Websense Data Security

Arbel Lior– Director, Strategic Data Security Solutions

We are already doing DLP!

websense®

Email Encryption

URL filtering

Intrusion Prevention

What solutions are already installed in their network?

- Not data aware
- Unaware of business process
- Everyone says they do DLP…
- What about DLP day 2?
- Effective for Web 2.0 or SSL?

Device Control

Disk Encryption

Access Control

So, what is a DLP solution?

websense®

DLP = Data Leakage (loss) Prevention

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

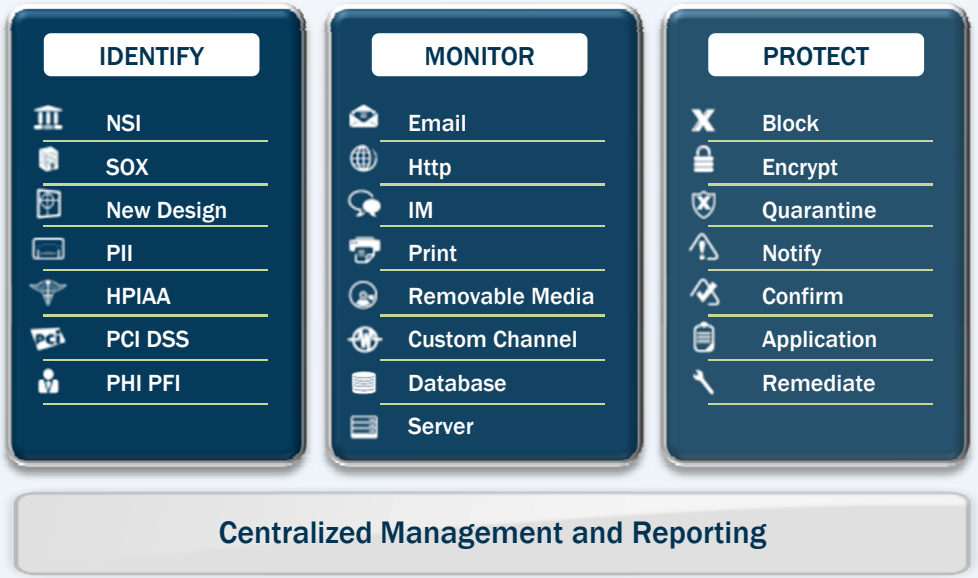
Rich Mogull (securosis.com) – former Gartner analyst for DLP

Websense Data Security Suite

websense®

Market-leading Data Loss Prevention technology to identify, monitor and protect confidential data

- **Unified Policy Design**
  - Only offering with unified policy design
  - Manage all facets of effective Data Loss Prevention policy
  - Powerful monitoring capability to track ever changing data (stored and in transit)
- **Low Cost and Complexity**
  - Modular solution tailors to specific customer requirements
  - Simple deployment and reduced box-count with tight feature integration



Unified and Selective

websense

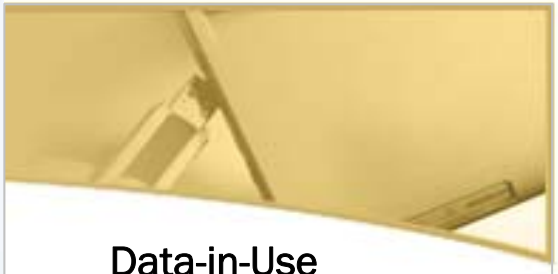
E N F O R C E M E N T

Data-in-Motion

- Monitoring/Auditing
- Notification
- Quarantine
- Block
- Encrypt*

Data-at-Rest

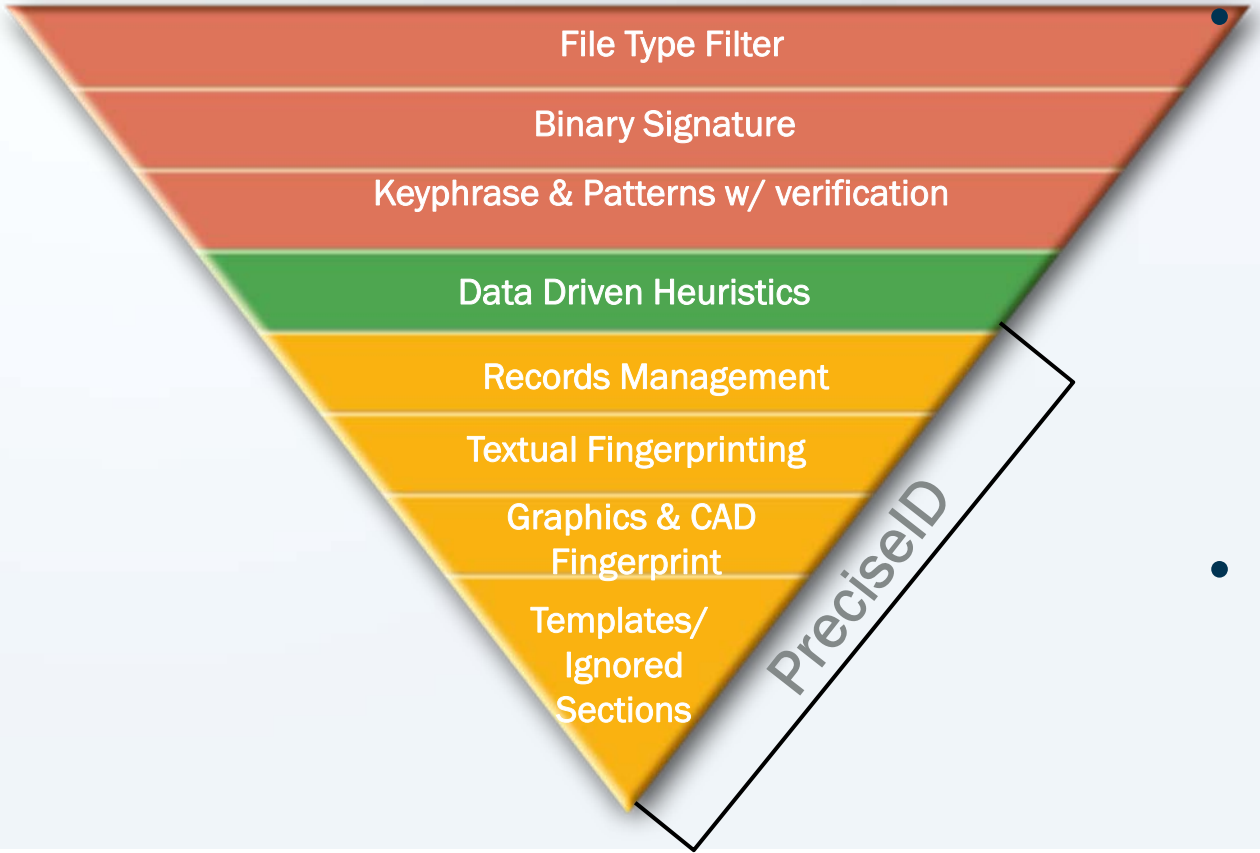
- Monitoring/Auditing
- Remediation



Data-in-Use

- Monitoring/Auditing
- Notification
- Confirm
- Block
- Encrypt

Deep content analysis



- **Websense uses several methods to identify and classify data**
  - File type policies
  - File signature (exact document matching)
  - Key phrases
  - Regular expressions
  - Threshold counters
  - Data-driven heuristics
- **PreciseID is the most accurate and precise method**

DLP: Your Company Policy

websense®

- Based on the last few slides what will your answer be now … ?
- Do you currently have any DLP solution[Chose One]
  - A: Yes, On the Endpoint
  - B: Yes, using Discovery
  - C: Yes, On the Gateway
  - D: No, but planning to deploy in 3-12 months
  - E: No

Overview

websense®

- Websense Data Security
  - Websense DLP solution originated from the acquisition of PortAuthority Technologies
  - Technology exists for more than 10 years
  - 27 patents and patents pending
  - First product to introduce full DLP for Web channel
  - First product to introduce full DLP for Email channel
  - The only solution to provide network printer agent with OCR (included in the network license)
  - The only solution that allows SalesForce.com fingerprinting
  - The only solution to provide same protection on network and endpoint agents (even while offline)
  - Nearly 1000 customers in more than 40 countries
  - DLP Leader in Gartner MQ and Forrester Wave for the last 6 years

TRITON: Customers who rely on us

websense®

TRITON

Leading Provider of Healthcare

40,000 users > Healthcare
St. Louis, MO

Reduced Content Security Infrastructure from 64 boxes to 26 (41%), while extending coverage to mobile users when they are off network.

