Understanding and Selecting a DLP Solution

Rich Mogull
Securosis

No Wonder We're Confused

- Data Loss Prevention
- Data Leak Prevention
- Data Loss Protection
- Information Leak Prevention
- Extrusion Prevention
- Content Monitoring and Filtering
- Content Monitoring and Protection

"Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use through deep content analysis."

-Rich Mogull

Feature vs. Product

Feature	Product
Includes some of the detection and enforcement of DLP products, but are not dedicated to the task of protecting content and data.	Centralized management, policy creation, and enforcement workflow dedicated to the monitoring and protection of content and data.

Financial Services Uses

- **Protect customer PII from leakage**
  - Support PCI, GLBA, and breach notification compliance
- **Identify locations of PII/ account information in storage**
- **Automatically encrypt outbound customer communications with account information**
- **Scan employee laptops for unprotected account information**
- **Stop transfer of financial information to portable storage**

In Motion

At Rest

In Use

Content Awareness

- **Context scanning is different from content scanning**
  - You want both
- **Understand the different between simple metadata and business context**

Rules

- **Regular expressions, keywords, and other basic pattern matching techniques best suited for basic structured data.**

```
^(?:(?<Visa>4\d{3})|(?<Mastercard>5[1-5]\d{2})|(?<Discover>6011)|(?<DinersClub>(?:3[68]\d{2})|(?:30[0-5]\d))|(?<AmericanExpress>3[47]\d{2}))([ -]?)(?(DinersClub)(?:\d{6}\1\d{4})|(?(AmericanExpress)(?:\d{6}\1\d{5})|(?:\d{4}\1\d{4}\1\d{4})))$
```

Credit Card Numbers

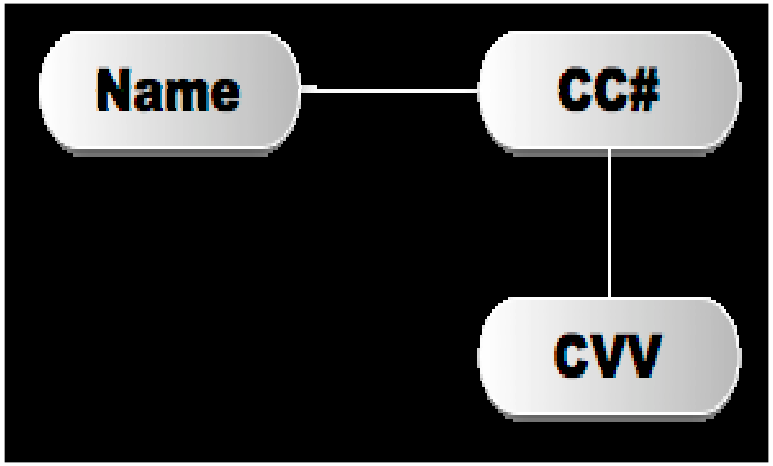
```
^(?!000)(?!666)(?<SSN3>[0-6]\d{2}|7(?:[0-6]\d|7[012]))([-]?)(?!00)(?<SSN2>\d\d)\1(?!0000)(?<SSN4>\d{4})$
```

Social Security Numbers

Regular expressions from: **Jerry Schmersahl at http://regexlib.com/DisplayPatterns.aspx?cattabindex=3&categoryId=4**

Database Fingerprinting

- **Searching for exact matches to data loaded from a database, which can include multiple-field combinations.**



Exact File Matching

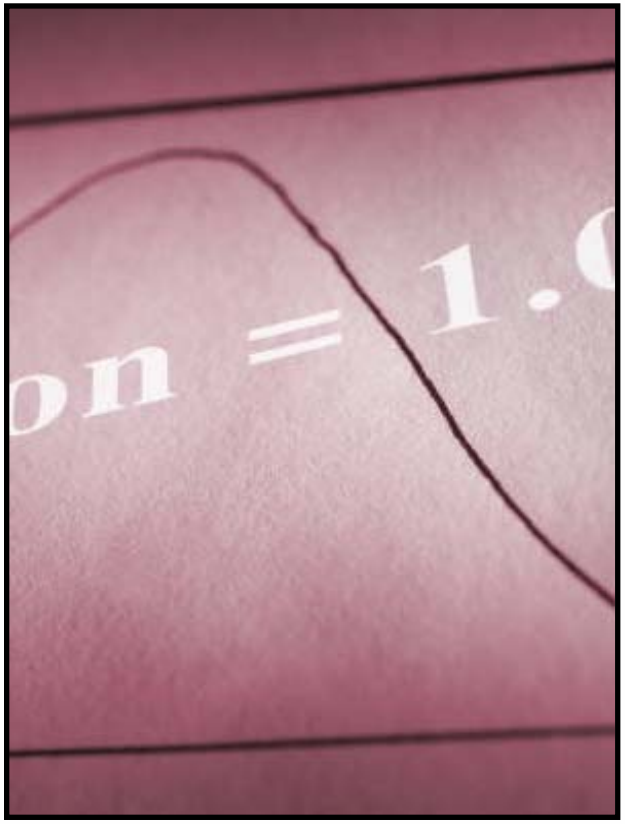
Binary Hash

Partial Document Matching

- **Cyclical hashing, sometimes with additional linguistic analysis**
- **Eliminate whitespace, hash a range, offset, hash again**

Statistical Analysis

- **Bayesian, machine learning, and other statistical techniques that analyze a corpus of content to recognize other content that may be similar.**



Conceptual/Lexicon

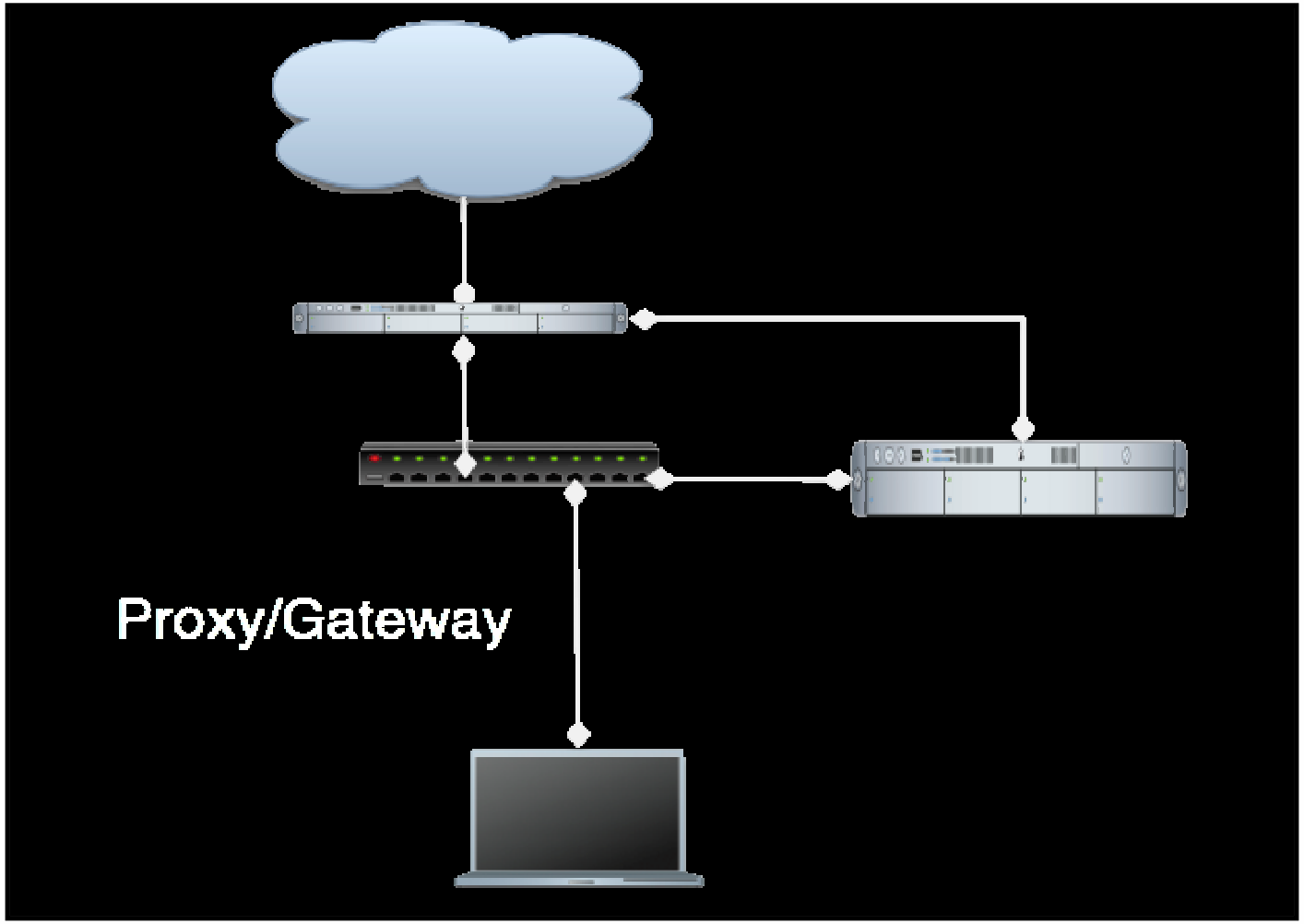
- **A combination of dictionaries, rules, and other analysis to protect loosely defined ideas.**

