Trend Micro LeakProof 3.0 (TMLP)

Data Leak Prevention

Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro Channel Confidential
May 2008

Data Leak Prevention: PAIN Worldwide

INDUSTRYWEEK IW

Manufacturers Losing Profits From Compromised Intellectual Property Rights

Almost half of survey respondents report lost market share.

Com

Dec.
surve
prop
Intell
in a
desi
doc

Technology
THE JOURNAL REPORT
THE WALL STREET JOURNAL.
© 2006 Dow Jones & Company, Inc. All Rights Reserved.

The Dangers Within

BREAKING NEWS!

Boeing Breach

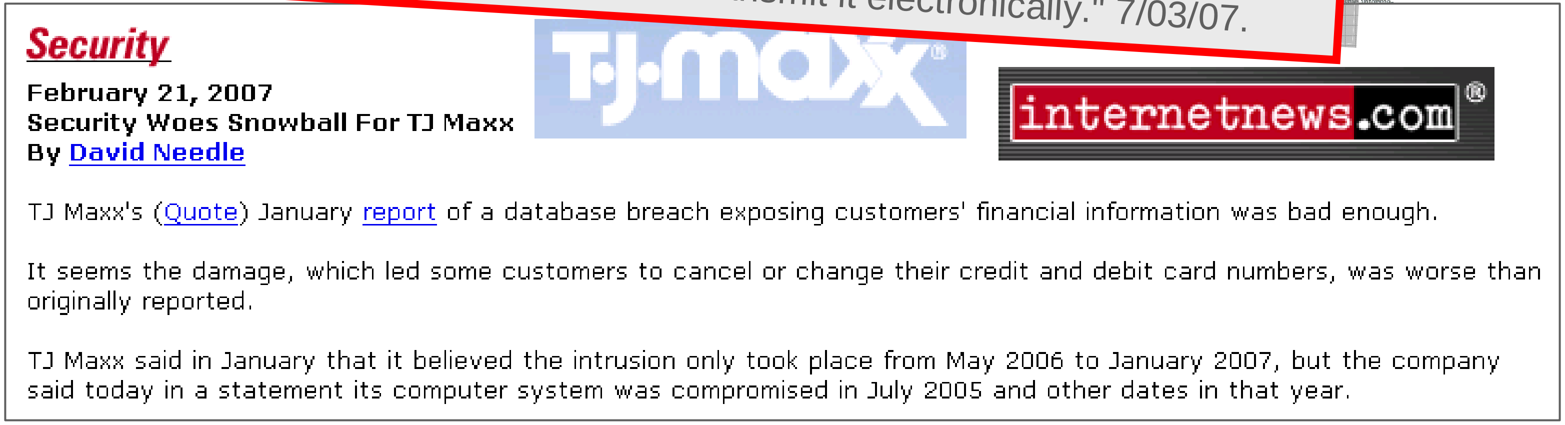
InformationWeek

"Police reported finding a thumb drive that was connected to his computer terminal via a USB cord that ran along the back of the terminal to the storage device that was "hidden in a drawer" in his desk." 7/11/07.

Fidelity NIS Theft

CSO

"To avoid detection, the administrator appears to have downloaded the data to a storage device rather than transmit it electronically." 7/03/07.



T.J.maxx®

internetnews.com®

Security

February 21, 2007
Security Woes Snowball For TJ Maxx
By David Needle

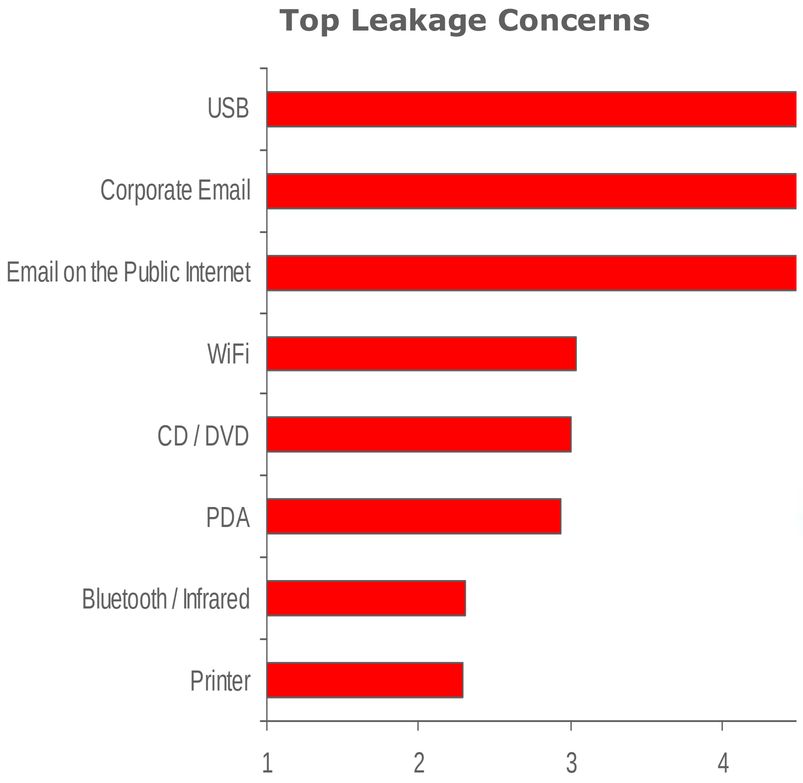
TJ Maxx's (Quote) January report of a database breach exposing customers' financial information was bad enough.

It seems the damage, which led some customers to cancel or change their credit and debit card numbers, was worse than originally reported.

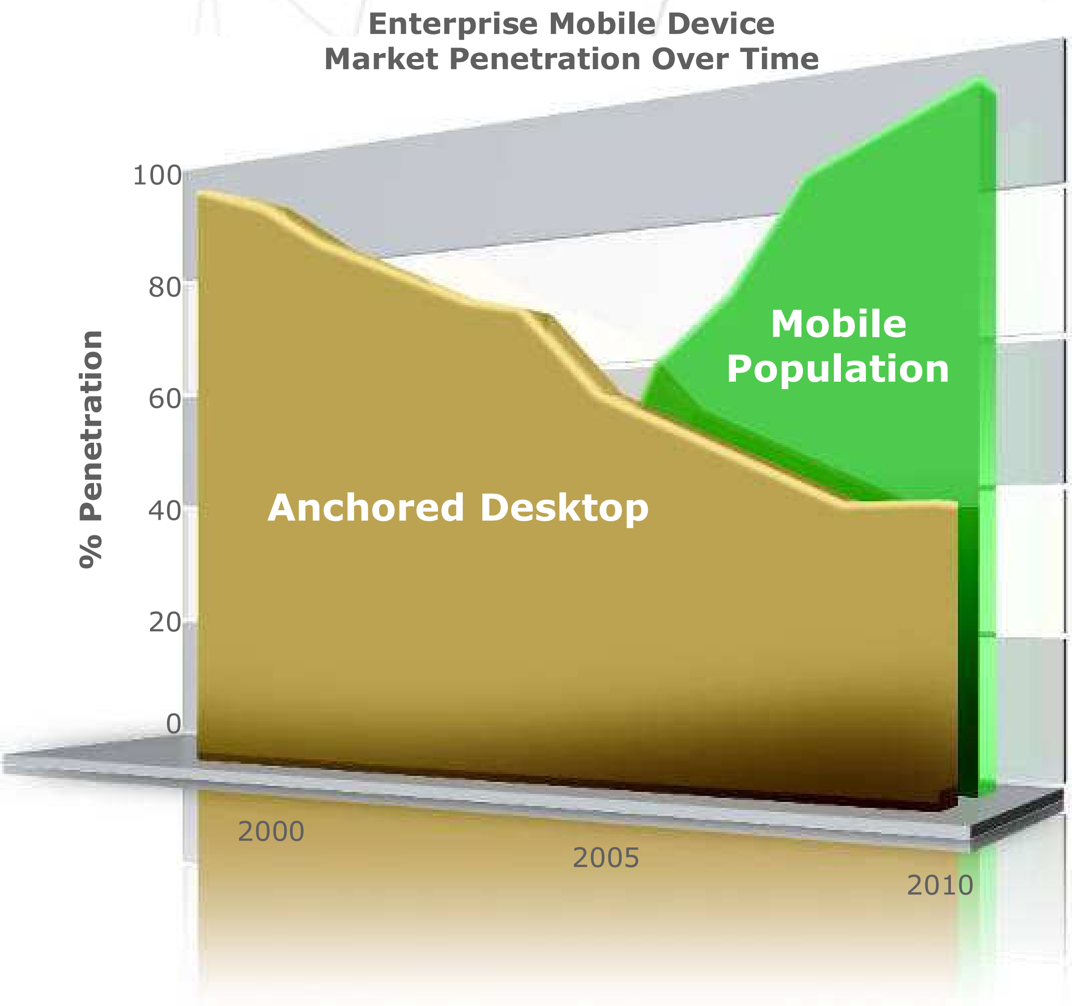
TJ Maxx said in January that it believed the intrusion only took place from May 2006 to January 2007, but the company said today in a statement its computer system was compromised in July 2005 and other dates in that year.

Mobile Insecurity

- Desktop and Mobile Leakage



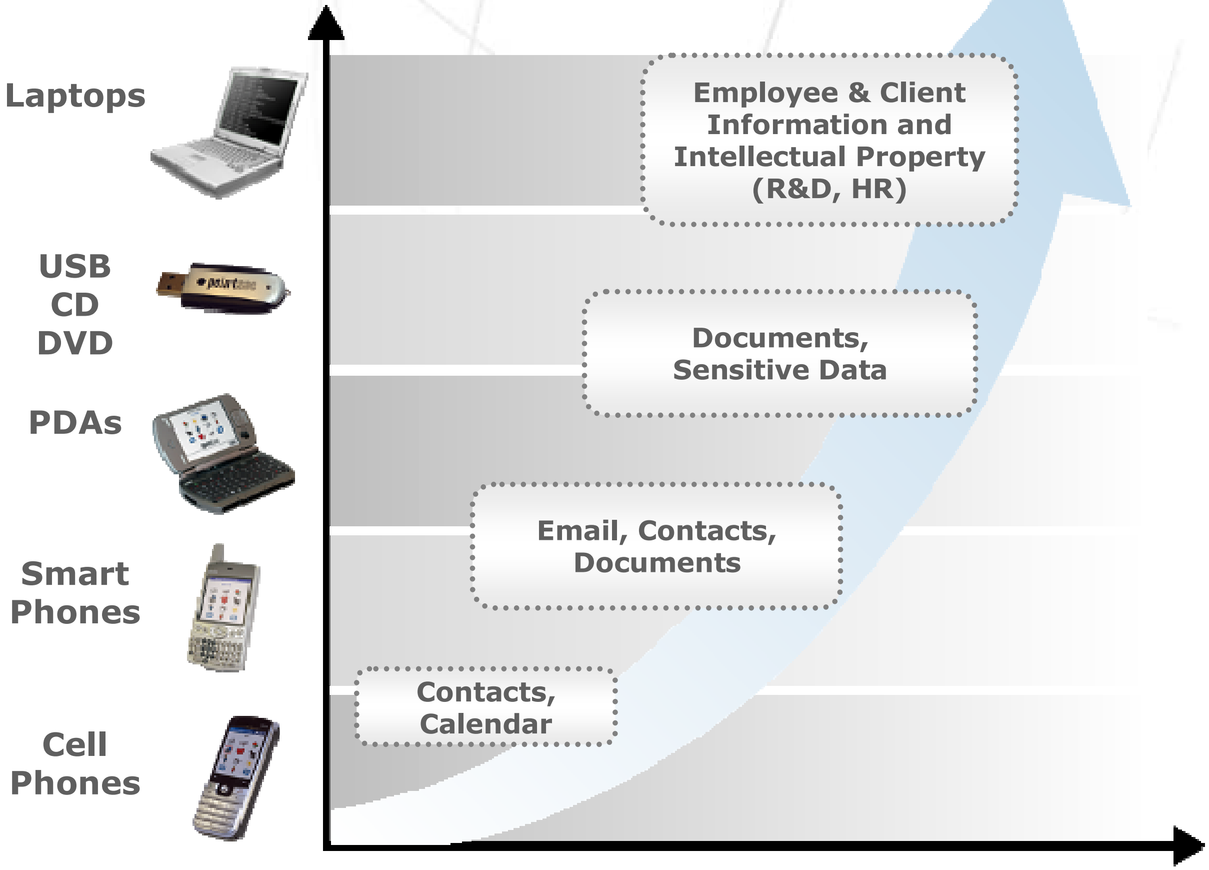
Source: Market Research International



Source: The 451 Group and Infolock

Data Security & Protection

- Why Data Security?
- Data is more mobile
- Mobile devices more powerful
- Difficult to secure the ‘infrastructure’ in a mobile world