Consolidation of web, messaging, and data controls saved organization $2 million over 3 years in HW/SW cost alone.

Strategic Partner and Industry Advisor to Websense.

FRAMING THE PROBLEM OF DATA LEAKS

What me Worry?

websen

TWO WAYS THAT CYBER-CRIMINALS

CONSISTENTLY

BY-PASS TRADITIONAL SECURITY CONTROLS

1: They're pro-actively test against your AV

websense®

- "The most popular antivirus applications on the market are rendered useless by around 80 percent of new malware"

  - ZDNet: 80% of New Malware Defeats Anti-virus

- Polymorphic malware is harmful, destructive or intrusive computer software such as a virus, worm, Trojan or spyware that constantly changes ("morphs"), making it difficult to detect with anti-malware programs.

  – Definitions @ SearchSecurity.com

- Sophisticated pieces of malware can be bought "off the shelf," ready to use, making it simple for anyone to launch an online life of crime."

  - "Making Money From Cybercrime Easier Than Ever", MSNBC.com

- "Symantec issued more antivirus signatures last year than in its 17 previous years combined." – Francis deSouza, Symantec VP Enterprise Security, RSA - 2009

#2 They're Using Exploit Script and Code

websense®

Aurora hits Google, Adobe and 30+ large organizations. Used 0-day in IE.

Zeus has compromised over 74,000 FTP accounts on websites of such companies as Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek.

RSA reports they have been a target of an APT using a 0-day in Adobe Flash coming via attached XLS file.

- 368 Adobe Acrobat Exploits in 2010/2011
- 122 IE Exploits in 2010/2011
- 107 MS Office Exploits in last 12 months

Let's consider the situation....

websense®

- If the bad guys are pro-actively testing against your AV signatures.....
- If they are using exploit script and exploit code to gain uncontested access to your machines.....
- And if 39% of malware on the internet has data stealing code.....

HOW DO YOU PROTECT AGAINST THAT?

Data Theft

Malicious Data Theft

52% of all Malware has data stealing code

87% of data theft

Advanced Persistent Threats

Leverages Context + Content Awareness

40% Risk Reduction
Success = Weeks

Compliance

Personal Identifiable Information

Customer Information

Leverages Context + Content Awareness

30% of Email has malicious URL's to data stealing code

30% Risk Reduction
Success = Months

Intellectual Property

Data Classification and Fingerprinting of IP

Discovery

Drawings

Source Code

M&A

Insure this phase is last :

30% Risk Reduction
Success = Years

Game Changing NEW Methodology

Fast Facts on data Leaks

websense®

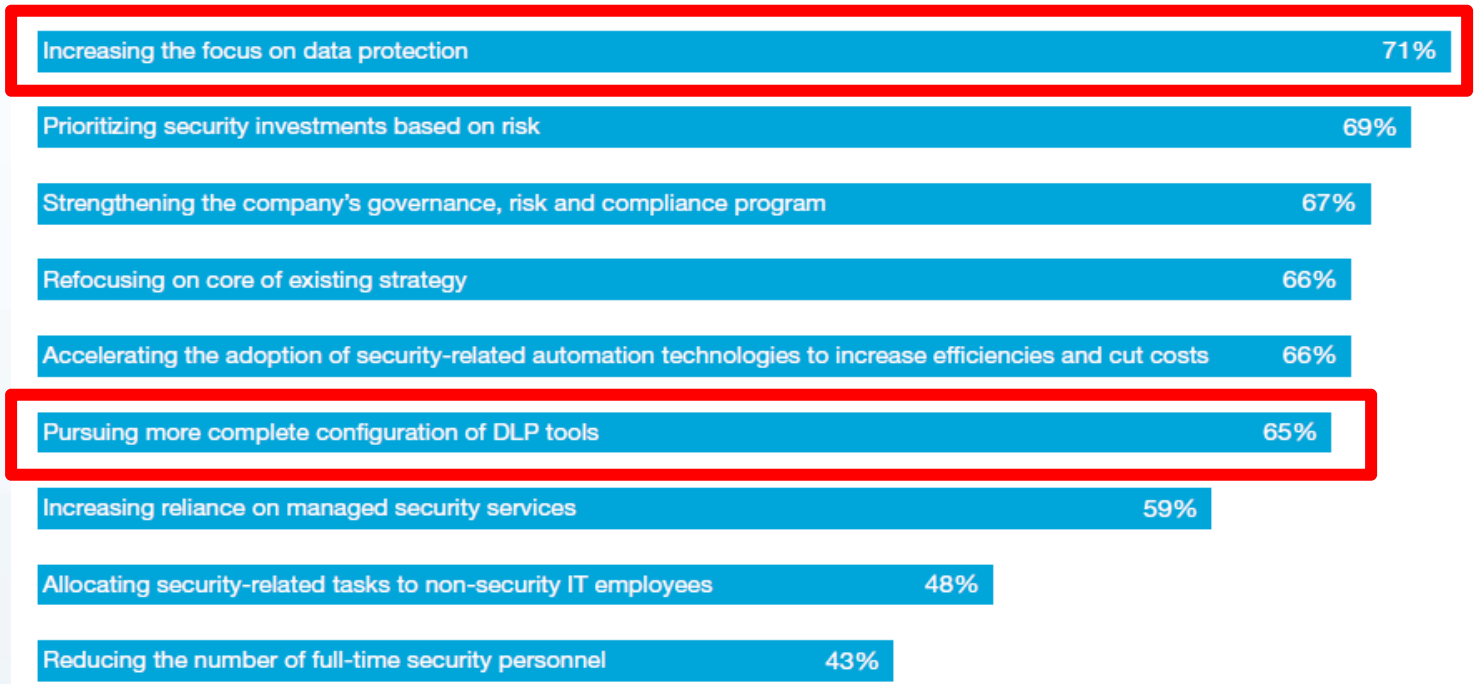
1. 93% of companies maintain IP in digital format
2. 90% of IT security spending focuses on “external” threats
3. 41% of data breaches are because of insider "negligence"
4. 31% of data breaches are because of "malicious or criminal attacks"
5. 40% of IT Executive ranked protecting sensitive information as a top priority in 2011
6. 75% of IT Executives Use Email Accounts to Send Classified Files and Information as Attachments
7. 55% of IT executives said their companies provide – but do not enforce – policies and tools around sharing sensitive information

Source: Gartner Group, CSI/FBI Cybercrime Survey, CSO Magazine, IPSwitch survey at RSA 2011, Ponemon Institute's "2010 Annual Study: U.S. Cost of a Data Breach"

PWC - 2011 Global State of Information Security Survey

websense®

Figure 5: Percentage of respondents reporting that, in order to meet their security objectives in the context of the harsh economic realities, the following strategies are important. (5)

