

McAfee Data Protection Solutions



Tamas Barna
System Engineer CISSP, Security+
Eastern Europe

September 30, 2010



The Solution: McAfee Data Protection

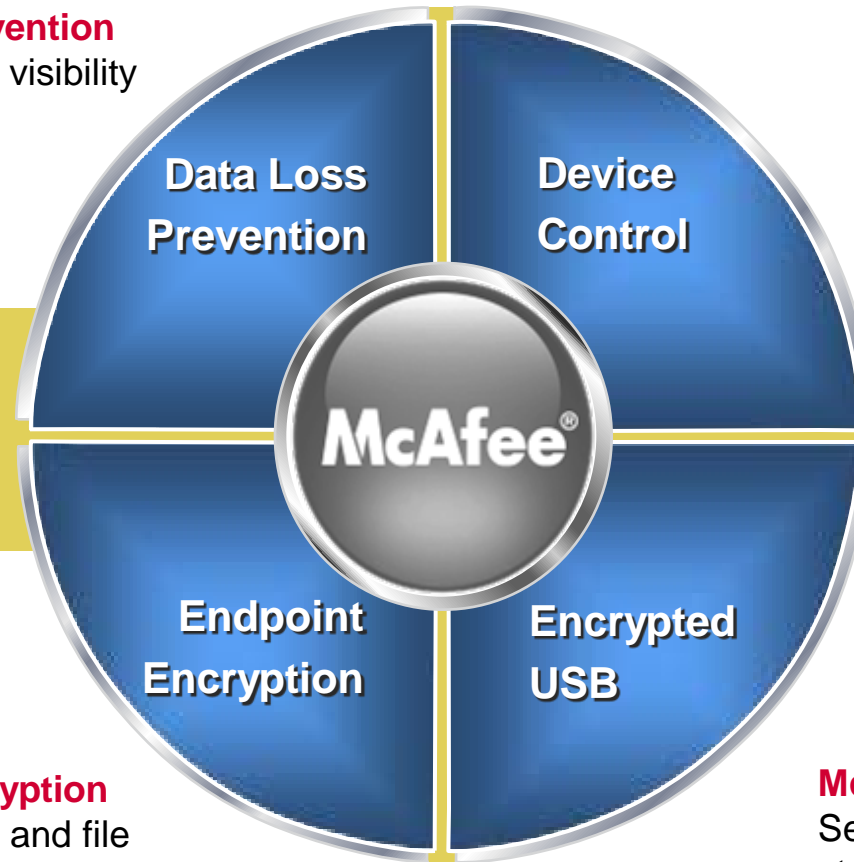


McAfee Data Loss Prevention

Full control and absolute visibility over user behavior

McAfee Device Control

Prevent unauthorized use of removable media devices



McAfee Total Protection™ for Data

Integrated technologies for a total data protection solution.

McAfee Endpoint Encryption

Full-disk, mobile device, and file and folder encryption coupled with strong authentication