Categories

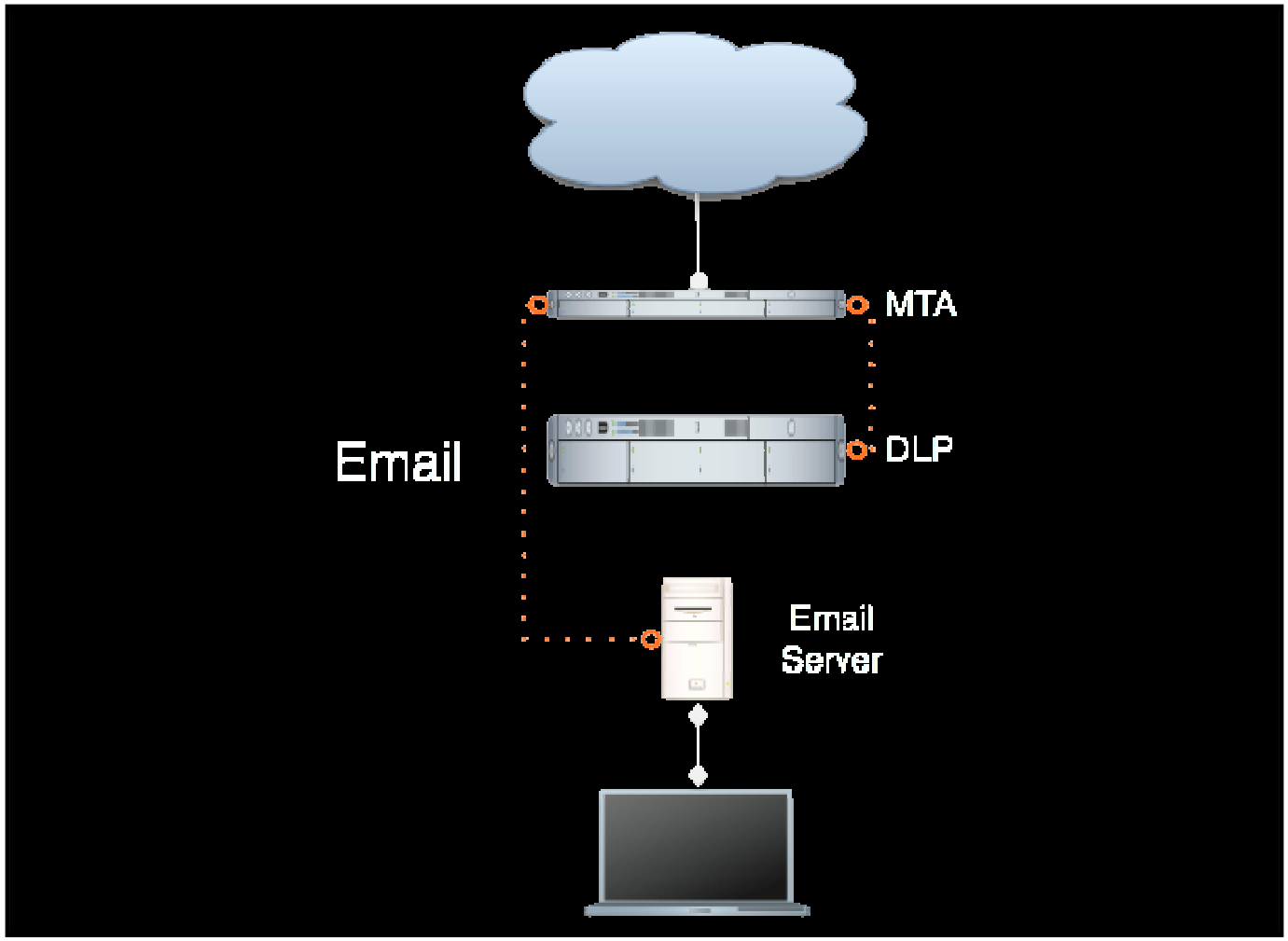
- **Pre-built categories with rules and dictionaries for common types of sensitive data.**