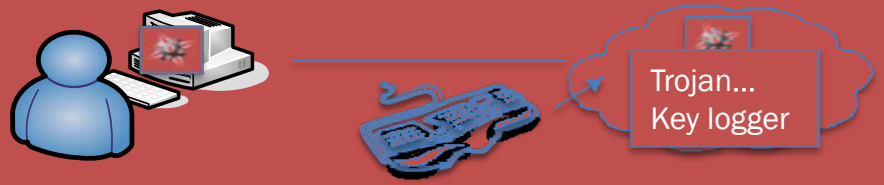


Relative Threats / Impact Multiplier

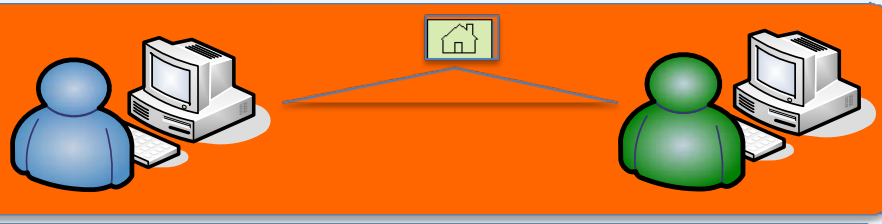
websense®

Unintentional Leaks:
By accident / ignorance

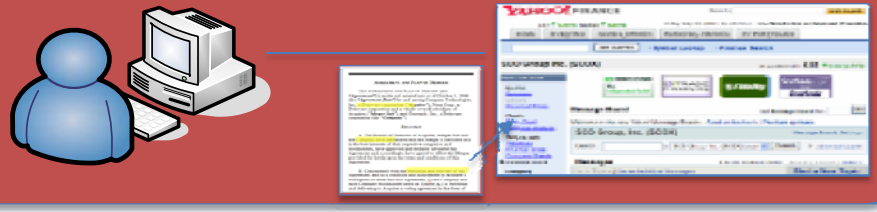
Un/intentional Leaks:
Malicious intent



Un/intentional Leaks:
No/bad business processes



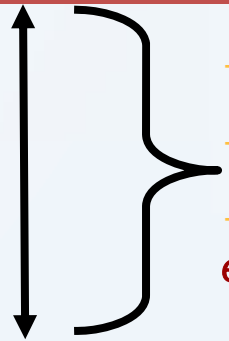
Intentional Leaks:
Malicious intent



Gap Between Policy & Behavior

websense®

Policy (Legal & Administrative Solutions)
- Employee Training
- Stated Privacy Policies
- E-mail Disclaimers



- *Lack of visibility into employee activity*
- *No audit trail of information flows*
- *No ability to automatically enforce existing policies*

Behavior (Technological Solutions)
- Automated Policy Enforcement
- Multiple Channels
- Detailed Audit Trail & Reporting

Use DLP to Educate Users

websense®

- DLP solutions can be **extremely powerful** in educating users, help them to treat sensitive data with more care, e.g.
  - "This email contains customer sensitive information" **Are you sure?**
  - "Copying finanicial information to this type of USB is not recommended" **Please choose your action and the justification for it**
  - "This is an unauthorized recipient" **Are you sure?**
  - "This content must be encrypted" **do you want to release it and automaticly encrypt it?**

THE MOST IMPORTANT STAGE IN DLP PROJECTS

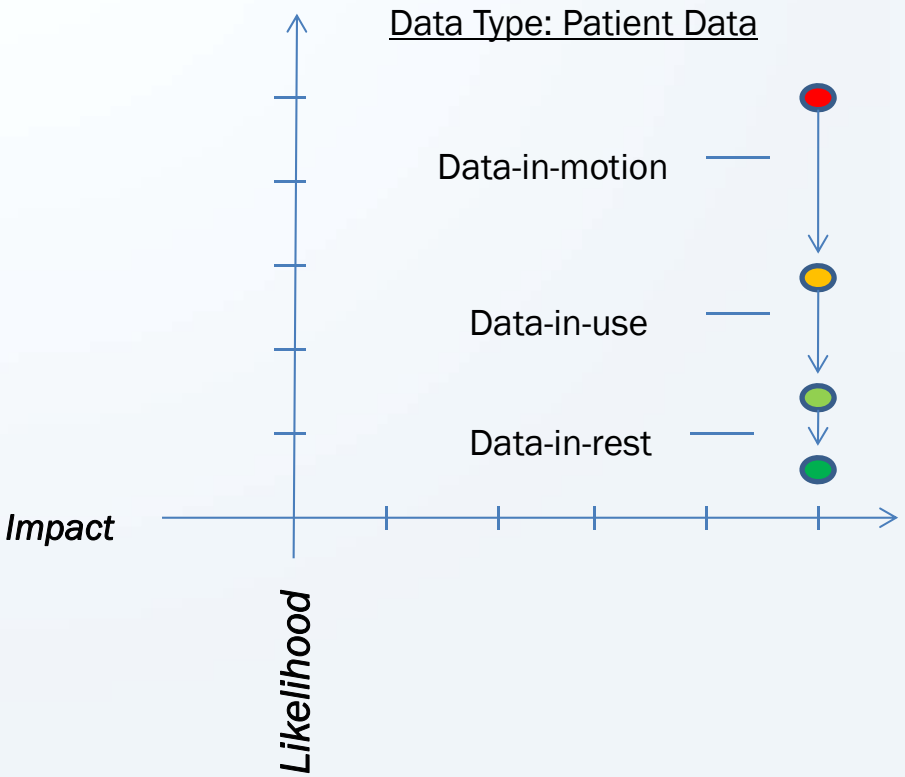
Day 2 – what will happen after the customer purchase a product ?

TRITON™

- Web security
- Email security
- Data security

Calculate customer risk

Risk = (Impact x % Likelihood)



What information, if lost, stolen, or compromised would have a severe impact on your organization? Use a scale of 1 – 5 to rate.

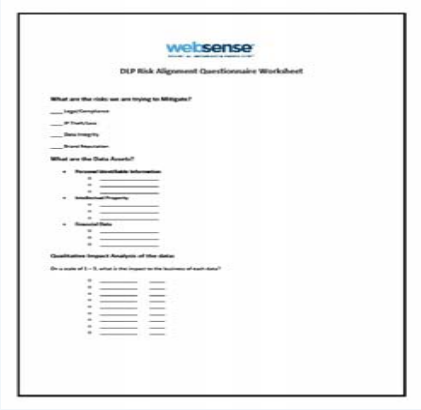
Likelihood is defined by the available avenues information can leave the environment. For example: web, email, file transfers, network printers, local printers, USB's, lost/stolen laptops, etc.

Technical security controls can not change the impact of data loss or theft. However, Websense DLP will give you the ability to lower the likelihood that something bad does happen by detecting and responding when your information assets are at risk.

Creating your Information Risk Profile

websense®

- **What are the Risk we are trying to Mitigate**
  - Legal/Compliance
  - IP Theft/Loss
  - Data Integrity
  - Brand Reputation
  - Loss of Continual Business Operations



- **What are the Data Assets**
  - Personal Identifiable Information
  - Intellectual Property
  - Financial Data

- **Define Impact:** Qualitative Risk Analysis
  - High, Medium, Low
  - 1 – 5 Scale

- **Define Likelihood:** Vulnerabilities (Helps assess the probability of Data Loss)
  - Network:
    - Email , Web, FTP, Network Printers, IM, and Custom Channels
  - Endpoint
    - USB Storage, Local Printers, Print Screens, Stolen/Lost Laptops

Interview Questions

websense®

1. What information does you/your department own, which if lost, stolen, damaged or compromised would have a severe impact on your business?

2. On a scale of 1 – 5, what would the impact be if that data was lost/stolen?

3. How comfortable are you today with your ability to demonstrate due care in the event of an accidental or malicious incident that resulted in data loss/theft?

4. Is there anyone else that you can think of who would also be impacted by this?

Establish Framework

Goal: Gain Network Visibility and Create Baseline.