McAfee Encrypted USB

Secure, portable external storage devices

Data types, risk areas, and DLP approach



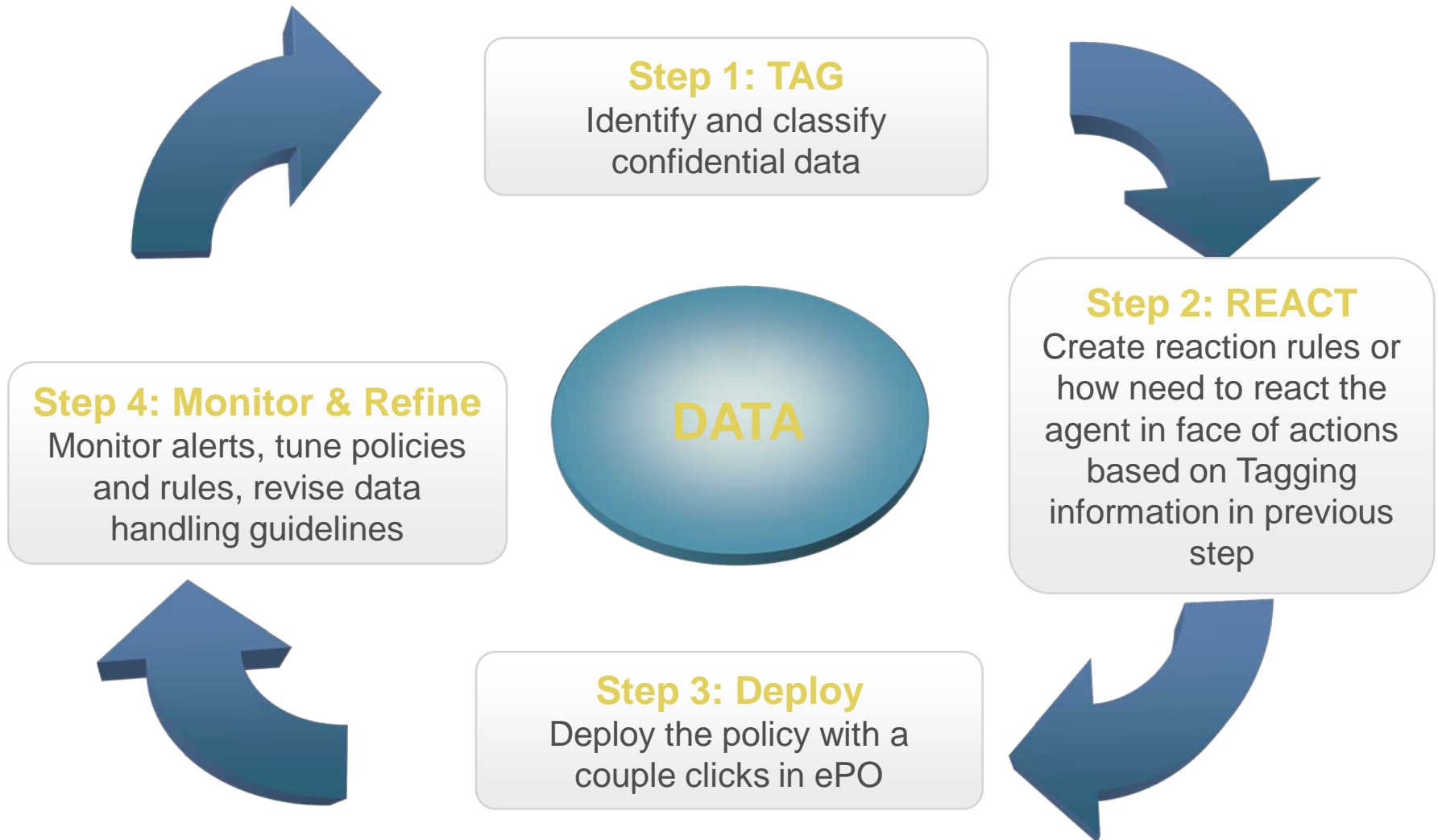
Data types

Risk areas

DLP approach



Data Loss Prevention Workflow



Tagging/Classification Methods

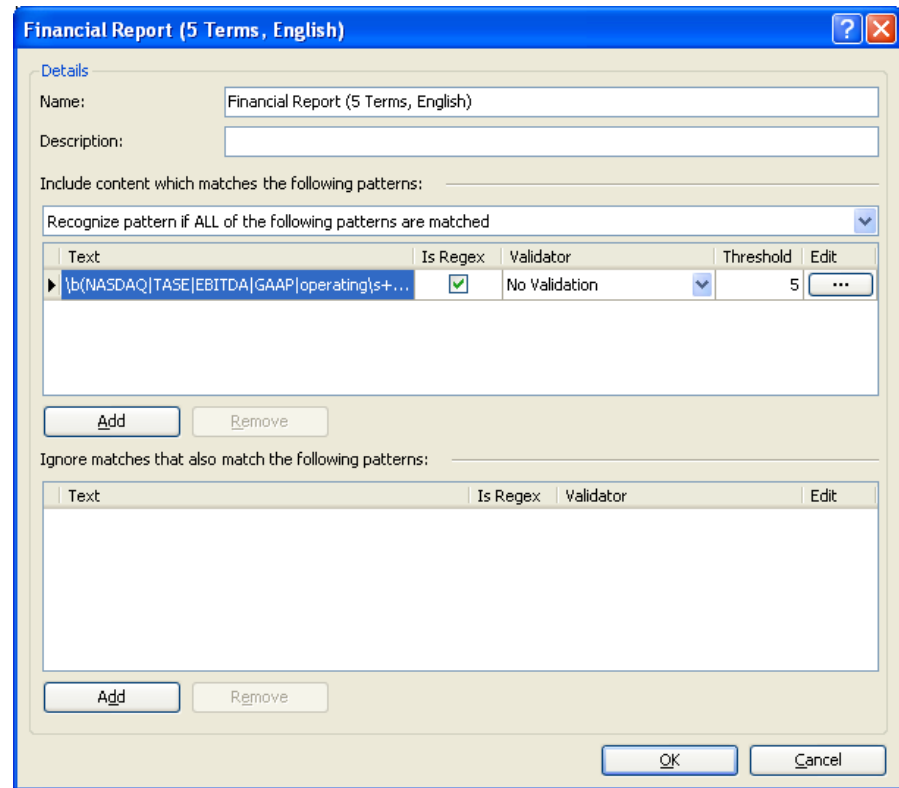


- Content Based
- Application Based
- Location Based
- Manual
- Tags are Named

Content Based Tagging/Classification



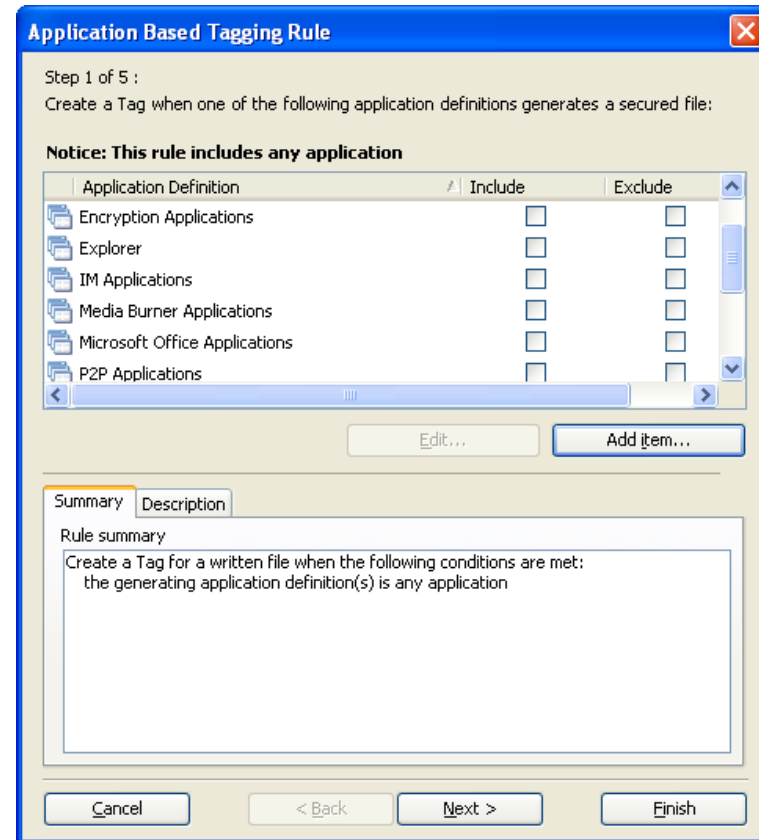
- Classify data according to:
 - Regular Expressions
e.g., Social Security number
Credit Card Number
 - Keywords
e.g., Financial terms
Patients discharge terms
- Thresholds may apply
 - e.g., Classify as sensitive if more than 10 credit card numbers appear in the document



Application Based Tagging



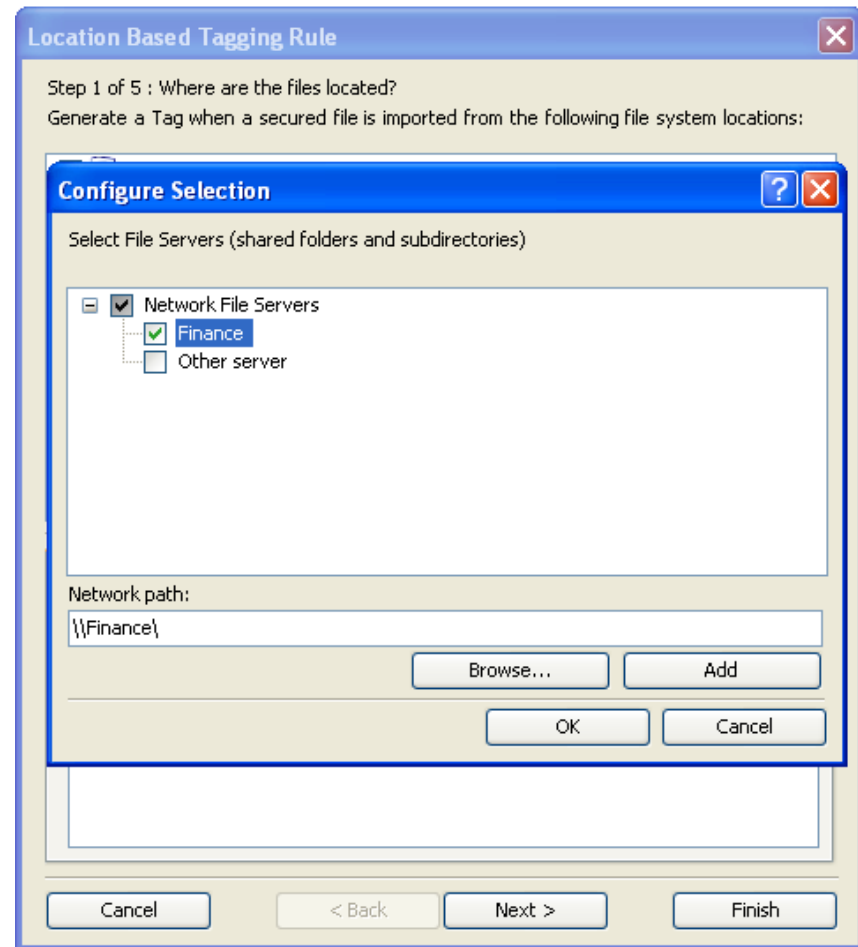
- Classify data according to application that created it
- Most common usage:
 - Files that are not text based e.g., Graphic design, Game authoring



Location Based Tagging



- Classify data according to its origin
- Tag files as they are being copied from a network share
 - e.g., tag all files tagged from the finance network share
- Tagging can be narrowed by:
 - File type
 - File extension
 - File contents (as in Content classification)



Reaction Rules



- Enforcing DLP policy
- Rules are per leakage channel
- Possible reactions:
 - Block
 - Monitor
 - Notify User
 - Store Evidence
- Can be applied to Online/Offline user state

Reaction Rules Types



- Email
 - Prevent tagged data from leaking through emails
 - Recipient granularity
- Removable Storage
 - Prevent tagged data from being copied to removable storage
 - e.g. USB keys, iPod, etc.
- Printing
 - Prevent tagged content from being printed
 - Printer granularity

- Web post
 - Prevent tagged content from being posted to websites
 - e.g. Block posting to non company websites
- Network Connections
 - Block network connectivity to applications which access tagged data
 - e.g. IM/P2P
 - May be used to restrict network usage to specific applications (e.g. IE)
- Network Share
 - Monitor tagged data which is copied to network shares