Technical Architecture

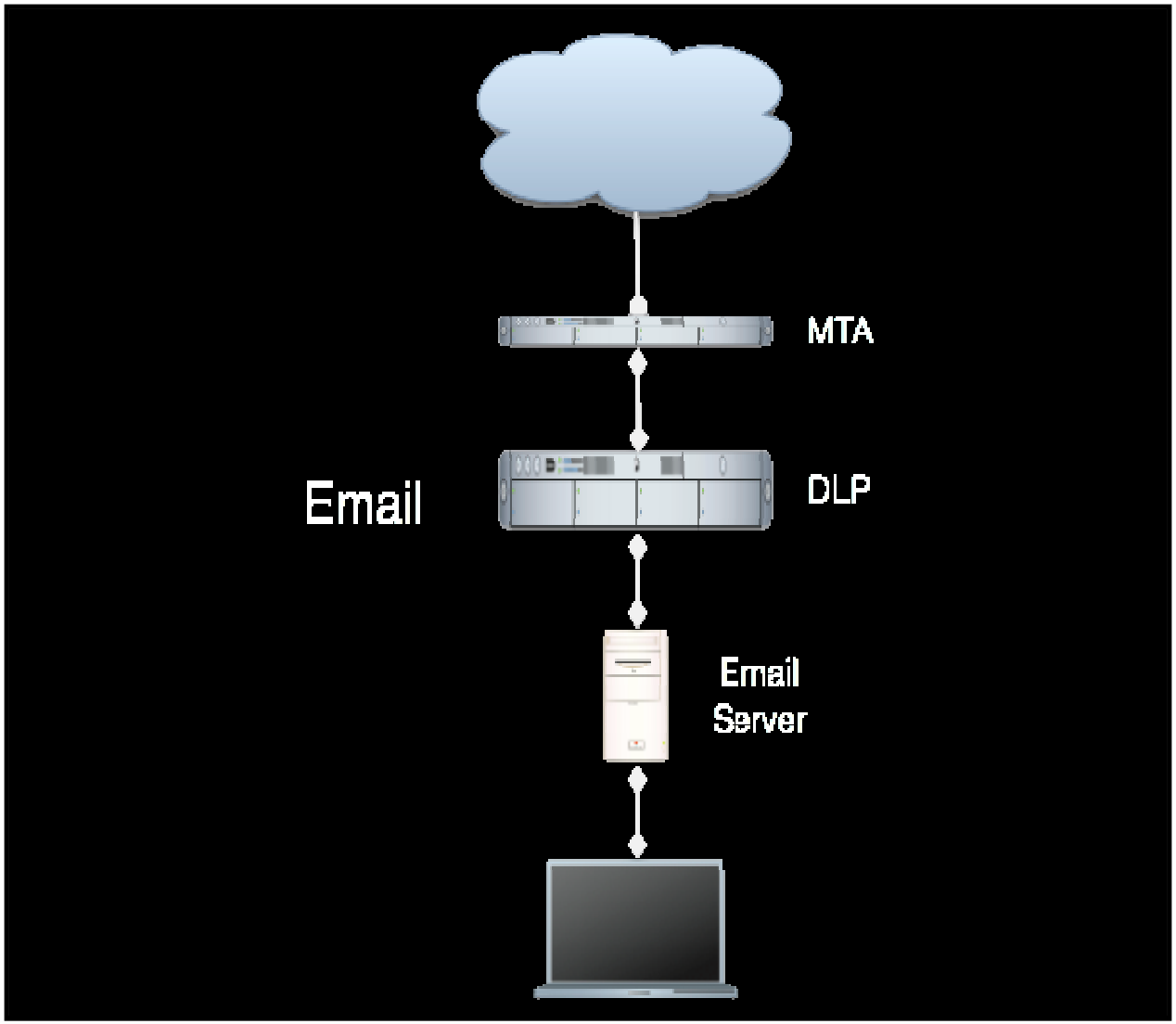
Data In Motion



Data In Motion



Data In Motion

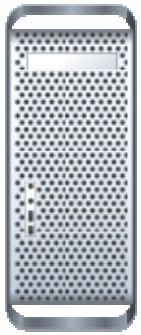


Blocking

Bridge, Proxy, or Inject

Content Discovery

Endpoint



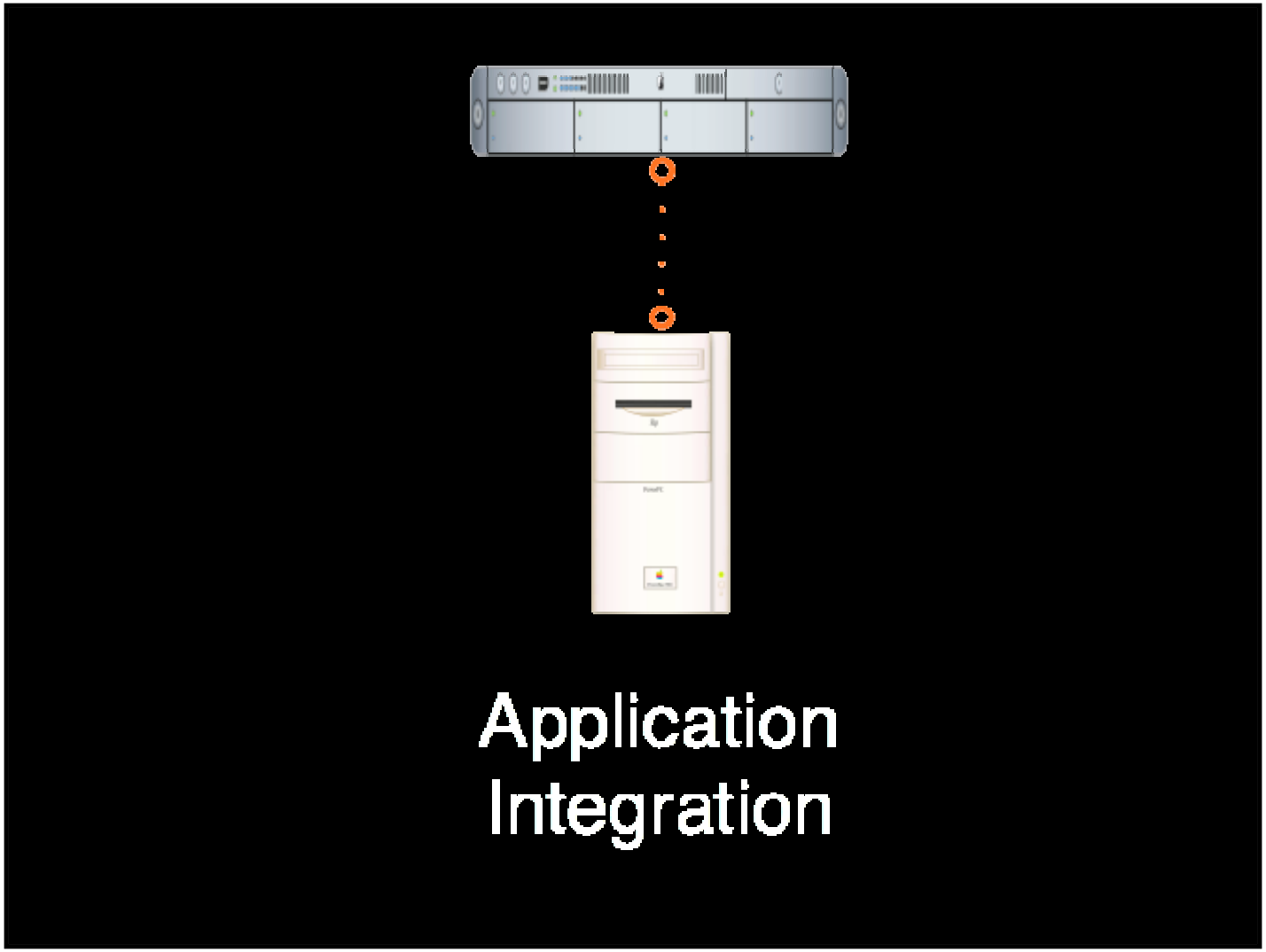
Storage

Application/Server

Content Discovery

Content Discovery

Content Discovery



Enforcement Actions

- Alert/Report
- Warn the User
- Quarantine- Move
- Quarantine- Encrypt
- Quarantine- Access Controls
- Remove/Delete