Objectives:

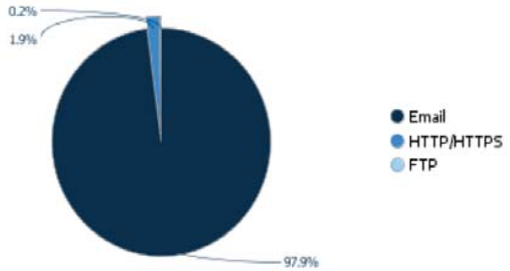
- Technical Install, Tuning, and Training to monitor data-in-motion
- Selective endpoint roll out to high risk users and/or endpoints to mitigate data-in-use and rest.
- Monitor network channels to create baseline / Block known Malicious Destinations
- Executive Updates: Current status and options/recommendations to reduce risk.
- Execute Strategy: Selective enforcement, automate end user notifications, report results.

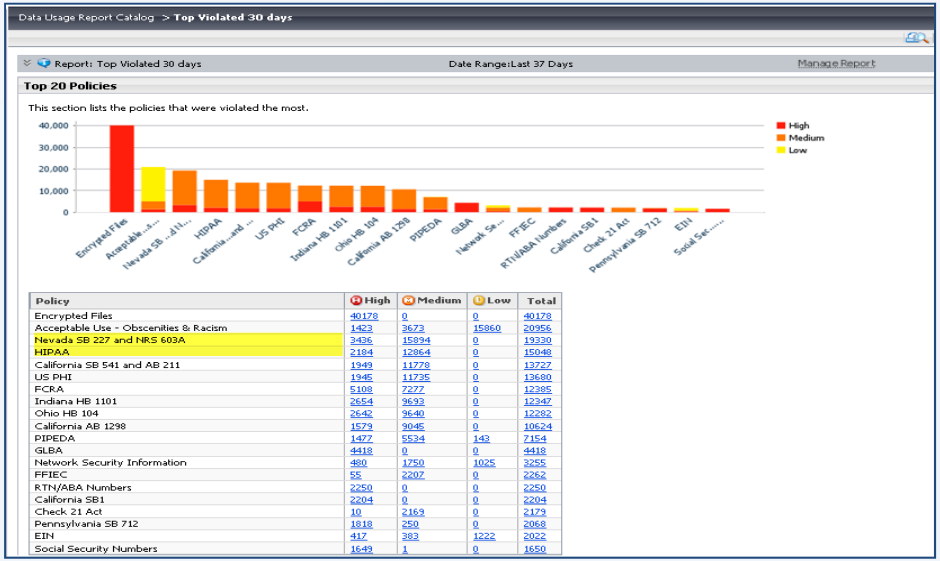
PHASE I	Monday	Tuesday	Wednesday	Thursday	Friday
Week 1 – Install/Tune/Train					
Week 2 – Monitor					
Week 3 – Monitor					
Week 4 –Executive Update 1			**Executive Update**		
Week 5 – Selective enforcement and end user notifications.					
Week 6 – Executive Update 2					Executive Update

Summary of Findings

Top 5 Channels

Channel	Incidents
Email	93362
HTTP/HTTPS	1780
FTP	189



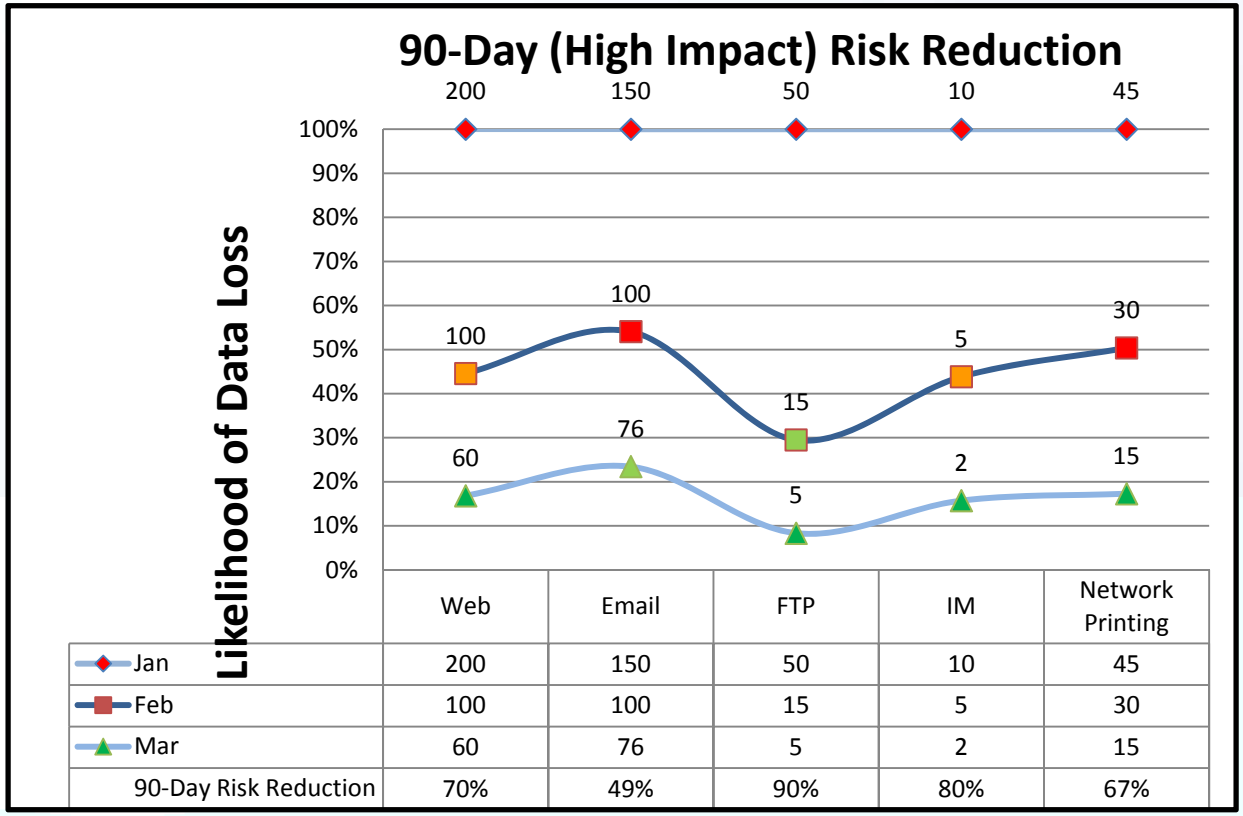


Policy	High	Medium	Low	Total
Encrypted Files	40178	0	0	40178
Acceptable Use - Obscenities & Racism	1423	3673	15860	20956
Nevada SB 227 and NRS 603A	3436	15894	0	19330
HIPAA	2184	12864	0	15048
California SB 541 and AB 211	1949	11778	0	13727
US PHI	1945	11735	0	13680
FCRA	5108	7277	0	12385
Indiana HB 1101	2654	9693	0	12347
Ohio HB 104	2642	9640	0	12282
California AB 1298	1579	9045	0	10624
PIPEDA	1477	5534	143	7154
GLBA	4418	0	0	4418
Network Security Information	480	1750	1025	3255
FFIEC	55	2207	0	2262
RTN/ABA Numbers	2250	0	0	2250
California SB1	2204	0	0	2204
Check 21 Act	10	2169	0	2179
Pennsylvania SB 712	1818	250	0	2068
EIN	417	383	1222	2022
Social Security Numbers	1649	1	0	1650

Summary

- Over 95k incidents during initial two weeks of monitoring
- Over 15k HIPPA Violations
- Email incidents consist of both inbound and outbound
  - 62% of email incidents detected were inbound
- FTP incidents are for encrypted files being sent and potential breach vector

