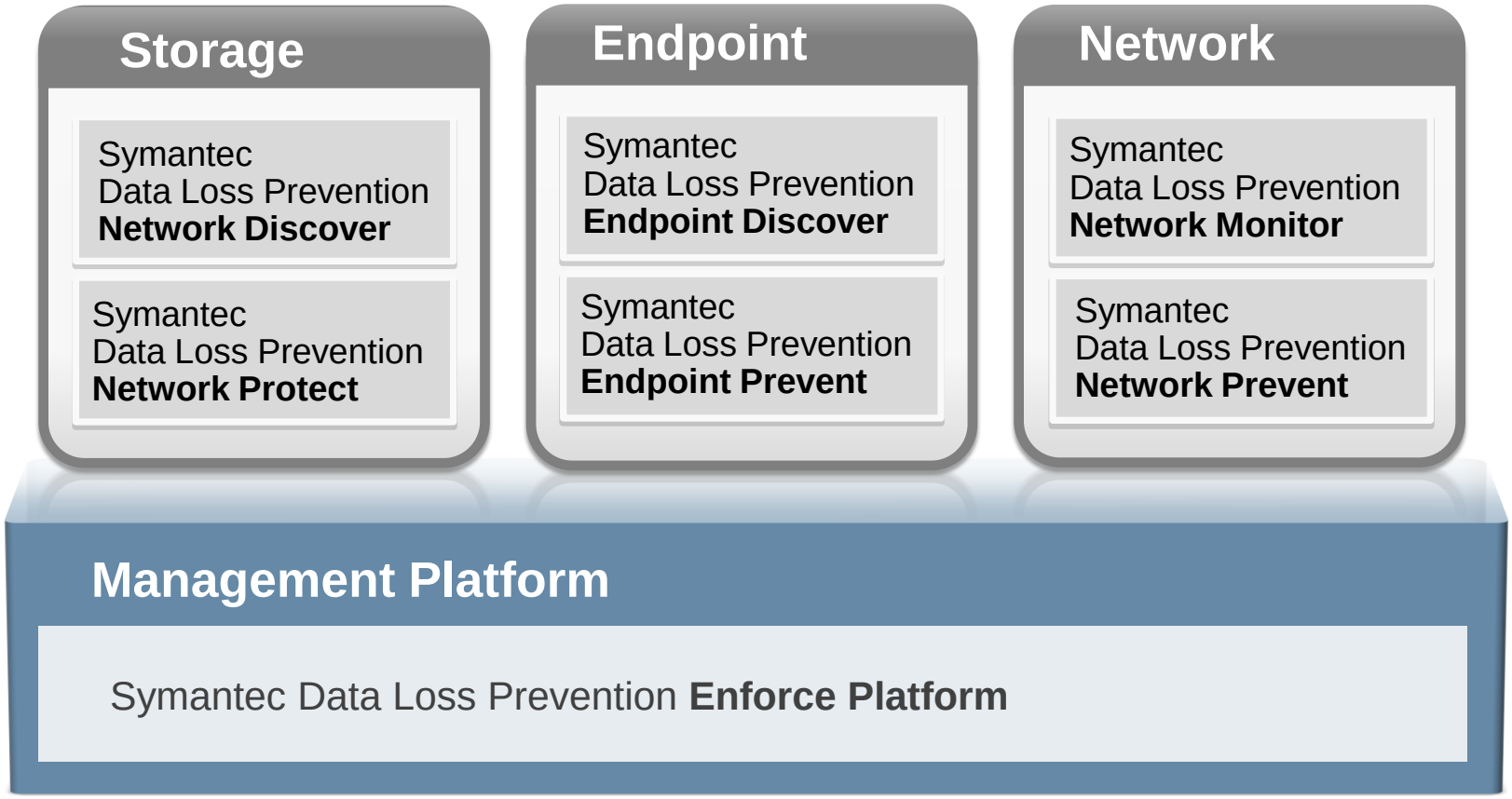
How is it being used?

How best to prevent its loss?

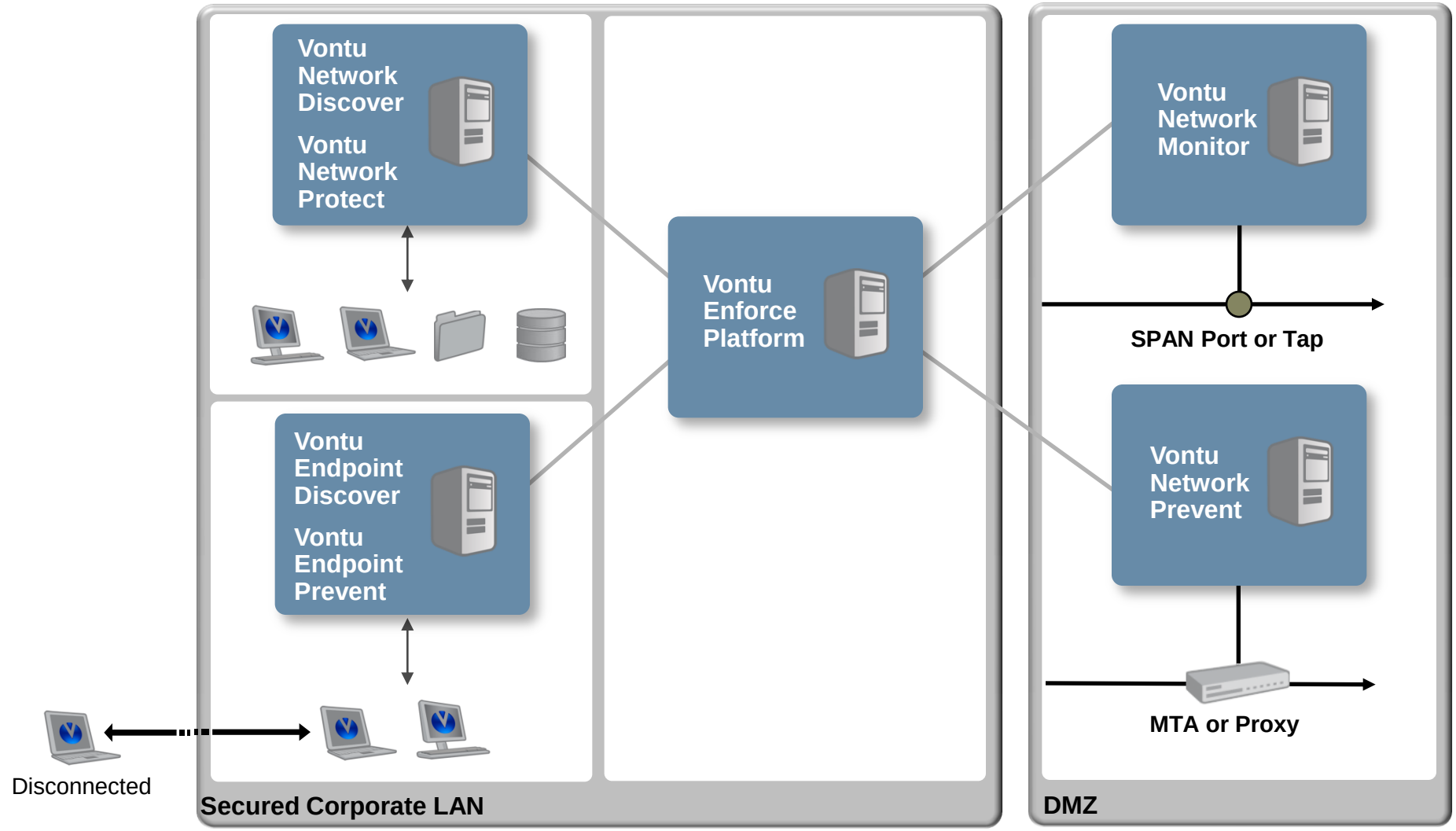
DISCOVER | **MONITOR** | **PROTECT**

DATA LOSS PREVENTION (DLP)

Symantec Data Loss Prevention



Symantec DLP Architecture



Symantec DLP TrueMatch™ Detection

Policy

Policy Builder

- Boolean logic
- Response rules
- Best practice policy templates
- Group based policies

Detection Technologies

DCM
Described Content Matching

Described Data

- Non-indexable data
- Lexicons
- Data identifiers

EDM
Exact Data Matching

Structured Data
Customer Data

- Customer/Employee/ Pricing
- 300M+ rows per server
- Partial row matching
- Near perfect accuracy

