Symantec™

San Francisco DLP User Group
- DLP Reporting Now and Future

July, 2012

Stefano Paoletti – DLP Product Management

Agenda for Today

Overview of DLP IT Analytics

DLP IT Analytics Demo

Discussion of Operational Reports

Q&A

Introduction

DLP Suite Reporting Overview

IT Analytics

- **Executive Reports**
  - DLP Program Evolution and Results
  - Audit Reports
  - Policy Management
- **Analytics**
  - Pivot tables
  - Drill downs
  - Indexing and Text Search

Enforce

- **Operational Reports**
  - Incident Remediation Reports
  - System Management Reports

Overview of DLP IT Analytics

Symantec Data Loss Prevention IT Analytics

What

Advanced reporting module with pre-calculated and summarized data pulled from DLP Oracle database

How

Runs on the Symantec Management Console

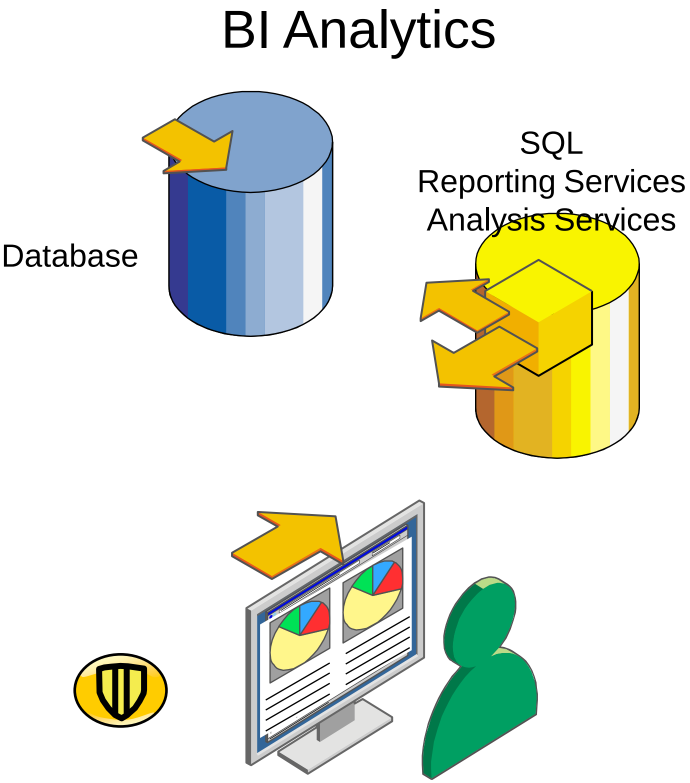
When

Available now via Symantec Installation Manager

Advantages

- High performance
- Wide range of DLP data
- Executive & Audit dashboards and reports
- Pivot table like report engine

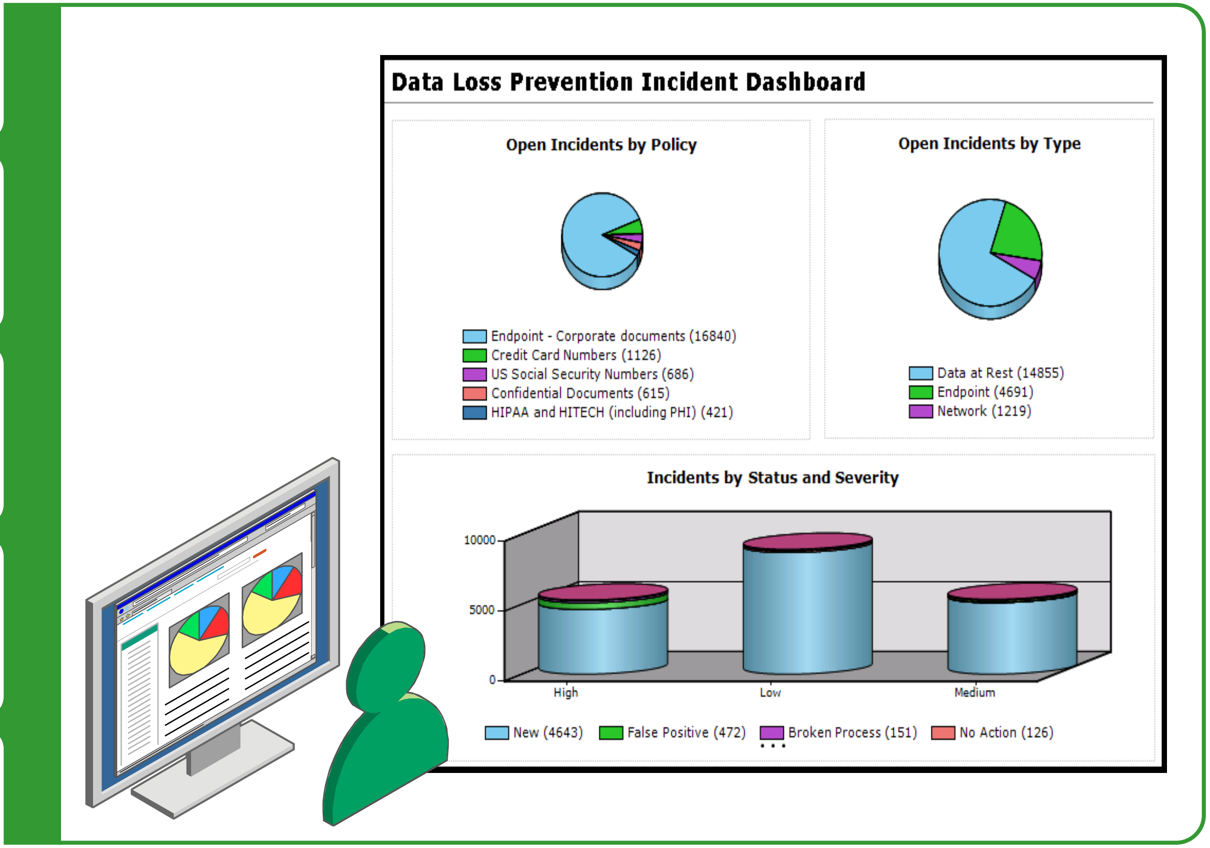
Application Reporting vs BI Analytics



- Data is pulled from Database and summarized the night before
- As the database becomes larger, report performance is not impacted
- Offers advanced reporting capabilities

DLP ITA Provides Advanced Reporting

- Graphical Dashboards
- Multiple level of data aggregation
- Customizable Pivot Table Reports
- Performance Indicators
- Cross Product Reporting


Data Loss Prevention Incident Dashboard
Open Incidents by Policy
Endpoint - Corporate documents (16840)
Credit Card Numbers (1126)
US Social Security Numbers (686)
Confidential Documents (615)
HIPAA and HITECH (including PHI) (421)
Open Incidents by Type
Data at Rest (14855)
Endpoint (4691)
Network (1219)
Incidents by Status and Severity
10000
5000
0
High
Low
Medium
New (4643)
False Positive (472)
Broken Process (151)
No Action (126)
...