Executive Trend Report



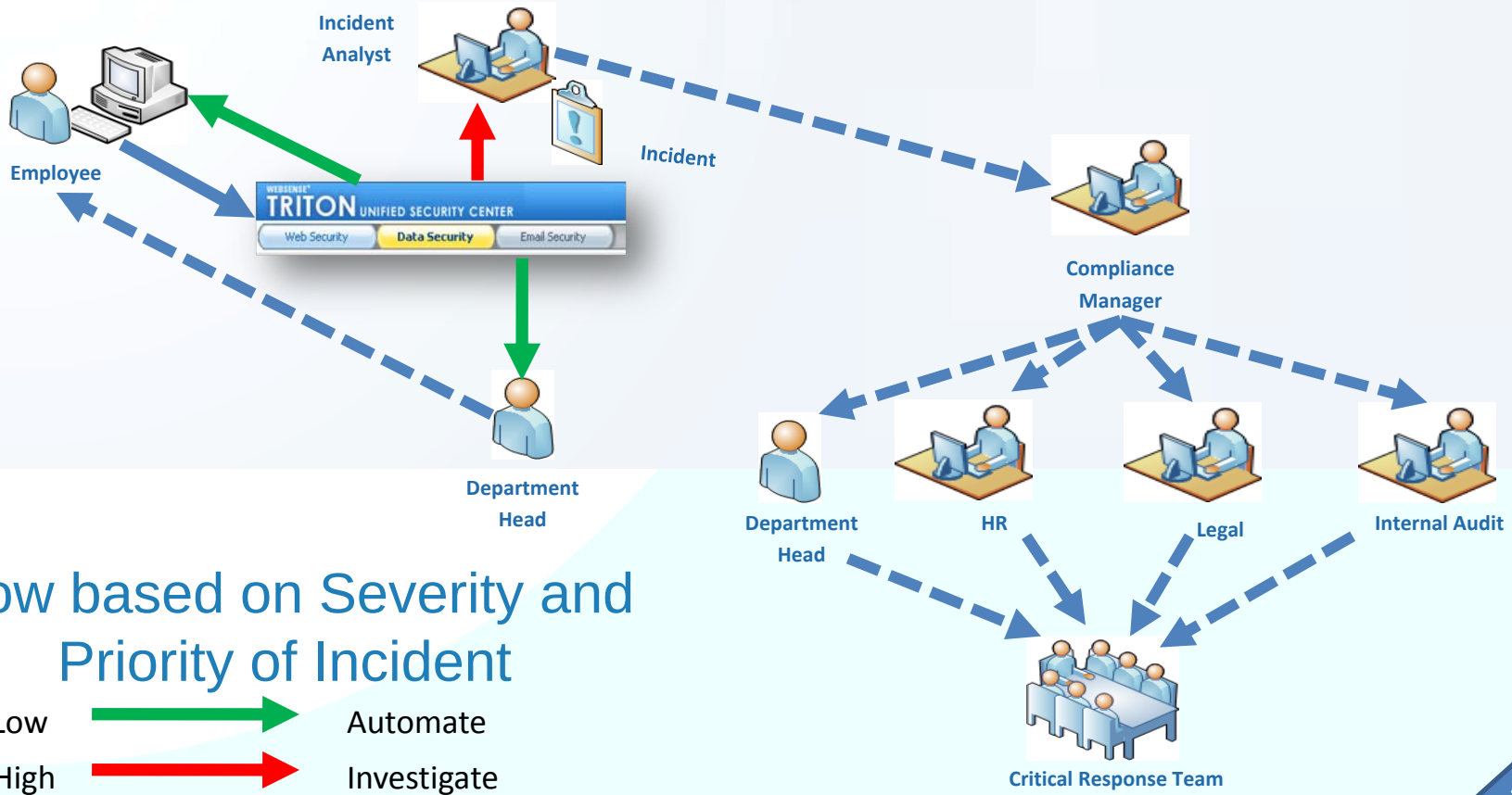
	Web	Email	FTP	IM	Network Printing
Jan	200	150	50	10	45
Feb	100	100	15	5	30
Mar	60	76	5	2	15
90-Day Risk Reduction	70%	49%	90%	80%	67%