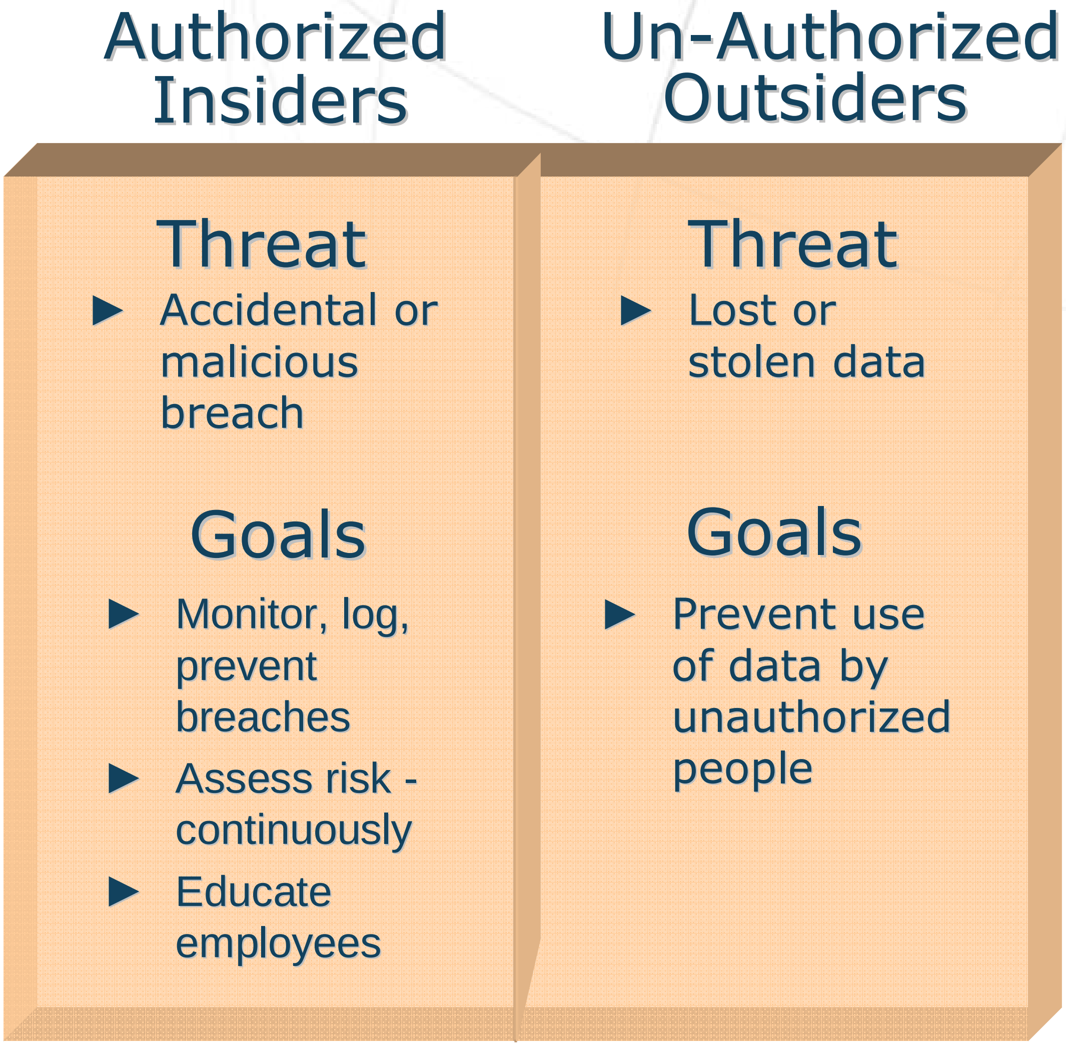

Laptops
USB
CD
DVD
PDAs
Smart Phones
Cell Phones
Employee & Client Information and Intellectual Property (R&D, HR)
Documents, Sensitive Data
Email, Contacts, Documents
Contacts, Calendar

Content Sensitivity & Threat Potential
(source: InfoLock)

According to Gartner, 47% of corporate data resides on mobile devices, and **350,000** mobile devices were lost or stolen in the U.S. over a two-year period

The ‘Insider Threat’

- **78% of data breaches come from Authorized Insiders**
  - **Ponemon Institute Study – 2006**



Authorized Insiders

Threat

- ▶ Accidental or malicious breach

Goals

- ▶ Monitor, log, prevent breaches
- ▶ Assess risk - continuously
- ▶ Educate employees

Un-Authorized Outsiders

Threat

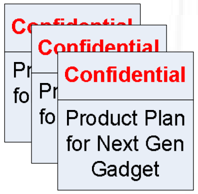
- ▶ Lost or stolen data

Goals

- ▶ Prevent use of data by unauthorized people

Scenes of Mobile Data Leakage

Scene 1



Confidential

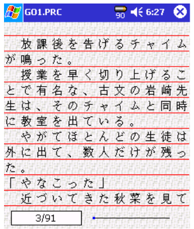
Product Plan for Next Gen Gadget

Gmail

Kristina, at Starbucks™… …edits a confidential document… …and emails it

How do you know? *How can you tell it wasn’t a love letter?* *Could you have stopped it?*

Scene 2



　放課後を告げるチャイムが鳴った。

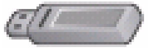
　授業を早く切り上げることで有名な、古文の岩崎先生は、そのチャイムと同時に教室を出ている。

　やがてほとんどの生徒は外に出て、数人だけが残った。

「やなこった」

　近づいてきた秋菜を見て

149dl209y
kw9731la1
d992;f9ska
98f02l0399



USB Drive

Gary, at a branch office… …encrypts customer data… …and copies it

How do you know? *Is he authorized?* *Can you centrally monitor & log?*

Securing Enterprise Data

LeakProof enables companies to reduce the risk of data breaches and ensure privacy and compliance

LeakProof understands the content of data at rest, in use, and in motion on every enterprise endpoint, providing protection of sensitive data

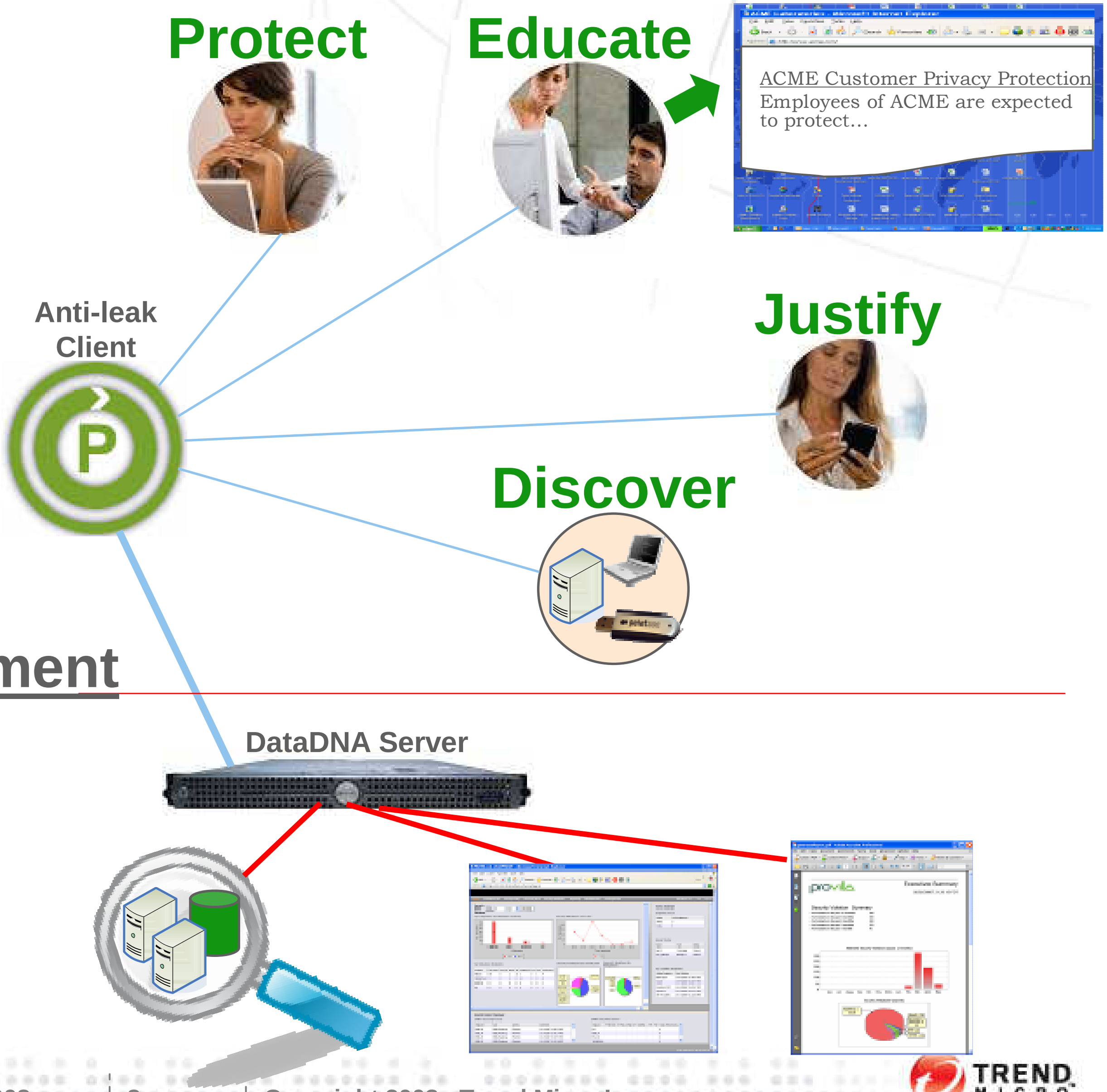
LeakProof™ Secures From the Endpoint

Client Software

- Intelligent
  - Fingerprint, Regex, Keyword, Meta-data
- Interactive New 3.0
- Invisible
- Independent
- Robust

Enterprise Management

- Policy
- Visibility
- Workflow



ACME Customer Privacy Protection
Employees of ACME are expected to protect…

Defining Sensitive Information

- Three Methods of Detecting Content
  - Sensitive Document DataDNA™ Fingerprinting
    - Unstructured Data
  - Entity Templates (Regular Expressions)
    - Structured Data
  - Keyword Lists
    - Structured Data
- Data is categorized by
  - Classification (as many as you need)
  - Sensitivity (High/Low)
  - Regulation (associated with a classification)
- Sensitive Data and Security Policies are linked by:
  - Matching Level Thresholds (High/Medium/Low)
  - Sensitivity Level Thresholds (High/Low)
  - Classification
  - Regulation

Sensitive Documents DataDNA™

- Servers with sensitive data are identified
- Sources (or file paths) within Servers identified
- Sources are given Classification and Sensitivity.
- Examples:
  - \\server\files\contracts\*.doc = Contract Documents/High Sensitivity
  - \\myserver\files\CVS\*.* = Source Code/Low Sensitivity
- Documents are retrieved by the appliance.
- Fingerprints are added to the database and policy.

Unique Fingerprinting Technology

- Fast
- Small
- Accurate
- Language independent

Comma
is that one
detect all
shortcomin
lation tech
detector d
the assum
haps wide
ing some d
then, enha
ages of ind
the anomal

age that is superior to the coverage of any one detector. No studies have been done, however, in which measured effects of diversity in anomaly detectors have been obtained.

This paper explores the effects of using diverse anomaly-detection algorithms (algorithmic diversity) in intrusion detection. Experimental results indicate that while performance/coverage improvements can in fact be effected by combining diverse detection algorithms, the gains are surprisingly not the result of combining large, non-overlapping regions of the anomaly space. Rather, the gains are seen at the edges of the space, and are heavily dependent on the parameter values of the detectors, as well as on the characteristics of the anomalies.

As a consequence of this study, defenders can be provided with detailed knowledge of diverse detectors, how to combine and parameterize them, and under what conditions, to effect diverse detection performance that is superior to the performance of a single detector.