Endpoint Priorities

- **Portable Storage**
- **Unmanaged Networks**
- **Data in Use**

Endpoint Layers

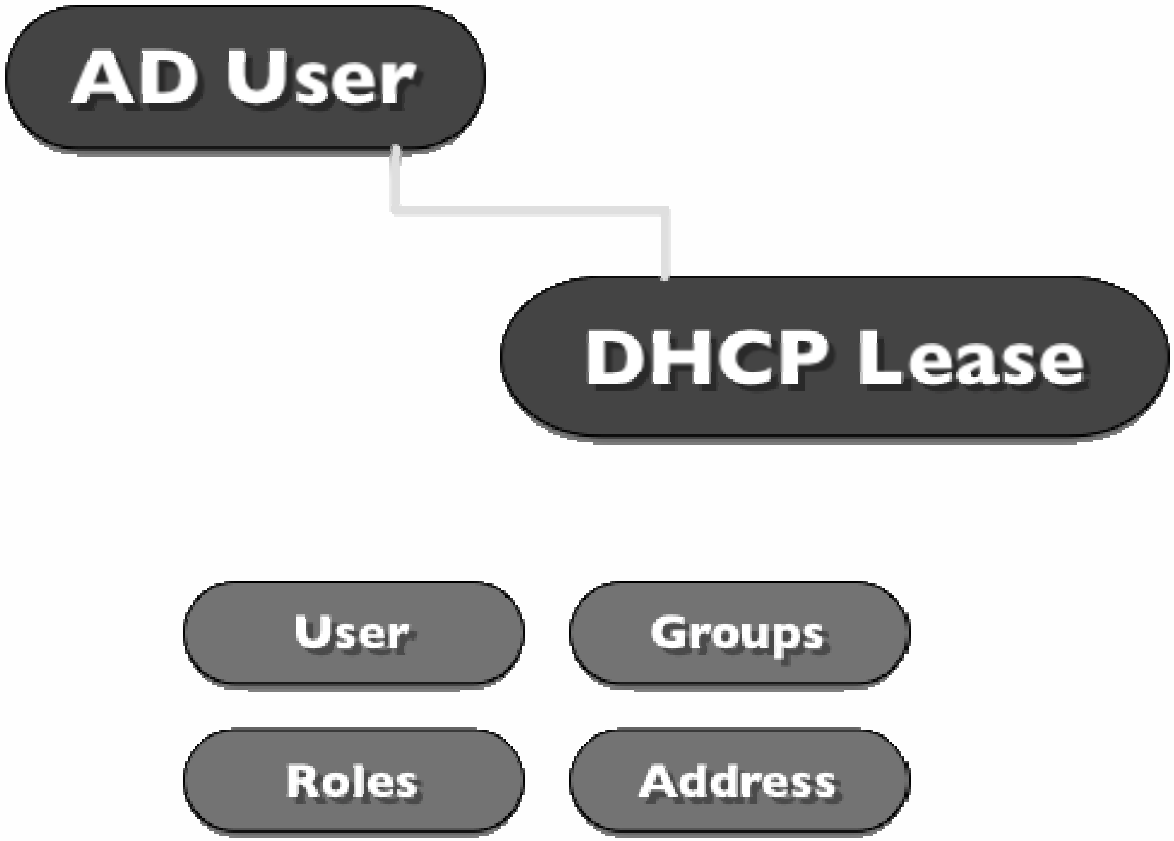
GUI/Kernel

File

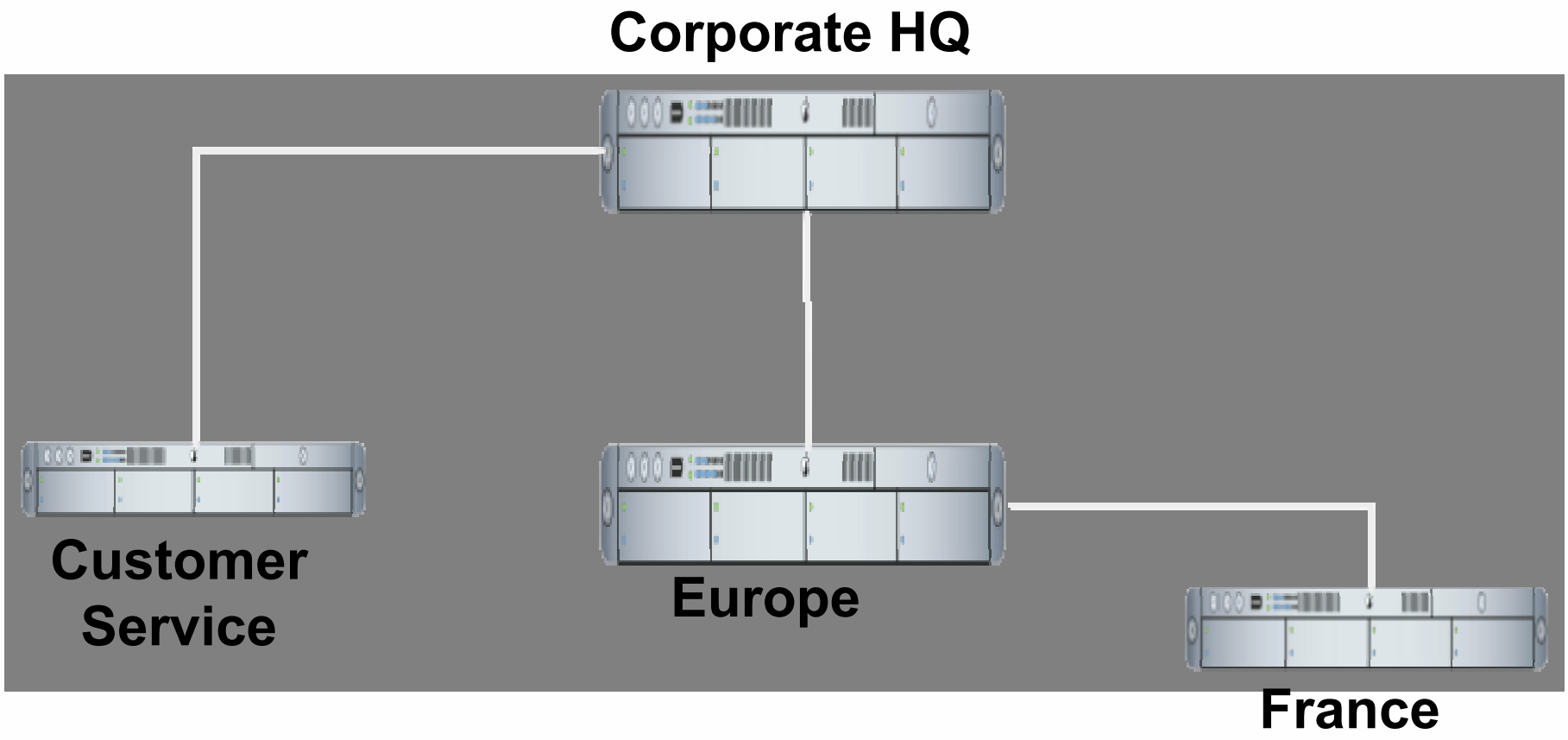
Network

Central Management

Directory Integration



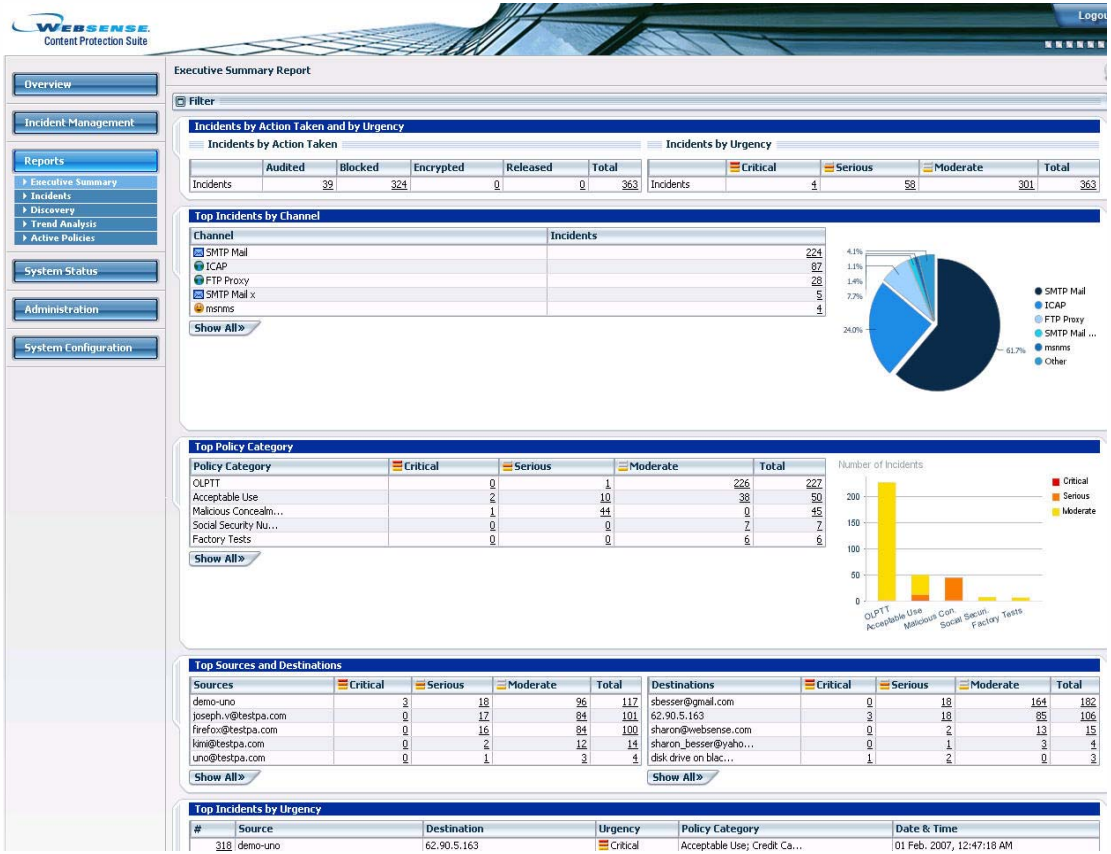
Hierarchical Management



Role Based Administration

- System Administrator
- Policy Creator
- Incident Handler
- Investigator
- Business Unit Manager
- Supervisor

Dashboard


WEBSENSE
Content Protection Suite
Logou
Overview
Incident Management
Reports
Executive Summary
Incidents
Discovery
Trend Analysis
Active Policies
System Status
Administration
System Configuration
Executive Summary Report
Filter
Incidents by Action Taken and by Urgency
Incidents by Action Taken
Audited Blocked Encrypted Released Total
Incidents 39 324 0 0 363
Incidents by Urgency
Critical Serious Moderate Total
Incidents 4 58 301 363
Top Incidents by Channel
Channel Incidents
SMTP Mail 224
ICAP 87
FTP Proxy 28
SMTP Mail x 5
msnms 4
Show All»
4.1%
1.1%
1.4%
7.7%
24.0%
61.7%
SMTP Mail
ICAP
FTP Proxy
SMTP Mail ...
msnms
Other
Top Policy Category
Policy Category Critical Serious Moderate Total
OLPTT 0 1 226 227
Acceptable Use 2 10 38 50
Malicious Concealm... 1 44 0 45
Social Security Nu... 0 0 7 7
Factory Tests 0 0 6 6
Show All»
Number of Incidents
Critical
Serious
Moderate
200
150
100
50
0
OLPTT
Acceptable Use
Malicious Con
Social Secun
Factory Tests
Top Sources and Destinations
Sources Critical Serious Moderate Total
demo-uno 3 18 96 117
joseph.v@testpa.com 0 17 84 101
firefox@testpa.com 0 16 84 100
kimi@testpa.com 0 2 12 14
uno@testpa.com 0 1 3 4
Show All»
Destinations Critical Serious Moderate Total
sbesser@gmail.com 0 18 164 182
62.90.5.163 3 18 85 106
sharon@websense.com 0 2 13 15
sharon_besser@yaho... 0 1 3 4
disk drive on blac... 1 2 0 3
Show All»
Top Incidents by Urgency
Source Destination Urgency Policy Category Date & Time
318 demo-uno 62.90.5.163 Critical Acceptable Use; Credit Ca... 01 Feb. 2007, 12:47:18 AM

VERICEPT

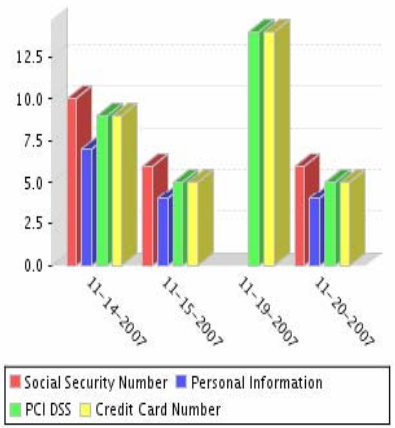
Administrator Logout | Preferences | Help