DLP ITA Cubes

Executive & Audit Cubes

- DLP Administrative Events
- DLP Policy History
- DLP Incident History
- DLP Discover Scans
- DLP Agent Status
- DLP Messages

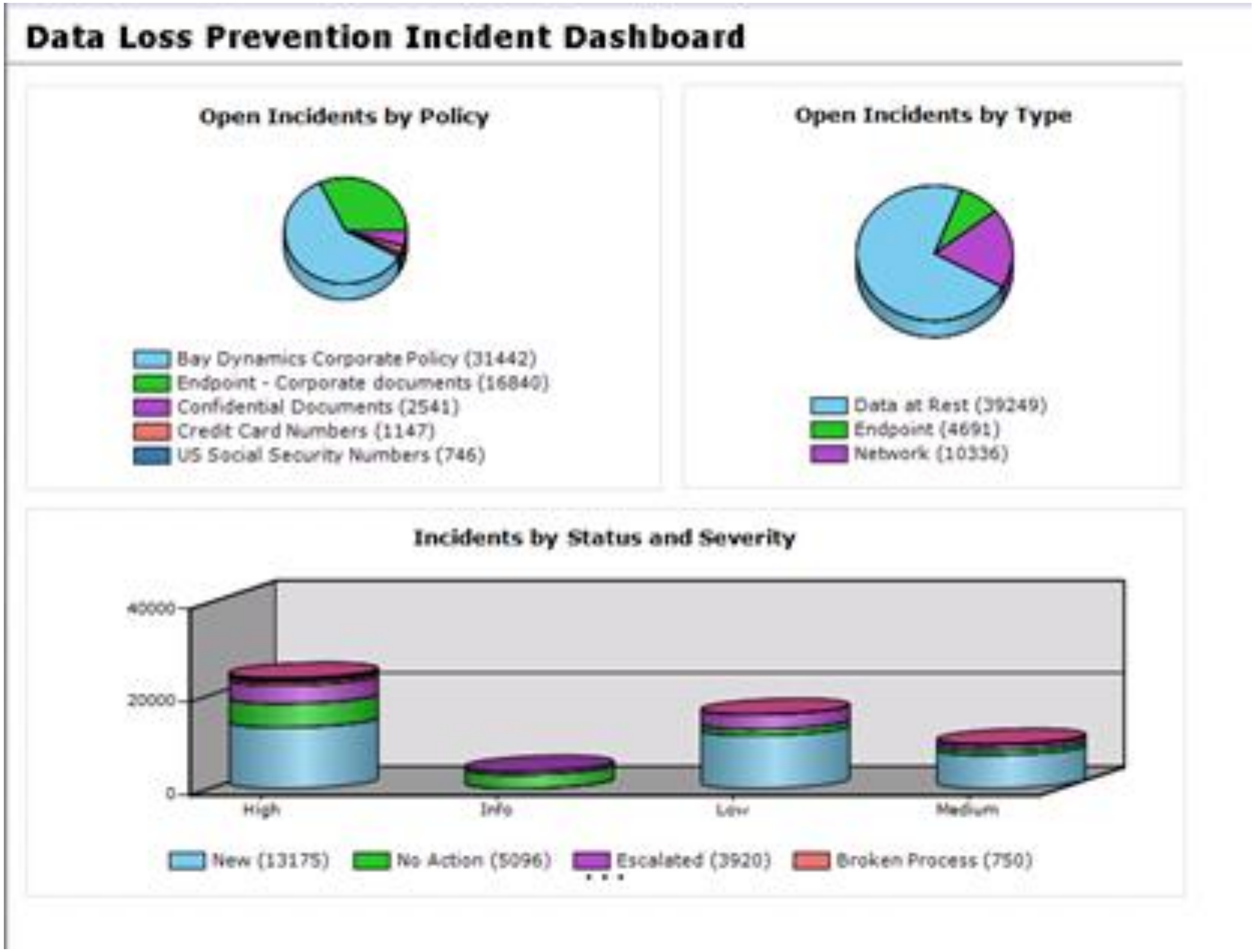
Operational Cubes

- DLP Incident Summary
- DLP Incident Details
- DLP Discover Incident Summary
- DLP Discover Incident Details
- DLP Endpoint Incident Summary
- DLP Endpoint Incident Details
- DLP Network Incident Summary
- DLP Network Incident Details