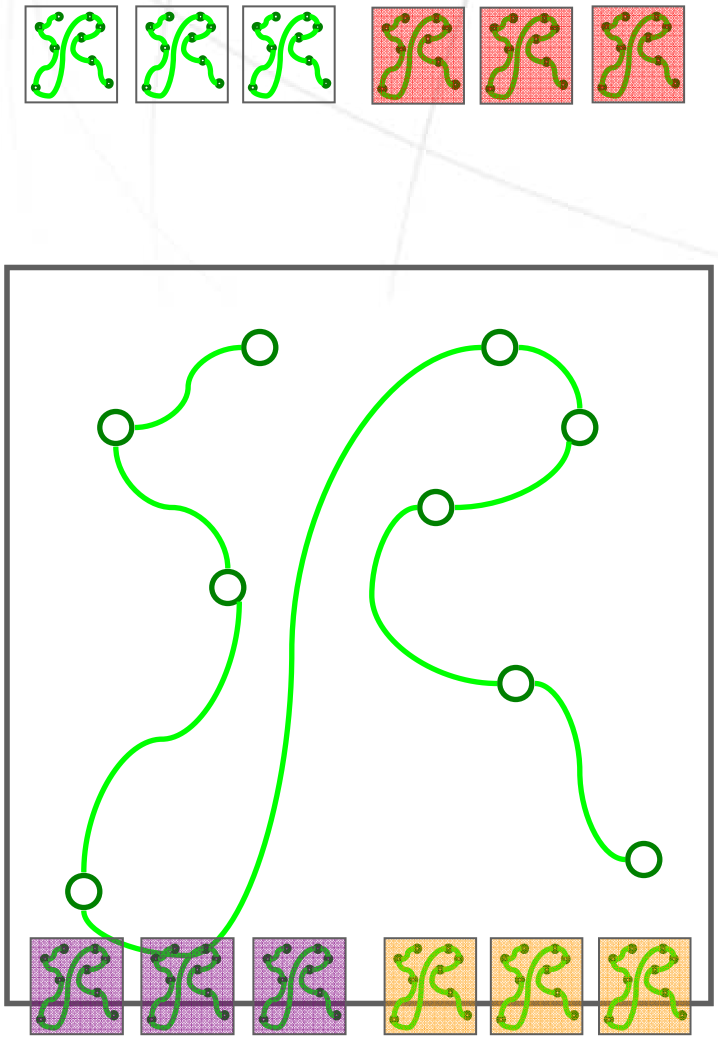
1 Introduction

There are many problems that plague anomaly-based intrusion detectors today, e.g., high false-alarm rates [3], inconsistency of detector performance [10, 30], training issues, e.g., how often should an anomaly detection system be retrained to ensure acceptable performance [2], inadvertent incorporation of intrusive behavior into a detector's concept of normal behavior possibly causing the intrusion to be missed by the detector [13], and so forth.

The effort to address the sluggish progress in the area of anomaly-based intrusion detection requires a slight shift in focus from the creation of ever-more, ever-new, anomaly detection algorithms. Strategies are needed that attempt to evaluate, understand and harness the strengths of the detectors that are already present in the literature [29, 26, 30]. These efforts have served to highlight the paucity of evaluation methods for establishing the operational effectiveness of anomaly detectors in a manner that is consistent and repeatable. The lack of such evaluation strategies makes it extremely difficult to assess the effectiveness of anomaly detectors, compare their relative strengths and weaknesses, make measurable improvements and – perhaps more interestingly – understand how to select and combine anomaly detectors effectively to improve detection performance, taking advantage of their inherent algorithmic diversity.

It is interesting to observe that despite the variety of anomaly detectors currently present in the intrusion detection literature, there appears to be an implicit assumption that a single anomaly detection algorithm is all that is required to detect intrusions or attacks on any given system. This assertion is supported by a further two observations. First, intrusion detection systems claiming to perform anomaly detection typically employ only one kind of anomaly detection algorithm (e.g., [8, 10, 9, 28]). There is however, no evidence to suggest that a single anomaly detector will be sufficient for a given intrusion detection task. This is mainly because there is currently no study showing that the kinds of anomalies arising as manifestations of at-

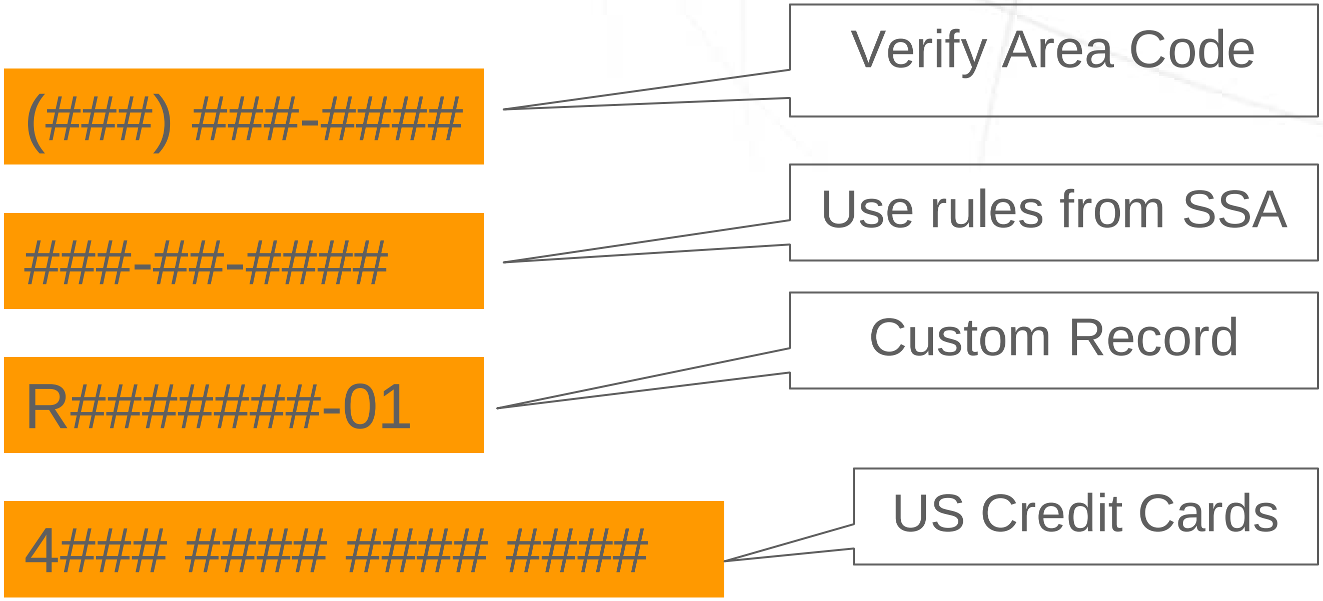
1



Entity Templates

- Patterns are called Entities (Regular Expressions)
  - SSN or National Identification Numbers
  - Credit Cards
  - Addresses
  - Phone Numbers
- Entities are combined into Templates
- Templates have rules for which Entities must be found.
- Entities have a score assigned as part of the rule
  - Credit Cards + SSN = 100
- Score determines which Security Policy Rule will apply.

Defining an Entity Template



(###) ###-#####

Verify Area Code

###-##-#####

Use rules from SSA

R#######-01

Custom Record

4### #### #### ####

US Credit Cards

Keyword Lists

- Multiple lists of words are possible.
- Each list is assigned a Classification and Sensitivity.
- Primary Use: Identify Document Types
  - C Source Code: printf(), scanf(), atoi()
  - Java Source Code: public static void, System.out.println()
  - Legal Documents: indemnification, easement, escrow
  - Medical Documents: anemia, ganglion, pancreatic

Keyword Lists

Programming

atof(
atoi(
atol(
else if
#endif
errno.h
java.applet
java.awt
java.beans
java.io
java.lang

Legal Dictionary

MALICE
ADJOURNMENT
DISMISSAL
AFFIDAVIT
ALIMONY
CURIAE
BIFURCATION
TRUST
CAPITAL
GAIN
CAPITAL

Medical Terms

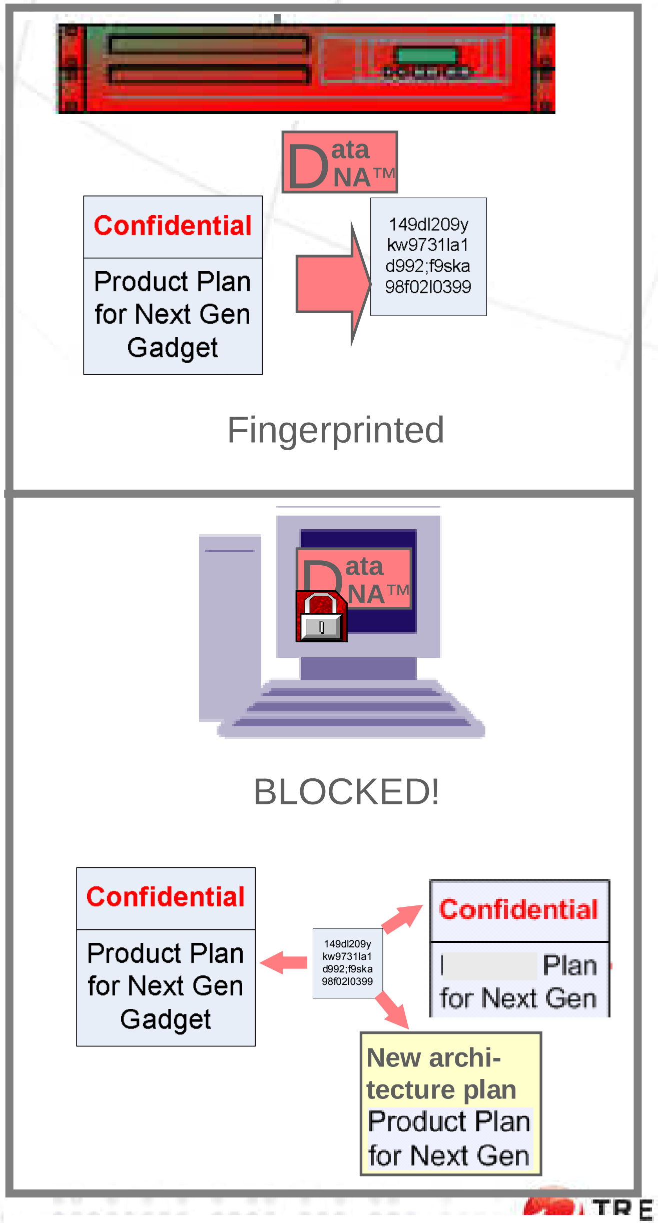
Abdominalgia
parathyroid gland
Vascular
Hypoproconvertinemia
Polyonychia
Gangrene
Osteomyelitis
spinal curvature
Tumor
Osteomyelitis
chylomicronemia

Security Policy Components

- Security Policies are made up of rules
- Each rule has the following components
  - Target (All, Workgroup, Workstation, Group)
  - Sensitive Information Attributes
    - Classification and Regulation
    - Sensitivity threshold (Low or High)
    - Match Level threshold (Low, Medium, or High)
  - OR File Meta Data
    - File extension
    - File Size
    - Special File Types (Archive, Encrypted, Unknown)
  - Activity
    - Email, Web, Instant Message, File Write
  - Action (online/offline)
    - Log, Warn, Block, Forensics, Alerts, Justify

Core Filtering Technology

- DataDNA™ Matching Engine
  - High confidence, low false positives
  - Language independent
  - Multiple matching methods
    - Signature/fingerprint
    - Entity / Regex
    - Keyword
    - File meta-data
- Robust Anti-Leak A/L Agent
  - DataDNA matching engine protects
    - Online OR offline
    - On edited, re-saved, cut/pasted content
  - Broadest coverage
    - Devices, channels, applications, email clients, network protocols
    - Authorizes encryption