GOALS	
30-days	Base Line
60-days	25%+ reduction
90-day	50%+ reduction

MARKER LEGEND
HIGH
MODERATE
LOW
ACCEPTABLE

Example

Incident Work Flow



Flow based on Severity and Priority of Incident

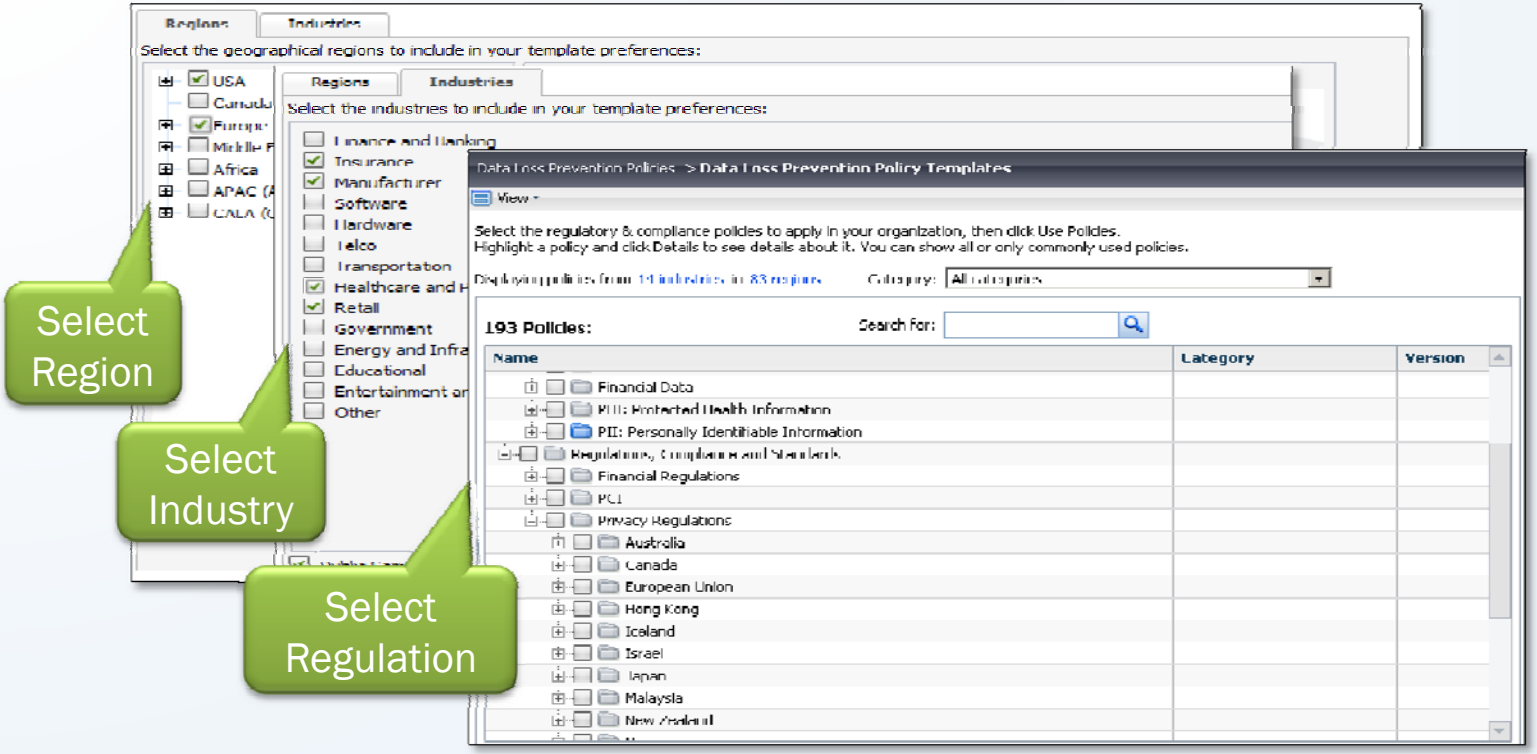
Low → Automate

Med-High → Investigate

Example

Utilizing vendor capabilities

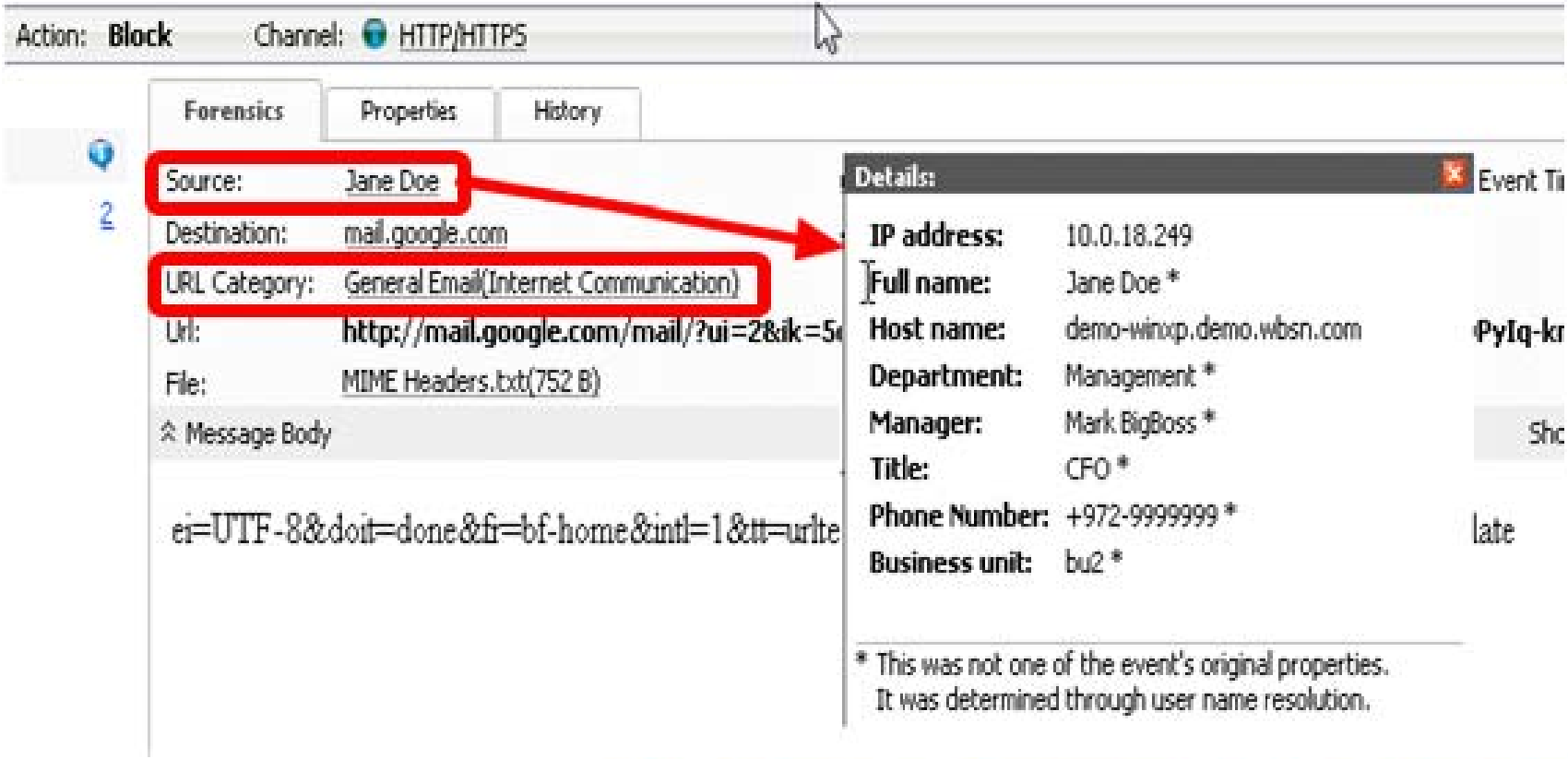
Built-in Best Practices



- No need to translate vague or complex regulation into technical DLP policies
- Derived from years of experience meeting worldwide compliance requirements

Web User and Destination Awareness

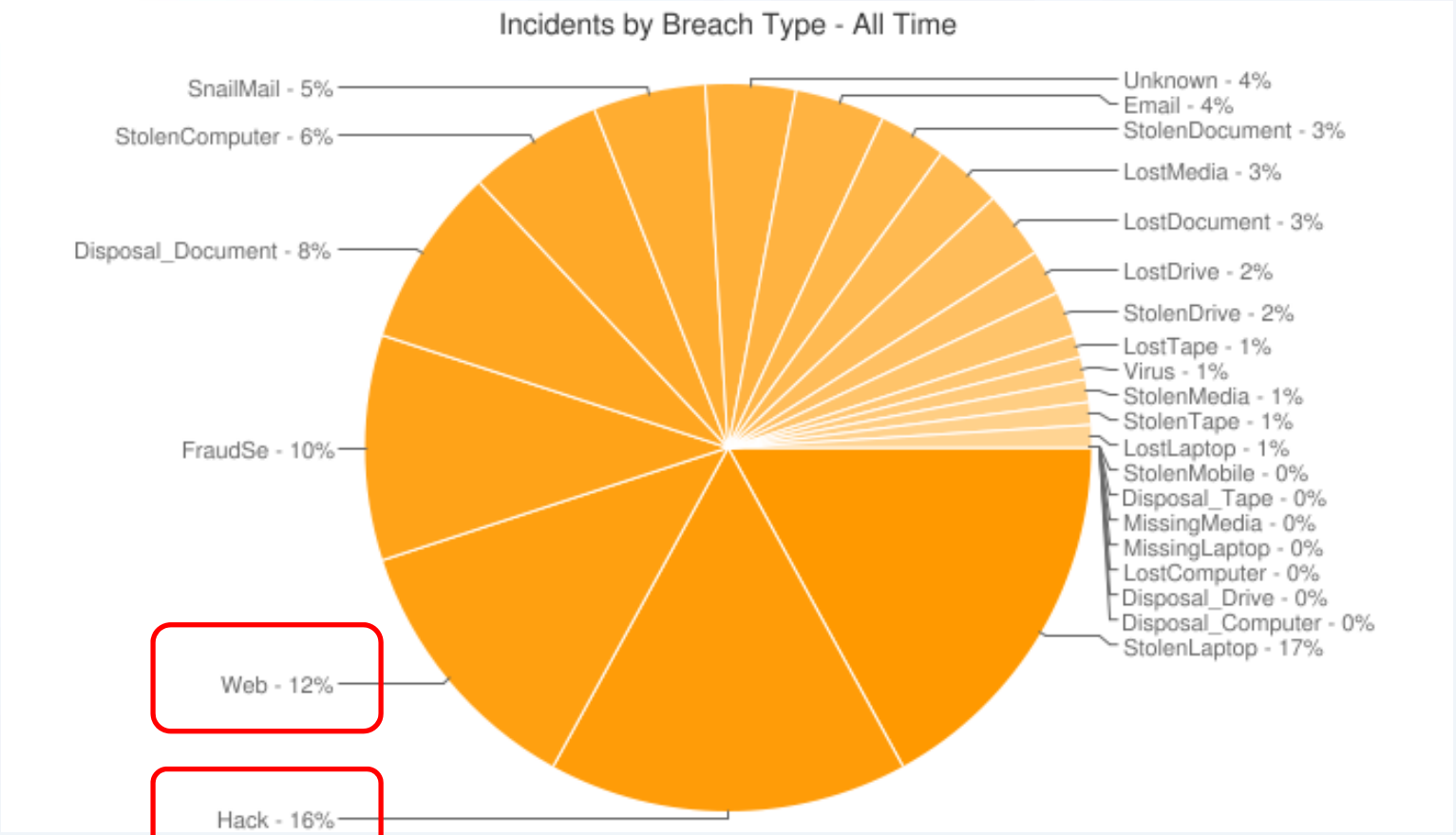
websense®



WHAT ABOUT THIS ALERT?