Additional Features

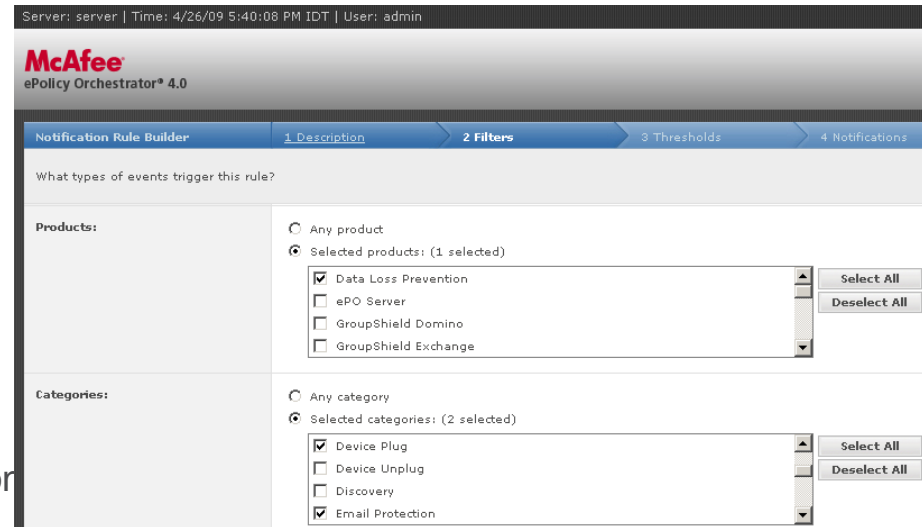


- Privileged users
 - Block reaction is converted to monitor only
- Bypass
 - Help desk generate bypass key for DLP override
 - Generated for limited time only

Technology Integrations - ePO



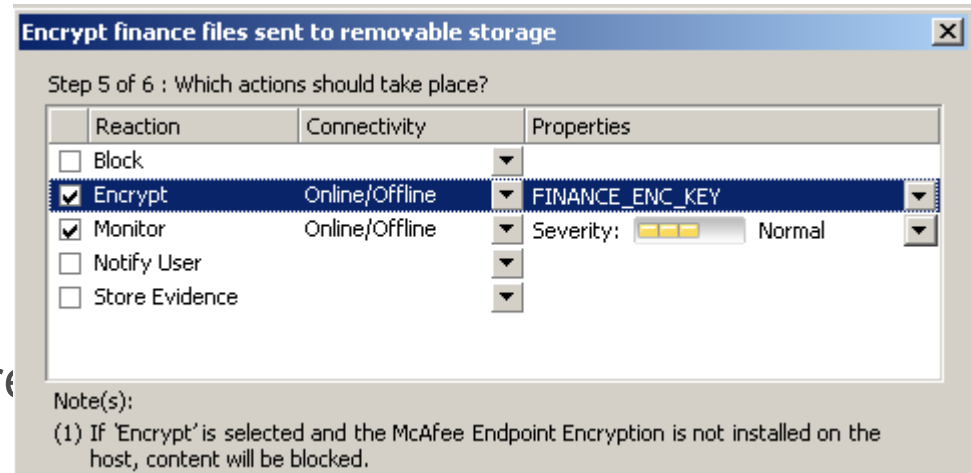
- Events reported via CMA
 - No Event Collector required
- ePO SQL used
 - No additional database
- ePO reporting
 - Using ePO reporting mechanism
 - No need for SQL reporting services installation
- ePO Notifications mechanism integration
 - Email, SNMP trap, external command



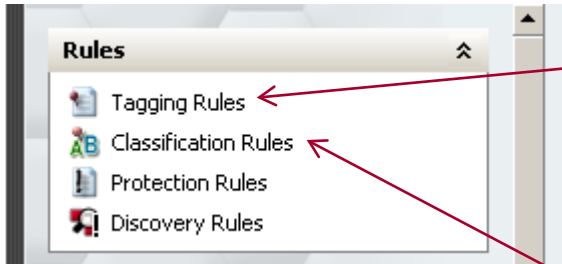
Technology Integrations – Endpoint Encryption



- Encrypt on demand
When copying to:
 - Removable storage
 - Network Shares
- Block unless encrypted
 - Email/Webpost
- McAfee Encrypted devices pre
- Requires McAfee Endpoint Encryption



Classification – New Terminology



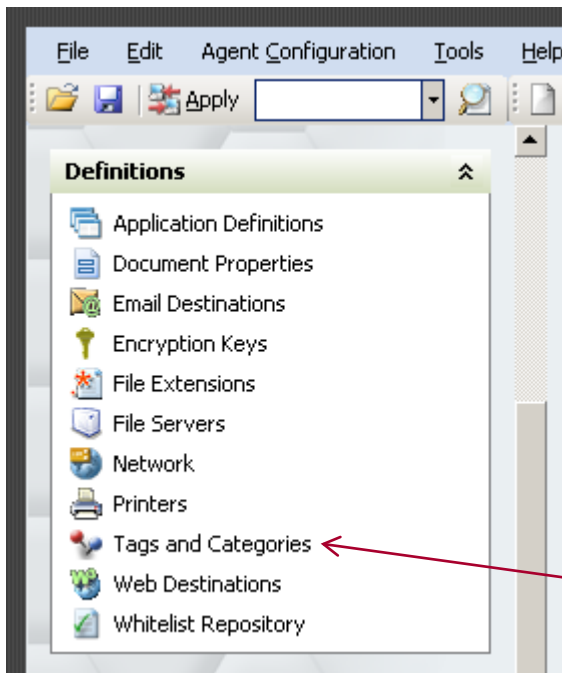
- Tagging Rules

- Creates physical tag on files (“Sticky Tag”)
- Location/Application based tagging

- Classification Rules

- Creates Categories
- Content based
 - Regular expression
 - Dictionaries
 - Registered Documents
- “Non- Sticky”

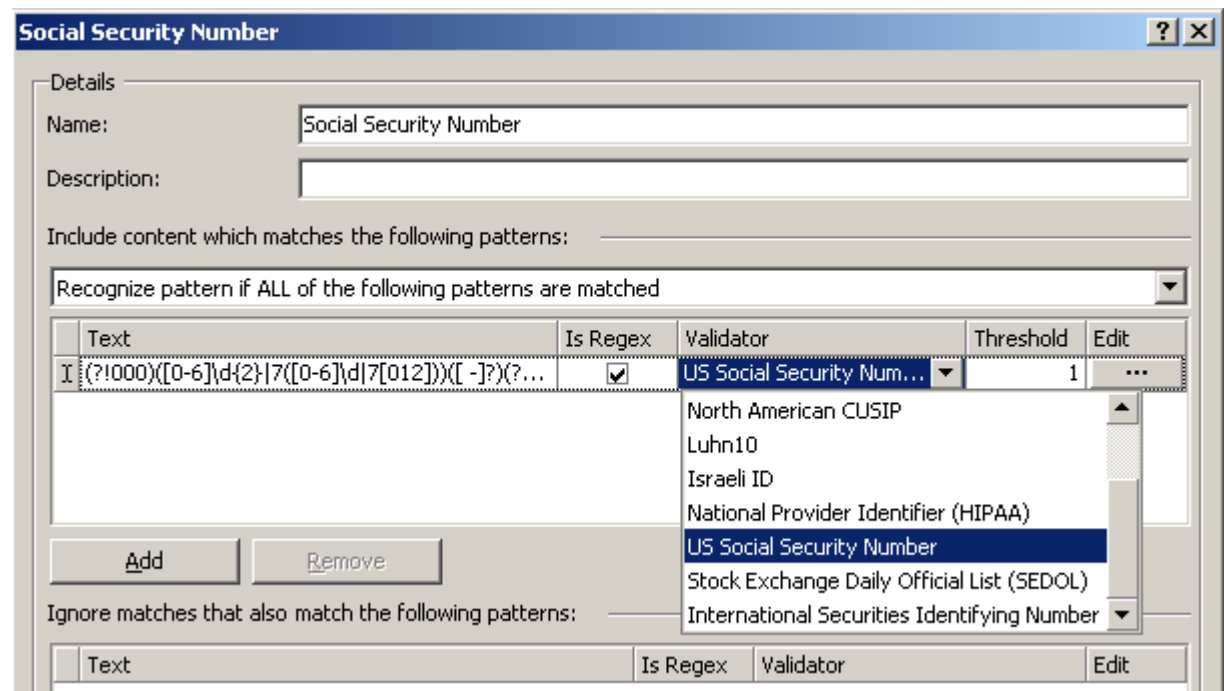
- Tags and Categories are defined and used interchangeably