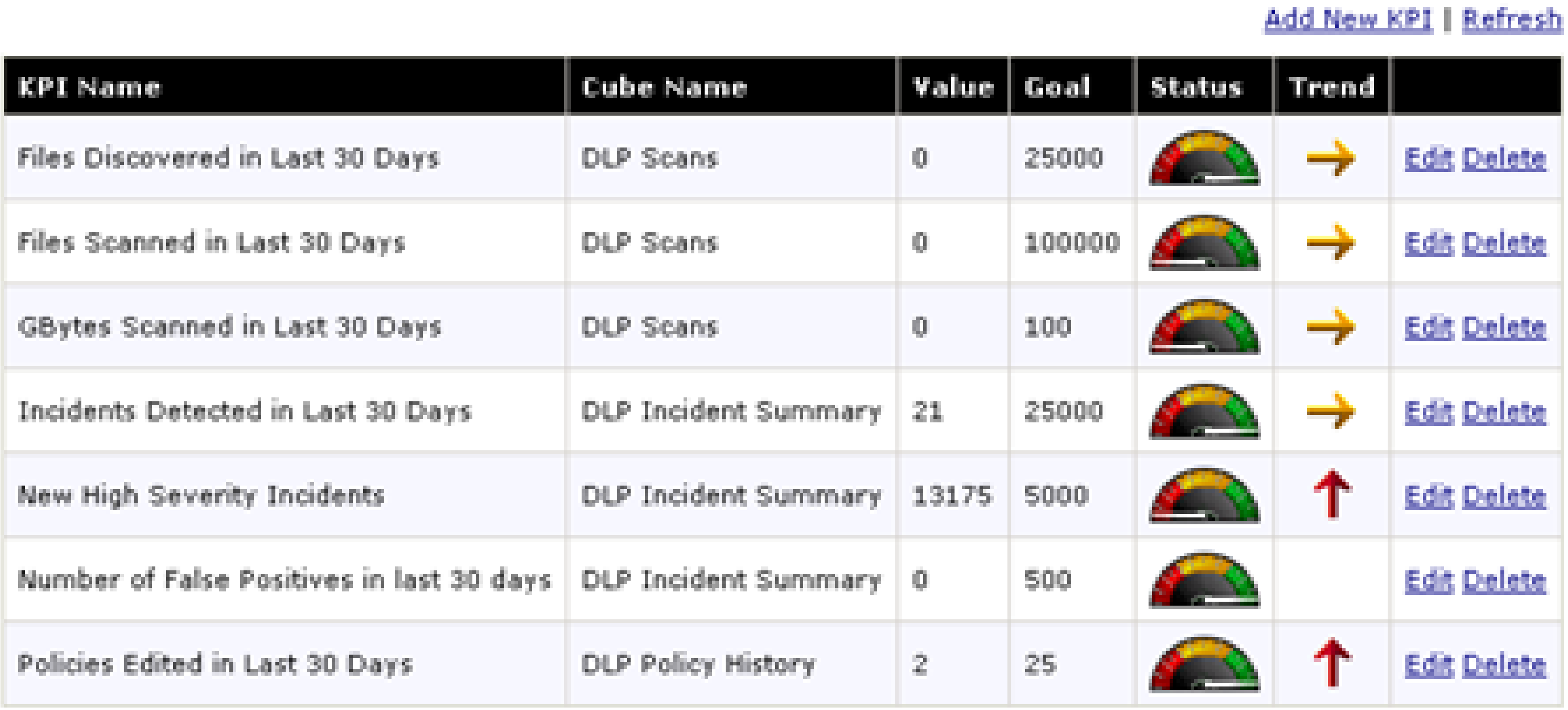
DLP ITA Answers Key Management Questions

- CISO: “Where is most of my data risk coming from?”
- DLP Program Mgr: “Am I meeting my goals?”
- Risk Mgr: “How are incidents trending?”
- Compliance Mgr: “Which policies are violated the most?”
- Legal Counsel: “Show all incidents that contain file xyz?”
- Auditor: “Was policy X active all of last year?”
- DLP Policy Manager: “When and how did policy Y change in the last 6 months?”

CISO: Where is most of my data risk coming from?


Data Loss Prevention Incident Dashboard
Open Incidents by Policy
Bay Dynamics Corporate Policy (31442)
Endpoint - Corporate documents (16840)
Confidential Documents (2541)
Credit Card Numbers (1147)
US Social Security Numbers (746)
Open Incidents by Type
Data at Rest (39249)
Endpoint (4691)
Network (10336)
Incidents by Status and Severity
40000
20000
0
High
Info
Low
Medium
New (13175)
No Action (5096)
Escalated (3920)
Broken Process (750)
. . .

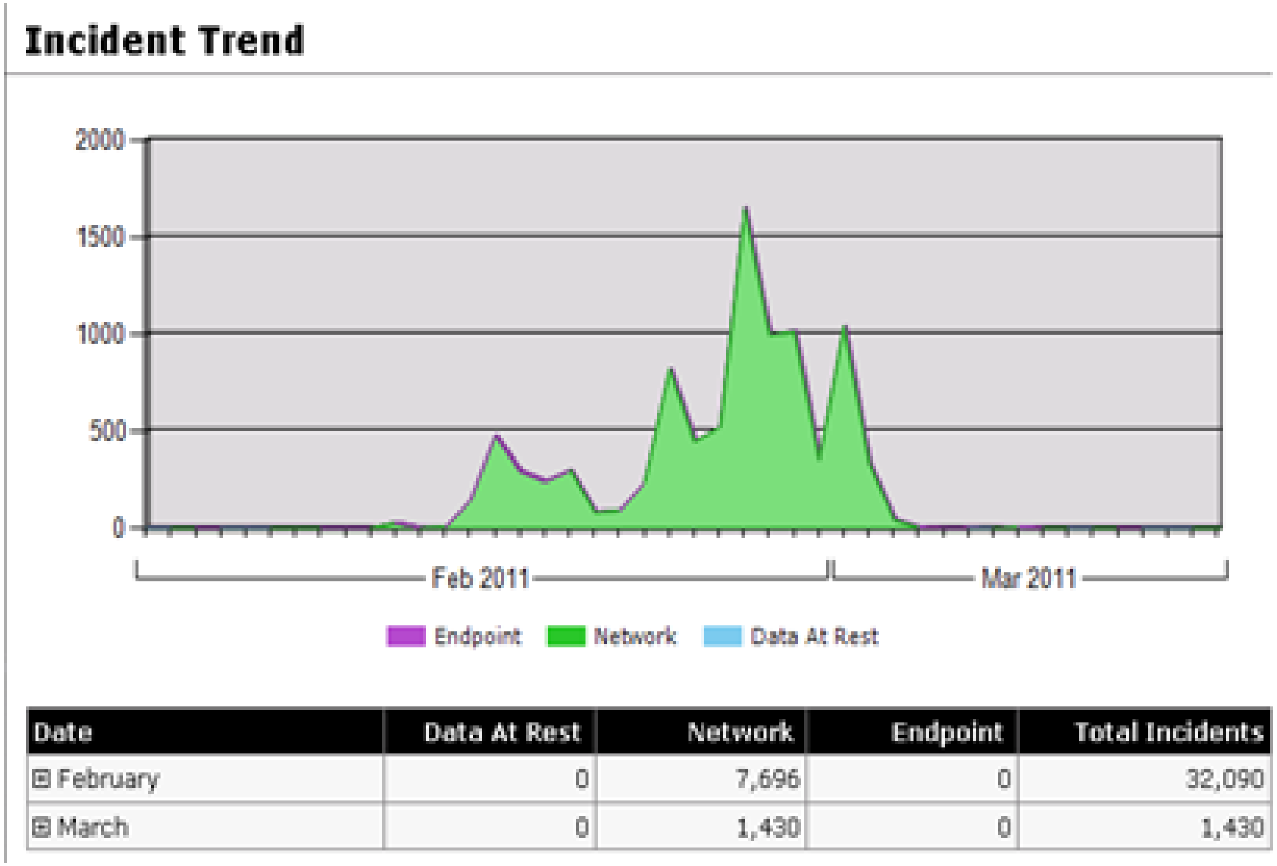
DLP Program Mgr: Am I meeting my goals?