Why it is important .... ?

websense®



Source : DatalossDB.org

The Power of URL Categories

websense®

Quick Analysis:

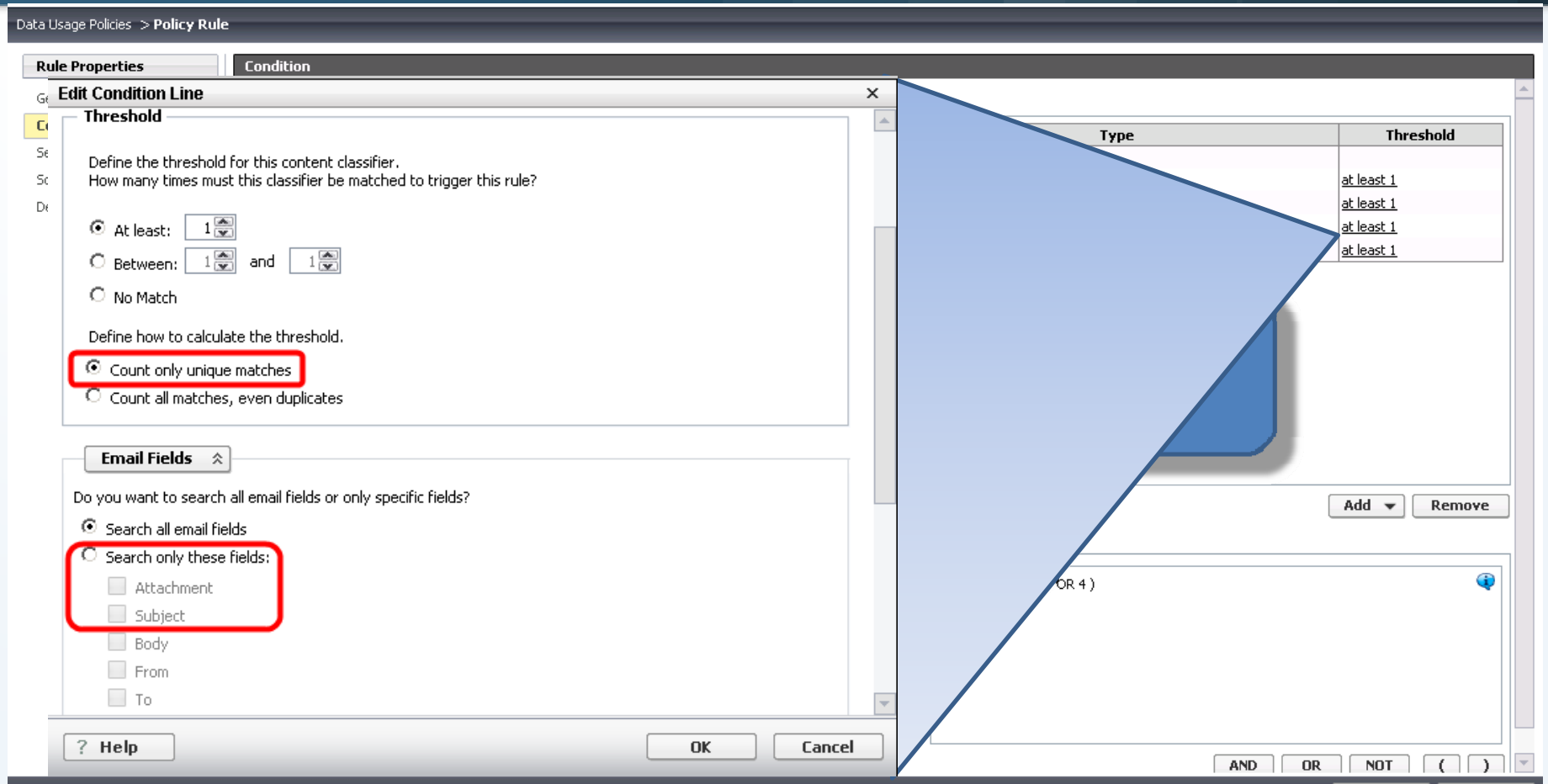
- **1792 Total Incidents in 30 days**
- 296 High Impact Incidents
- **2 incidents of Data Theft**
- 22 instances of uploading to online storage and back up.
- **General Email # 1 Leak Vector**
  - **157 High Impact (53%)**
  - 289 Medium Impact
  - 278 Low Impact
  - **724 Total (40%)**

Show All

URL Category	High	Medium	Low	Total
General Email	157	289	278	724
Social Networking	8	36	265	309
Web Chat	0	2	265	267
Advertisements	2	38	81	121
Search Engines and Portals	16	26	44	86
Uncategorized	44	5	37	86
Information Technology	1	34	53	88
Internet Radio and TV	0	7	60	67
Government	30	0	37	67
Games	0	10	57	67
Business and Economy	2	2	36	40
Shopping	2	4	23	29
Job Search	1	25	2	28
Financial Data and Services	24	0	1	25
Personal Network Storage and Backup	0	5	17	22
Message Boards and Forums	0	1	16	17
Entertainment	0	5	8	13
Reference Materials	7	4	1	12
Advocacy Groups	0	0	11	11
News and Media	1	4	6	11
Educational Institutions	0	1	9	10
Travel	0	2	7	9
Instant Messaging	0	0	8	8
Illegal or Questionable	7	0	0	7
Professional and Worker Organizations	0	0	7	7
Society and Lifestyles	0	0	6	6
Blogs and Personal Sites	0	0	6	6
Streaming Media	0	1	5	6
Sports	0	0	5	5
Service and Philanthropic Organizations	0	1	4	5
Proxy Avoidance	0	0	4	4
Hosted Business Applications	0	2	0	2
Gay or Lesbian or Bisexual Interest	0	1	1	2
Phishing and Other Frauds	2	0	0	2
Personals and Dating	0	1	1	2

Minimizing False Positives

websense®



Reports

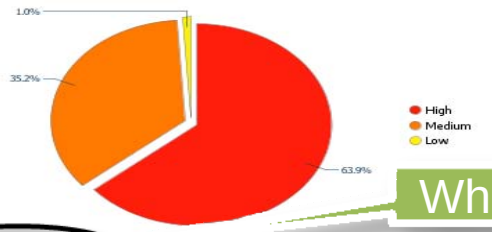
websense®

Who's using the data?

Incidents by Severity

This section shows the incidents by severity.

Severity	Incidents
High	4508
Medium	2482
Low	68



Top 5 Destinations

This section lists the destinations with the most violations.

Destinations	High	Medium	Low	Total
wbsndemo@gmail.com	4439	2402	0	6841
dssdemo@gmail.com	32	22	2	56
sharepoint.wbsn-demo.com	3	0	48	51
74.125.19.83	10	33	1	44
2.0 USB Flash Drive	9	5	7	21

Where is it going?

Who's sending it?

Top 5 Sources

This section lists the sources with the most violations.

Sources	High	Medium	Low	Total
jlondon	4460	2411	0	6871
Jack London	13	44	0	57
10.34.50.98	3	0	53	56
TMLAB\mlee	12	9	12	33
mlee	8	13	2	23

Show All

Top 5 Policies

This section lists the policies that were violated the most.