IDM
Indexed Document Matching

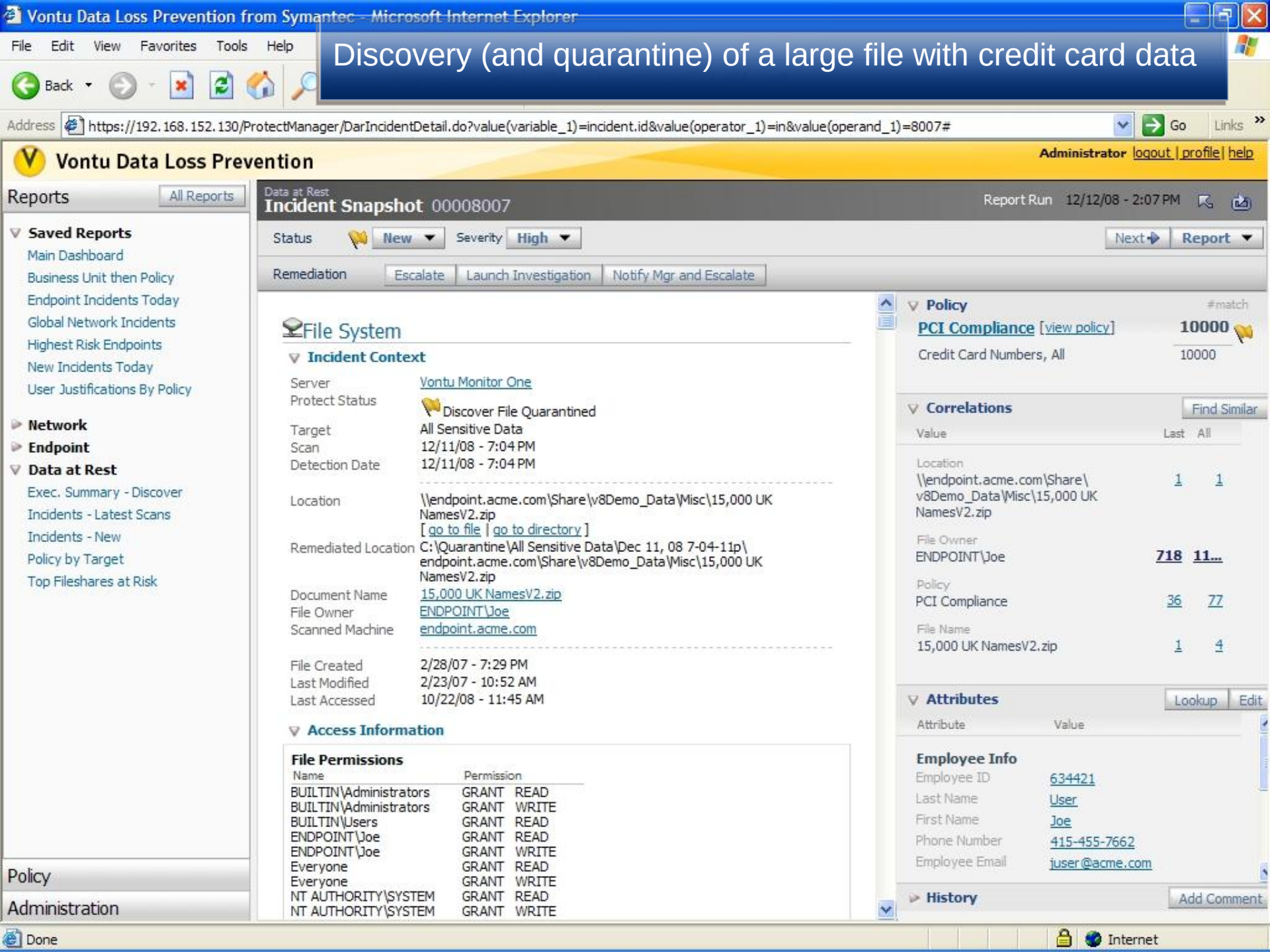
Unstructured Data
Intellectual Property

- Designs/Source/ Financials
- 5M+ docs per server
- Derivative & passage match
- Near perfect accuracy

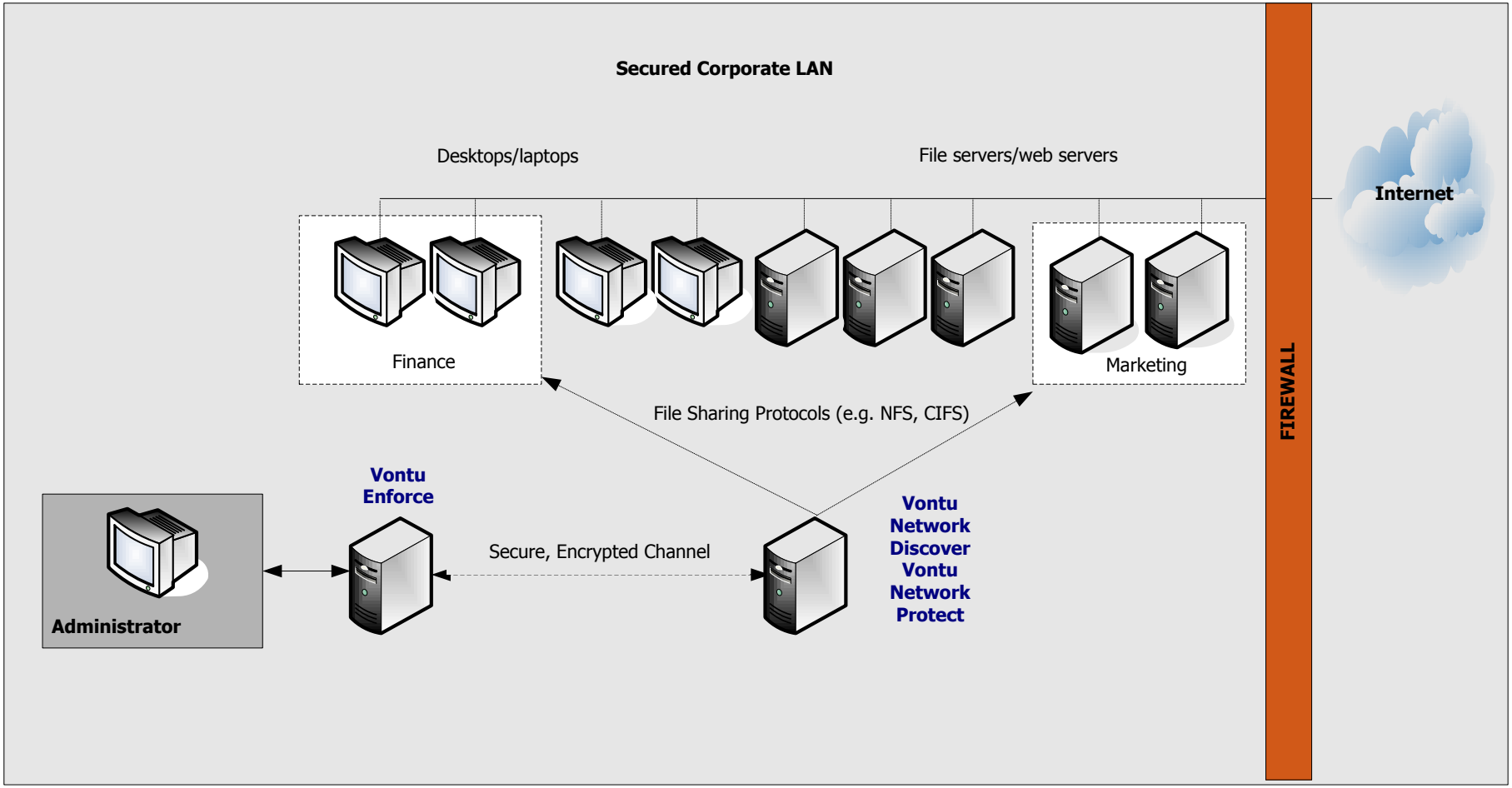
Complete Coverage: Discover

- **Find data wherever it is stored**
  - File servers
  - Distributed machines
  - Document and email repositories
  - Web content and applications
  - Databases
- **Create inventory of sensitive data**
  - Scheduled scanning
  - Incremental scanning
  - “Out of compliance” scan mode
- **Manage data clean up**
  - Incident match count
  - File details (date, owner)
  - Access control information
  - Data owner look up

SCAN TARGETS	
FILE SERVERS	
WINDOWS VIA CIFS	●
UNIX VIA NFS	●
LOCAL WINDOWS	●
LOCAL UNIX (LINUX, AIX, AND SOLARIS)	●
NOVELL	●
NAS FILERS	●
DISTRIBUTED MACHINES	
LAPTOPS	●
DESKTOPS	●
DOCUMENT AND EMAIL REPOSITORIES	
SHAREPOINT	●
LIVELINK	●
DOCUMENTUM	●
LOTUS NOTES	●
MICROSOFT EXCHANGE	●
PST	●
WEB CONTENT AND APPLICATIONS	
CORPORATE WEB SITES	●
INTRANET	●
EXTRANET	●
CUSTOM APPLICATIONS	●
DATABASES	
ORACLE	●
MICROSOFT	●
IBM DB2	●
SYBASE	●


Vontu Data Loss Prevention from Symantec - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Discovery (and quarantine) of a large file with credit card data
Back
Address https://192.168.152.130/ProtectManager/DarIncidentDetail.do?value(variable_1)=incident.id&value(operator_1)=in&value(operand_1)=8007#
Go
Links
Vontu Data Loss Prevention
Administrator logout | profile | help
Reports
All Reports
Saved Reports
Main Dashboard
Business Unit then Policy
Endpoint Incidents Today
Global Network Incidents
Highest Risk Endpoints
New Incidents Today
User Justifications By Policy
Network
Endpoint
Data at Rest
Exec. Summary - Discover
Incidents - Latest Scans
Incidents - New
Policy by Target
Top Fileshares at Risk
Policy
Administration
Data at Rest
Incident Snapshot 00008007
Report Run 12/12/08 - 2:07 PM
Status New
Severity High
Next
Report
Remediation
Escalate
Launch Investigation
Notify Mgr and Escalate
File System
Incident Context
Server Vontu Monitor One
Protect Status Discover File Quarantined
Target All Sensitive Data
Scan 12/11/08 - 7:04 PM
Detection Date 12/11/08 - 7:04 PM
Location \\endpoint.acme.com\Share\v8Demo_Data\Misc\15,000 UK NamesV2.zip
[go to file | go to directory]
Remediated Location C:\Quarantine\All Sensitive Data\Dec 11, 08 7-04-11p\endpoint.acme.com\Share\v8Demo_Data\Misc\15,000 UK NamesV2.zip
Document Name 15,000 UK NamesV2.zip
File Owner ENDPOINT\Joe
Scanned Machine endpoint.acme.com
File Created 2/28/07 - 7:29 PM
Last Modified 2/23/07 - 10:52 AM
Last Accessed 10/22/08 - 11:45 AM
Access Information
File Permissions
Name Permission
BUILTIN\Administrators GRANT READ
BUILTIN\Administrators GRANT WRITE
BUILTIN\Users GRANT READ
ENDPOINT\Joe GRANT READ
ENDPOINT\Joe GRANT WRITE
Everyone GRANT READ
Everyone GRANT WRITE
NT AUTHORITY\SYSTEM GRANT READ
NT AUTHORITY\SYSTEM GRANT WRITE
Policy
#match
PCI Compliance [view policy] 10000
Credit Card Numbers, All 10000
Correlations
Find Similar
Value Last All
Location \\endpoint.acme.com\Share\v8Demo_Data\Misc\15,000 UK NamesV2.zip 1 1
File Owner ENDPOINT\Joe 718 11...
Policy PCI Compliance 36 77
File Name 15,000 UK NamesV2.zip 1 4
Attributes
Lookup
Edit
Attribute Value
Employee Info
Employee ID 634421
Last Name User
First Name Joe
Phone Number 415-455-7662
Employee Email juser@acme.com
History
Add Comment
Done
Internet

