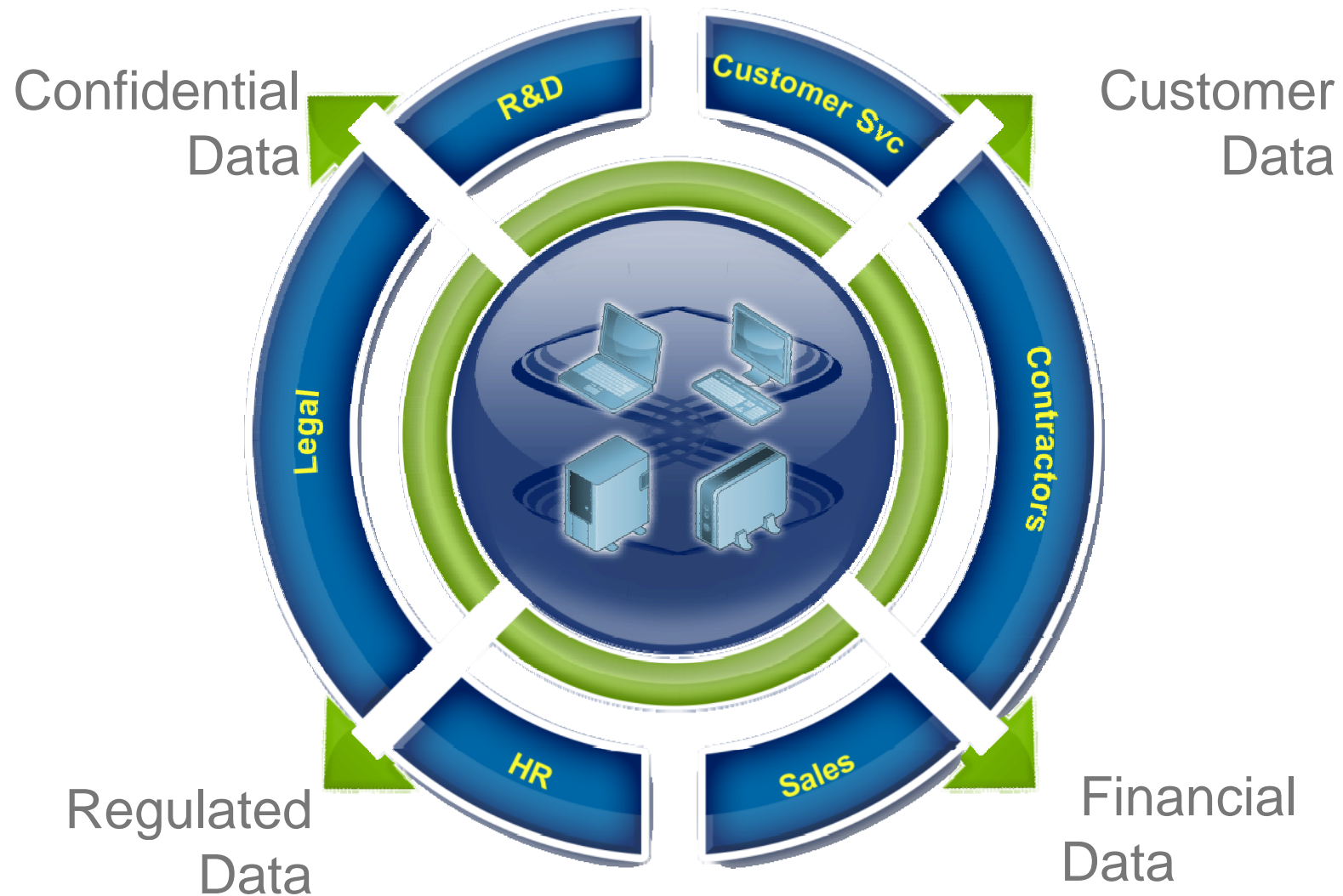


# Stallioni SÜgisseminar

Quentin Authelet,  
System Engineer  
 Websense

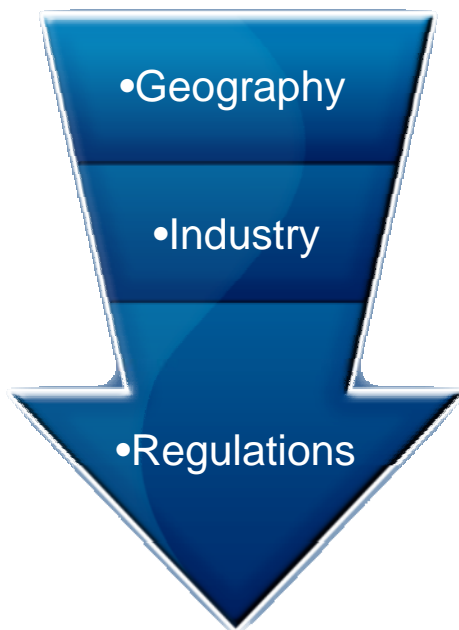