Classification – Regular Expression Validators



- Adding algorithms for validating regular expression
- Reducing false-positives



Classification – Dictionaries



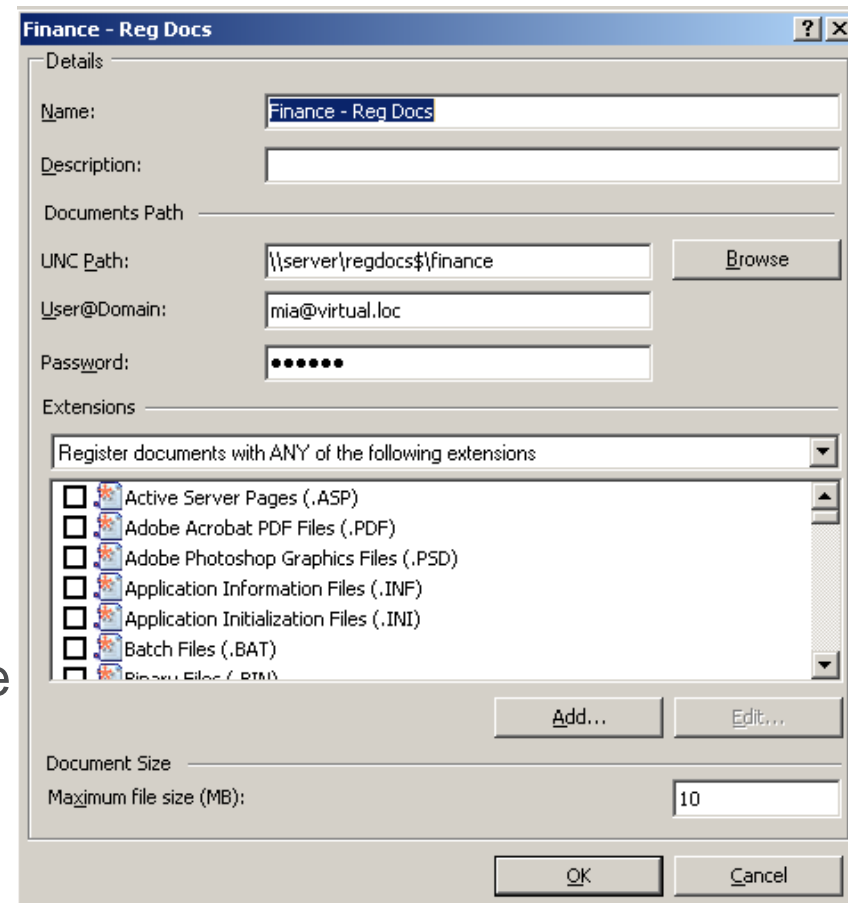
- Dictionary is a list of phrases associated with a common subject e.g.:
 - Bank transfer terms
 - Patient discharge terms
- Weight can be assigned to each phrase (including negative weight)
- Threshold is defined per dictionary
- Phrases occurrences can be counted as unique or multiple
- Dictionaries can be imported

Keyword or key phrase	Weight (+/-)
Depressants	1
Gamma Hydroxybutyrate	1
Hallucinogens	1
Hashish	1
Hashish Oil	1
Codeine	1
Dextropropoxyphene	1
Cocaine	1
Dextromethorphan	1
Flunitrazepam	1
Hydrocodone	1
Lycerin Acid Diethylamide	1

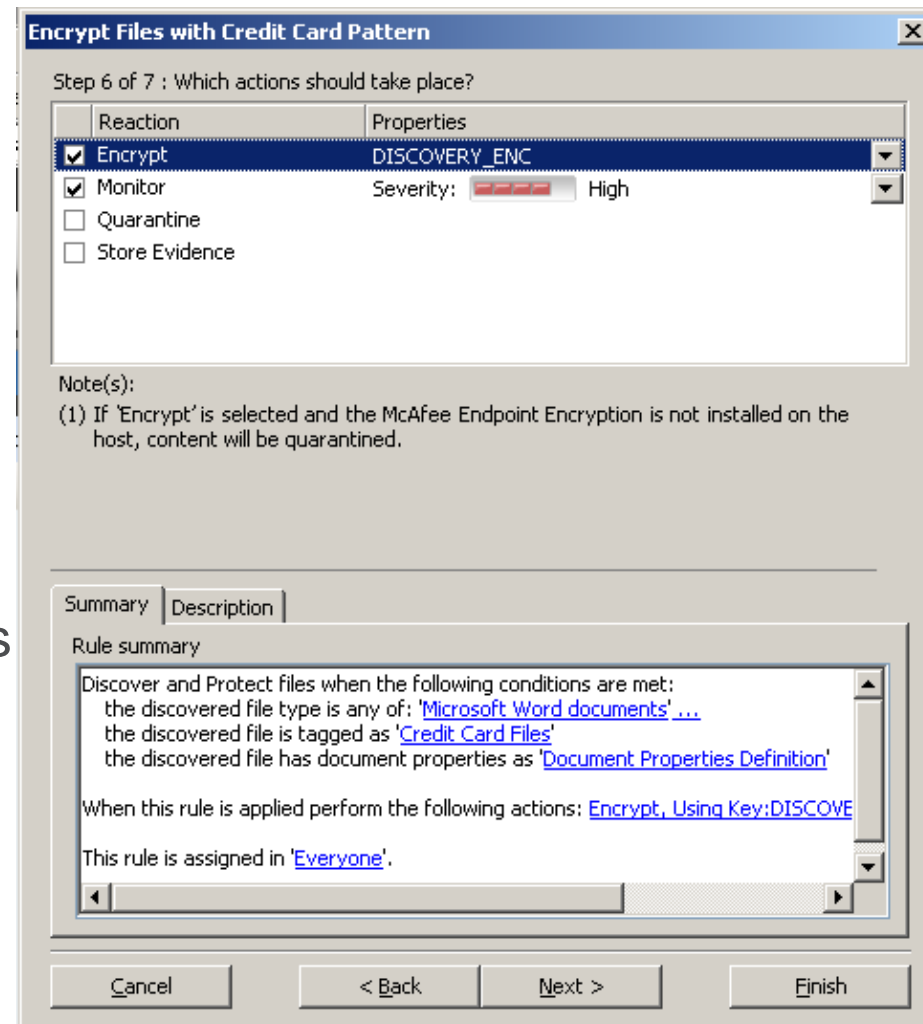
Classification – Registered Documents



- Registered document enable to protect sensitive files no matter how they reached the endpoint
- Several repositories of Registered Documents can be defined e.g.: Per department
- Scheduled runs of Host DLP management creates fingerprints (indexes) database of the files
- Fingerprints database incrementally transferred to the endpoints
- Registered documents are Category classified
- Endpoints can protect against leakage of content derived from registered documents



- Crawl local drives looking sensitive data-at-rest
- Each Discovery rule can be configured to:
 - File Type/Extension
 - Tag/Category
 - File Creation/Modification Date
 - User Group
- Reactions
 - Encrypt (Using Endpoint Encryption)
 - Monitor
 - Quarantine (Locally , AES encrypted)
 - Store Evidence
 - Delete (Advanced Configuration)
- Discovery can open Endpoint Encryption encrypted files



Discovery – Global Settings



- Discovery process can be restricted to CPU/Memory consumption
- Included/Excluded Directories
- Flexible Scheduling

The screenshot shows the 'Agent Configuration' window with the 'Discovery Settings' tab selected. The window is divided into several sections:

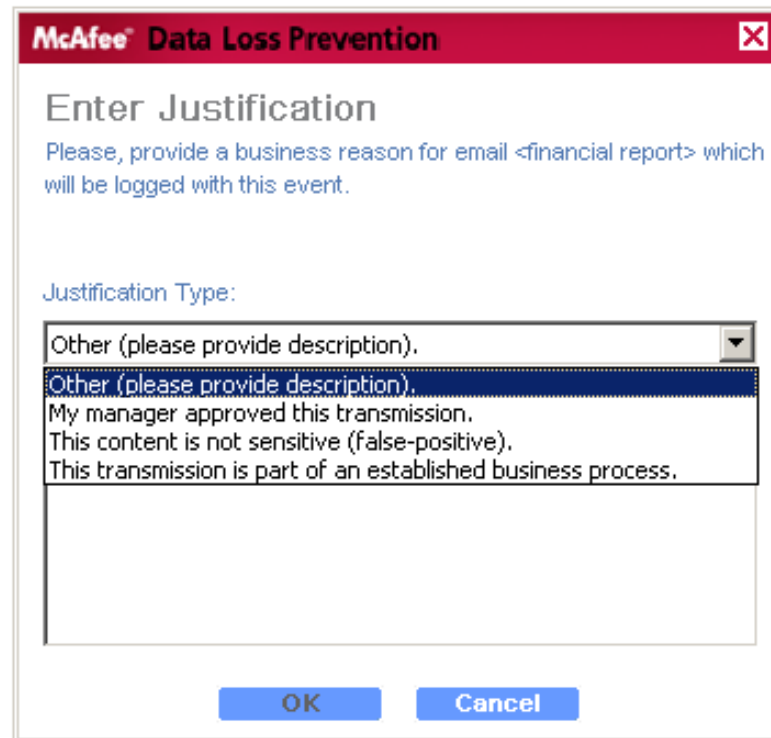
- Performance:** Contains three settings with spinners:
 - 'Suspend scan when the system's CPU is above (%)': 80
 - 'Suspend scan when the system's used RAM is above (%)': 80
 - 'Do not scan files larger than (MB)': 50
- Folders:** Contains two text boxes for folder paths, each with a 'Browse' button.
 - 'Scan the following folders:'
 - 'Do not scan the following folders:'
- Notifications:** Contains two checked checkboxes and text input fields:
 - 'Replace quarantined files with text notification'. The text field contains: 'File was quarantined by DLP discovery policy'.
 - 'Replace deleted files with text notification'. The text field contains: 'File was deleted by DLP discovery policy'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Enforcement – Business Justification



- Education/Cooperative Enforcement
- The user can bypass blocking in case justification is provided, or cancel the operation
- Configurable justifications (Including free text)



Fear of the Unknown Creates Data Anxiety



**Solved
problems**

- Lost laptops
- Lost USB devices
- Employee education
- Device Control

**Unmet
needs**

“Where” is
the
information?

How do I get effective
protection in place in a
“timely” manner?

How do I
“automate”
processes to
reduce audit
costs?

“What”
information
needs
protection?

“Who” should
have access?

Current solutions do not solve this problem

Manager

Monitor

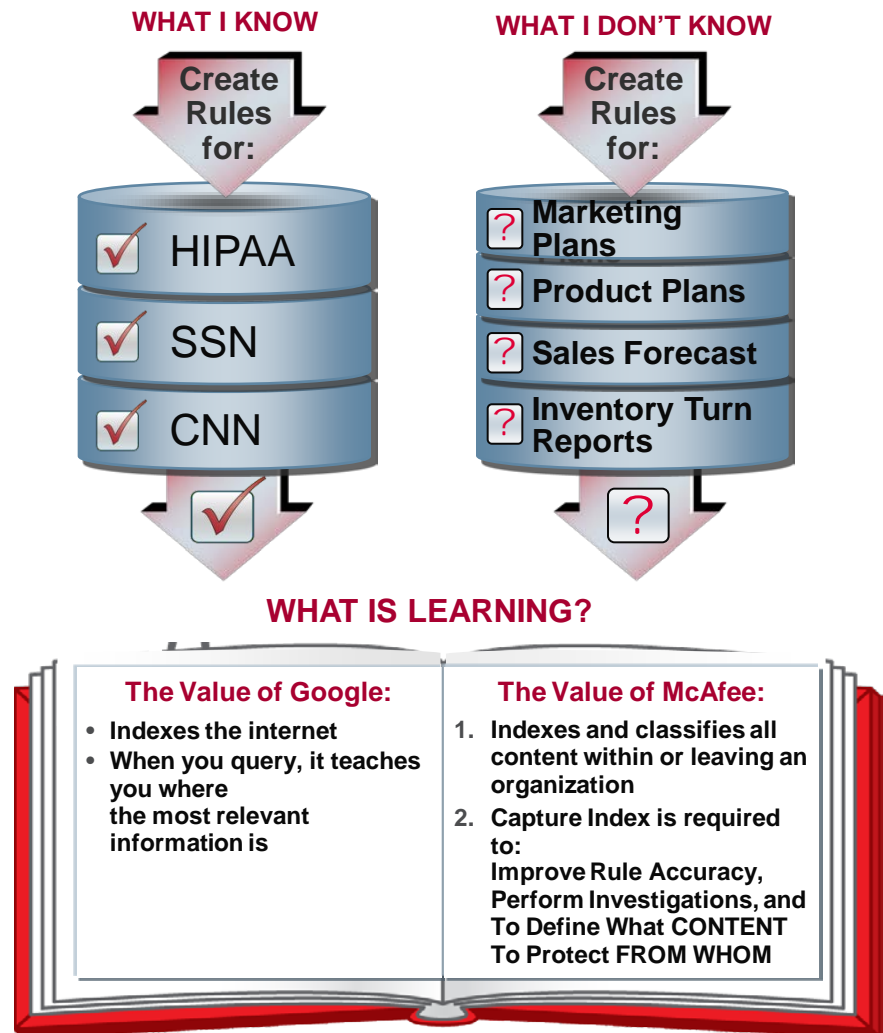
Prevent

Discover

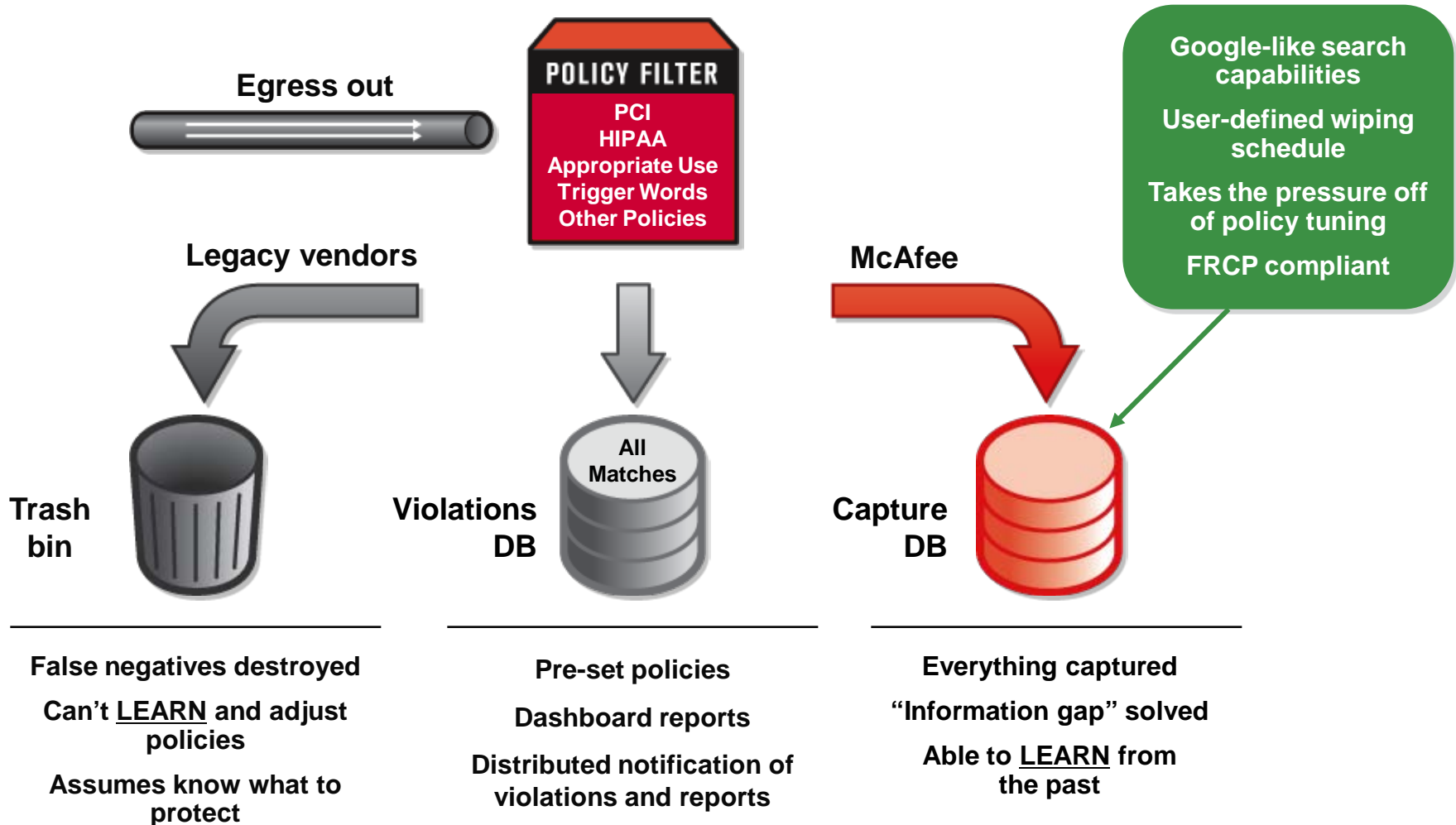
What Makes Us Unique?