DLP Network Discover Deployment



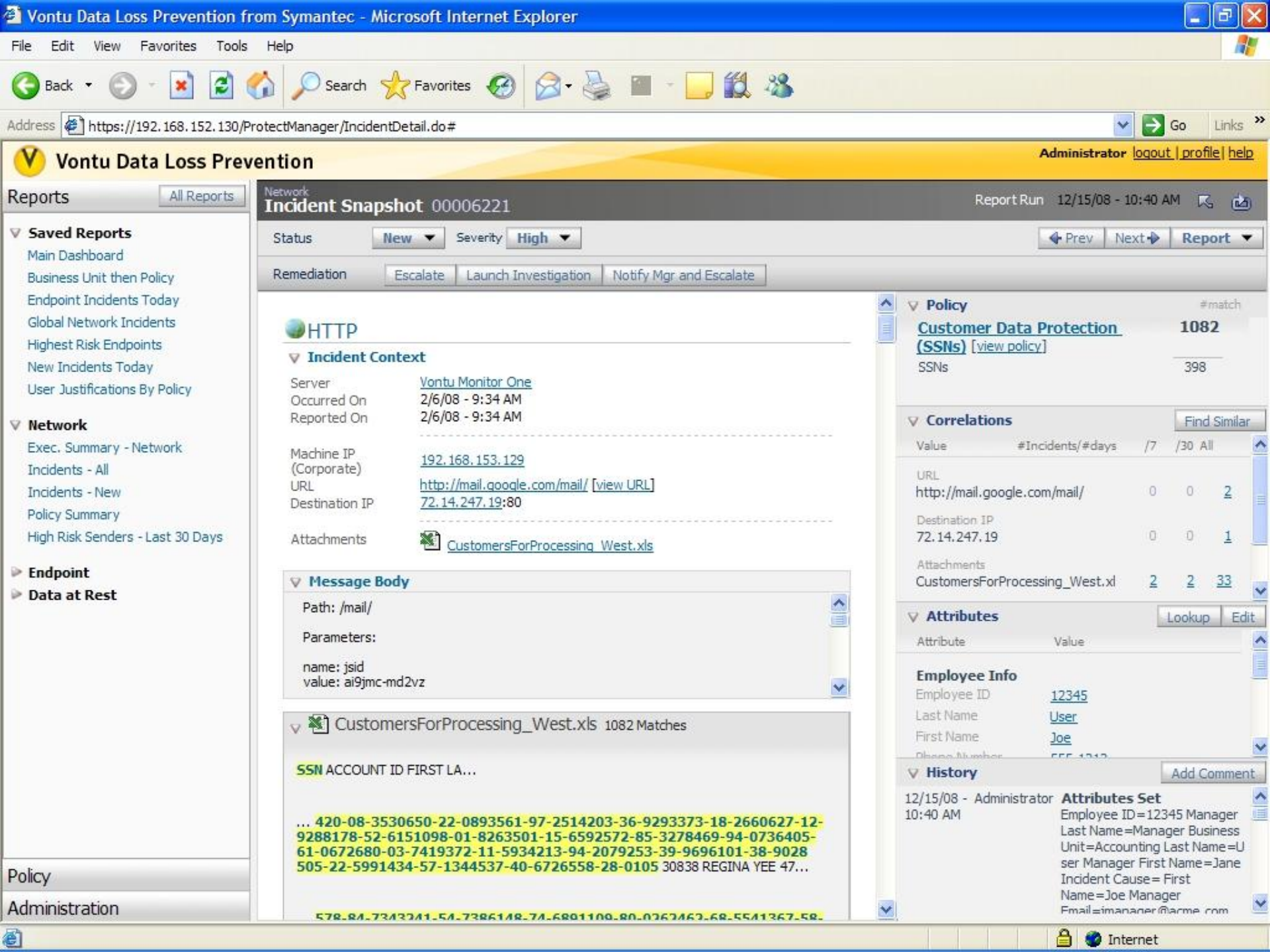
Complete Coverage: Monitor

- **Understand how data is being used**
  - Network protocol coverage
  - Endpoint event coverage
  - Content- and context-aware detection
  - Automated sender/manager notification
- **Monitor on the network**
  - Standard hardware
  - Signature-based protocol recognition
  - Gigabit monitoring without “sampling” or dropped packets
  - Queue incidents
- **Monitor at the endpoint**
  - Online and offline
  - Unmanaged devices and OSes
  - On-screen pop up notification

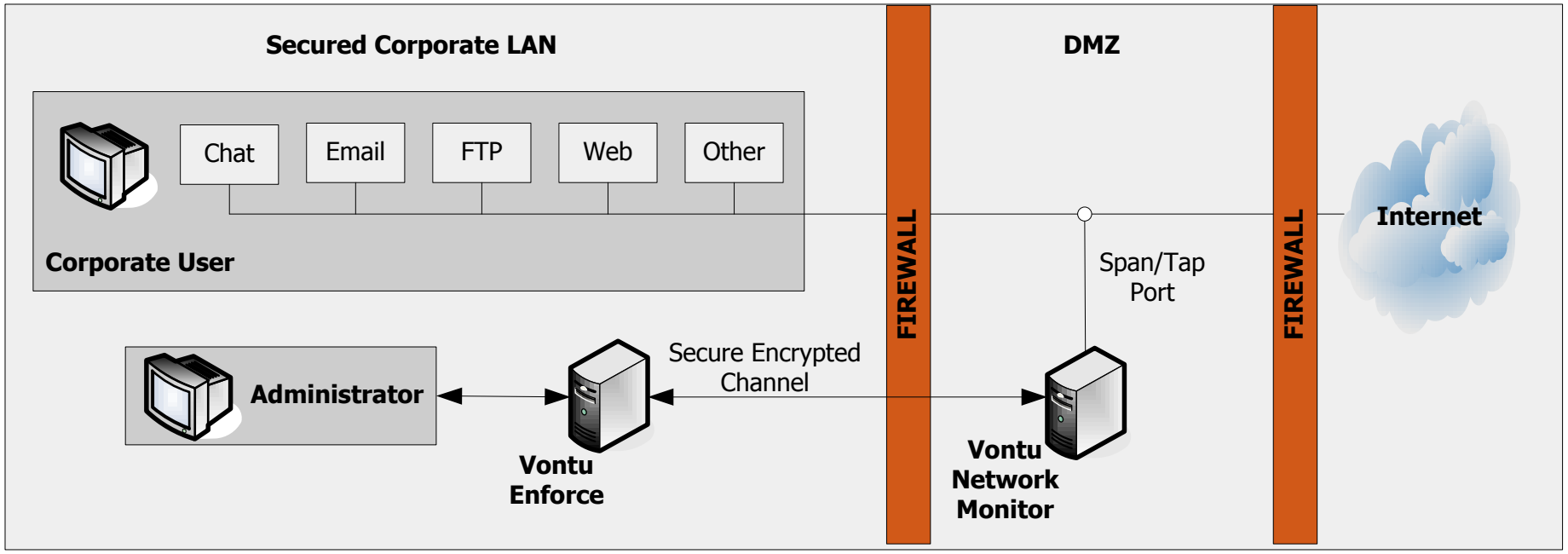
PROTOCOLS & EVENTS	NETWORK	ENDPOINT
CONTENT-AWARE MONITORING		
HTTPS*	●	●
HTTP	●	●
MAIL**	●	●
IM (YAHOO!, AOL, MSN)	●	●
FTP	●	●
PTP	●	
GENERIC TCP	●	
NNTP	●	
USB / FIREWIRE		●
CD / DVD		●
PRINT / FAX		●
COPY / PASTE		●
LOCAL DRIVE		●

* Internet Explorer and Firefox plug-ins at the endpoint

** Outlook and Lotus Notes plug-ins at the endpoint


Vontu Data Loss Prevention from Symantec - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.152.130/ProtectManager/IncidentDetail.do#
Go Links
Vontu Data Loss Prevention
Administrator logout | profile | help
Reports All Reports
Saved Reports
Main Dashboard
Business Unit then Policy
Endpoint Incidents Today
Global Network Incidents
Highest Risk Endpoints
New Incidents Today
User Justifications By Policy
Network
Exec. Summary - Network
Incidents - All
Incidents - New
Policy Summary
High Risk Senders - Last 30 Days
Endpoint
Data at Rest
Policy
Administration
Network
Incident Snapshot 00006221
Report Run 12/15/08 - 10:40 AM
Status New Severity High
Prev Next Report
Remediation Escalate Launch Investigation Notify Mgr and Escalate
HTTP
Incident Context
Server Vontu Monitor One
Occurred On 2/6/08 - 9:34 AM
Reported On 2/6/08 - 9:34 AM
Machine IP (Corporate) 192.168.153.129
URL http://mail.google.com/mail/ [view URL]
Destination IP 72.14.247.19:80
Attachments CustomersForProcessing_West.xls
Message Body
Path: /mail/
Parameters:
name: jsid
value: ai9jmc-md2vz
CustomersForProcessing_West.xls 1082 Matches
SSN ACCOUNT ID FIRST LA...
... 420-08-3530650-22-0893561-97-2514203-36-9293373-18-2660627-12-9288178-52-6151098-01-8263501-15-6592572-85-3278469-94-0736405-61-0672680-03-7419372-11-5934213-94-2079253-39-9696101-38-9028505-22-5991434-57-1344537-40-6726558-28-0105 30838 REGINA YEE 47...
Policy
#match
Customer Data Protection (SSNs) [view policy] 1082
SSNs 398
Correlations
Find Similar
Value #Incidents/#days /7 /30 All
URL http://mail.google.com/mail/ 0 0 2
Destination IP 72.14.247.19 0 0 1
Attachments CustomersForProcessing_West.xl 2 2 33
Attributes
Lookup Edit
Attribute Value
Employee Info
Employee ID 12345
Last Name User
First Name Joe
History
Add Comment
12/15/08 - 10:40 AM Administrator Attributes Set
Employee ID=12345 Manager Last Name=Manager Business Unit=Accounting Last Name=User Manager First Name=Jane Incident Cause= First Name=Joe Manager
Internet