Leading Agent Performance and Technology

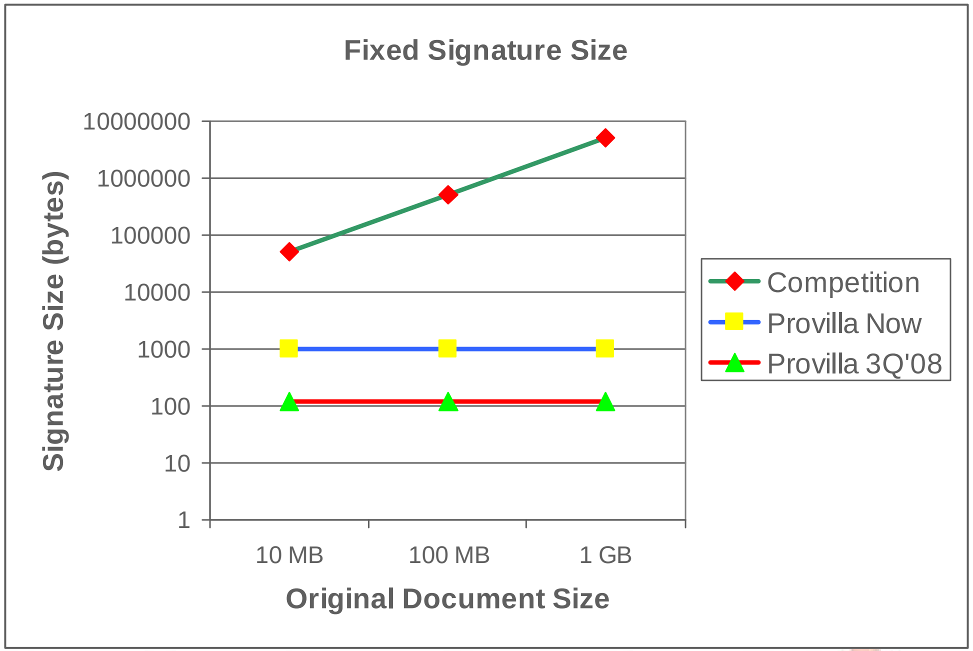
- Fast and light

Performance/ Footprint	Provilla A/L Agent
CPU cycles	2.54% (1/2)
Run-time Memory	8,280K (1/5)

- Fastest matching engine

Search	Provilla A/L Agent	Competition
Keywords: 1000	12.0 MB/s (10x)	1.3 MB/s
Entity –SSN, Phone, Date	190 MB/s (40x)	4.75 MB/s

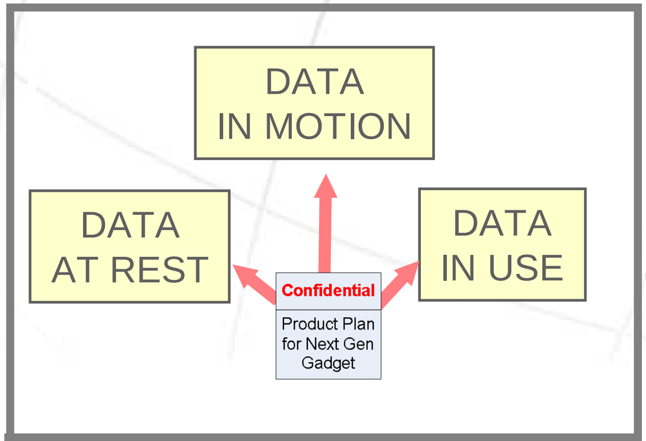
- Smallest signatures

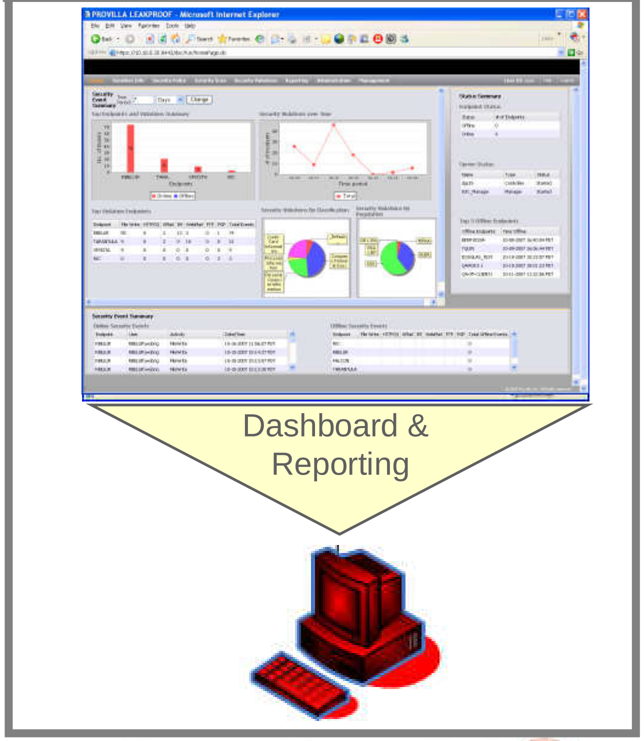

Fixed Signature Size

- Unobtrusive, Invisible
  - Not in task manager
  - Not in service list
  - Hidden files/directory

Enterprise Workflow & Policy

- Leak Protection Policies
  - Logging, alerting, blocking
  - Education, Encryption, Justification
  - By endpoint, user, or group
  - By data classification
    - HIPAA, Customer, SOX, SS#
  - Separate online and offline policies
- Inventory & Forensics
  - Discovery
    - By endpoint, group, policy
  - Investigate events, see actual sensitive content
- Scalability, Availability
  - Server clustering
  - Agent monitoring




PROVILLA LEAKPROOF - Microsoft Internet Explorer

LeakProof 3.0 Extends Endpoint Leadership

- Broadest DLP Threat Protection at the Endpoint
  - USB, Email (Outlook, Lotus Notes), Webmail (MSN, Yahoo, Gmail, AOL), IM (MSN, AIM, Yahoo), Network (HTTP/HTTPS, FTP, SMTP)…
  - New – Windows Vista / Office 2007, PrintScreen Blocking
- Interactive Employee Education & Workflow
  - Log, Block, Client Alert
  - New – Education: Custom messages and URL links
  - New – Encryption for USB copying
  - New – Justification
- Discovery of Sensitive Data
  - New – Stand-alone discovery/scan module
- Administrative Workflow
  - Enhanced – Dashboard, Policies, and Monitoring

Compelling Results

Sony Ericsson

OSH Complete Home & Garden

RFA

ISSI

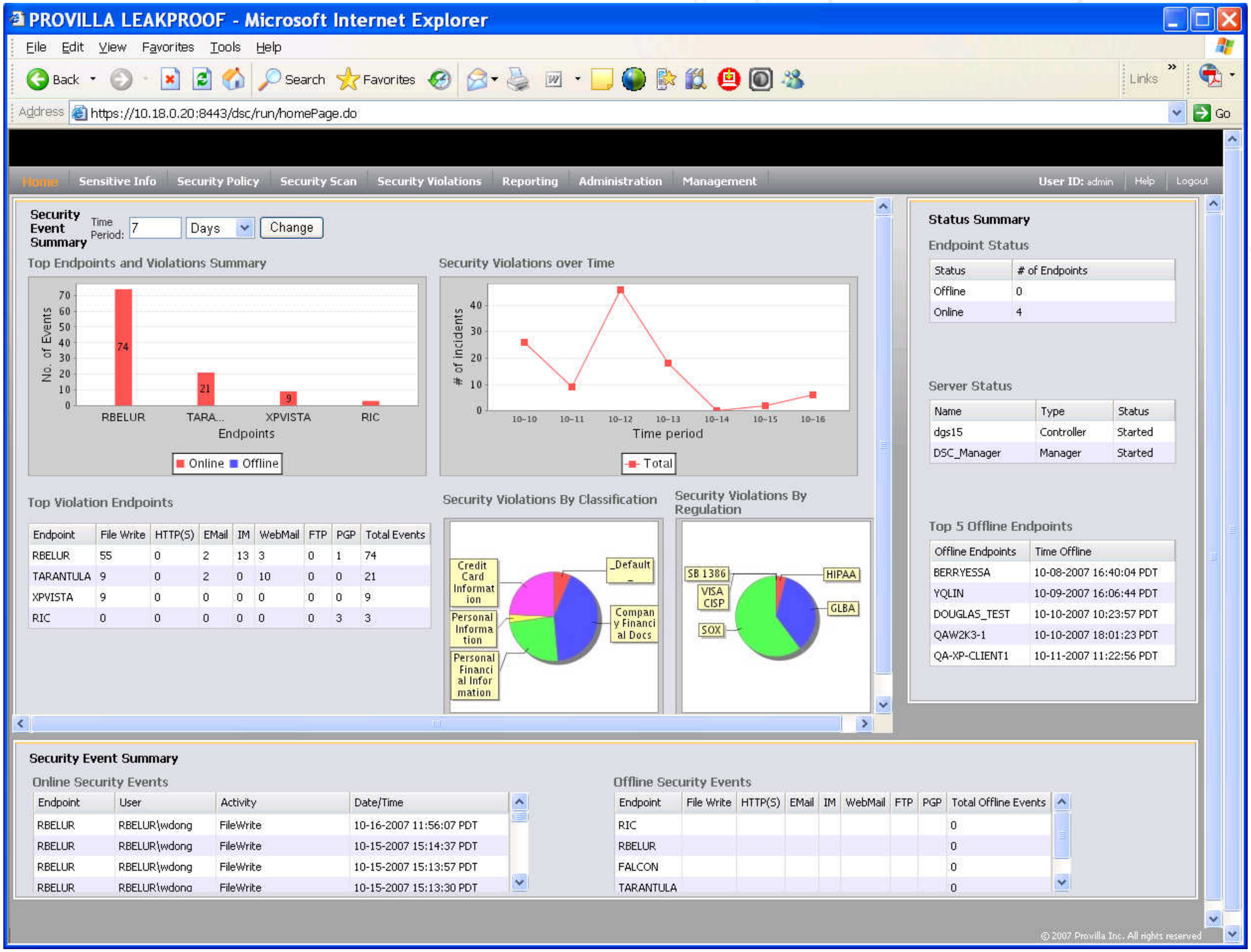
HMS•Holdings•Corp.

American Heritage FEDERAL CREDIT UNION

AFCO

- Sony Ericsson: Global mobile handset manufacturer
  - Over 100 security violation incidents in first 3 weeks
- ISSI: Technology manufacturer
  - Detected large number of file copies after employee resigned
- Leading financial services company
  - Protected customer privacy to address compliance regulations GLBA etc

New Dashboard and Workflow



Address: https://10.18.0.20:8443/dsc/run/homePage.do

User ID: admin

Security Event Summary Time Period: 7 Days

Top Endpoints and Violations Summary

Security Violations over Time

Top Violation Endpoints

Endpoint	File Write	HTTP(S)	EMail	IM	WebMail	FTP	PGP	Total Events
RBELUR	55	0	2	13	3	0	1	74
TARANTULA	9	0	2	0	10	0	0	21
XPVISTA	9	0	0	0	0	0	0	9
RIC	0	0	0	0	0	0	3	3

Security Violations By Classification

Security Violations By Regulation

Status Summary

Endpoint Status

Status	# of Endpoints
Offline	0
Online	4

Server Status

Name	Type	Status
dgs15	Controller	Started
DSC_Manager	Manager	Started

Top 5 Offline Endpoints

Offline Endpoints	Time Offline
BERRYESSA	10-08-2007 16:40:04 PDT
YQLIN	10-09-2007 16:06:44 PDT
DOUGLAS_TEST	10-10-2007 10:23:57 PDT
QAW2K3-1	10-10-2007 18:01:23 PDT
QA-XP-CLIENT1	10-11-2007 11:22:56 PDT