Add New KPI | Refresh

KPI Name	Cube Name	Value	Goal	Status	Trend	
Files Discovered in Last 30 Days	DLP Scans	0	25000		→	Edit Delete
Files Scanned in Last 30 Days	DLP Scans	0	100000		→	Edit Delete
GBytes Scanned in Last 30 Days	DLP Scans	0	100		→	Edit Delete
Incidents Detected in Last 30 Days	DLP Incident Summary	21	25000		→	Edit Delete
New High Severity Incidents	DLP Incident Summary	13175	5000		↑	Edit Delete
Number of False Positives in last 30 days	DLP Incident Summary	0	500			Edit Delete
Policies Edited in Last 30 Days	DLP Policy History	2	25		↑	Edit Delete

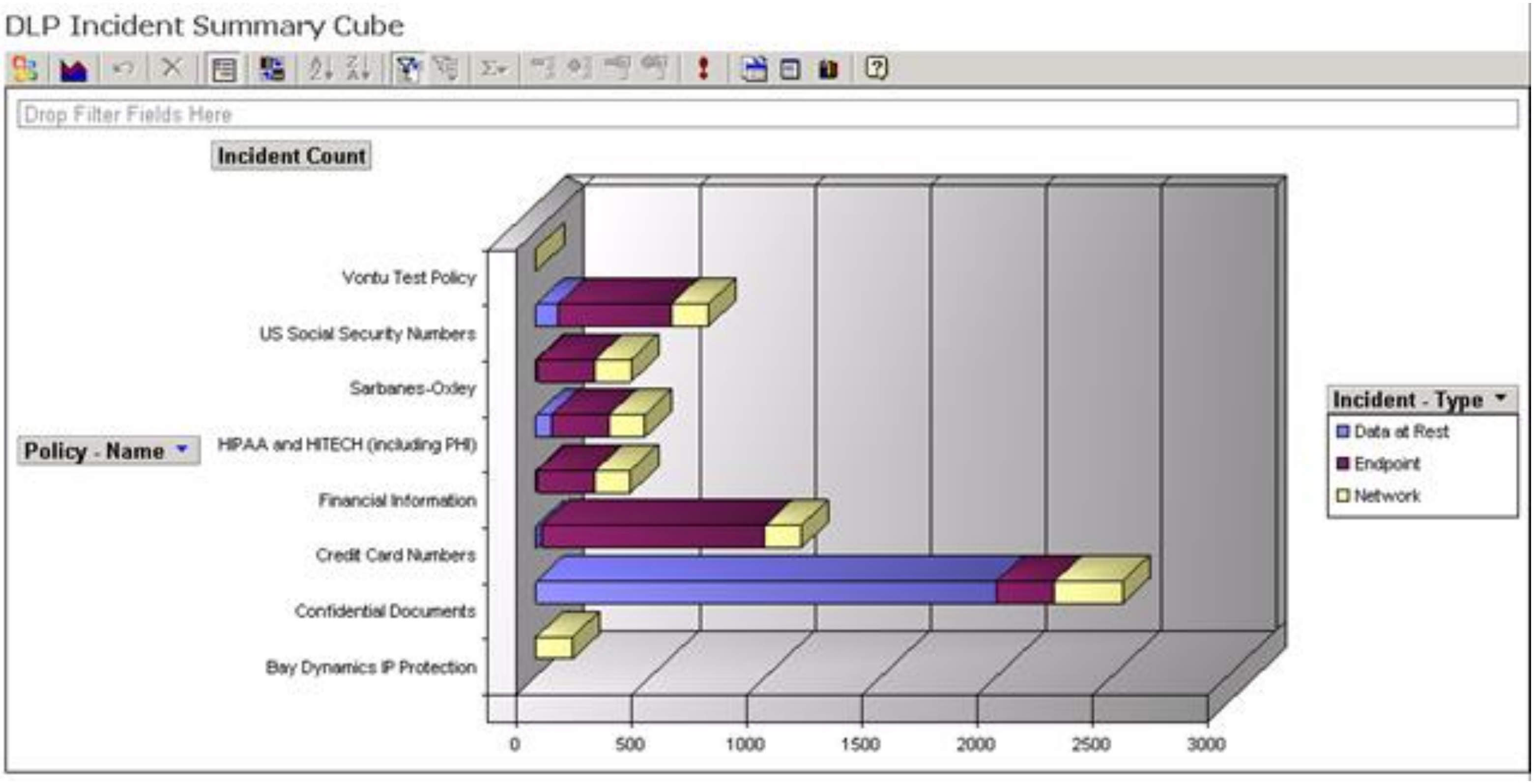
Risk Mgr: How are incidents trending?