DLP Network Monitor Deployment



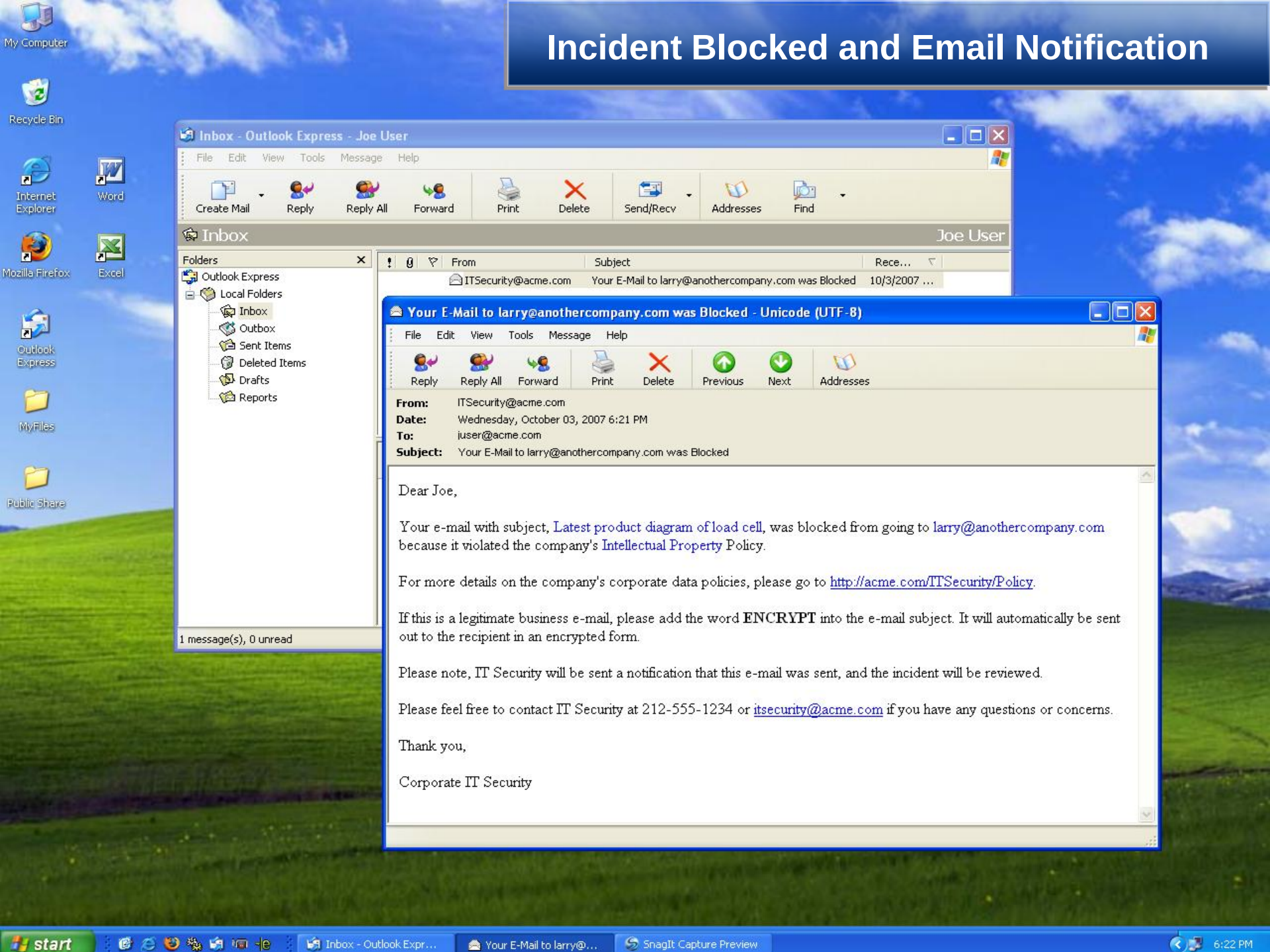
Complete Coverage: Protect

- **Proactively secure stored data**

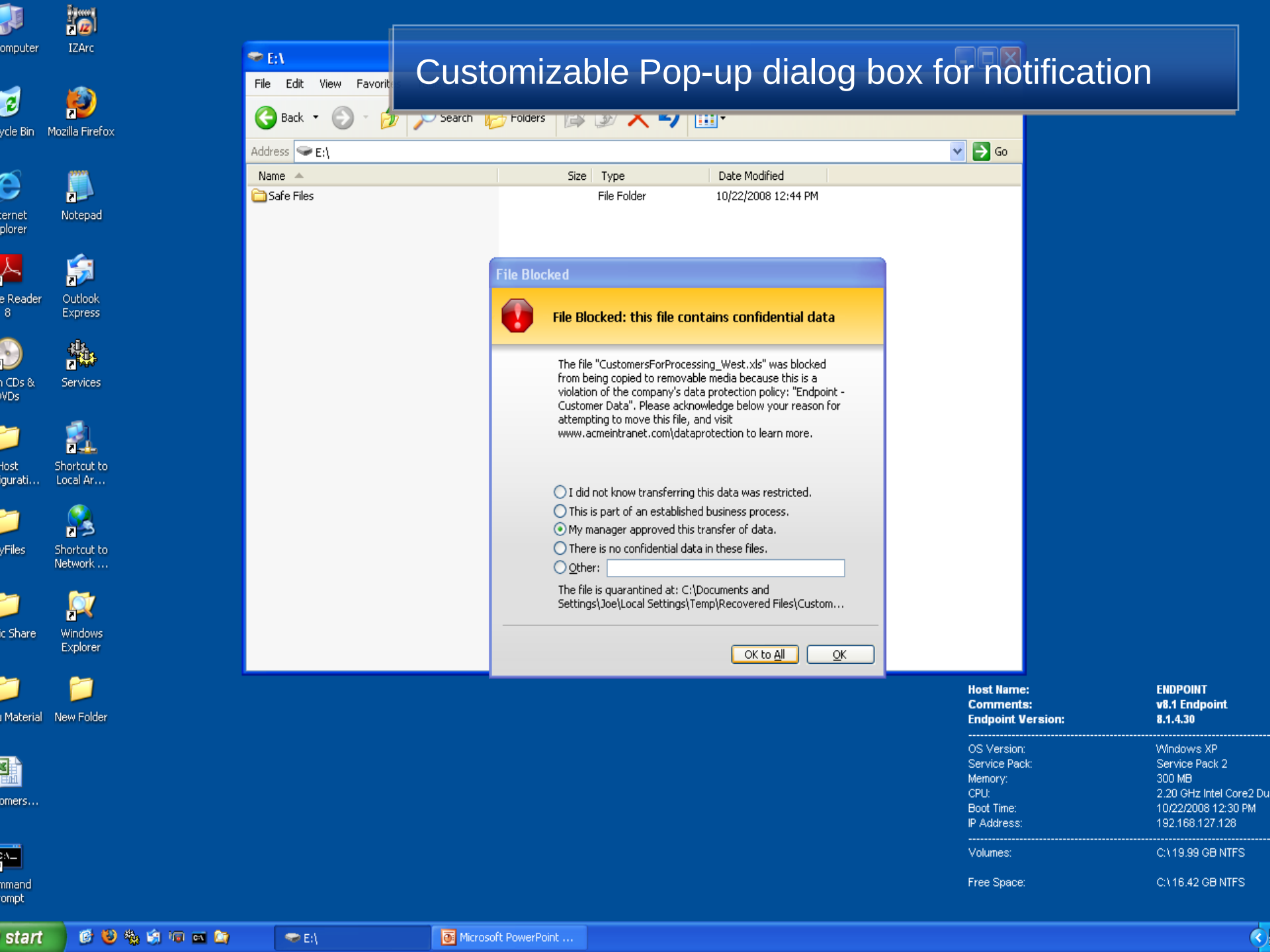
  - Relocate data to an encrypted location
  - Automatically quarantine, copy, or remove data
  - Broadest scan target coverage
- **Prevent confidential data loss**
  - Real-time blocking on network and endpoint
  - Conditionally quarantine/route emails for encryption
  - Selectively remove content from web postings
  - Certified ICAP integration with leading web proxies
  - Support for all SMTP compliant MTAs
- **Enforce confidential data policies**
  - Real-time email notifications
  - Seamless interaction with Web 2.0 sites
  - On-screen pop-up notification on the endpoint
  - “Ransom note” in place of relocated stored data

CONTENT-AWARE PROTECTION	
NETWORK	
HTTP/S	●
SMTP	●
FTP	●
ENDPOINT	
HTTP/S	●
EMAIL (OUTLOOK, LOTUS NOTES)	●
IM (YAHOO! AOL, MSN)	●
FTP	●
USB / FIREWIRE	●
CD / DVD	●
PRINT / FAX	●
COPY / PASTE	●