- Most DLP products require you to **KNOW** what you should protect
- But how do you deal with what you **DO NOT KNOW** how to find?
 - Intellectual property
 - Product/marketing plans
 - Forecasts
 - Financial records
 - Legal discovery
- McAfee’s **“LEARNING”** capabilities are what enable adaptive protection
 - Google’s value is in indexing the internet
 - Reconnex’s **Google**-like “learning” focuses on corporate information in-motion, at-rest
 - “Learning” mines knowledge of content and its use, tunes protection



The McAfee Difference: Capture All Leakage!



Knowledge Mining: The Key to Learning



- Capture and index all content in-motion and at-rest
- Identify sensitive data
- Investigate activity
- Tune rules

Search for 'confidential'

Input Type: ?
Date/Time: Search Save Search

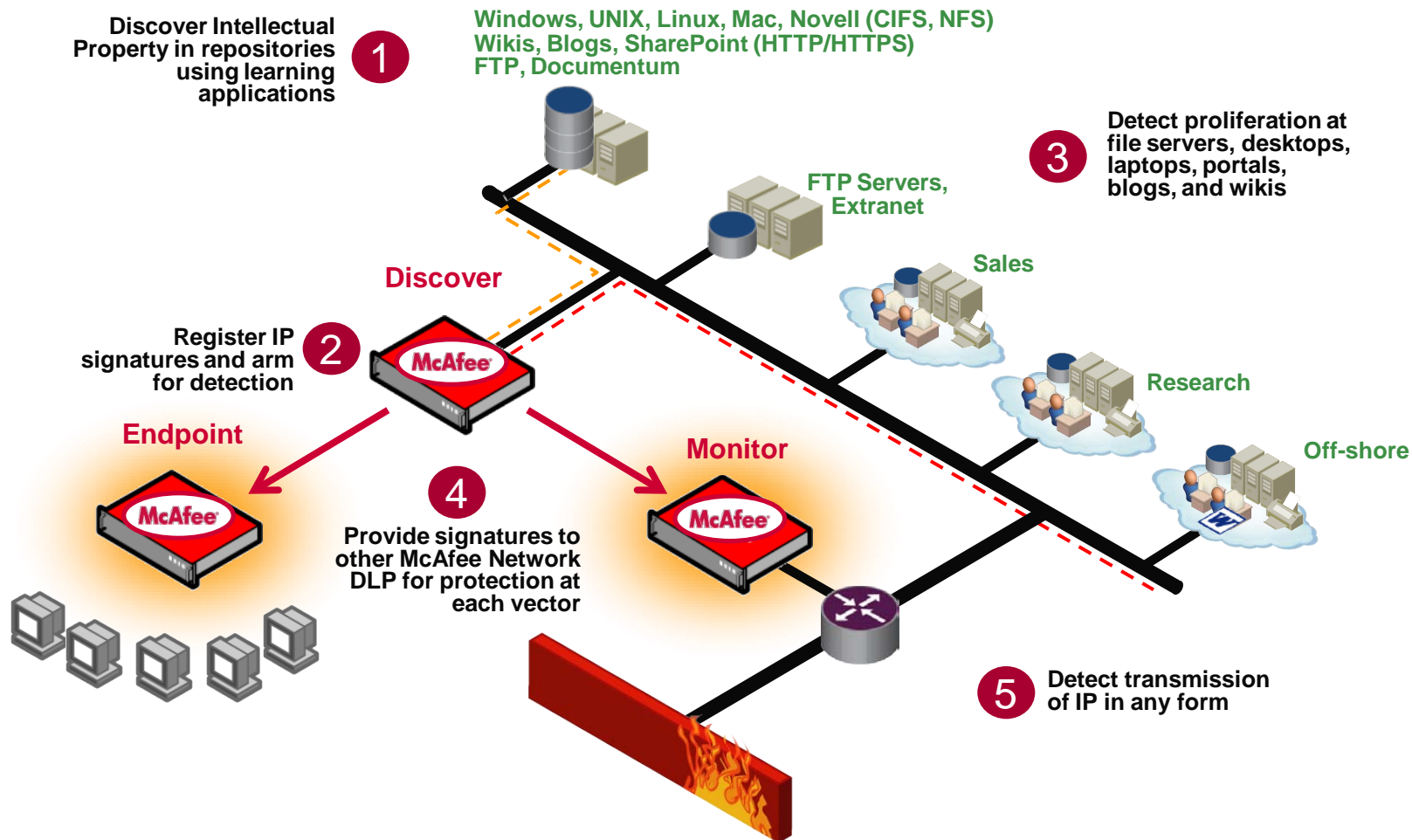
Who sent it out, and to where?

RecipientDomain	Sender	Hits
mega.org	Total	13
	Diana Cox (dcox@mail.arc.mega.org)	6
	Gustavo Barba (gbarba@copac.es)	4
	Craig Ouzounian@compucom.com	2
	Richard Mains (rmains@mainsgate.com)	1
Halk	Total	4
	Sophia Fegan (sfegan@mail.arc.mega.org)	4
aol.com	Total	3
	Scott Barkow (Scott.Barkow@BigBank.com)	2
	Tom Lillard (Tom.Lillard@BigBank.com)	1
BigBank.com	Total	3
	Switzer; Susan (sswitzer@oppenheimerfunds.com)	1
	Donaghey; Chris (chris_donaghey@rhco.com)	1
	Randy (randy@mail.bullmkt.com)	1
puresense.com	Total	2
	John Williamson (jwillamson@puresense.com)	2