Security Event Summary

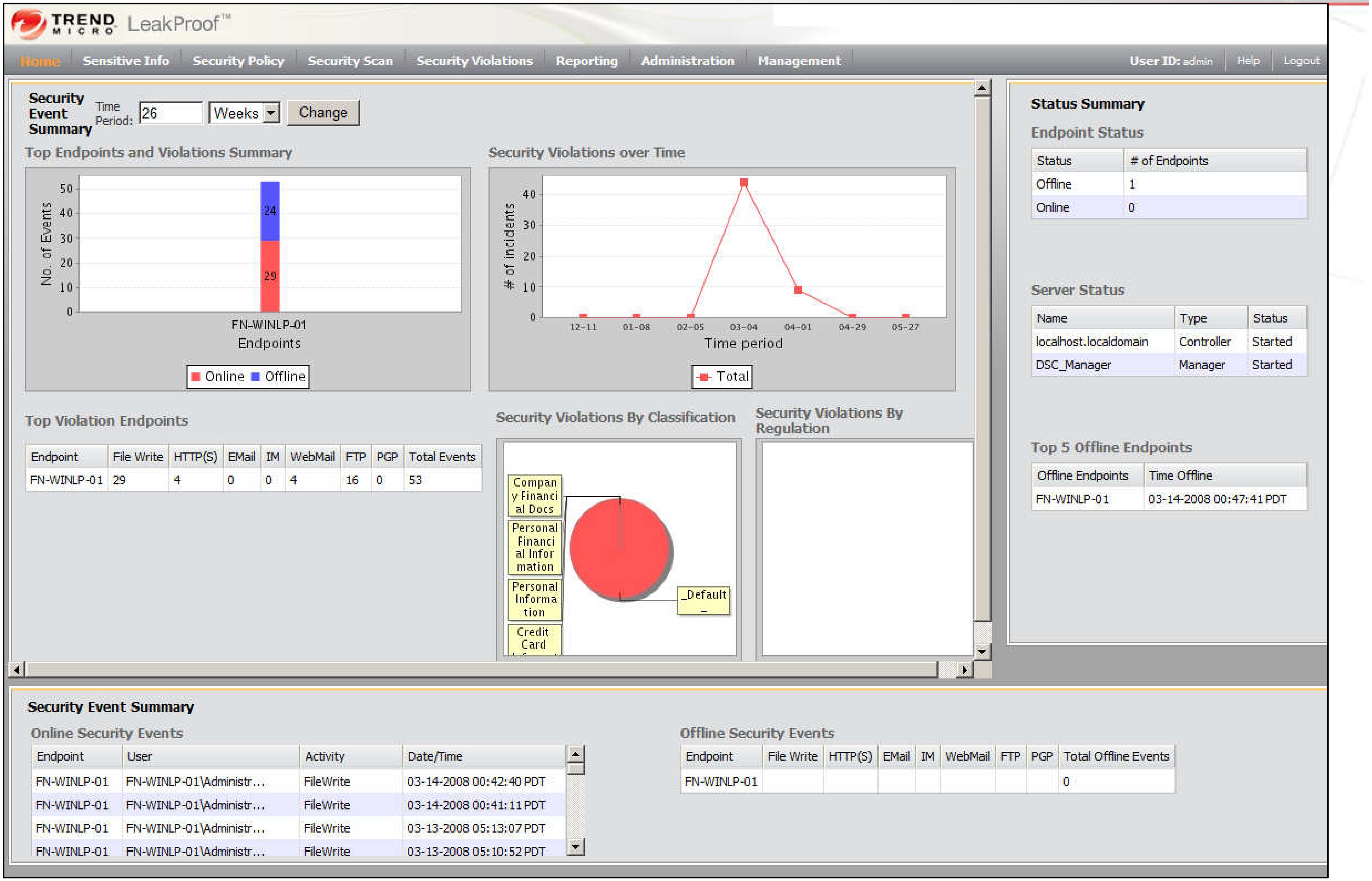
Online Security Events

Endpoint	User	Activity	Date/Time
RBELUR	RBELUR\wdong	FileWrite	10-16-2007 11:56:07 PDT
RBELUR	RBELUR\wdong	FileWrite	10-15-2007 15:14:37 PDT
RBELUR	RBELUR\wdong	FileWrite	10-15-2007 15:13:57 PDT
RBELUR	RBELUR\wdong	FileWrite	10-15-2007 15:13:30 PDT

Offline Security Events

Endpoint	File Write	HTTP(S)	EMail	IM	WebMail	FTP	PGP	Total Offline Events
RIC								0
RBELUR								0
FALCON								0
TARANTULA								0

LeakProof Management – Summary



Security Event Summary Time Period: 26 Weeks

Top Violation Endpoints

Endpoint	File Write	HTTP(S)	EMail	IM	WebMail	FTP	PGP	Total Events
FN-WINLP-01	29	4	0	0	4	16	0	53

Status Summary

Endpoint Status

Status	# of Endpoints
Offline	1
Online	0

Server Status

Name	Type	Status
localhost.localdomain	Controller	Started
DSC_Manager	Manager	Started

Top 5 Offline Endpoints

Offline Endpoints	Time Offline
FN-WINLP-01	03-14-2008 00:47:41 PDT

Security Event Summary

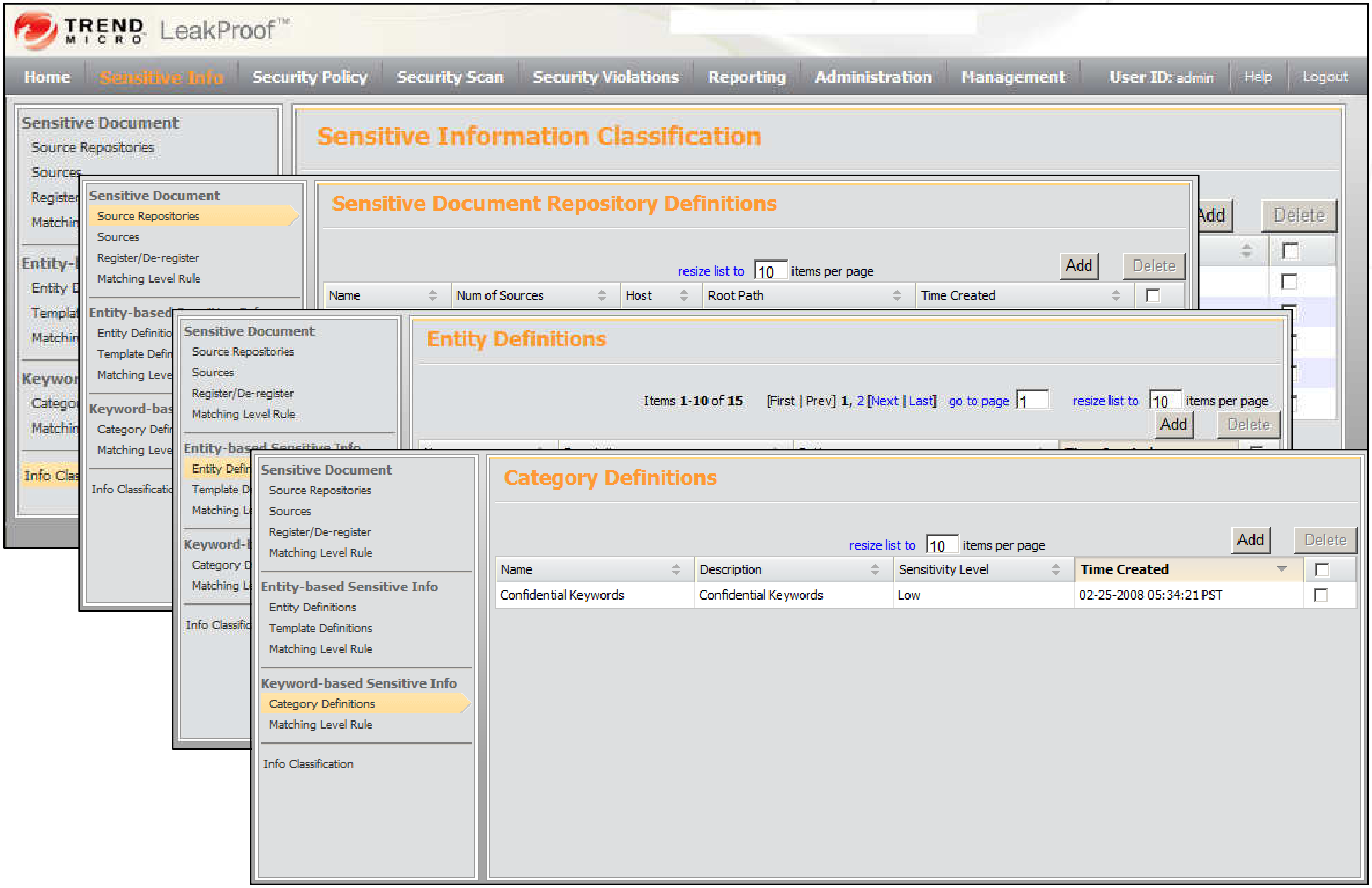
Online Security Events

Endpoint	User	Activity	Date/Time
FN-WINLP-01	FN-WINLP-01\Administr...	FileWrite	03-14-2008 00:42:40 PDT
FN-WINLP-01	FN-WINLP-01\Administr...	FileWrite	03-14-2008 00:41:11 PDT
FN-WINLP-01	FN-WINLP-01\Administr...	FileWrite	03-13-2008 05:13:07 PDT
FN-WINLP-01	FN-WINLP-01\Administr...	FileWrite	03-13-2008 05:10:52 PDT

Offline Security Events

Endpoint	File Write	HTTP(S)	EMail	IM	WebMail	FTP	PGP	Total Offline Events
FN-WINLP-01								0

LeakProof Management – Sensitive Info



Sensitive Information Classification

Sensitive Document Repository Definitions

resize list to 10 items per page

Name	Num of Sources	Host	Root Path	Time Created	□

Entity Definitions

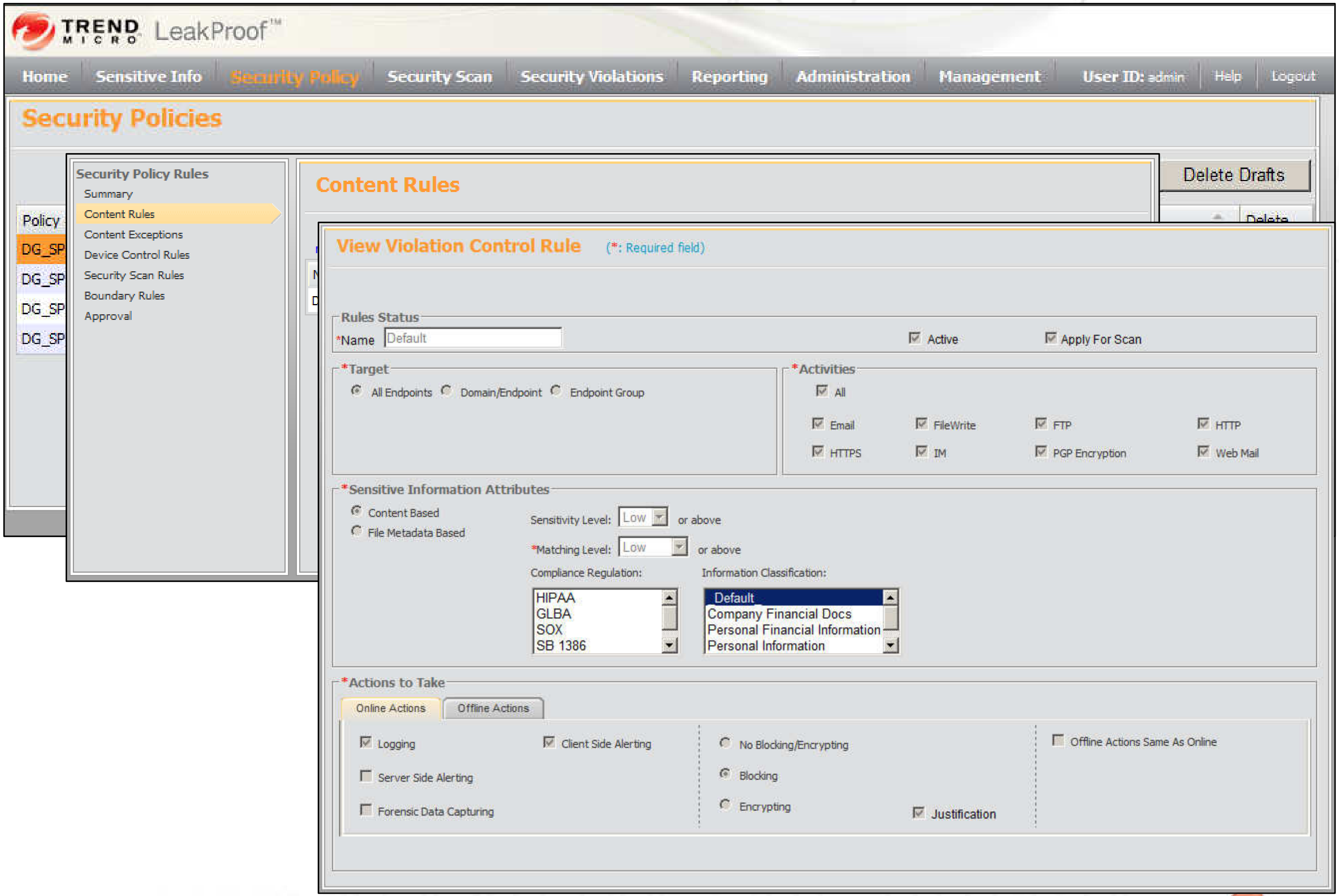
Items **1-10** of **15** [First | Prev] **1**, 2 [Next | Last] go to page 1 resize list to 10 items per page