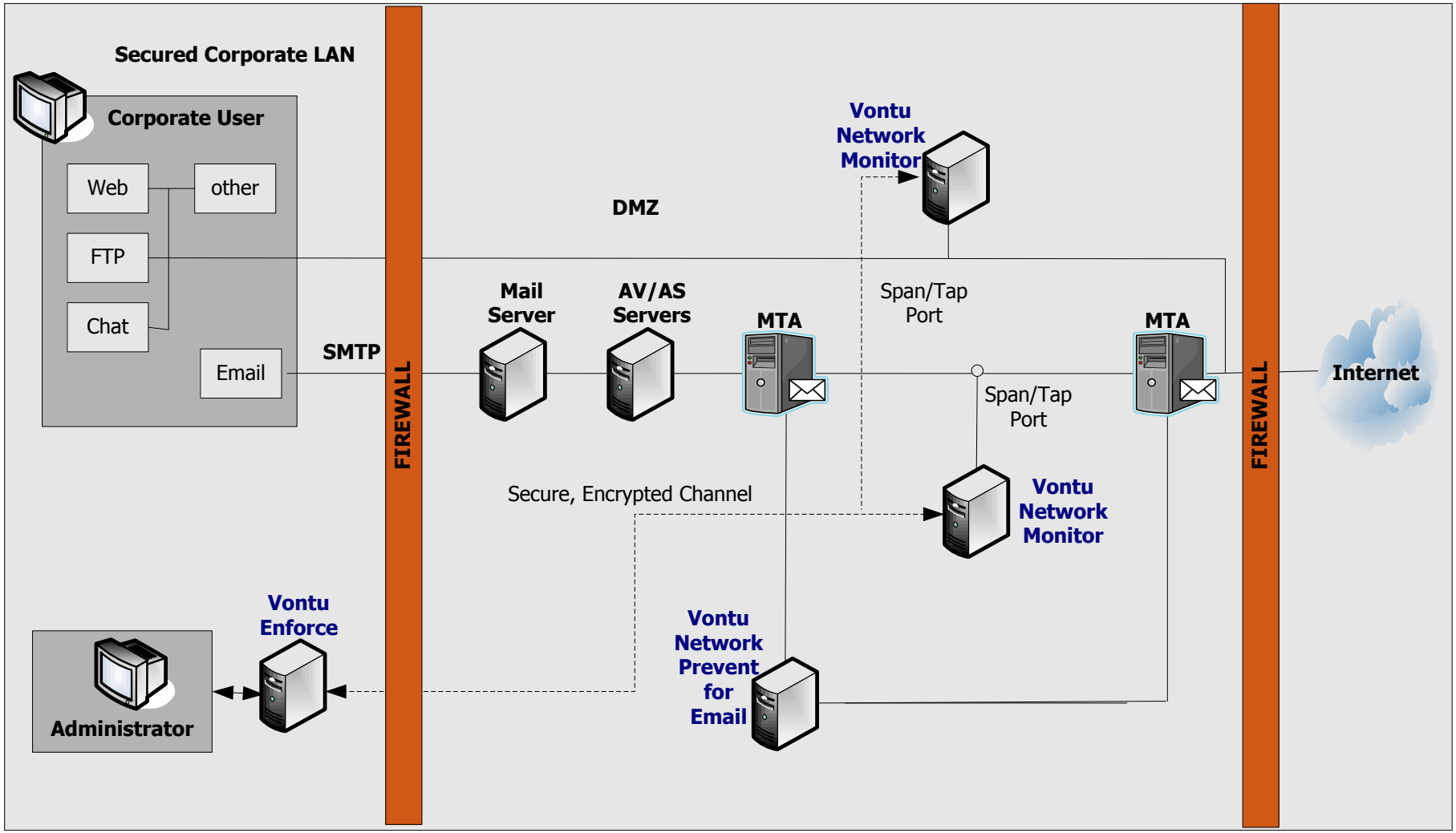
Incident Blocked and Email Notification



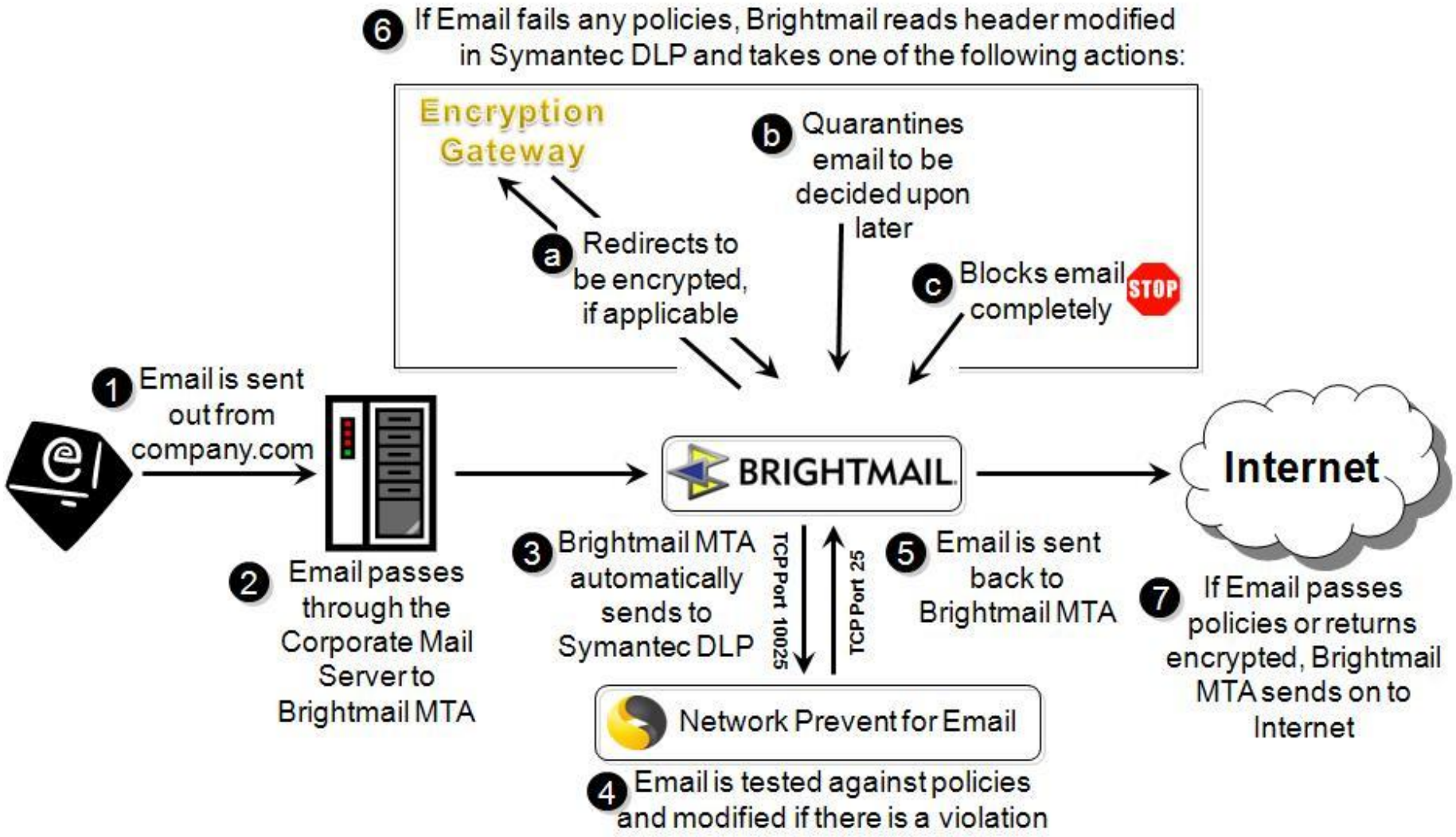
Customizable Pop-up dialog box for notification