Home Reports Search Categories Policies Workflow Administration Help

Reports: Homepage

Filters: Categories | Date Range | Filter

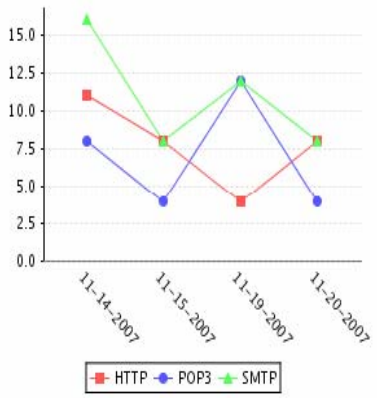
Category - Last 7 days (by day)



Top Hosts - Last 7 days (by day)

Host	Count
10.7.1.2	60
10.7.1.11	49
10.7.1.12	44
us.f638.mail.yahoo.com	27
us.f636.mail.yahoo.com	4

Protocol - Last 7 days (by day)



Showing first 10 results. Show All

		Date/Time	Category	State	Match Count	To Host	Protocol
		2007-11-05 17:51:49.0	Personal Information	NEW	53	10.7.1.2	smtp
		2007-11-05 17:51:49.0	Personal Information	NEW	53	us.f638.mail.yahoo.com	www-post
		2007-11-05 17:51:49.0	Personal Information	NEW	42	10.7.1.11	pop
		2007-11-05 17:51:49.0	Personal Information	NEW	53	10.7.1.2	smtp

System Administration

- Performance Monitoring
- Backup and Restore
- Import and Export
- Load Balancing/ Clustering
- User Management
- Database Management
- Archiving
- Endpoint Agent Management
- Storage Scanning/Agent Management
- Internal Groups

Policy Creation

Content + Channel + Users + Handlers + Severity + Action

Users + Handlers + Severity + Action

Channel

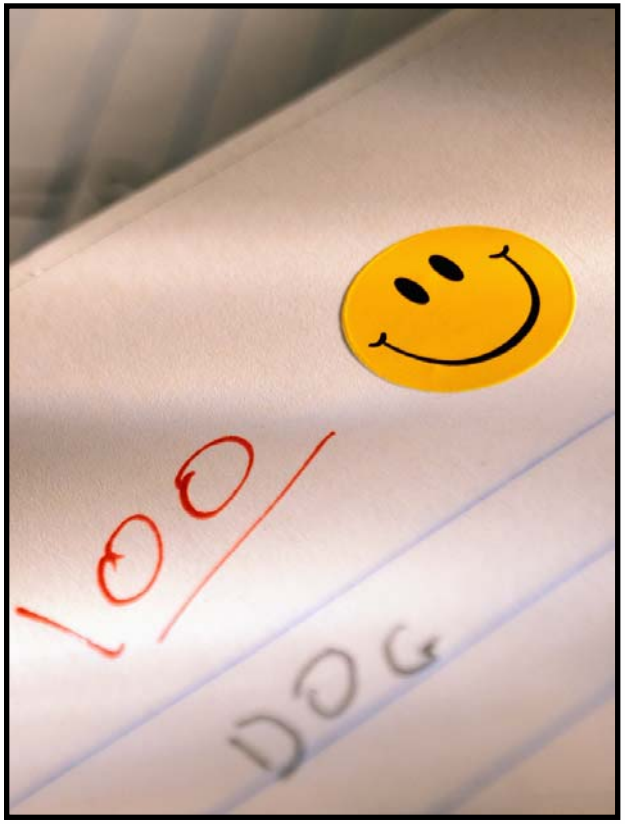
Location

Endpoint

Non-Technical Wizards

Test Mode

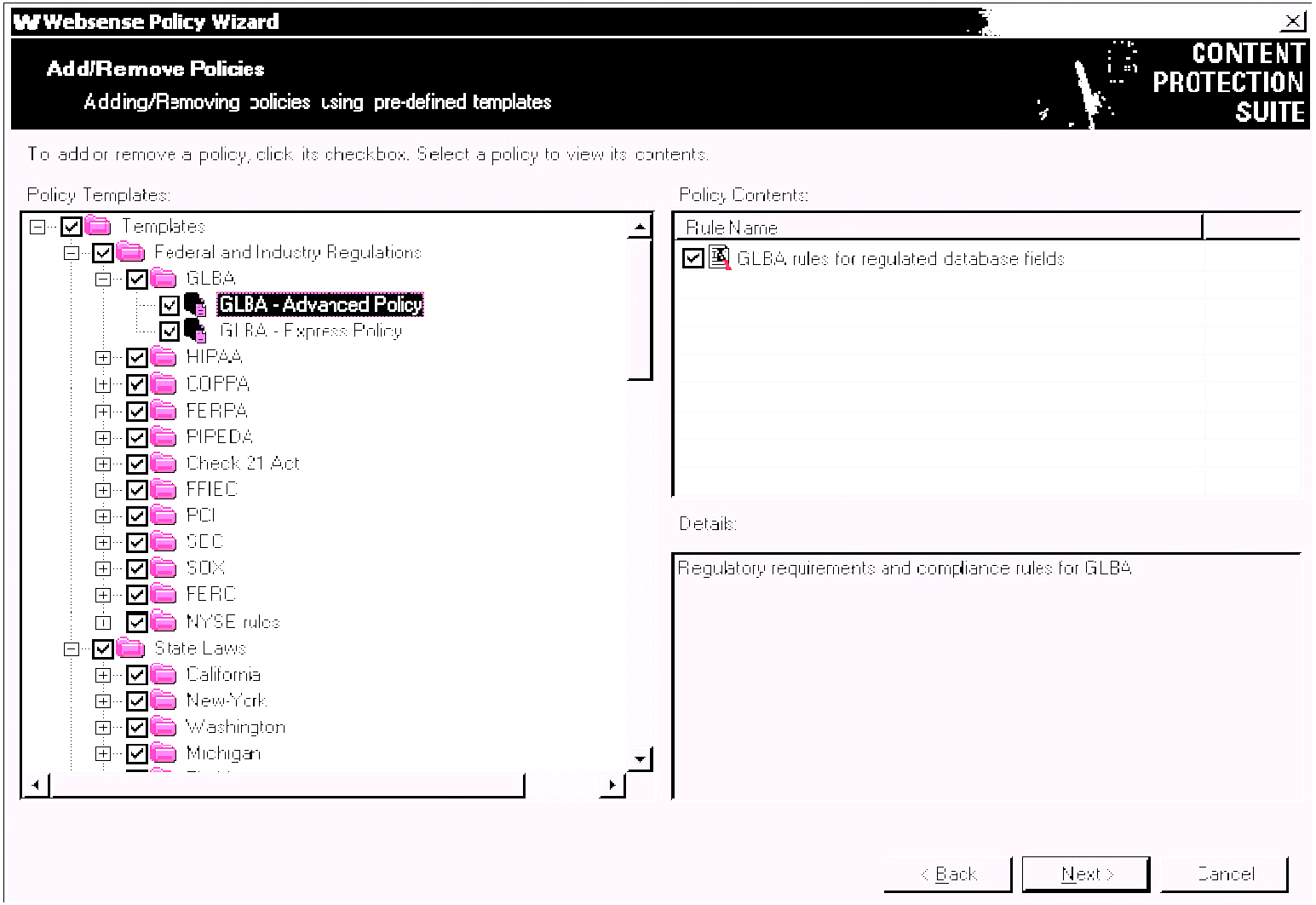
- **Evaluate policies in monitoring only mode separate from production incident queue to support tuning.**



Policies Are Data

- **Hash, encrypt, and restrict policies**
- **Business unit policies may need to be restricted from handlers**