Policy	High	Medium	Low	Total
Strategic planning documents	3390	0	0	3390
US and Canada PII	1487	1759	0	3246
Employee IDs	1037	695	0	1732
Strategic planning documents_1	1103	0	0	1103
GLBA	956	0	0	956

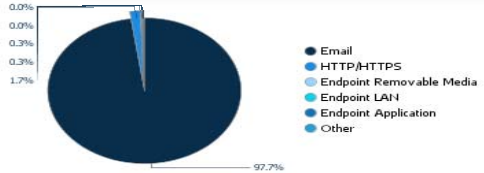
Show All

How is it being sent?

Top 5 Channels

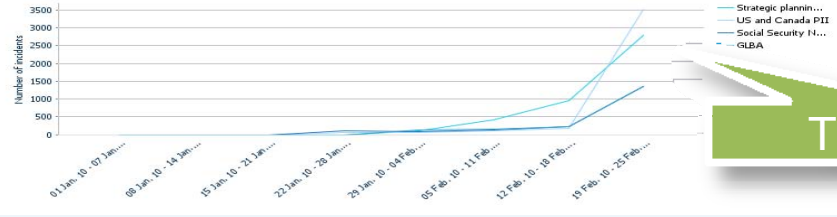
This section shows the channels where security violations occurred the most.

Channel	Incidents
Email	6899
HTTP/HTTPS	118
Endpoint Removable Media	21
Endpoint LAN	18
Endpoint Application	1



Top Policies

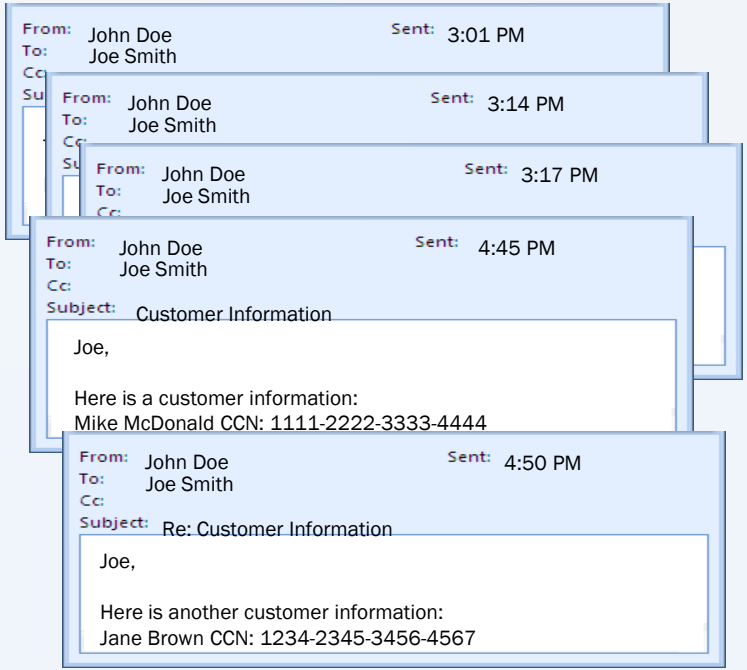
Listed below are the policies that were violated most frequently during the defined period, and the number of incidents generated for each.



Trend Report

Drip DLP

- **Detect multiple instances of small data leaks**
  - Configure policy spanning specific range of time
  - Detect results of multiple incidents adding up to a potentially large data loss
- **Administrators can manage business policies; not just incidents**



Only available from Websense

Mobile Capabilities

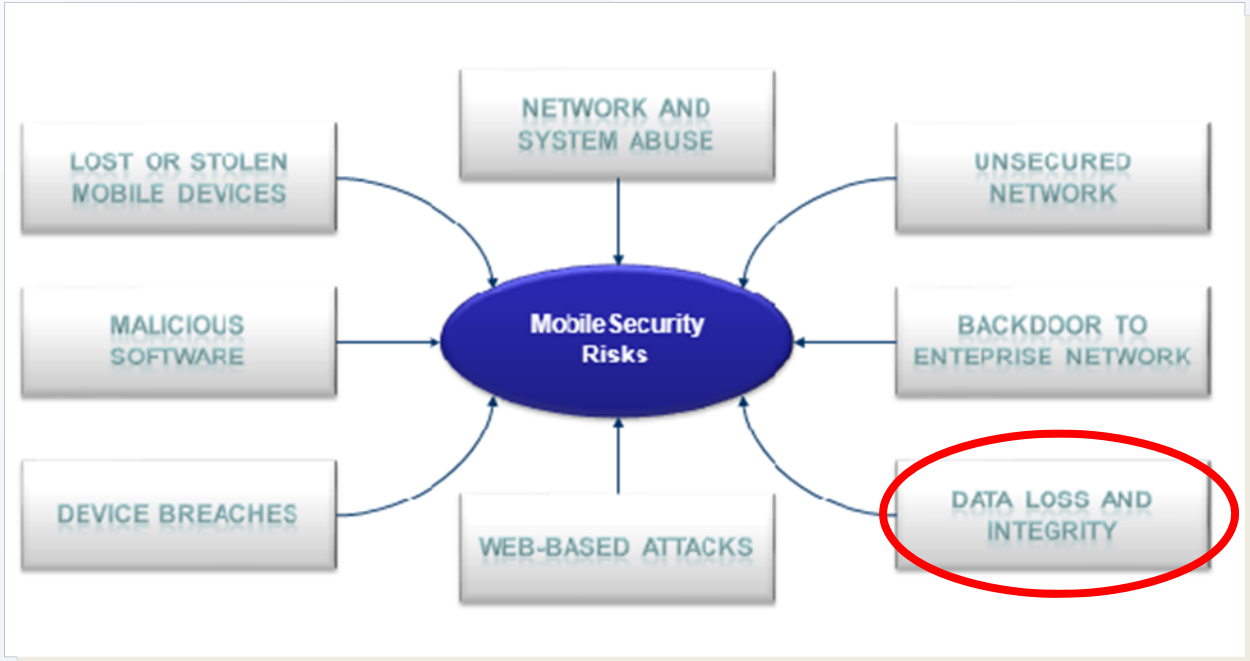
websense®

- Cloud Enabled
- Social + Work
- Specific Apps
- Easy to Use

Frost & Sullivan

Mobile Risks

- Over 250 variants of Android OS
- Consumer facing solutions today
- Mobility drives cloud security services



Frost & Sullivan

Mobile Security

Frost & Sullivan

Best Practices for Mobile Devices

websense®

- Choose mobile devices carefully
- Turn on encryption
- Require authentication
- Utilize remote wipe
- Disable Bluetooth when not in use

Profile of a Mobile User

websense®

Types of devices

Methods of access

Corporate Data Center

Public WiFi

3G

Types of data

Corporate Data

Personal Data

Storage options

Cloud Storage

On-Device Storage

External Storage

Apps used

Business Apps

Personal Apps

Phase 1: Manage Mobile Devices Over Corp WiFi

websense®

- **Customer Problems**
  - Enforce web and data security policies to mobile devices (e.g. iPads) connecting to corporate WiFi network
- **Websense Solution**
  - Use existing Websense Web Security Gateway to extend user policies for web and data to these devices
    - Transparent user identification and authentication
    - Ability to apply same user policies as laptops and desktops
    - Ability to report on user activities from these devices
  - KB article link:
    - http://www.websense.com/support/article/kbarticle/Authenticate-or-identify-Mac-users-for-user-or-group-based-filtering

Phase 2: Manage Email Content Delivered to Device

websense®

- **Customer Problems**
  - Manage sensitive data from being delivered to mobile device
- **Websense Solution**
  - Ability to inspect and prevent sensitive emails from being delivered to mobile device
  - No endpoint or Exchange agent required to prohibit sensitive data transferred to mobile devices
  - Leverages your existing investment in Websense Data Security Suite

websense®

Questions

Thank You For Listening