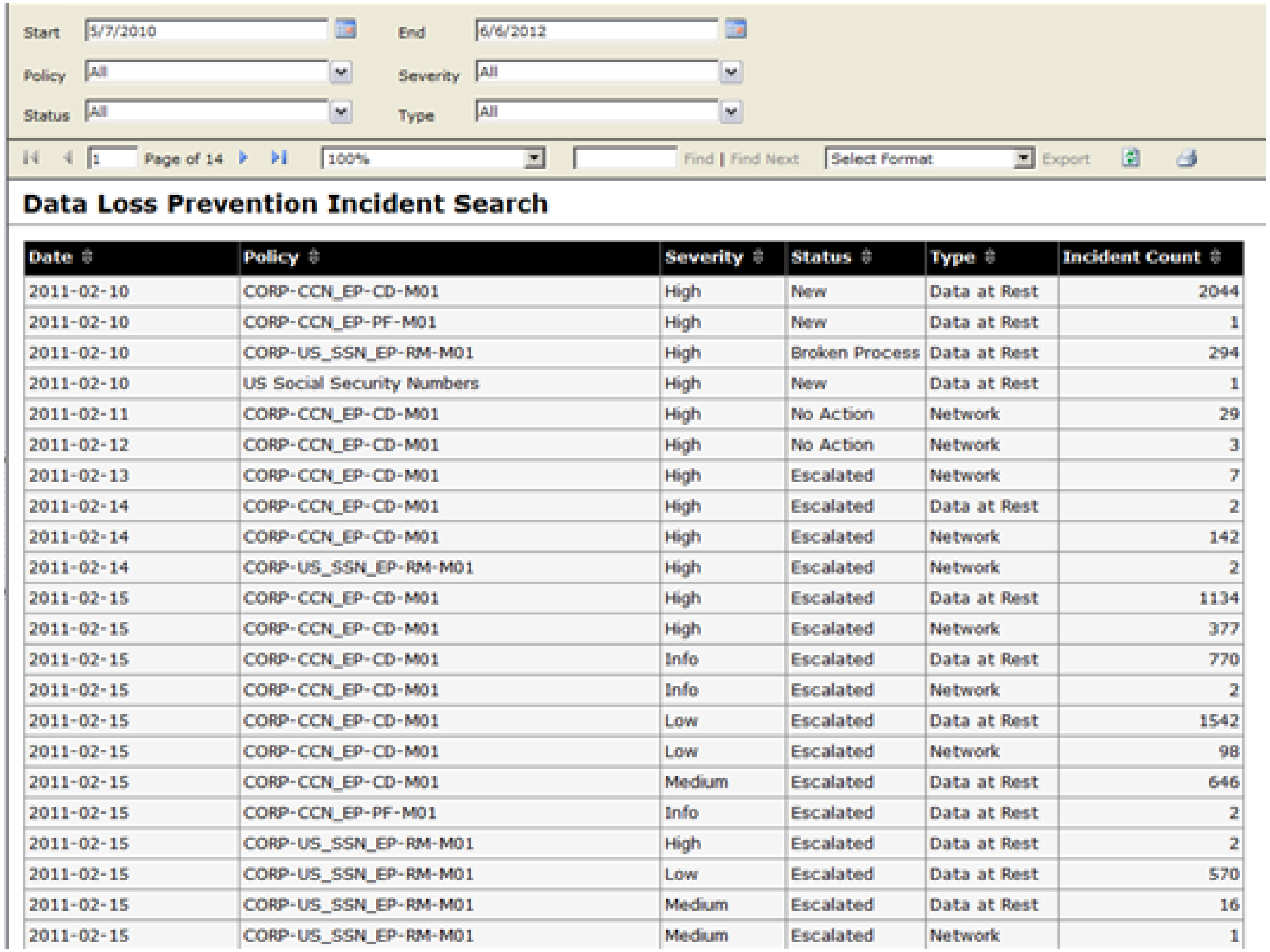
Incident Trend

Date	Data At Rest	Network	Endpoint	Total Incidents
⊞ February	0	7,696	0	32,090
⊞ March	0	1,430	0	1,430

Compliance Mgr: Which policies are violated the most?



Legal Counsel: Show all incidents that contain file xyz?