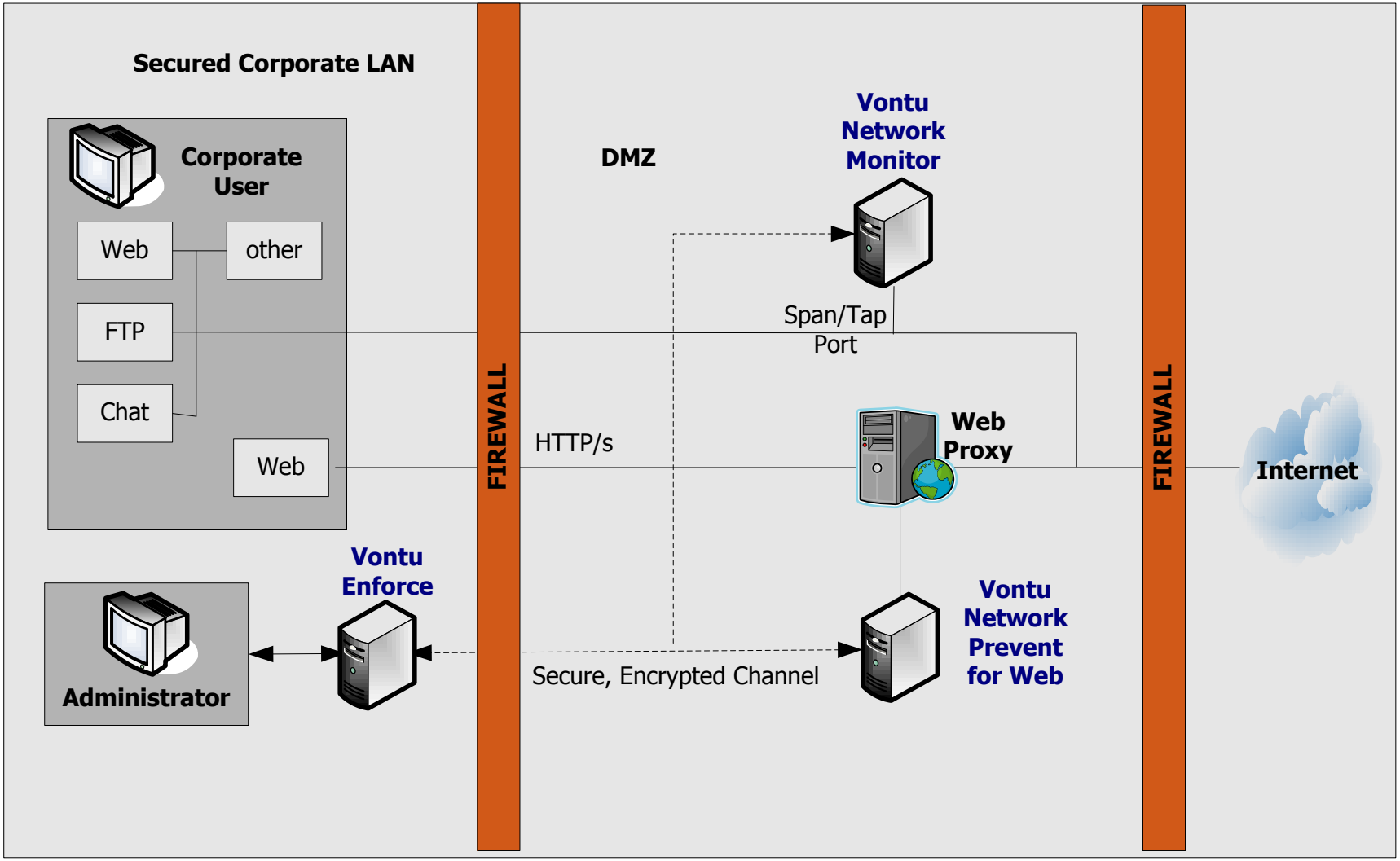
DLP Network Email Prevent Deployment



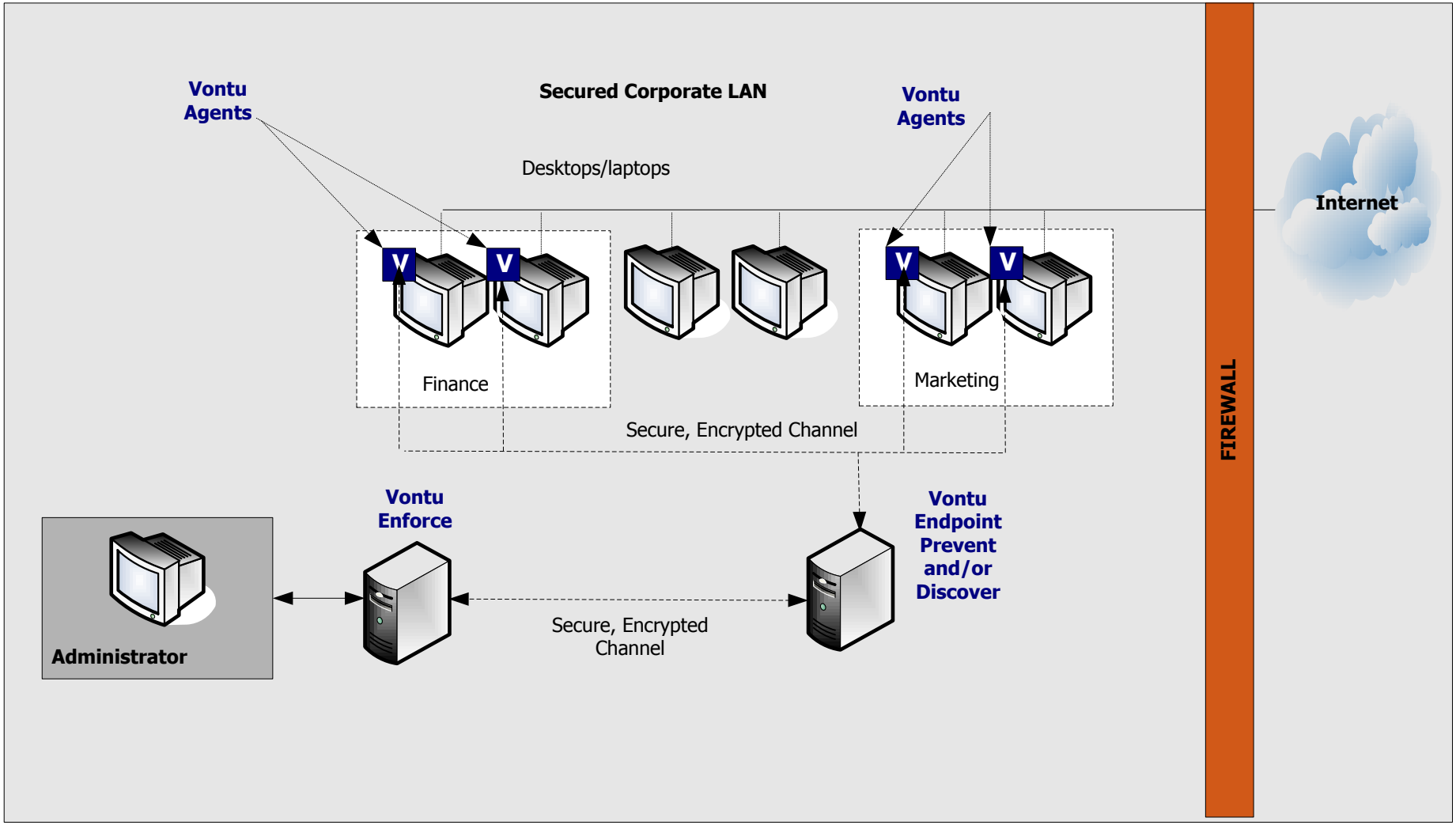
DLP Email Prevent Integration



DLP Network Web Prevent Deployment



DLP Endpoint Deployment

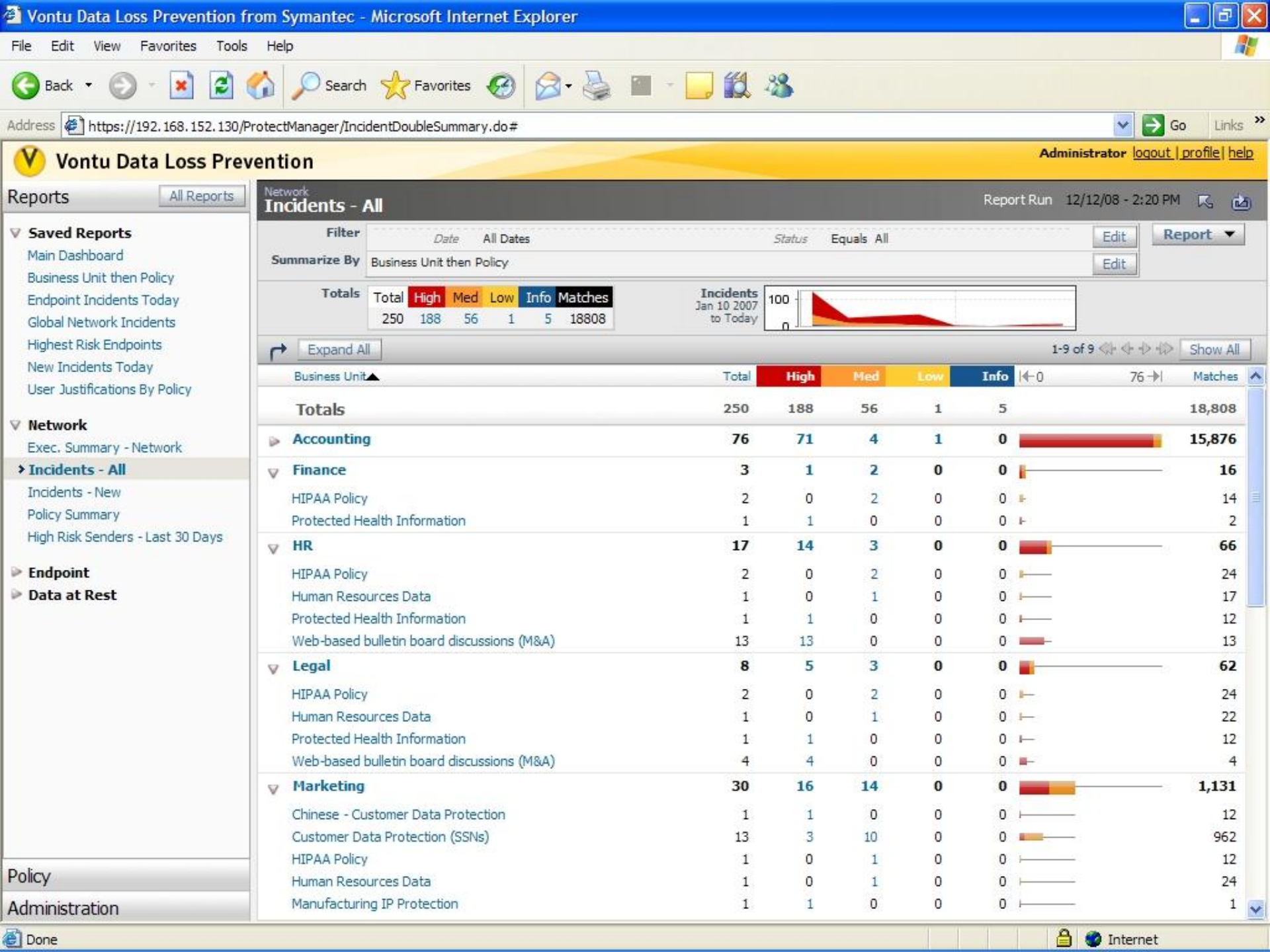


Complete Coverage: Manage

- **Universal DLP Policy**
  - "Define once, enforce everywhere"
  - 60+ pre-built policy templates
  - Custom detection and response rules
- **Accurate TrueMatch Detection**
  - Content and context, enterprise scale
  - Comprehensive EDM, IDM, and DCM
- **Automated Remediation and Workflow**
  - Automated action and response
  - "5 second incident triage"
  - "One-click response"
- **Comprehensive Reporting**
  - 40+ pre-configured reports
  - Business unit risk assessment
- **Scalable and Secure Management**
  - Distributed architecture with high-availability
  - Advanced security design