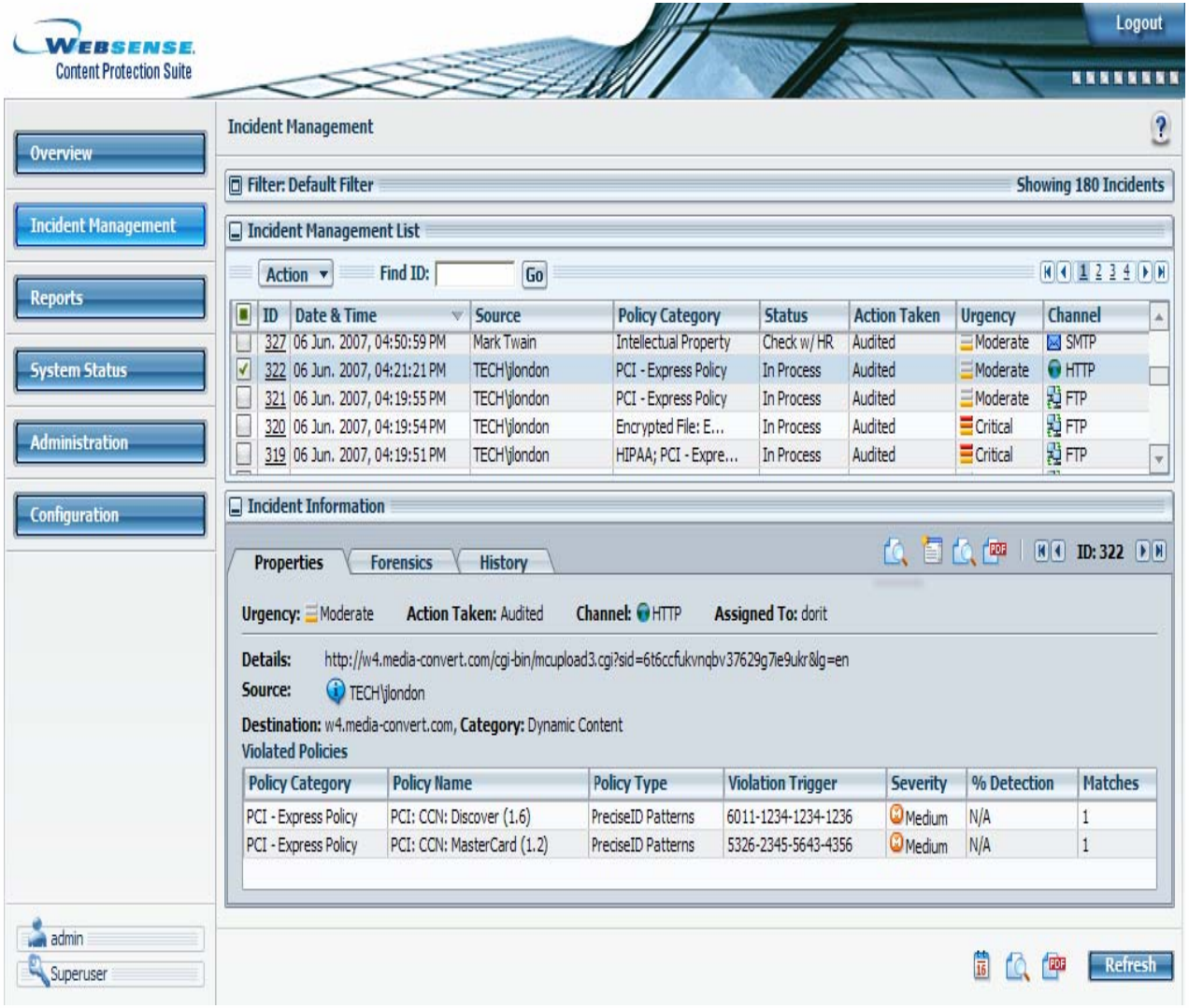
Websense


Websense Policy Wizard
Add/Remove Policies
Adding/Removing policies using pre-defined templates
CONTENT PROTECTION SUITE
To add or remove a policy, click its checkbox. Select a policy to view its contents.
Policy Templates:
Templates
Federal and Industry Regulations
GLBA
GLBA - Advanced Policy
GLBA - Express Policy
HIPAA
COPPA
FERPA
PIPEDA
Check 21 Act
FFIEC
PCI
SEC
SOX
FERC
NYSE rules
State Laws
California
New York
Washington
Michigan
Policy Contents:
Rule Name
GLBA rules for regulated database fields
Details:
Regulatory requirements and compliance rules for GLBA
< Back
Next >
Cancel

Incident Workflow

Incident Queue

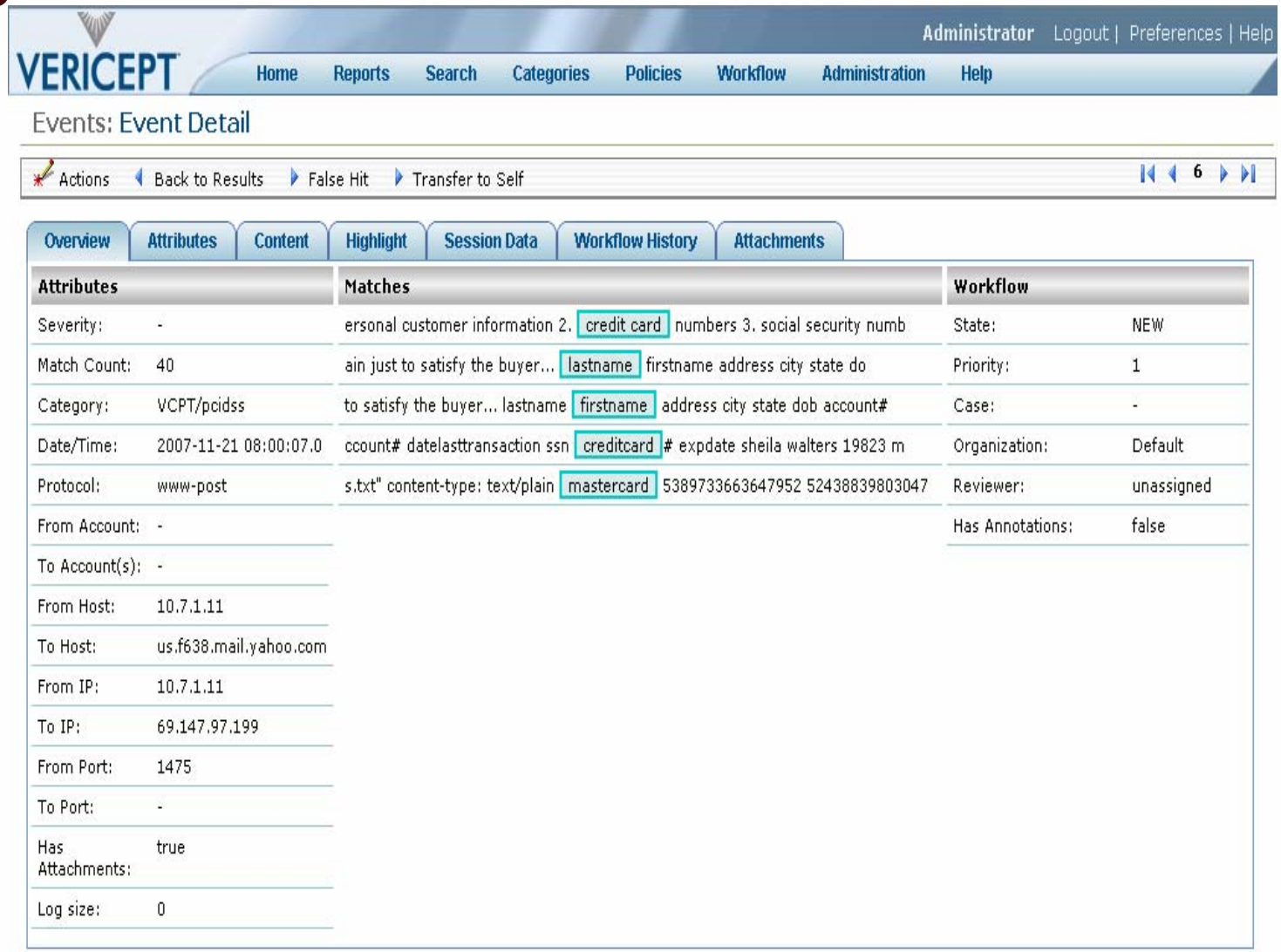
ID	Time	Policy	Channel	Severity	User	Action	Status
1138	1625	PII	Email	1.2 M	rmogull	Blocked	Open
1139	1632	HIPAA	IM	2	jsmith	Notified	Assigned
1140	1702	PII	HTTP	1	192.168.0.213	None	Closed
1141	1712	R&D/Product X	USB	4	bgates	Notified	Assigned
1142	1730	Financials	Storage	4	192.168.1.94	Encrypt	Escalated
1143	12/1/08	Source Code	Cut/Paste	12	sjobs	Confirm	Open