Category Definitions

resize list to 10 items per page

Name	Description	Sensitivity Level	**Time Created**	□
Confidential Keywords	Confidential Keywords	Low	02-25-2008 05:34:21 PST	□

LeakProof Management – Security Policy



View Violation Control Rule (*: Required field)

Rules Status

*Name: Default ☑ Active ☑ Apply For Scan

*Target

● All Endpoints ○ Domain/Endpoint ○ Endpoint Group

*Activities

☑ All

☑ Email ☑ FileWrite ☑ FTP ☑ HTTP

☑ HTTPS ☑ IM ☑ PGP Encryption ☑ Web Mail

*Sensitive Information Attributes

● Content Based

○ File Metadata Based

Sensitivity Level: Low or above

*Matching Level: Low or above

Compliance Regulation:
HIPAA
GLBA
SOX
SB 1386

Information Classification:
Default
Company Financial Docs
Personal Financial Information
Personal Information

*Actions to Take

Online Actions | Offline Actions

☑ Logging ☑ Client Side Alerting

☐ Server Side Alerting

☐ Forensic Data Capturing

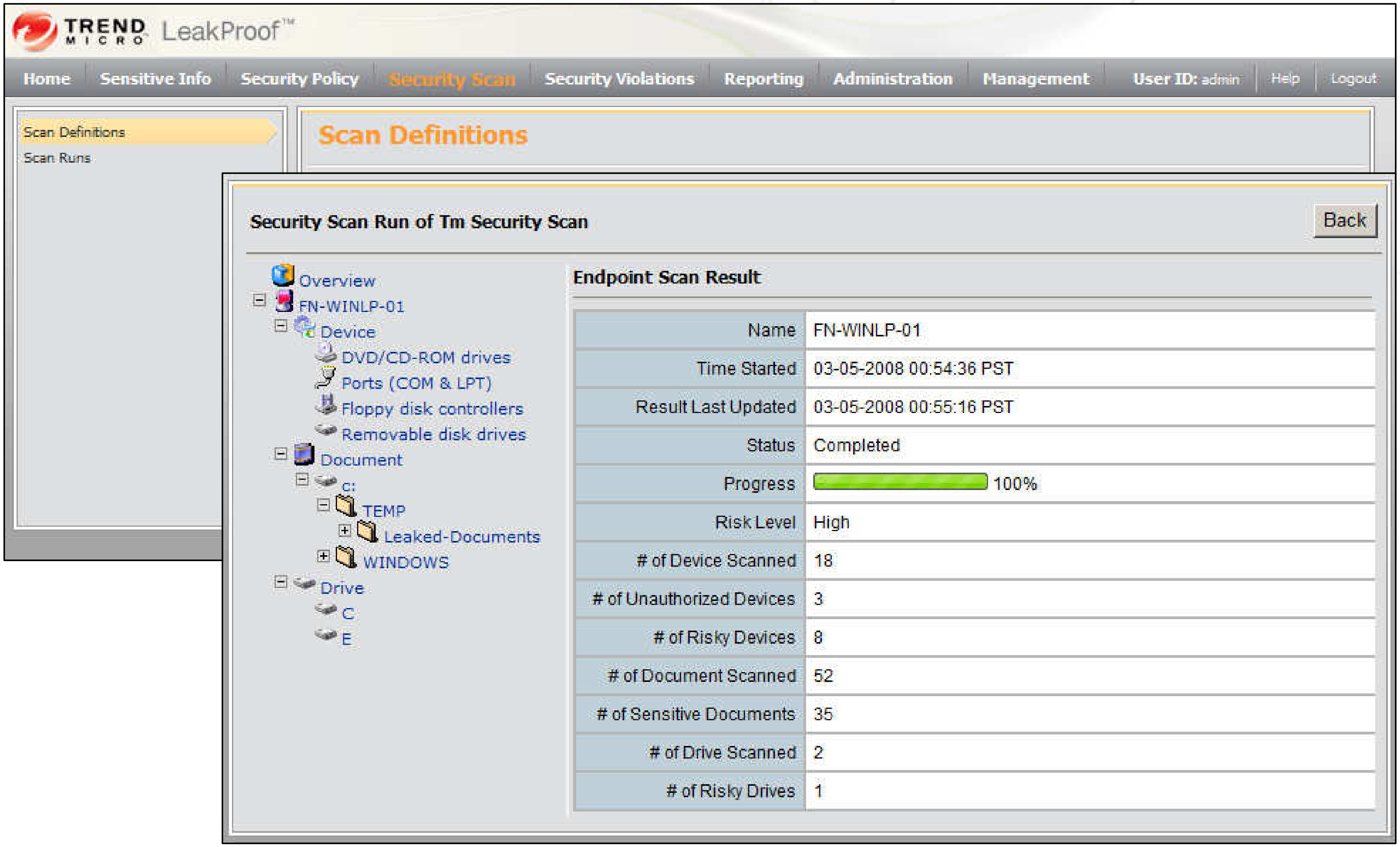
○ No Blocking/Encrypting

● Blocking

○ Encrypting ☑ Justification

☐ Offline Actions Same As Online

LeakProof Management – Security Scan

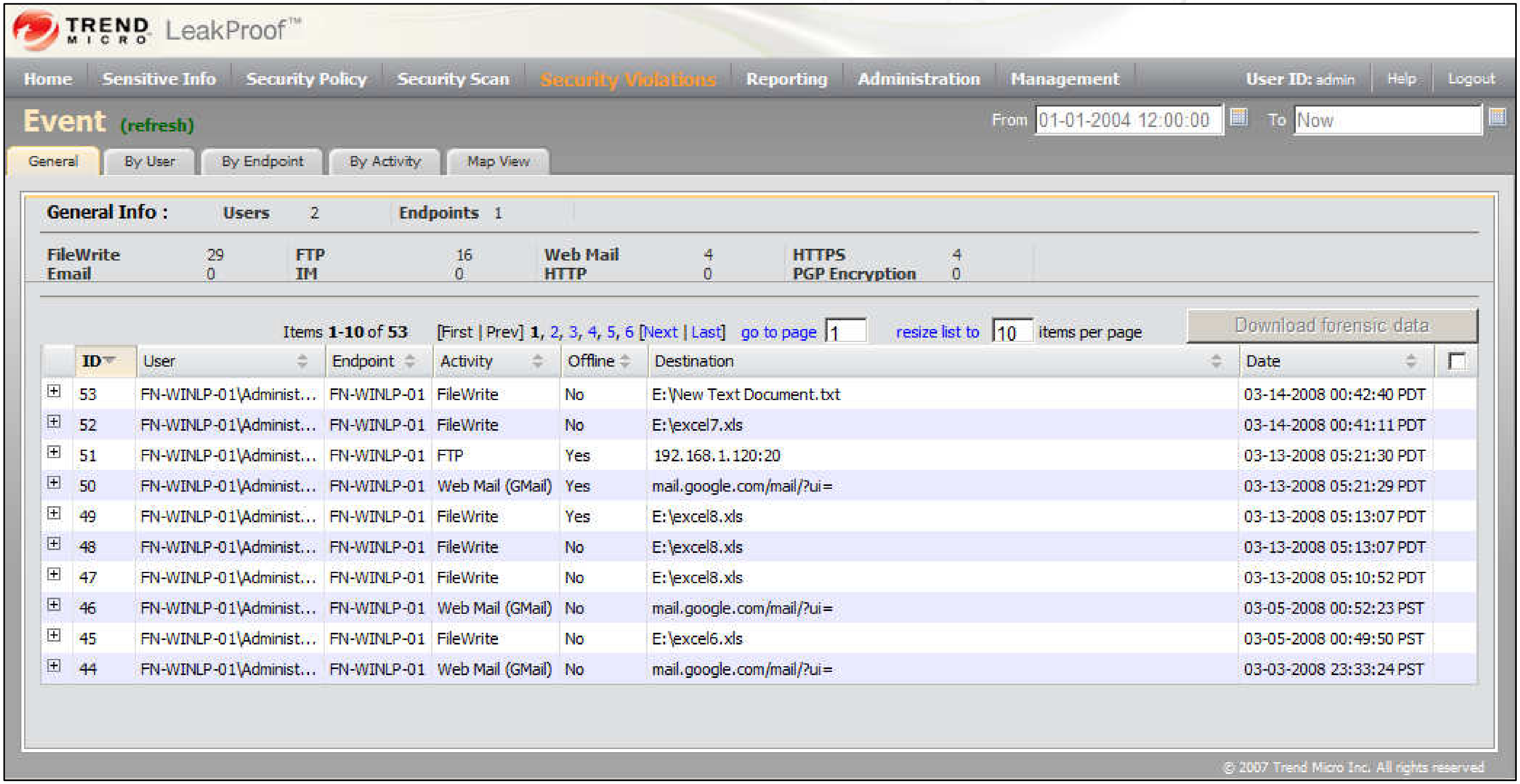


Security Scan Run of Tm Security Scan

Endpoint Scan Result

Name	FN-WINLP-01
Time Started	03-05-2008 00:54:36 PST
Result Last Updated	03-05-2008 00:55:16 PST
Status	Completed
Progress	100%
Risk Level	High
# of Device Scanned	18
# of Unauthorized Devices	3
# of Risky Devices	8
# of Document Scanned	52
# of Sensitive Documents	35
# of Drive Scanned	2
# of Risky Drives	1

LeakProof Management – Security Violations



Event (refresh)

From 01-01-2004 12:00:00 To Now

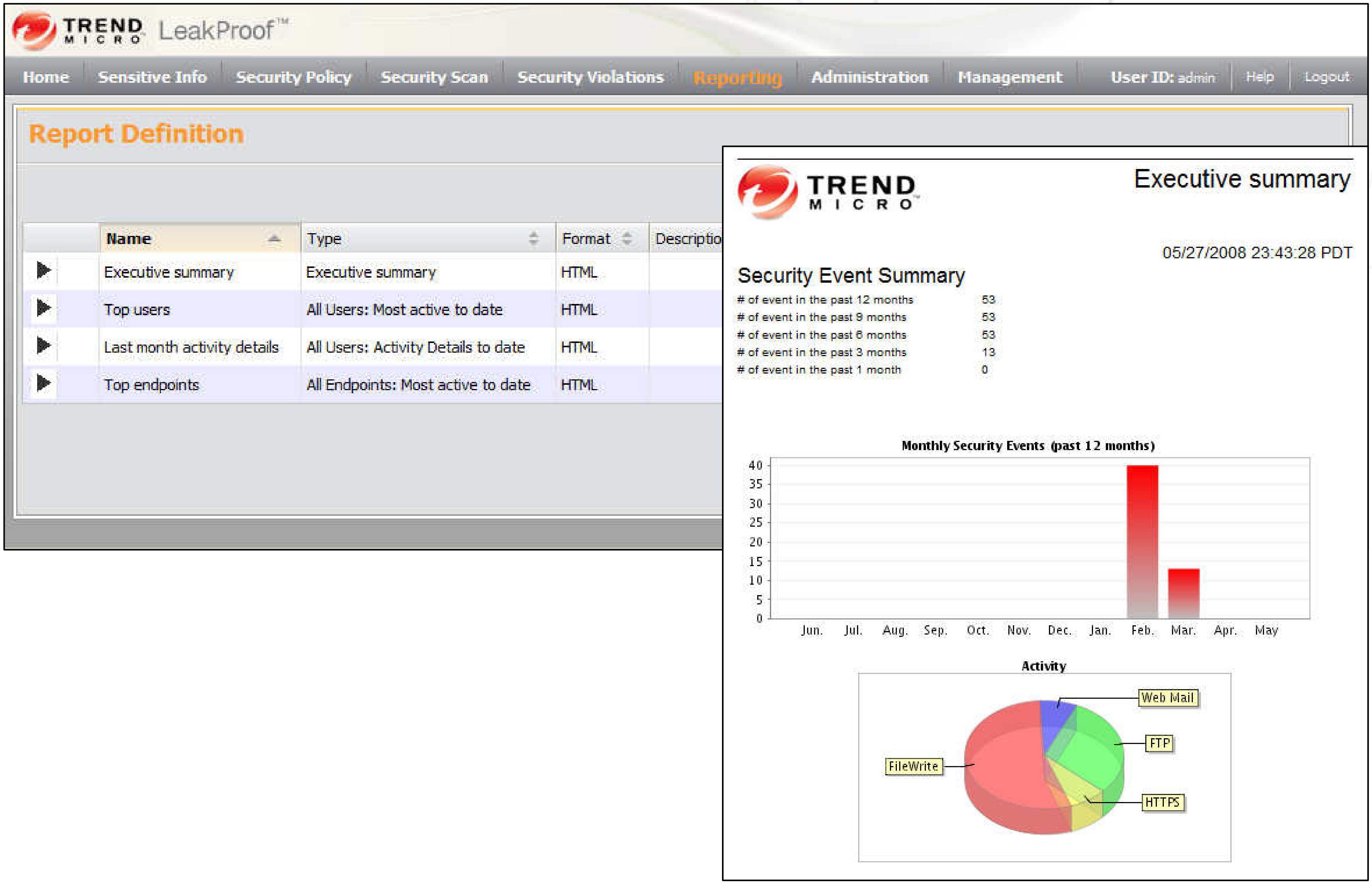
General Info : **Users** 2 **Endpoints** 1