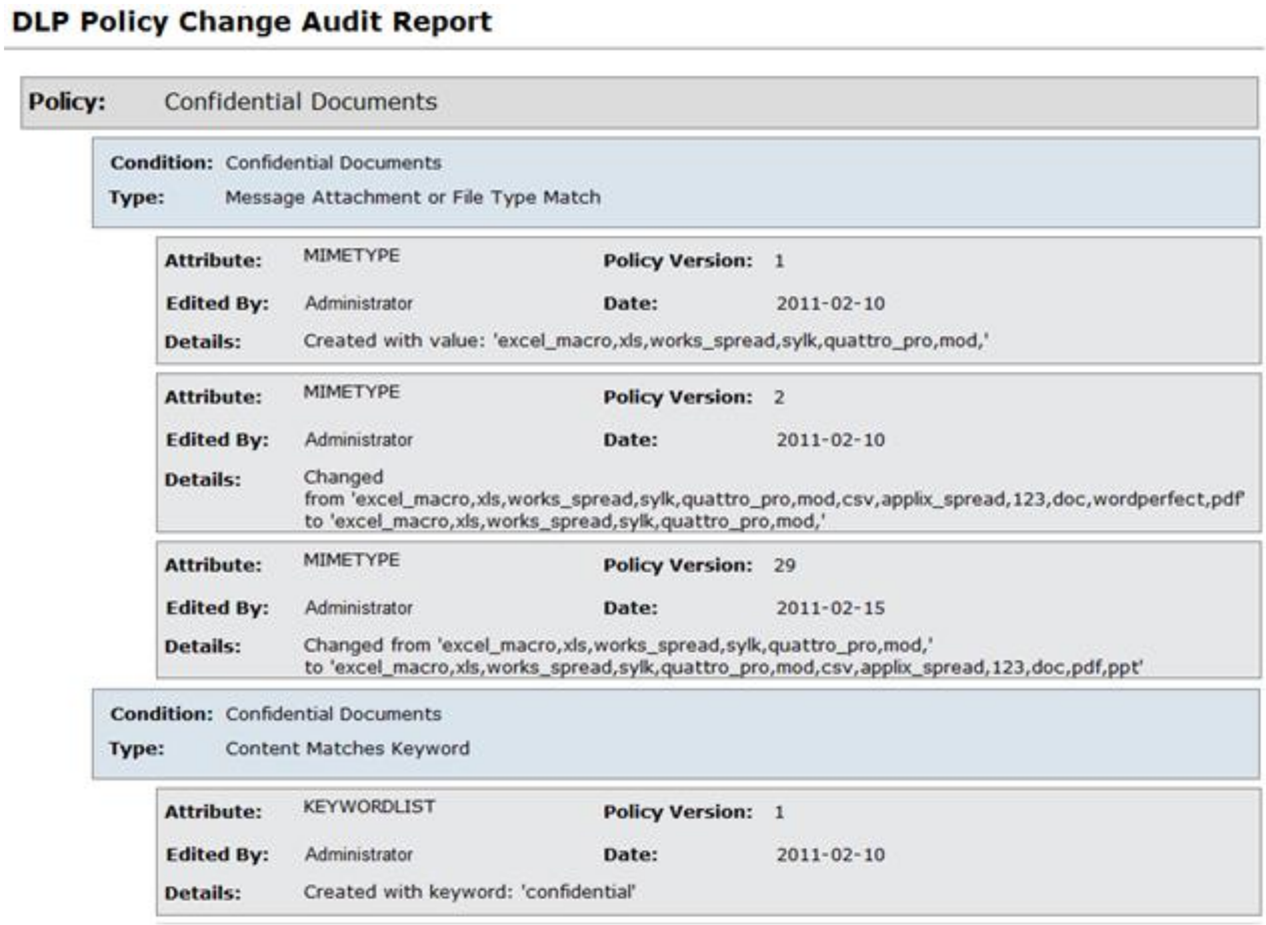


Start	5/7/2010	End	6/6/2012
Policy	All	Severity	All
Status	All	Type	All

Data Loss Prevention Incident Search

Date ⇕	Policy ⇕	Severity ⇕	Status ⇕	Type ⇕	Incident Count ⇕
2011-02-10	CORP-CCN_EP-CD-M01	High	New	Data at Rest	2044
2011-02-10	CORP-CCN_EP-PF-M01	High	New	Data at Rest	1
2011-02-10	CORP-US_SSN_EP-RM-M01	High	Broken Process	Data at Rest	294
2011-02-10	US Social Security Numbers	High	New	Data at Rest	1
2011-02-11	CORP-CCN_EP-CD-M01	High	No Action	Network	29
2011-02-12	CORP-CCN_EP-CD-M01	High	No Action	Network	3
2011-02-13	CORP-CCN_EP-CD-M01	High	Escalated	Network	7
2011-02-14	CORP-CCN_EP-CD-M01	High	Escalated	Data at Rest	2
2011-02-14	CORP-CCN_EP-CD-M01	High	Escalated	Network	142
2011-02-14	CORP-US_SSN_EP-RM-M01	High	Escalated	Network	2
2011-02-15	CORP-CCN_EP-CD-M01	High	Escalated	Data at Rest	1134
2011-02-15	CORP-CCN_EP-CD-M01	High	Escalated	Network	377
2011-02-15	CORP-CCN_EP-CD-M01	Info	Escalated	Data at Rest	770
2011-02-15	CORP-CCN_EP-CD-M01	Info	Escalated	Network	2
2011-02-15	CORP-CCN_EP-CD-M01	Low	Escalated	Data at Rest	1542
2011-02-15	CORP-CCN_EP-CD-M01	Low	Escalated	Network	98
2011-02-15	CORP-CCN_EP-CD-M01	Medium	Escalated	Data at Rest	646
2011-02-15	CORP-CCN_EP-PF-M01	Info	Escalated	Data at Rest	2
2011-02-15	CORP-US_SSN_EP-RM-M01	High	Escalated	Data at Rest	2
2011-02-15	CORP-US_SSN_EP-RM-M01	Low	Escalated	Data at Rest	570
2011-02-15	CORP-US_SSN_EP-RM-M01	Medium	Escalated	Data at Rest	16
2011-02-15	CORP-US_SSN_EP-RM-M01	Medium	Escalated	Network	1

DLP Policy Manager: When and how did policy Y change in the last 6 months?



DLP Policy Change Audit Report

Policy: Confidential Documents

Condition: Confidential Documents
Type: Message Attachment or File Type Match

Attribute:	MIMETYPE	**Policy Version:**	1
Edited By:	Administrator	**Date:**	2011-02-10
Details:	Created with value: 'excel_macro,xls,works_spread,sylk,quattro_pro,mod,'		

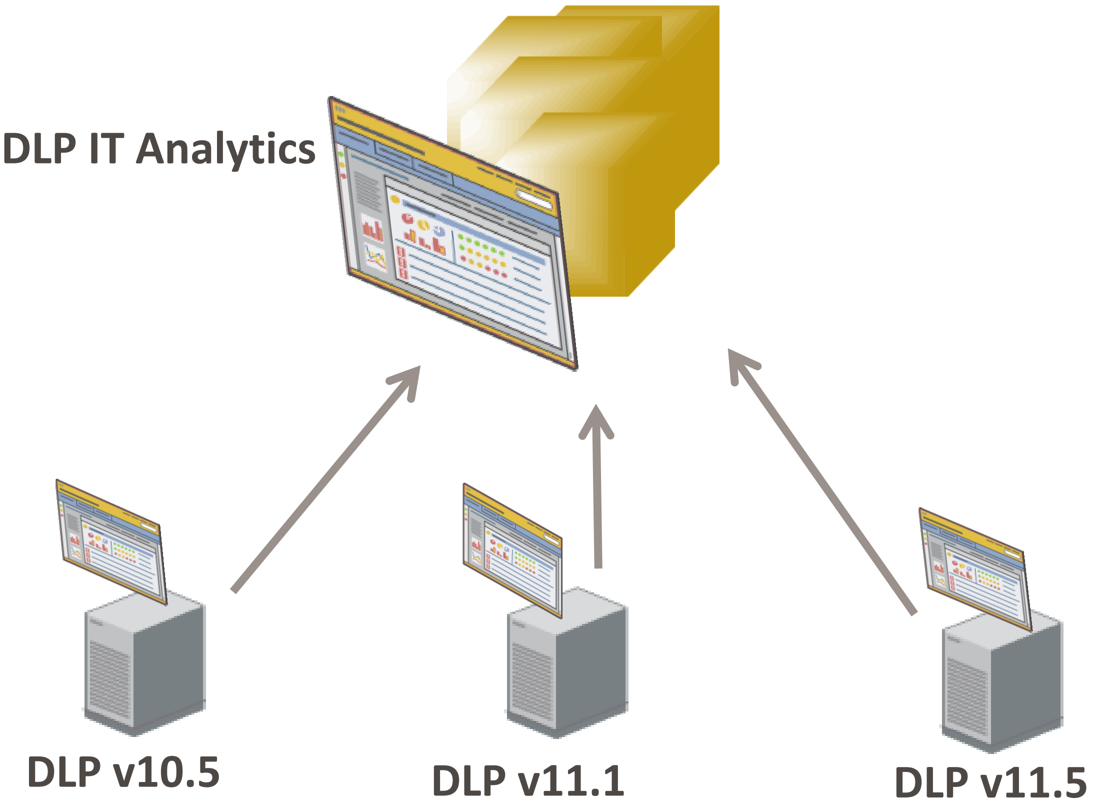
Attribute:	MIMETYPE	**Policy Version:**	2
Edited By:	Administrator	**Date:**	2011-02-10
Details:	Changed from 'excel_macro,xls,works_spread,sylk,quattro_pro,mod,csv,applix_spread,123,doc,wordperfect,pdf' to 'excel_macro,xls,works_spread,sylk,quattro_pro,mod,'		