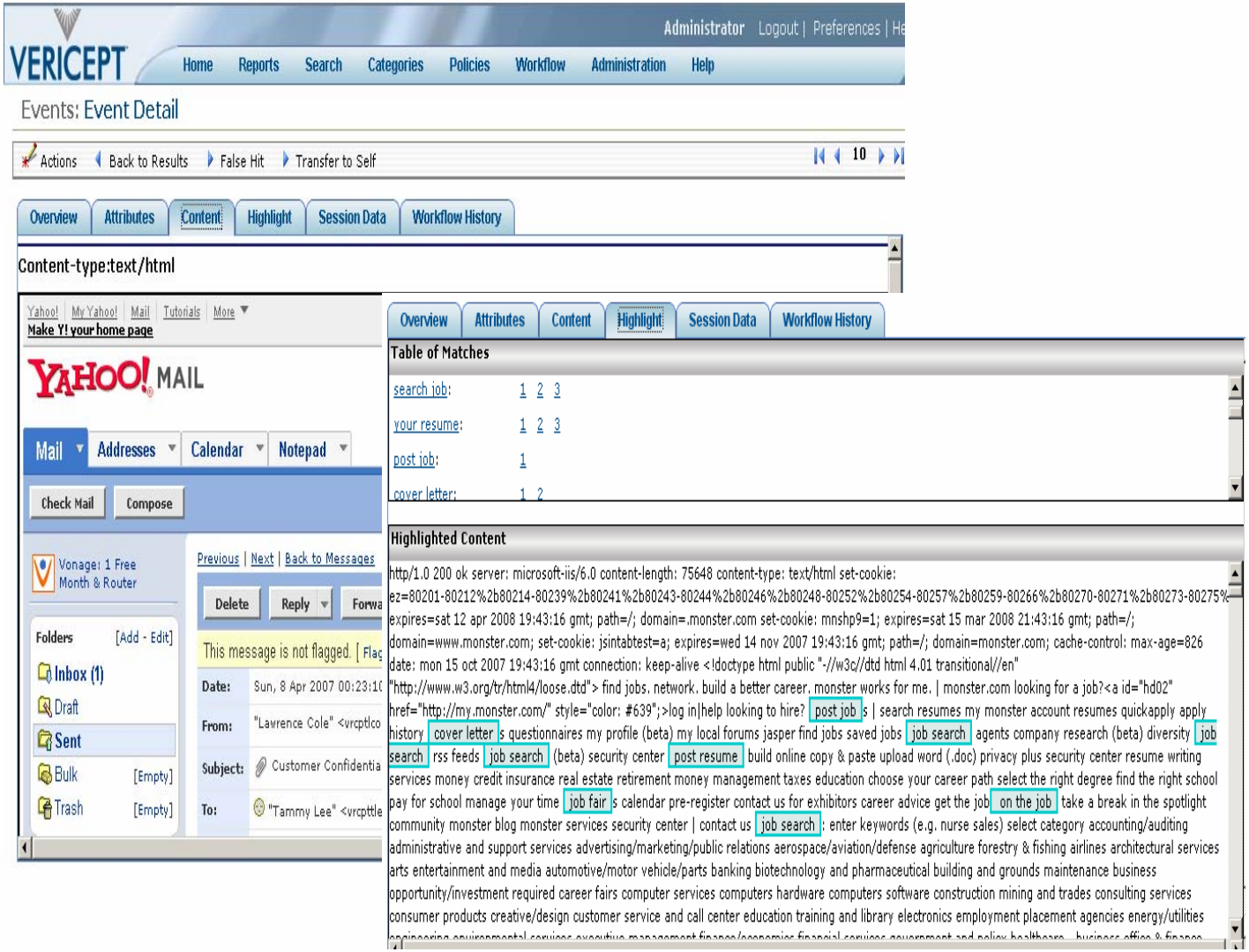

WEBSENSE.
Content Protection Suite
Logout
Overview
Incident Management
Reports
System Status
Administration
Configuration
admin
Superuser
Incident Management
Filter: Default Filter
Showing 180 Incidents
Incident Management List
Action
Find ID:
Go
1 2 3 4
ID | Date & Time | Source | Policy Category | Status | Action Taken | Urgency | Channel
327 | 06 Jun. 2007, 04:50:59 PM | Mark Twain | Intellectual Property | Check w/ HR | Audited | Moderate | SMTP
322 | 06 Jun. 2007, 04:21:21 PM | TECH\jlondon | PCI - Express Policy | In Process | Audited | Moderate | HTTP
321 | 06 Jun. 2007, 04:19:55 PM | TECH\jlondon | PCI - Express Policy | In Process | Audited | Moderate | FTP
320 | 06 Jun. 2007, 04:19:54 PM | TECH\jlondon | Encrypted File: E... | In Process | Audited | Critical | FTP
319 | 06 Jun. 2007, 04:19:51 PM | TECH\jlondon | HIPAA; PCI - Expre... | In Process | Audited | Critical | FTP
Incident Information
Properties
Forensics
History
ID: 322
Urgency: Moderate
Action Taken: Audited
Channel: HTTP
Assigned To: dorit
Details: http://w4.media-convert.com/cgi-bin/mcupload3.cgi?sid=6t6ccfukvnqbv37629g7ie9ukr&lg=en
Source: TECH\jlondon
Destination: w4.media-convert.com, Category: Dynamic Content
Violated Policies
Policy Category | Policy Name | Policy Type | Violation Trigger | Severity | % Detection | Matches
PCI - Express Policy | PCI: CCN: Discover (1.6) | PreciseID Patterns | 6011-1234-1234-1236 | Medium | N/A | 1
PCI - Express Policy | PCI: CCN: MasterCard (1.2) | PreciseID Patterns | 5326-2345-5643-4356 | Medium | N/A | 1
Refresh

Technical vs. Business

User interfaces and workflow should account for technical and non-technical users

Single Incident View




VERICEPT
Administrator Logout | Preferences | He
Home Reports Search Categories Policies Workflow Administration Help
Events: Event Detail
Actions Back to Results False Hit Transfer to Self
10
Overview Attributes Content Highlight Session Data Workflow History
Content-type:text/html
Yahoo! My Yahoo! Mail Tutorials More
Make Y! your home page
YAHOO! MAIL
Mail Addresses Calendar Notepad
Check Mail Compose
Vonage: 1 Free Month & Router
Folders [Add - Edit]
Inbox (1)
Draft
Sent
Bulk [Empty]
Trash [Empty]
Previous | Next | Back to Messages
Delete Reply
This message is not flagged.
Date: Sun, 8 Apr 2007 00:23:1
From: "Lawrence Cole" <vrcptlco
Subject: Customer Confidentia
To: "Tammy Lee" <vrcpttle
Overview Attributes Content Highlight Session Data Workflow History
Table of Matches
search job: 1 2 3
your resume: 1 2 3
post job: 1
cover letter: 1 2
Highlighted Content
http/1.0 200 ok server: microsoft-iis/6.0 content-length: 75648 content-type: text/html set-cookie: ez=80201-80212%2b80214-80239%2b80241%2b80243-80244%2b80246%2b80248-80252%2b80254-80257%2b80259-80266%2b80270-80271%2b80273-80275% expires=sat 12 apr 2008 19:43:16 gmt; path=/; domain=.monster.com set-cookie: mnshp9=1; expires=sat 15 mar 2008 21:43:16 gmt; path=/; domain=www.monster.com; set-cookie: jsintabtest=a; expires=wed 14 nov 2007 19:43:16 gmt; path=/; domain=monster.com; cache-control: max-age=826 date: mon 15 oct 2007 19:43:16 gmt connection: keep-alive <!doctype html public "-//w3c//dtd html 4.01 transitional//en" "http://www.w3.org/tr/html4/loose.dtd"> find jobs. network. build a better career. monster works for me. | monster.com looking for a job?<a id="hd02" href="http://my.monster.com/" style="color: #639";>log in|help looking to hire? post job s | search resumes my monster account resumes quickapply apply history cover letter s questionnaires my profile (beta) my local forums jasper find jobs saved jobs job search agents company research (beta) diversity job search rss feeds job search (beta) security center post resume build online copy & paste upload word (.doc) privacy plus security center resume writing services money credit insurance real estate retirement money management taxes education choose your career path select the right degree find the right school pay for school manage your time job fair s calendar pre-register contact us for exhibitors career advice get the job on the job take a break in the spotlight community monster blog monster services security center | contact us job search : enter keywords (e.g. nurse sales) select category accounting/auditing administrative and support services advertising/marketing/public relations aerospace/aviation/defense agriculture forestry & fishing airlines architectural services arts entertainment and media automotive/motor vehicle/parts banking biotechnology and pharmaceutical building and grounds maintenance business opportunity/investment required career fairs computer services computers hardware computers software construction mining and trades consulting services consumer products creative/design customer service and call center education training and library electronics employment placement agencies energy/utilities