FileWrite	29	**FTP**	16	**Web Mail**	4	**HTTPS**	4
Email	0	**IM**	0	**HTTP**	0	**PGP Encryption**	0

Items **1-10** of **53** [First | Prev] **1**, 2, 3, 4, 5, 6 [Next | Last] go to page 1 resize list to 10 items per page

	ID	User	Endpoint	Activity	Offline	Destination	Date	□
⊞	53	FN-WINLP-01\Administ...	FN-WINLP-01	FileWrite	No	E:\New Text Document.txt	03-14-2008 00:42:40 PDT	
⊞	52	FN-WINLP-01\Administ...	FN-WINLP-01	FileWrite	No	E:\excel7.xls	03-14-2008 00:41:11 PDT	
⊞	51	FN-WINLP-01\Administ...	FN-WINLP-01	FTP	Yes	192.168.1.120:20	03-13-2008 05:21:30 PDT	
⊞	50	FN-WINLP-01\Administ...	FN-WINLP-01	Web Mail (GMail)	Yes	mail.google.com/mail/?ui=	03-13-2008 05:21:29 PDT	
⊞	49	FN-WINLP-01\Administ...	FN-WINLP-01	FileWrite	Yes	E:\excel8.xls	03-13-2008 05:13:07 PDT	
⊞	48	FN-WINLP-01\Administ...	FN-WINLP-01	FileWrite	No	E:\excel8.xls	03-13-2008 05:13:07 PDT	
⊞	47	FN-WINLP-01\Administ...	FN-WINLP-01	FileWrite	No	E:\excel8.xls	03-13-2008 05:10:52 PDT	
⊞	46	FN-WINLP-01\Administ...	FN-WINLP-01	Web Mail (GMail)	No	mail.google.com/mail/?ui=	03-05-2008 00:52:23 PST	
⊞	45	FN-WINLP-01\Administ...	FN-WINLP-01	FileWrite	No	E:\excel6.xls	03-05-2008 00:49:50 PST	
⊞	44	FN-WINLP-01\Administ...	FN-WINLP-01	Web Mail (GMail)	No	mail.google.com/mail/?ui=	03-03-2008 23:33:24 PST	

LeakProof Management – Reporting



Report Definition

	Name	Type	Format	Descriptio
▶	Executive summary	Executive summary	HTML	
▶	Top users	All Users: Most active to date	HTML	
▶	Last month activity details	All Users: Activity Details to date	HTML	
▶	Top endpoints	All Endpoints: Most active to date	HTML	

TREND MICRO

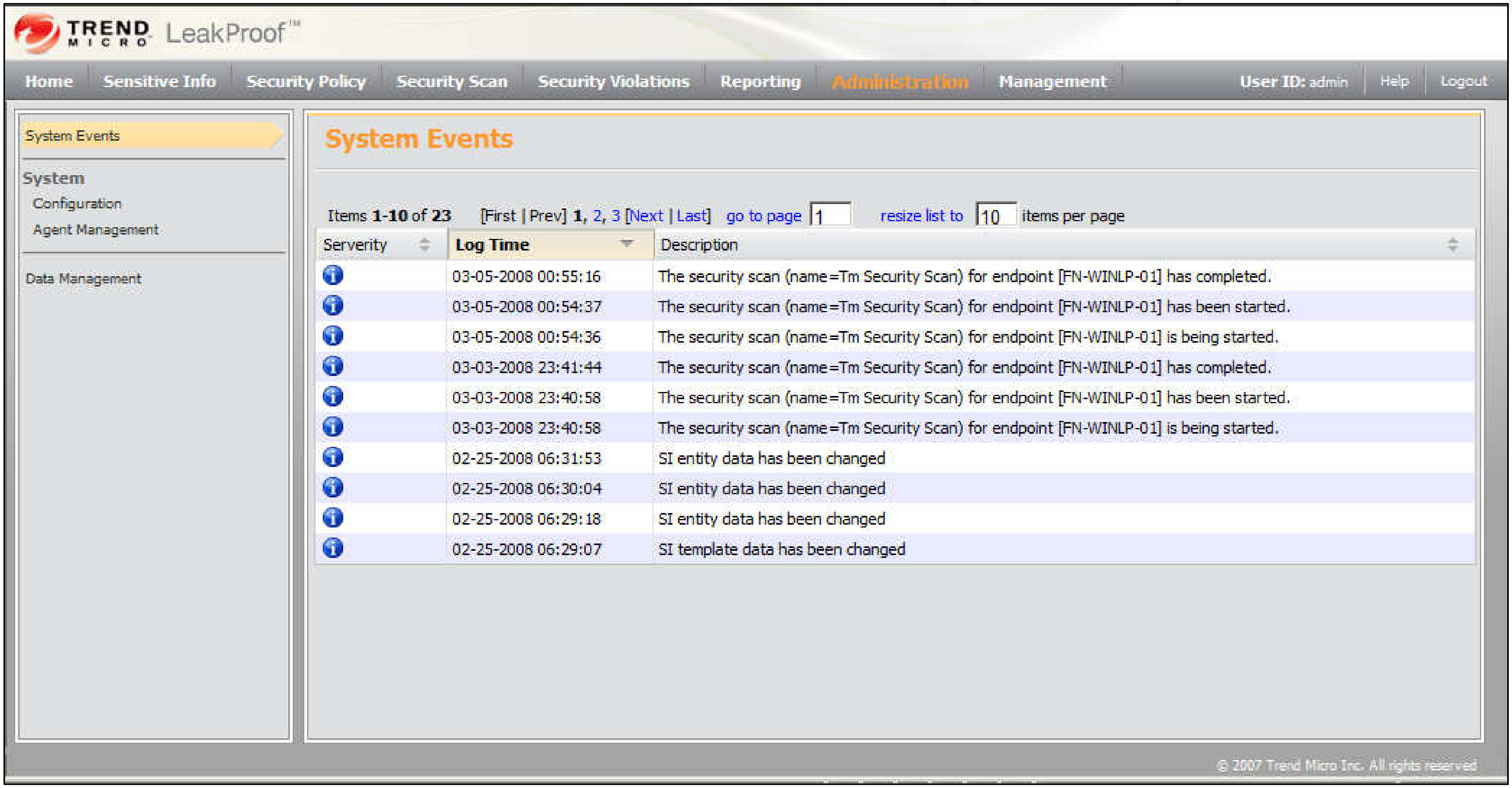
Executive summary

05/27/2008 23:43:28 PDT

Security Event Summary

# of event in the past 12 months	53
# of event in the past 9 months	53
# of event in the past 6 months	53
# of event in the past 3 months	13
# of event in the past 1 month	0

LeakProof Management – Administration

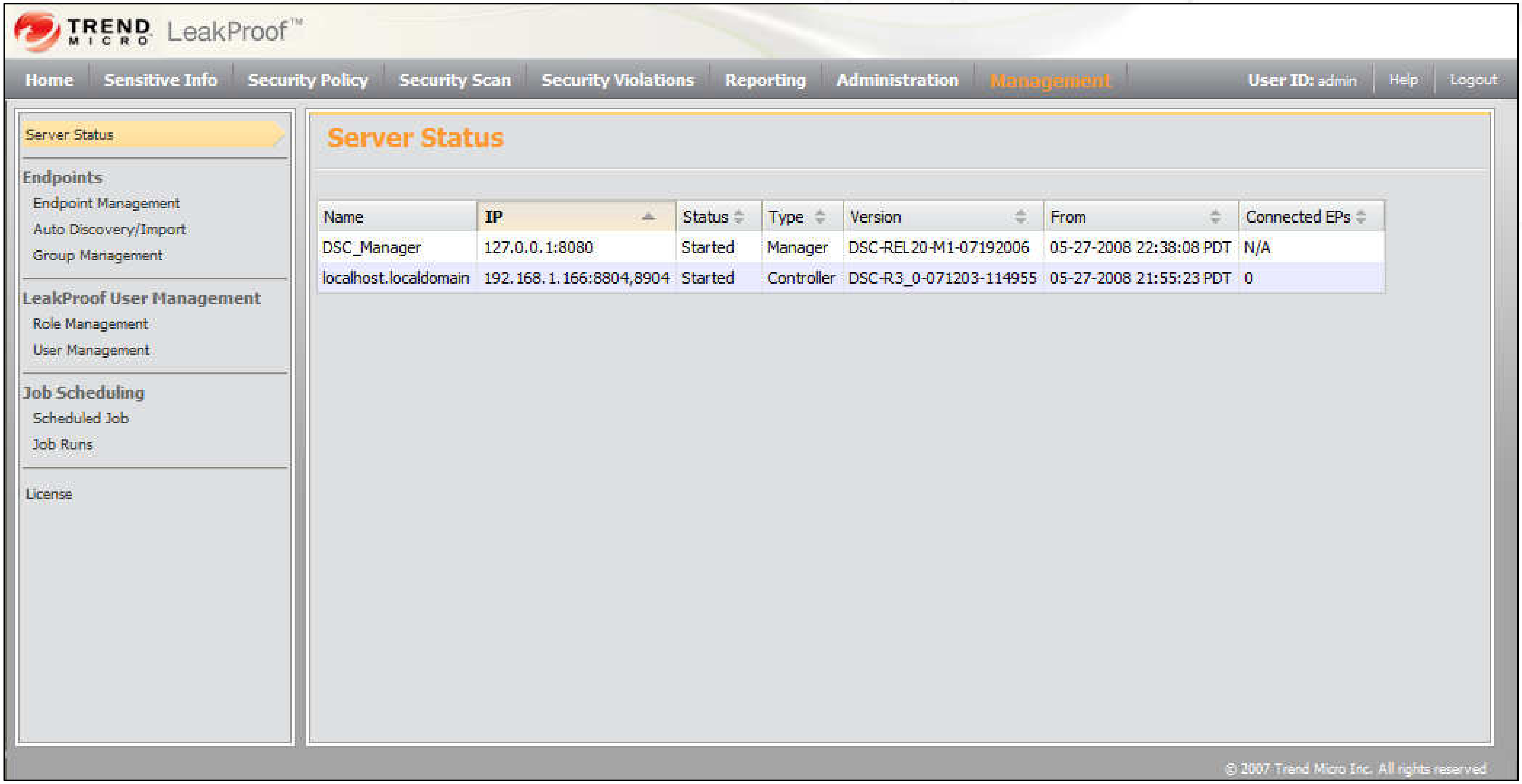


System Events

Items **1-10** of **23** [First | Prev] **1**, 2, 3 [Next | Last] go to page 1 resize list to 10 items per page

Serverity	Log Time	Description
ℹ	03-05-2008 00:55:16	The security scan (name=Tm Security Scan) for endpoint [FN-WINLP-01] has completed.
ℹ	03-05-2008 00:54:37	The security scan (name=Tm Security Scan) for endpoint [FN-WINLP-01] has been started.
ℹ	03-05-2008 00:54:36	The security scan (name=Tm Security Scan) for endpoint [FN-WINLP-01] is being started.
ℹ	03-03-2008 23:41:44	The security scan (name=Tm Security Scan) for endpoint [FN-WINLP-01] has completed.
ℹ	03-03-2008 23:40:58	The security scan (name=Tm Security Scan) for endpoint [FN-WINLP-01] has been started.
ℹ	03-03-2008 23:40:58	The security scan (name=Tm Security Scan) for endpoint [FN-WINLP-01] is being started.
ℹ	02-25-2008 06:31:53	SI entity data has been changed
ℹ	02-25-2008 06:30:04	SI entity data has been changed
ℹ	02-25-2008 06:29:18	SI entity data has been changed
ℹ	02-25-2008 06:29:07	SI template data has been changed