Attribute:	MIMETYPE	**Policy Version:**	29
Edited By:	Administrator	**Date:**	2011-02-15
Details:	Changed from 'excel_macro,xls,works_spread,sylk,quattro_pro,mod,' to 'excel_macro,xls,works_spread,sylk,quattro_pro,mod,csv,applix_spread,123,doc,pdf,ppt'		

Condition: Confidential Documents
Type: Content Matches Keyword

Attribute:	KEYWORDLIST	**Policy Version:**	1
Edited By:	Administrator	**Date:**	2011-02-10
Details:	Created with keyword: 'confidential'		

DLP ITA Enables Reporting Across Enforce Instances



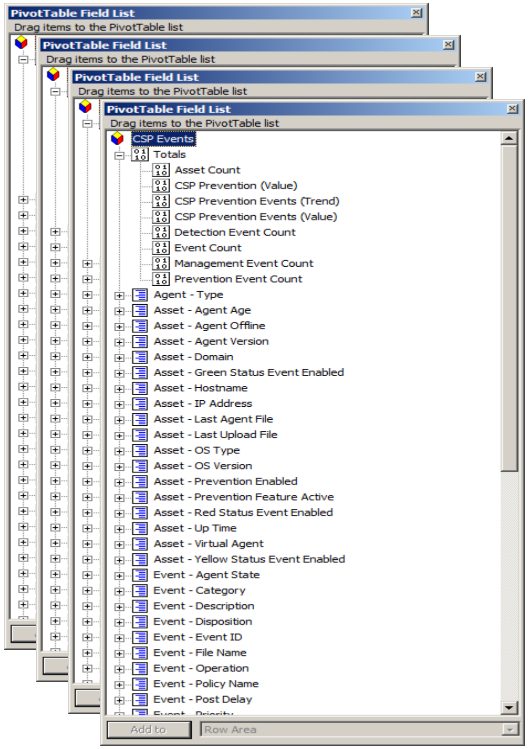
DLP IT Analytics

DLP v10.5

DLP v11.1

DLP v11.5

DLP ITA Supports Other BI Solutions



PivotTable Field List

Drag items to the PivotTable list

- CSP Events
  - Totals
    - Asset Count
    - CSP Prevention (Value)
    - CSP Prevention Events (Trend)
    - CSP Prevention Events (Value)
    - Detection Event Count
    - Event Count
    - Management Event Count
    - Prevention Event Count
  - Agent - Type
  - Asset - Agent Age
  - Asset - Agent Offline
  - Asset - Agent Version
  - Asset - Domain
  - Asset - Green Status Event Enabled
  - Asset - Hostname
  - Asset - IP Address
  - Asset - Last Agent File
  - Asset - Last Upload File
  - Asset - OS Type
  - Asset - OS Version
  - Asset - Prevention Enabled
  - Asset - Prevention Feature Active
  - Asset - Red Status Event Enabled
  - Asset - Up Time
  - Asset - Virtual Agent
  - Asset - Yellow Status Event Enabled
  - Event - Agent State
  - Event - Category
  - Event - Description
  - Event - Disposition
  - Event - Event ID
  - Event - File Name
  - Event - Operation
  - Event - Policy Name
  - Event - Post Delay
  - Event - Priority

COGNOS®

crystal reports.