Other Workflow Features

- **Case management**
- **Incident correlation**
- **Hierarchical incident management**
- **Identity correlation**
- **Historical analysis**
- ***Reporting***

Top Five Features

- ✓ Content Analysis
- ✓ Technical Architecture
- ✓ Central Management
- ✓ Policy Creation
- ✓ Incident Workflow

The 3-Step Selection Process

- Define scope and set expectations
- Formalize requirements
- Evaluate and select

Form Selection Committee

- **The selection committee should represent key stakeholders from IT and business**

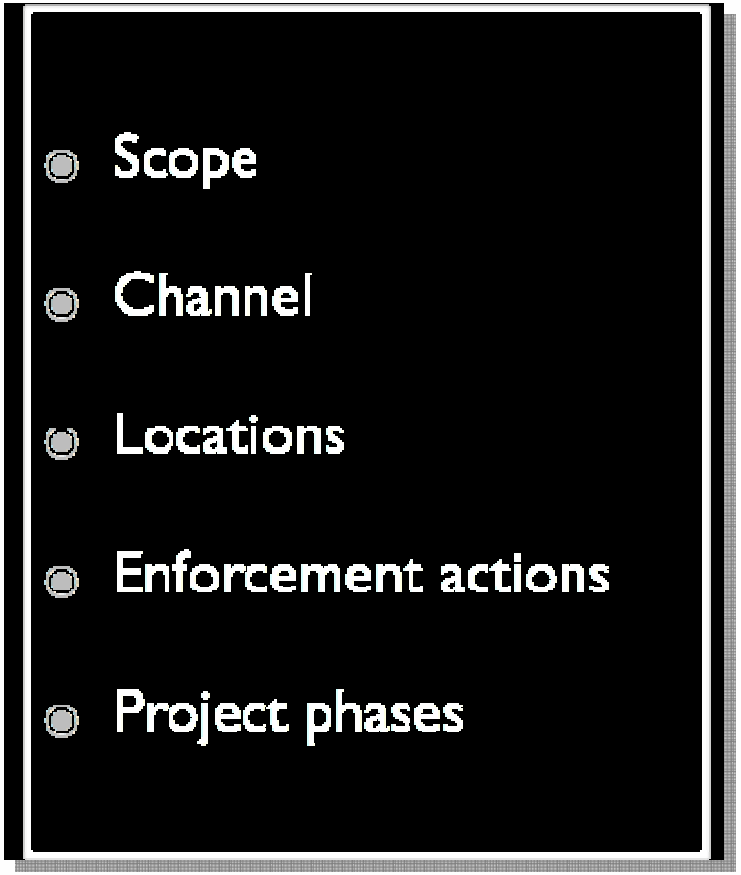
- IT/CIO
- IT Security
- Legal/Risk/Compliance
- Human Resources
- Key Business Units

Determine Protected Content Types

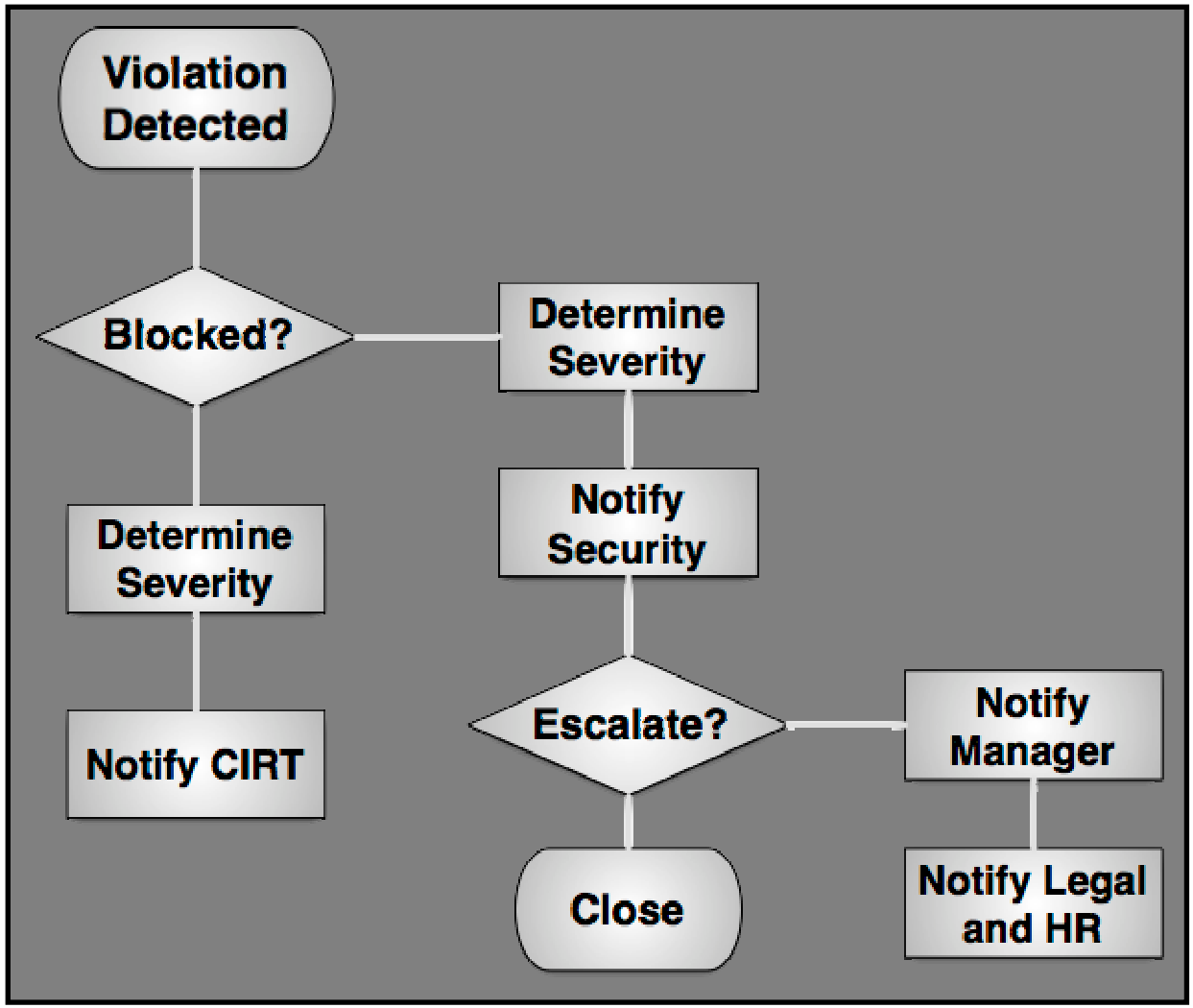
- PII/NPI
- Credit card numbers
- Social Security Numbers
- Healthcare data
- Engineering plans
- Chemical formulae
- Research documents
- Customer lists
- Corporate financials
- Source code
- Media files
- Legal documents

Define Protection Expectations

- **Determine where you want to protect the data, how you want to protect it, and set appropriate expectations.**



Outline Process Workflow



Formalize Requirements

- Issue a formal RFI
- Create a draft RFP
- Confirm requirements with selection committee

Evaluate and Select

1. Issue the RFI
2. Perform paper evaluation
3. Bring in 3 vendors for on-site presentations and risk assessment
4. Finalize RFP and issue to your short list
5. Assess responses and begin deep testing
6. Select, Negotiate, Buy

How To Test

- Compare products side by side
- Create a few representative policies
- View results in monitoring mode
- Test for false negatives
- Lab-test enforcement
- Lab-test integration

Financial Services Considerations

- **Focus on products with database fingerprinting**
  - Test carefully, and confirm exchange method meets your security requirements
- **Bad or test data can interfere with enforcement**
- **Don’t forget to use discovery**
- **FS is the primary market for these tools, so they tend to be well suited for your environment**

Key Testing Criteria

- Policy creation and content analysis.
- Email integration.
- Incident workflow- with real handlers.
- Directory integration.
- Storage integration on major platforms to test performance and compatibility for data-at-rest protection.
- Endpoint functionality on your standard image.
- Network performance- not just bandwidth, but any requirements to integrate the product on your network and tune it. Do you need to pre-filter traffic? Do you need to specify port and protocol combinations?
- Network gateway integration.

Navigating the Maze

- Understand your needs first, then start the selection process
- Focus on policy creation, workflow, and integration with your infrastructure
- Point solutions can solve part of the problem, but broad suites provide more flexibility
- Test products head to head

"Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use through deep content analysis."

-Rich Mogull

Rich Mogull
Securosis, L.L.C.

rmogull@securosis.com
http://securosis.com
AIM: securosis
Skype: rmogull