PRE-BUILT POLICY CATEGORIES	# OF TEMPLATES
REGULATORY ENFORCEMENT	24
CUSTOMER DATA PROTECTION	15
CONFIDENTIAL DATA PROTECTION	11
NETWORK SECURITY ENFORCEMENT	4
ACCEPTABLE USE ENFORCEMENT	14

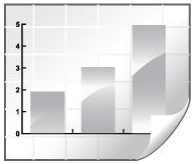
ACCURACY AND AUTOMATION	
DETECTION TECHNOLOGIES	
EXACT DATA MATCHING (EDM)	●
INDEXED DOCUMENT MATCHING (IDM)	●
DESCRIBED CONTENT MATCHING (DCM)	●
AUTOMATED RESPONSE ACTIONS	
BLOCK	●
ENCRYPT (RE-DIRECT)	●
NOTIFY	●
COPY	●
QUARANTINE	●
JUSTIFY	●


Vontu Data Loss Prevention from Symantec - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.152.130/ProtectManager/IncidentDoubleSummary.do#
Go Links
Vontu Data Loss Prevention
Administrator logout | profile | help
Reports All Reports
Saved Reports
Main Dashboard
Business Unit then Policy
Endpoint Incidents Today
Global Network Incidents
Highest Risk Endpoints
New Incidents Today
User Justifications By Policy
Network
Exec. Summary - Network
Incidents - All
Incidents - New
Policy Summary
High Risk Senders - Last 30 Days
Endpoint
Data at Rest
Policy
Administration
Network
Incidents - All
Report Run 12/12/08 - 2:20 PM
Filter Date All Dates Status Equals All Edit
Report
Summarize By Business Unit then Policy Edit
Totals
Total High Med Low Info Matches
250 188 56 1 5 18808
Incidents Jan 10 2007 to Today
100
0
Expand All
1-9 of 9
Show All
Business Unit
Total High Med Low Info 0 76 Matches
Totals 250 188 56 1 5 18,808
Accounting 76 71 4 1 0 15,876
Finance 3 1 2 0 0 16
HIPAA Policy 2 0 2 0 0 14
Protected Health Information 1 1 0 0 0 2
HR 17 14 3 0 0 66
HIPAA Policy 2 0 2 0 0 24
Human Resources Data 1 0 1 0 0 17
Protected Health Information 1 1 0 0 0 12
Web-based bulletin board discussions (M&A) 13 13 0 0 0 13
Legal 8 5 3 0 0 62
HIPAA Policy 2 0 2 0 0 24
Human Resources Data 1 0 1 0 0 22
Protected Health Information 1 1 0 0 0 12
Web-based bulletin board discussions (M&A) 4 4 0 0 0 4
Marketing 30 16 14 0 0 1,131
Chinese - Customer Data Protection 1 1 0 0 0 12
Customer Data Protection (SSNs) 13 3 10 0 0 962
HIPAA Policy 1 0 1 0 0 12
Human Resources Data 1 0 1 0 0 24
Manufacturing IP Protection 1 1 0 0 0 1
Done
Internet

Symantec DLP Success Model

Focus

Target High-Risk Data and
Identify Exposure

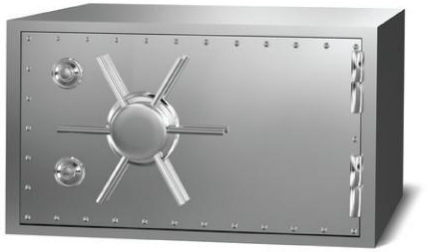


Communicate

Manage Risk,
Deliver Results

Design

Prepare Data Loss Policy,
Remediation and
Risk Reduction Blueprint

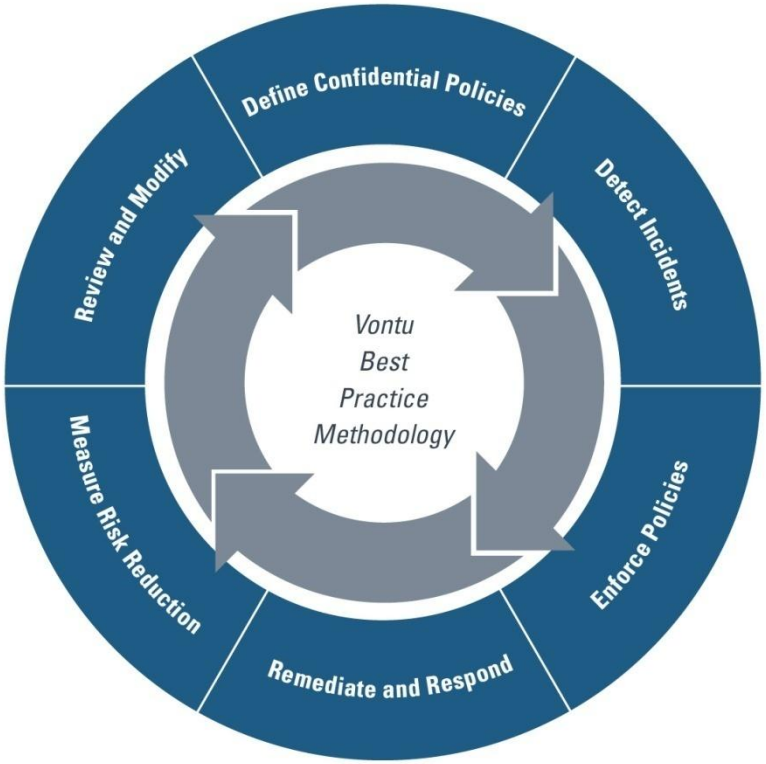


ACCUMULATED KNOWLEDGE

Implement

Protect and Prevent:
Engage Users

Characteristics of Successful DLP Programs

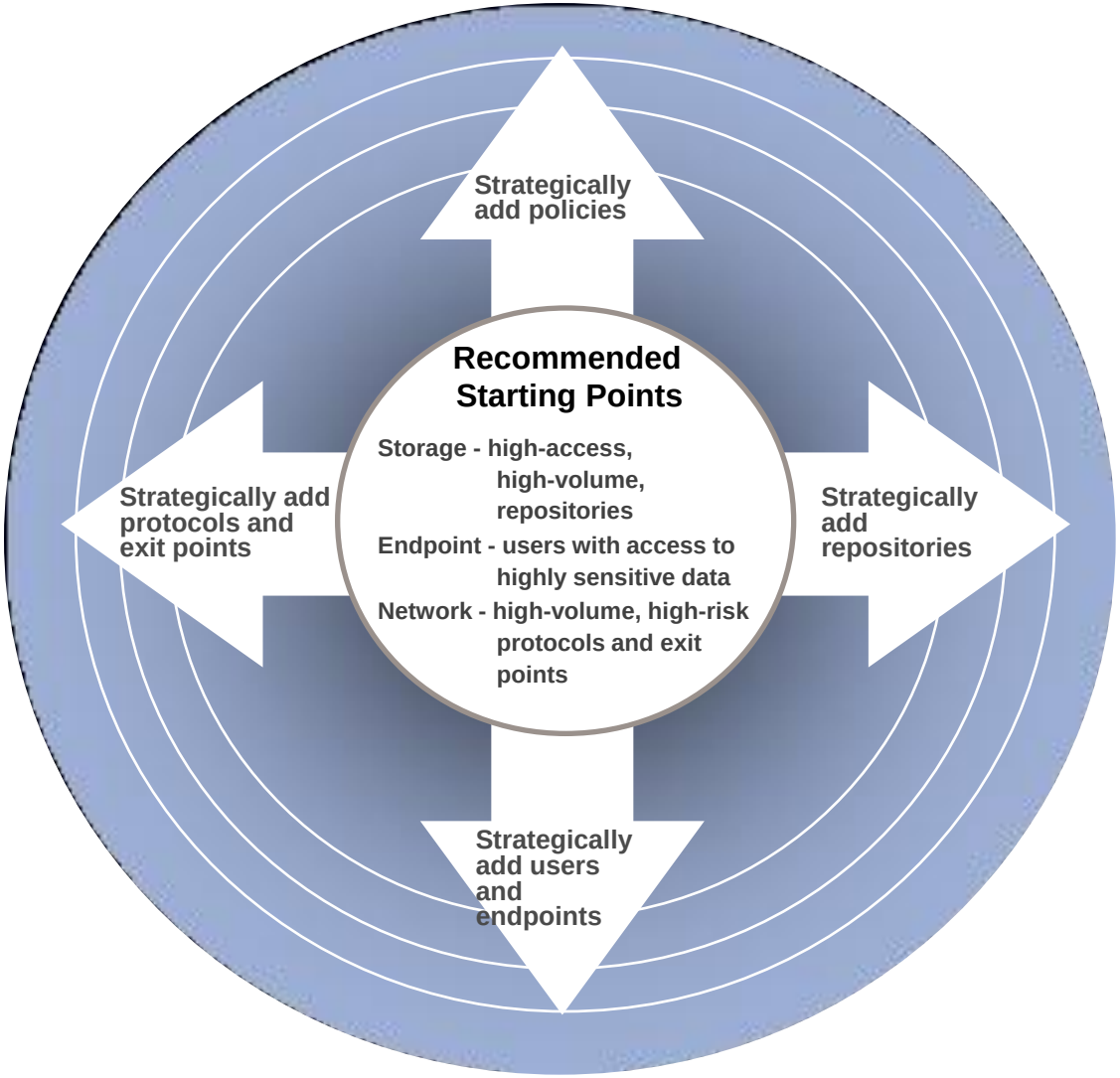


- Executive Level Involvement
- Prioritized Approach
- Incident Response Workflow
- Employee Education
- Measurable Risk Metrics