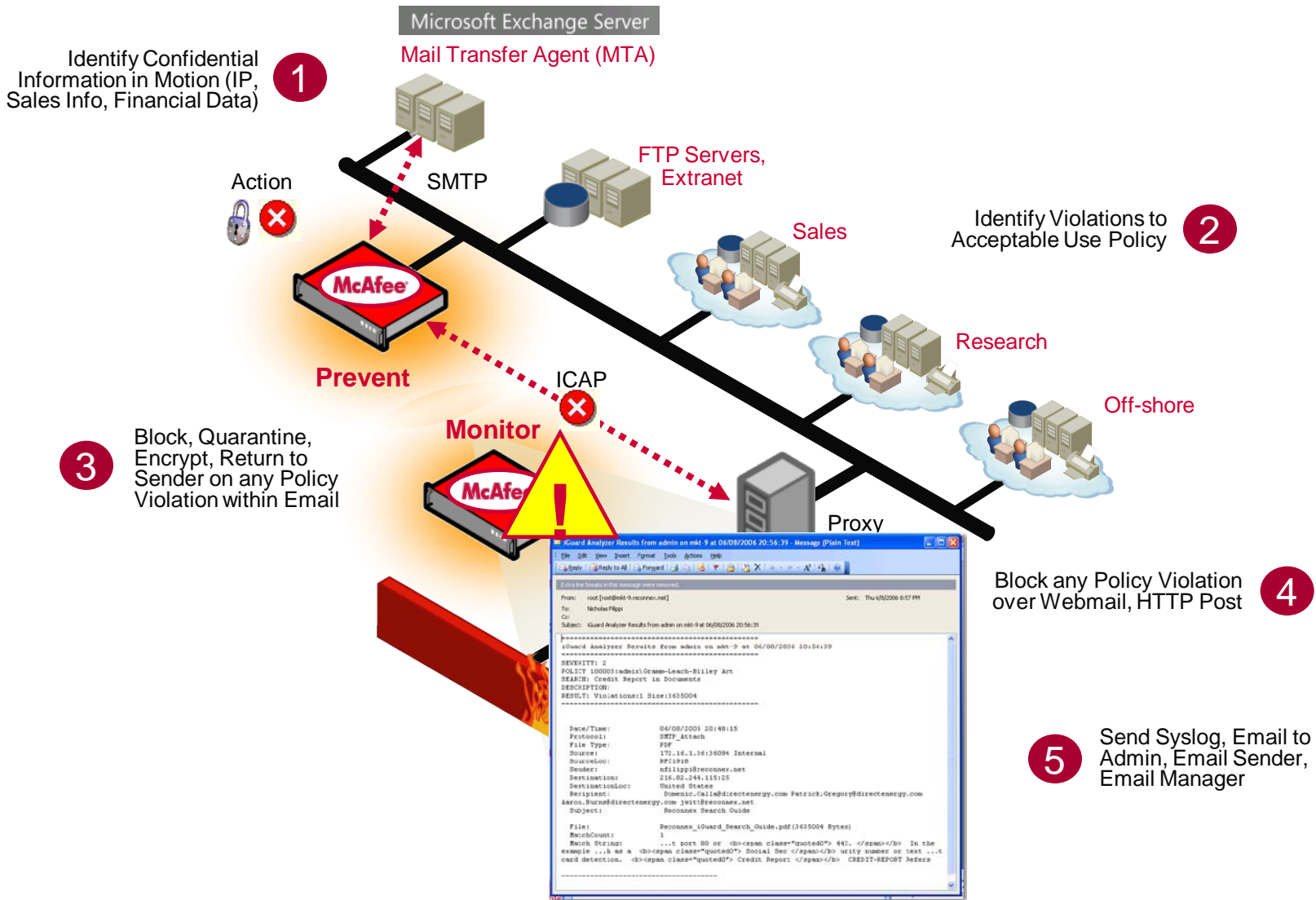
Where is it stored on my network?

HostIP	Content	Hits
192.168.254.151	Total	50
	PDF	15
	MSWord	13
	Excel	6
	Powerpoint	5
	PCAP	5

Data-at-Rest: Discovery and Classification



Data-in-Motion: Prevent Violations



Centralized Management



- Centralized system management
 - Unified policies and rules
 - Streamlined incident workflow
 - Unified and flexible reports
 - Device configuration and management
- Powerful case management
 - Aggregation of common incidents
 - Transfer of ownership and remediation
 - Roles-based access and permissions
- Centralized data mining, search, and analytics
 - Search historical data quickly
 - Find sensitive data and how it is used
 - Tune rules quickly, validate on-the-fly
 - Perform user investigations

Reconnex System Administration interface showing a list of devices. The table includes columns for Status, Device, Mode, CPU, Network, Used Disk, Health, Last Connection, Configure, Statistics, and Advanced. Devices listed include ashankar-53, ogo178, alpha-194, shub-120, shub-178, and shub-231.

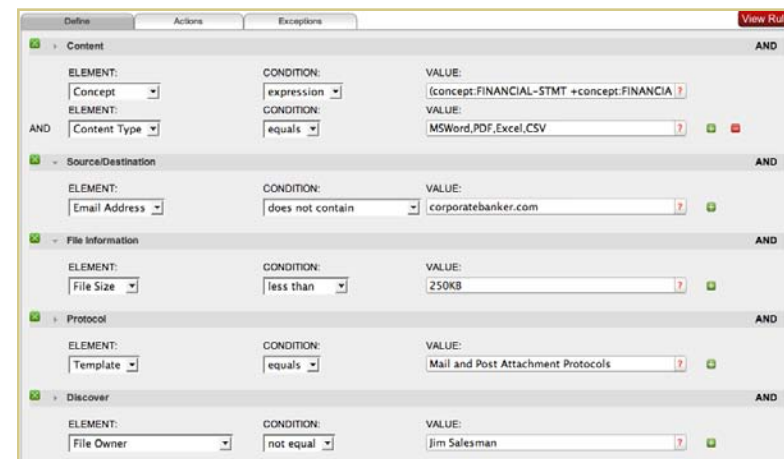
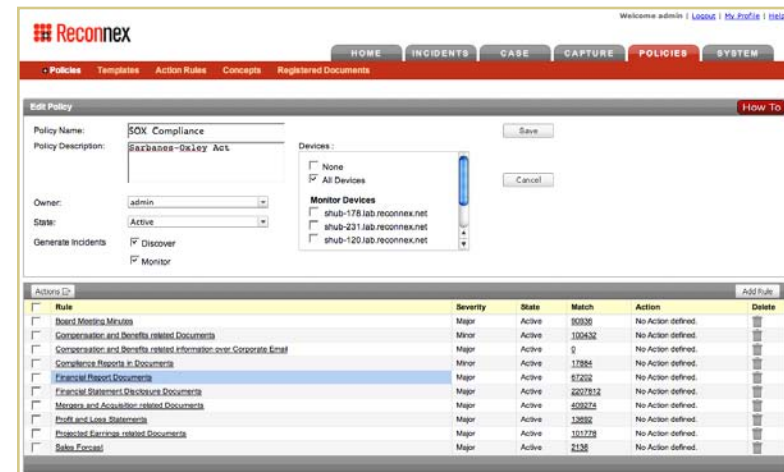
Reconnex Case Management interface showing a Case List table. The table includes columns for Details, Export, Caseid, Headline, Status, Priority, Owner, Submitter, Timestamp, Resolution, IncidentCount, and Delete. Cases listed include 'End Point' and 'damodar'.

Reconnex Dashboard interface showing a bar chart of incidents by recipient domain and policy. The chart displays incident counts for various domains and policies, such as SOX Compliance, ITAR Regulations, and Acceptable Use.