LeakProof Management – Management

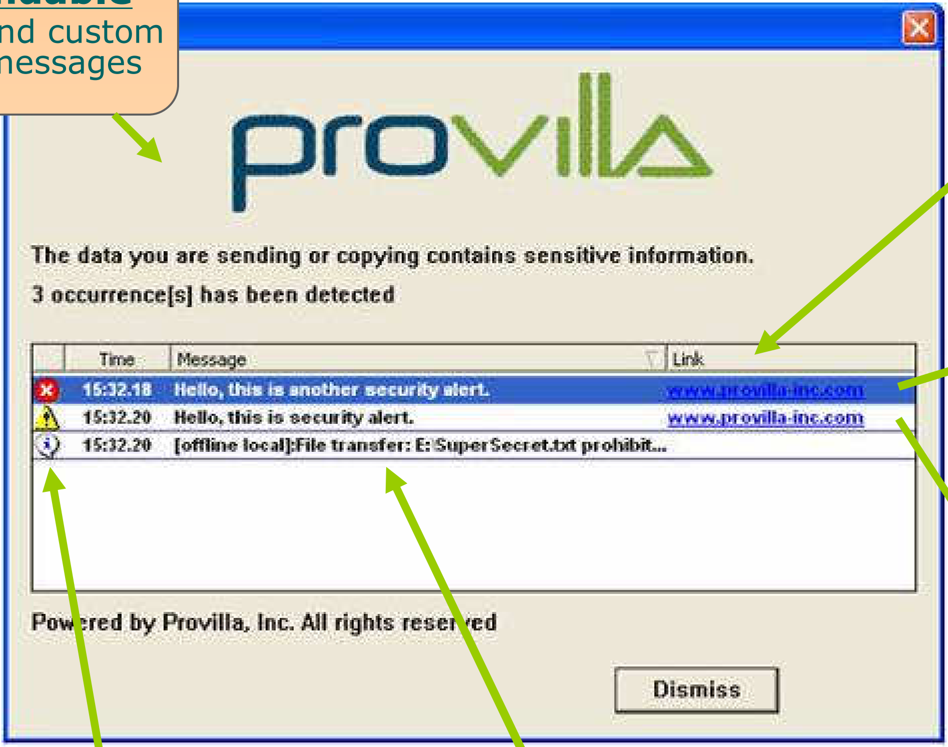


Server Status

Name	IP	Status	Type	Version	From	Connected EPs
DSC_Manager	127.0.0.1:8080	Started	Manager	DSC-REL20-M1-07192006	05-27-2008 22:38:08 PDT	N/A
localhost.localdomain	192.168.1.166:8804,8904	Started	Controller	DSC-R3_0-071203-114955	05-27-2008 21:55:23 PDT	0

LeakProof Client – Summary

Brandable
Logo and custom messages



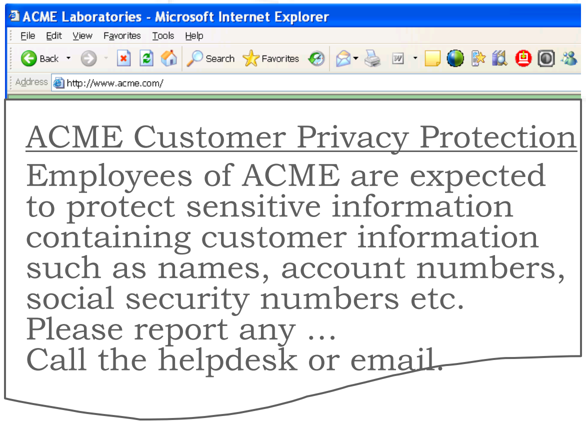
The data you are sending or copying contains sensitive information.

3 occurrence[s] has been detected

	Time	Message	Link
✖	15:32.18	Hello, this is another security alert.	www.provilla-inc.com
⚠	15:32.20	Hello, this is security alert.	www.provilla-inc.com
ℹ	15:32.20	[offline local]:File transfer: E:SuperSecret.txt prohibit...	

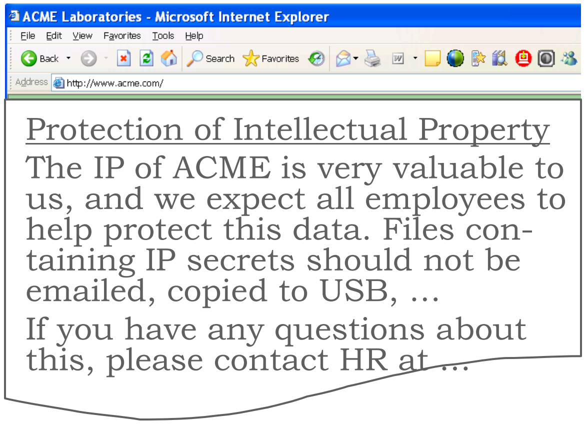
Powered by Provilla, Inc. All rights reserved

Custom Links
Company Policies


ACME Laboratories - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.acme.com/

ACME Customer Privacy Protection

Employees of ACME are expected to protect sensitive information containing customer information such as names, account numbers, social security numbers etc.
Please report any …
Call the helpdesk or email.


ACME Laboratories - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.acme.com/

Protection of Intellectual Property

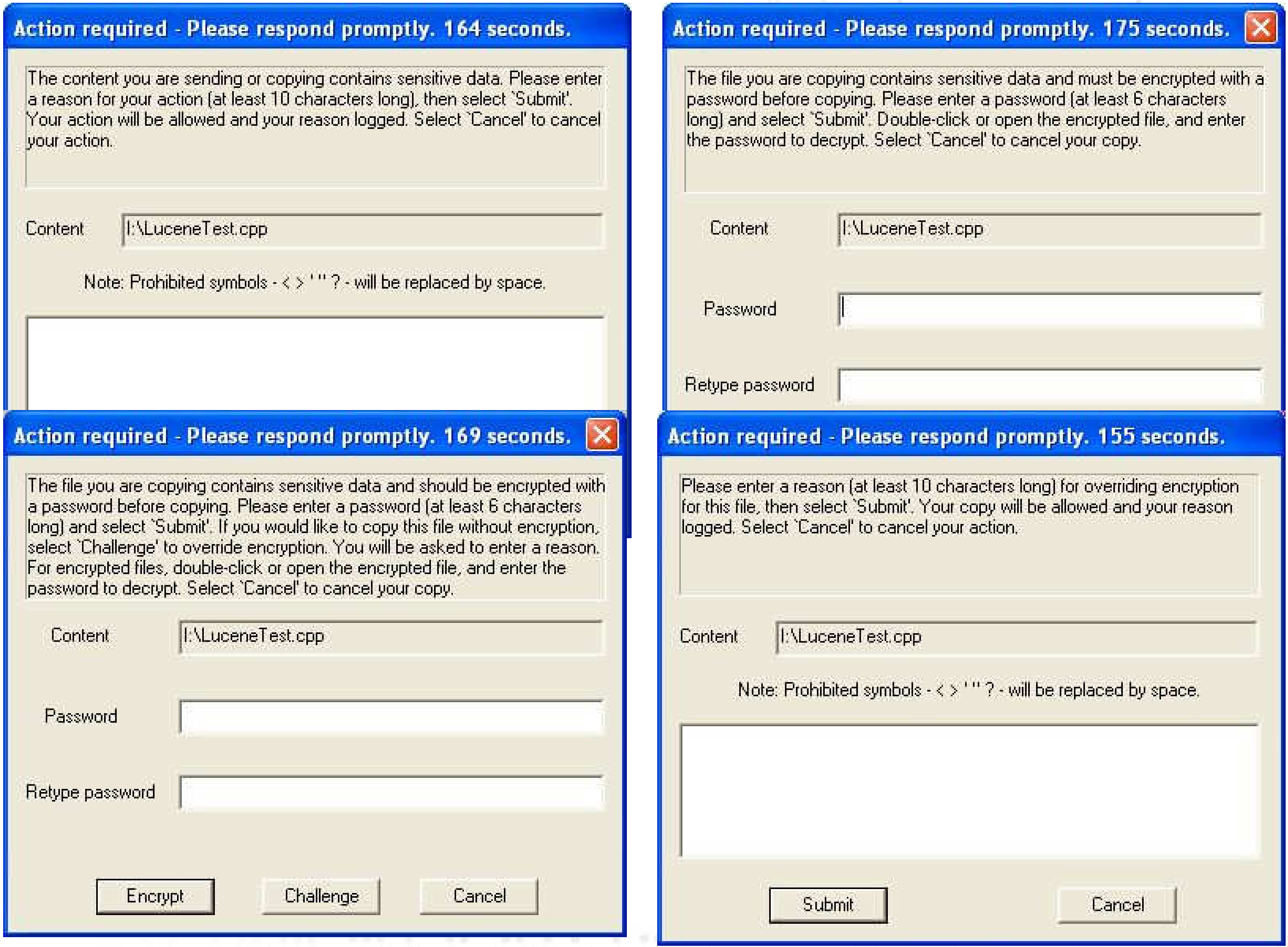
The IP of ACME is very valuable to us, and we expect all employees to help protect this data. Files containing IP secrets should not be emailed, copied to USB, …

If you have any questions about this, please contact HR at …

Severity:
Blocked,
Warn & Log,
Info only

Custom Alert Messages
File {name} contains {class} data and should not be sent via {channel}

LeakProof Client – Employee Education



Action required - Please respond promptly. 164 seconds.

The content you are sending or copying contains sensitive data. Please enter a reason for your action (at least 10 characters long), then select `Submit'. Your action will be allowed and your reason logged. Select `Cancel' to cancel your action.

Content: I:\LuceneTest.cpp

Note: Prohibited symbols - < > ' " ? - will be replaced by space.

Action required - Please respond promptly. 175 seconds.

The file you are copying contains sensitive data and must be encrypted with a password before copying. Please enter a password (at least 6 characters long) and select `Submit'. Double-click or open the encrypted file, and enter the password to decrypt. Select `Cancel' to cancel your copy.

Content: I:\LuceneTest.cpp

Password:

Retype password:

Action required - Please respond promptly. 169 seconds.

The file you are copying contains sensitive data and should be encrypted with a password before copying. Please enter a password (at least 6 characters long) and select `Submit'. If you would like to copy this file without encryption, select `Challenge' to override encryption. You will be asked to enter a reason. For encrypted files, double-click or open the encrypted file, and enter the password to decrypt. Select `Cancel' to cancel your copy.

Content: I:\LuceneTest.cpp

Password:

Retype password:

Action required - Please respond promptly. 155 seconds.

Please enter a reason (at least 10 characters long) for overriding encryption for this file, then select `Submit'. Your copy will be allowed and your reason logged. Select `Cancel' to cancel your action.

Content: I:\LuceneTest.cpp

Note: Prohibited symbols - < > ' " ? - will be replaced by space.

Trend Micro LeakProof 3.0

- Trend Micro LeakProof™ prevents enterprise data leaks with a unique approach that combines endpoint-based enforcement with highly accurate fingerprinting and content matching technology.
- The LeakProof Anti-Leak Client communicates with the LeakProof DataDNA™ Server appliance for intelligent content filtering and security policy enforcement. Patent-pending technology detects sensitive data with real-time filtering. Powerful algorithms extract information from content to create a unique DNA sequence or "fingerprint" for each document that enables endpoint-based enforcement on or offline.
- A web-based interface supports administrative workflows for discovery, classification, policy setting, and reporting. Interactive alerts educate employees on the proper handling of confidential information. LeakProof supports regulatory compliance by protecting sensitive information and customer privacy.

Trend Micro | Securing Your Web World

Veli-Pekka Kusmin
Pre-Sales Engineer

Trend Micro Baltics & Finland
Pakkalakuja 7, 3rd floor
FI-01510 Vantaa
Finland

Telephone	+358 9 4730 8300
Direct	+358 9 4730 8302
Fax	+358 9 4730 8999
Mobile	+358 40 596 7181

veli-pekka_kusmin@trendmicro.com
http://fi.trendmicro-europe.com