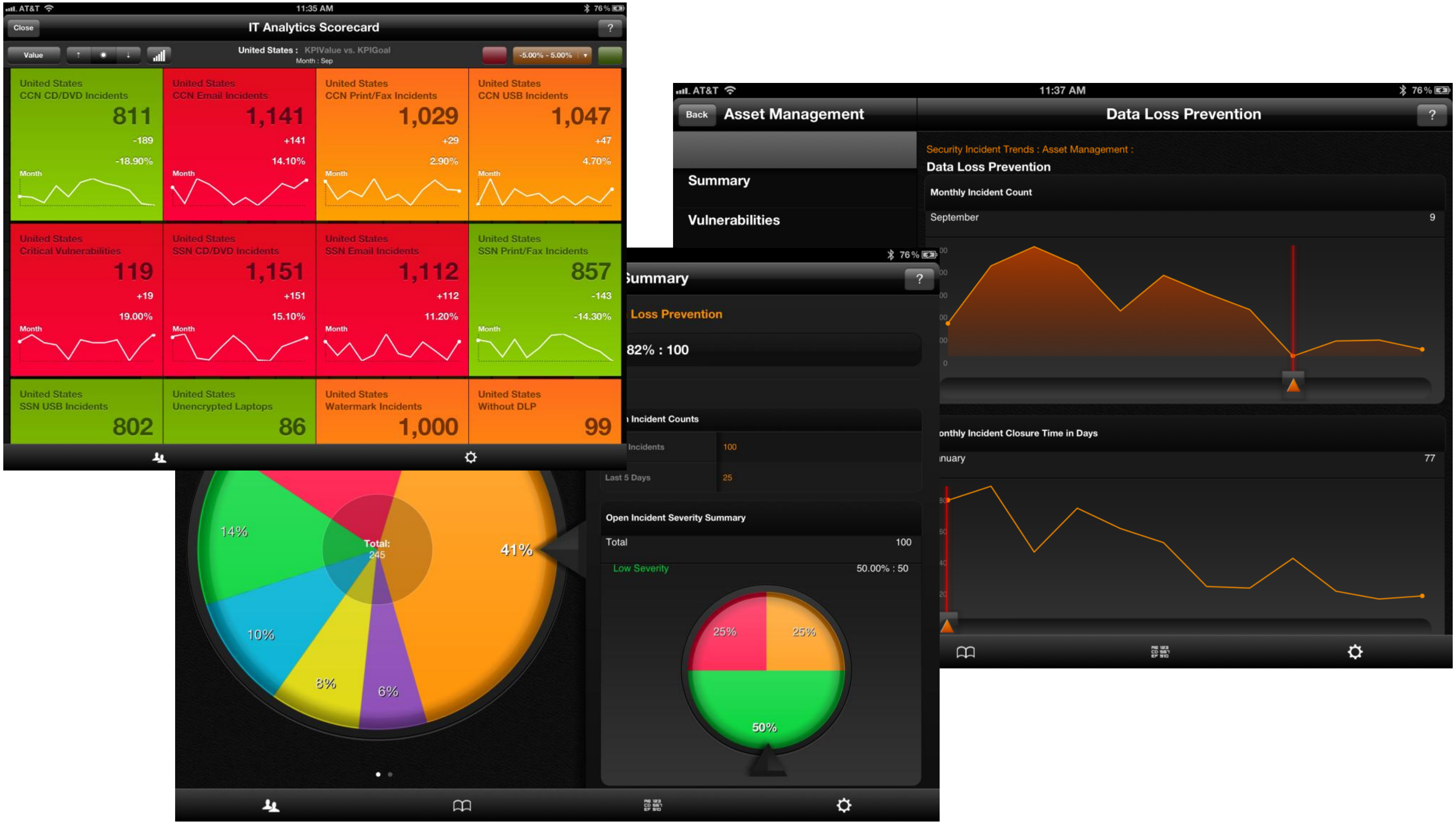
ORACLE®
BUSINESS INTELLIGENCE

Microsoft SQL Server Reporting Services

sas®

Roambi®

DLP ITA on a Roambi Mobile BI enabled iPad



IT Analytics Scorecard

United States : KPIValue vs. KPIGoal
Month : Sep

-5.00% - 5.00%

United States CCN CD/DVD Incidents 811 -189 -18.90%	United States CCN Email Incidents 1,141 +141 14.10%	United States CCN Print/Fax Incidents 1,029 +29 2.90%	United States CCN USB Incidents 1,047 +47 4.70%
United States Critical Vulnerabilities 119 +19 19.00%	United States SSN CD/DVD Incidents 1,151 +151 15.10%	United States SSN Email Incidents 1,112 +112 11.20%	United States SSN Print/Fax Incidents 857 -143 -14.30%
United States SSN USB Incidents 802	United States Unencrypted Laptops 86	United States Watermark Incidents 1,000	United States Without DLP 99

Summary

Loss Prevention

82% : 100

Incident Counts

Incidents	100
Last 5 Days	25

Open Incident Severity Summary

Total	100
Low Severity	50.00% : 50

Asset Management

Data Loss Prevention

- Summary
- Vulnerabilities

Security Incident Trends : Asset Management :
Data Loss Prevention

Monthly Incident Count

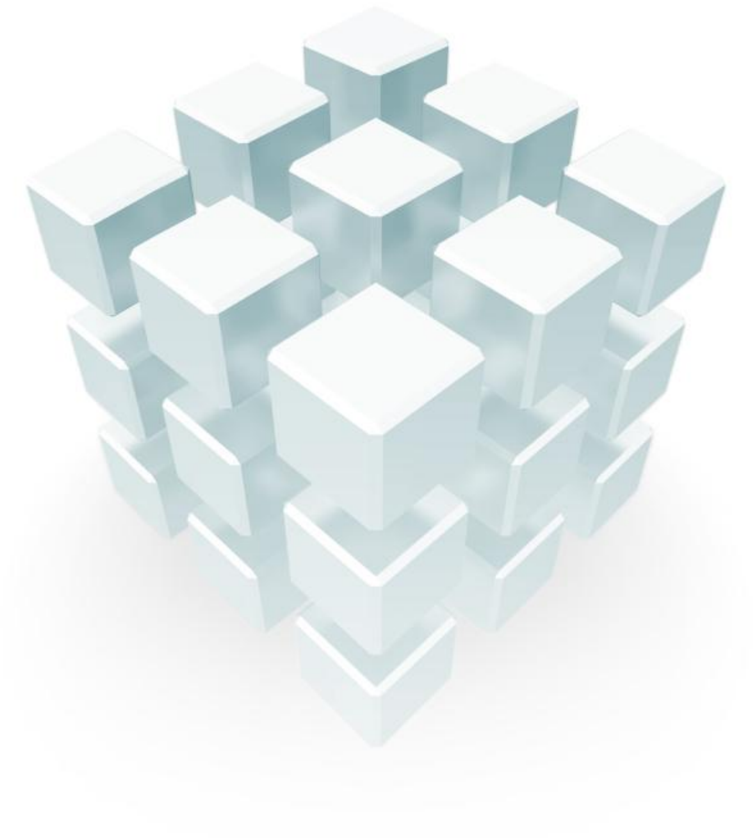
September	9

onthly Incident Closure Time in Days

nuary	77

Symantec Data Loss Prevention IT Analytics

- BI tool that delivers advanced, cube-based reporting for DLP
- Access to broad range of data: incidents, scans, and auditable actions, etc.
- Executive and audit level reports
- Rich analytics
- Consolidates data across channels and Enforce Platforms



Operational Reports

Aging Reports

- Identify no longer relevant incident
  - Older than …
  - Whitney: Last File Accessed Date for DAR
- Look for broken/stale workflow progress: show all incidents:
  - in a specified status for a specified length of time
  - hanged to a specified status during a specified date interval
  - which were sent notifications in a specified date interval
  - Which a specified action was applied in a specified date interval
  - Which status and other info has not changed in a specified period
  - Summarize user's incidents and sorts users by specified action was last taken (e.g. notification)

Aging Reports

- Look for non-malicious repeat offenders
  - Users that have violated same policy X number of times over Y length of time
  - Users that have violated a policy since being notified X times in the last Y periods of time
- Measure remediation operational productivity
  - Calculate the avg time of incident closure (moving form X status to Y status) by policy

Q&A