Unified Rules and Policies



- Unified policies for protection
 - Single interface for DiM, DaR rules
 - Unified construction limits sprawl
- Powerful default rules and policies
 - Compliance
 - Acceptable Use
 - Intellectual Property Protection
 - 20+ policies and 150+ rules default
- False positive workflow
 - Simple rule tuning from incident detail
 - Incident data to create exceptions
 - Complements learning applications
- Document registration
 - Increase accuracy of rules
 - Explicit protection for sensitive data
 - Scalable registration: Discover crawler



Simplified Incident Management



- Flexible incident visualization
 - Incident listing, grouping, summary
 - 40+ built-in views
 - Configurable, schedulable reports
- Automatic incident assignment
 - Incidents automatically assigned
 - Presented to users in home page
- Dynamic filtering and grouping
 - Create specific views for later use
 - Focus view to areas of interest
- False positive workflow
 - Streamline rule adjustments
 - Transfer parameters to rule exception

Reconnex Home | INCIDENTS | CASE | CAPTURE | POLICIES | SYSTEM

Welcome admin | Logout | My Profile | Help

Data-in-Motion Incidents

Details ID	Rule Name	Created
52698	Document attachments over Webma...	Wed Apr 30 15:28:25 PDT 2008
52699	Resume Tracker	Wed Apr 30 15:28:14 PDT 2008
52697	Document attachments over Webma...	Wed Apr 30 15:28:21 PDT 2008
52702	Document attachments over Webma...	Wed Apr 30 15:28:25 PDT 2008
52703	Mention of Discrimination in E...	Wed Apr 30 15:28:12 PDT 2008
52700	Document attachments over Webma...	Wed Apr 30 15:28:25 PDT 2008
52701	Document attachments over Webma...	Wed Apr 30 15:28:22 PDT 2008
52705	Document attachments over Webma...	Wed Apr 30 15:28:22 PDT 2008
52704	Document attachments over Webma...	Wed Apr 30 15:28:25 PDT 2008
52708	Document attachments over Webma...	Wed Apr 30 15:28:26 PDT 2008

Data-at-Rest Incidents

Details ID	Rule Name	Created
261992	Flashstone in Mail Attachments	Wed Apr 30 15:09:22 PDT 2008
261993	Compressed Attachments over Web...	Wed Apr 30 15:04:07 PDT 2008
261996	Compressed Attachments over Web...	Wed Apr 30 15:04:02 PDT 2008
261987	Compressed Attachments over Web...	Wed Apr 30 15:04:02 PDT 2008
261984	Compressed Attachments over Web...	Wed Apr 30 15:04:02 PDT 2008
261955	Flashstone in Mail Attachments	Wed Apr 30 15:05:07 PDT 2008
261950	Flashstone in Mail Attachments	Wed Apr 30 15:05:45 PDT 2008
261991	Flashstone in Mail Attachments	Wed Apr 30 15:08:01 PDT 2008
261588	Flashstone in Mail Attachments	Wed Apr 30 15:05:21 PDT 2008
261889	Flashstone in Mail Attachments	Wed Apr 30 15:05:39 PDT 2008

Top Data-in-Motion Rules Based on Incident Count

Name	Count
Document attachments over Webmail	12652
Document Attachments over Instant Messaging Services	2392
Social Security Number in Email and Instant Messaging Conv...	2783
Social Security Number in Email Conversations	2783
Audio/Video Content being Posted on the Web	2352
Social Security Number Violations	2345
Social Security Number in Documents	2345
Credit Card Related Violations	2065
Flashstone in Mail Attachments	1614
Resume Tracker	1433

Top Data-at-Rest Rules Based on Incident Count

Name	Count
Document Attachments over Instant Messaging Services	73386
Document attachments over Webmail	73386
Source Code Mailed to Competition	18449
Source Code Uploaded to Unsafe Servers	18449
Compressed Attachments over Webmail	8043
Pricing Information	7271
Engineering Drawings and Design Files being uploaded to Uns...	7264
Engineering Drawings and Design Files mailed to Competition	7264
Financial Statement Disclosure Documents	6288
Flashstone in Mail Attachments	2386

Reconnex Dashboard | My Views | INCIDENTS | CASE | CAPTURE | POLICIES | SYSTEM

Welcome admin | Logout | My Profile | Help

Total Incidents: 63021

Inc. By Severity vs. Status

Status	Critical	Major	Minor	Warning	Info
Not	13256	8603	7187	5653	18119
Viewed	2	0	0	1	0

Inc. By Policy Over Time

Top Policies

Policy	Incidents
Online Services Communications (admin)	16749
Personally Identifiable Information (admin)	5673
State Privacy Laws (admin)	5248
Acceptable Use (admin)	4458
SOX Compliance (admin)	3115

Top Protocols

Protocol	Incidents
HTTP_Webmail_Attach	17086
SMTP_Request	16032
SMTP_Attach	10301
HTTP_Post	5250
MSN_Chat	2478

Top Content

Content	Incidents
SMTP	16032
MSWord	11441
Excel	10591
PDF	8802
Powerpoint	2921

Integrated Case Management



- Centralized case management system and workflow
 - Correlate incidents
 - Assign owners and priority
 - Remediate
- Case audit trail
 - Automatic notifications
 - Notes for collaboration
 - Case history
- Collaborative approach
 - Leverage roles based access control
 - Facilitate interaction of stakeholders
 - Adjust broken business process
 - Correct user behavior
- Case export
 - Full HTML export of case, incidents
 - Includes associated files, context

Actions	Options	Showing 1-3 of 3	How To								
Details	Export	Caseld	Headline	Status	Priority	Owner	Submitter	Timestamp	Resolution	IncidentCount	
<input type="checkbox"/>			3	Joe Hacker Inappropriate Behavior	New	Urgent	Compliance	admin	Wed Apr 30 14:08:35 PDT 2008	Under Investigation	4
<input type="checkbox"/>			2	pls investigate	New	Normal	Legal	admin	Wed Apr 23 10:39:31 PDT 2008	Under Investigation	2
<input type="checkbox"/>			1	Case against Joel	New	Normal	HR	admin	Tue Apr 22 10:05:42 PDT 2008	Under Investigation	3

Case Details Apply Cancel

Case ID: 3 **Submitter:** admin

Headline: Joe Hacker **Keywords:**

Owner: Compliance **Incident Count:** Monitor:2 Discover:1 Endpoint:1

Status: New **Submitted Date:** Wed Apr 30 14:08:35 PDT 2008

Priority: Urgent **Last Modified:** Wed Apr 30 14:11:02 PDT 2008

Resolution: Under Investigation **Notify Submitter:**

Add Notes:

Options

Monitor Incident List	Discover Incident List	Endpoint Incident List	Notes	Log			
Details	Sender	Recipient	Policy	Rule	Timestamp	Protocol	Delete
<input type="checkbox"/>	Corp. Insider (insider@example.com)	bad.guy@hostile.net	Financials and Security Compliance	Financial Statement Disclosure Documents	Tue Apr 29 16:51:40 PDT 2008	SMTP_Attach	Delete
<input type="checkbox"/>	Corp. Insider (insider@example.com)	bad.guy@hostile.net	SOX Compliance	Financial Statement Disclosure Documents	Tue Apr 29 16:51:40 PDT 2008	SMTP_Attach	Delete

McAfee Network DLP Integration With ePO



Server: angelfish | Time: 9/4/08 3:46 PM PST | User: admin Log Off

McAfee
ePolicy Orchestrator® 4.0

Dashboards
Reporting
Software
Systems
Network
Automation
Configuration
Options ▼

Data-in-Motion Incident Status (by)

Status/Sev.	Critical	Major	Minor	Warning	Info
New	10	24	32	38	0
Viewed	2	0	0	0	0

[vert Labs WebImmune](#)
submit potentially infected files for analysis

[McAfee, Inc. Home Page](#)
Go to the McAfee home page

Data-at-Rest Top Shares

repository	137
------------	-----

Signature: Not present 5300.2777

Avert Security Threats: [10 unread](#)

Last check: 2008-09-04 15:54:32.1

Host DLP

Go

Data-in-Motion Top Policies

Personally Identifiable Information {admin}	28
FISMA Compliance {admin}	28
GLBA Compliance {admin}	27
SOX Compliance {admin}	22
PCI Compliance {admin}	18

0 Last Replication Succeeded 0 Last Replication Failed

Data-at-Rest Top Policies

Acceptable Use {admin}	46
FISMA Compliance {admin}	22
Competitive Edge {admin}	18
Human Resources {admin}	7
GLBA Compliance {admin}	4

0 Compliant 1 Non-Compliant

System Health and Monitoring

● Normal
 ● Critical
 ● Registering
 ● Unknown

Status	Device	Mode
●	miniEPO.hukkanet.com	inSight
●	beep-beep.hukkanet.com	Monitor
●	discover-demo.hukkanet.com	Discover
●	prevent-demo.hukkanet.com	Prevent

[HDLP PRODUCT DEMO]