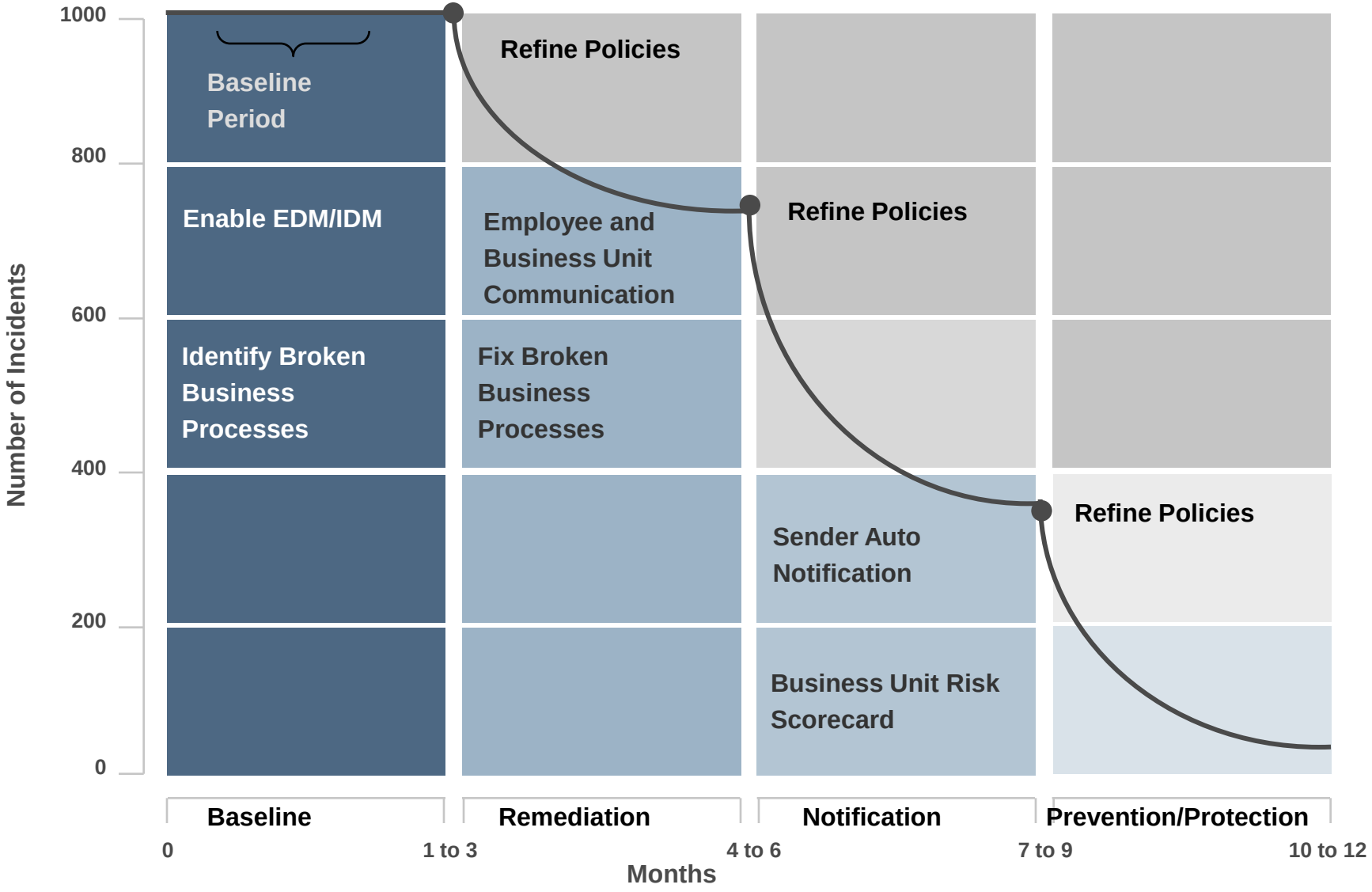
Keys to Success – People & Process

- Engage business units and data owners to define data protection priorities
- Define and gain consensus on project goals and success metrics
- Determine awareness and communication program for DLP
- Focus initial deployment on 3-5 key policies
  - Storage: target high-access, high-volume repositories
  - Endpoint: target users with access to highly-sensitive data and at-risk employees (high turnover)
  - Network: target high-volume and high-risk protocols (SMTP, HTTP, FTP) and high-access, high-volume repositories
- Train team prior to implementation
- Design policies and remediation based on current processes
- Configure policies and incident response workflow based on team capacity
- Regularly report results to key stakeholders and executives

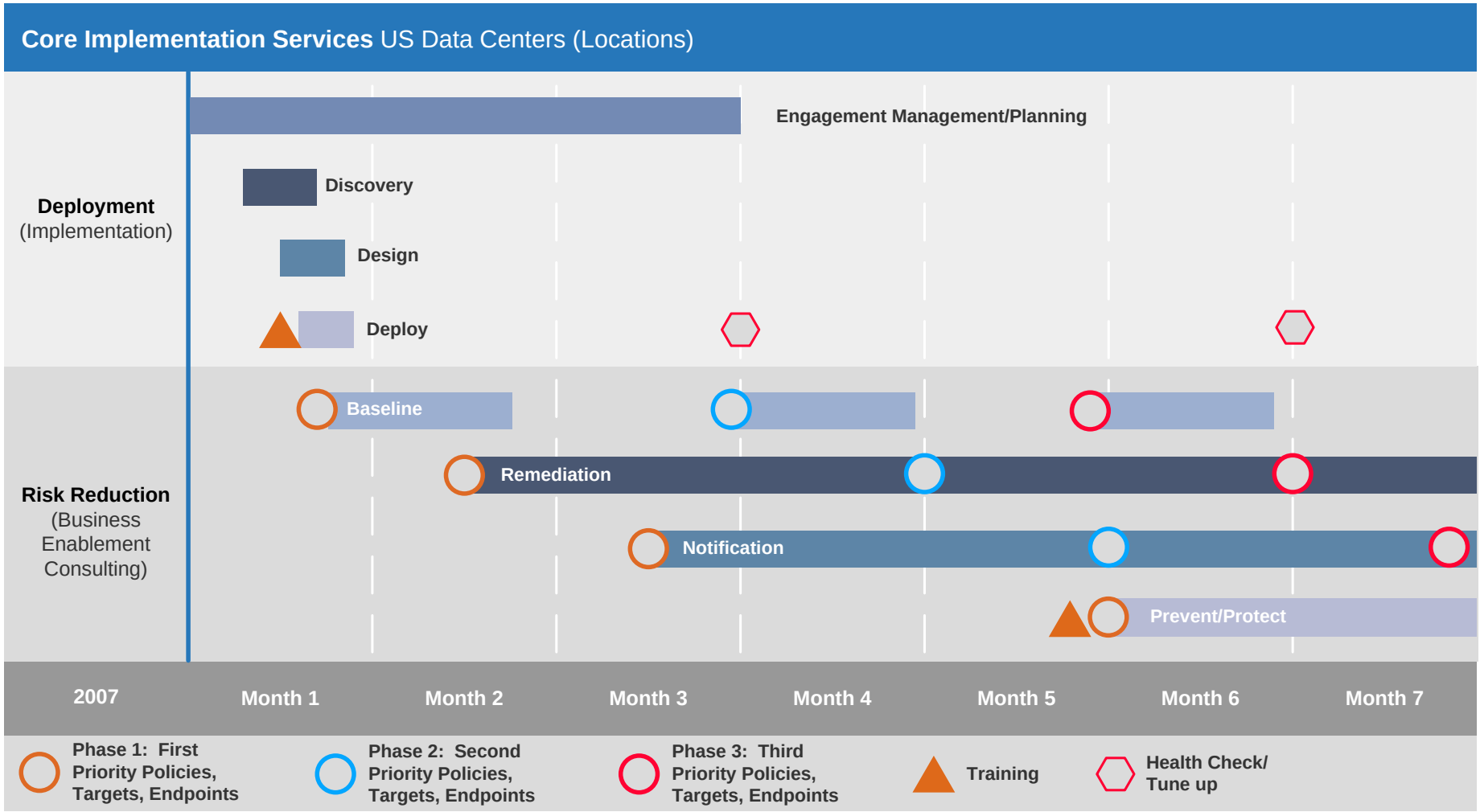
Target Most Sensitive Data First



Manage Risk Reduction Over Time



DLP Implementation Timeline



DLP Deployment Requirements

	Enforce	Network Monitor	Endpoint Server
NICs:	*Communicate with Network Monitor/Discover/Endpoint* 1 Copper or Fiber 1Gb/100MB Ethernet	*Communicate with Enforce:* 1 Copper or Fiber 1Gb/100MB Ethernet 1 Endace model 4.5 G2 for Copper or Fiber	*Communicate with Enforce:* 1 Copper or Fiber 1Gb/100MB Ethernet
Disk Space:	*Recommended:* 500 GB Ultra-fast SCSI *Recommended If Oracle DB on server:* RAID 0+1	*Recommended:* 100 GB Ultra-fast SCSI	
OS:	Microsoft Windows 2003 Enterprise Edition (32-bit) OR Red Hat Enterprise Linux 5		
Processor:	*Recommended:* (2) 3.x GHz Dual Core CPUs		
Memory:	*Recommended:* 8 GB RAM		

Thank You!