How easy Data Loss Prevention can be

# Data types a common organization will have



# How can I protect my valuable data ?

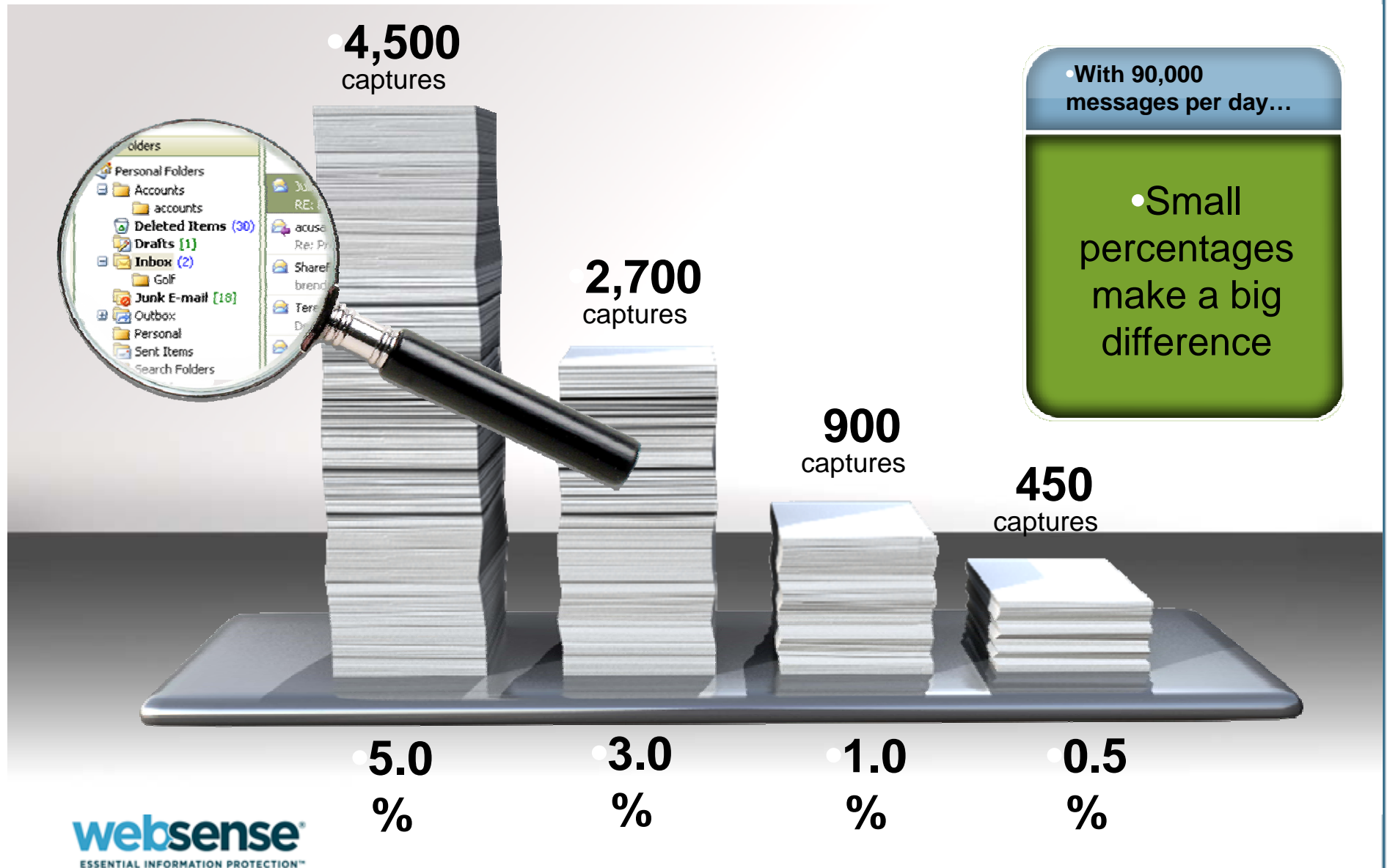
## Understanding Your Data



Private Data  
Corporate Data

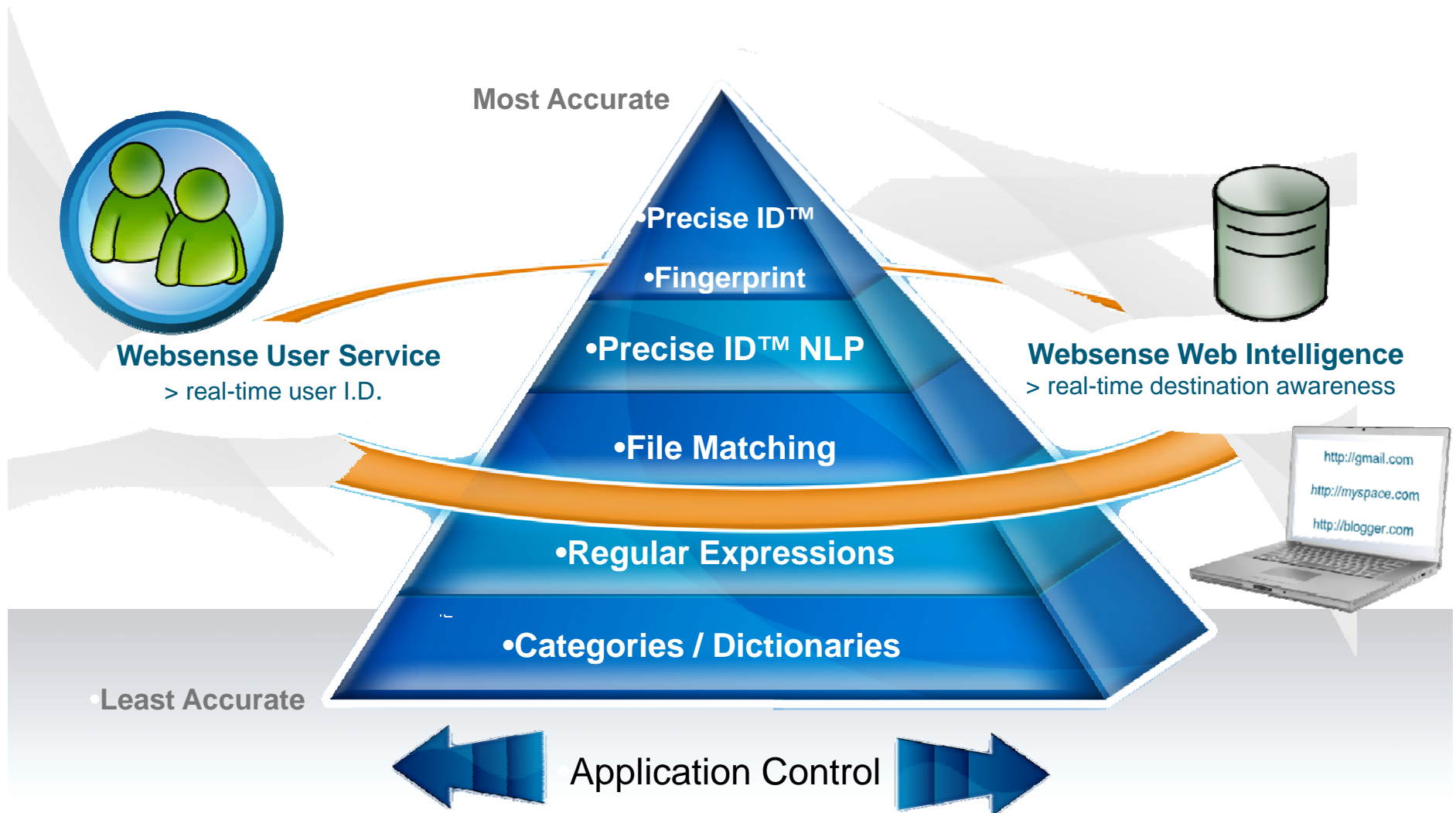


# PreciseID: The Need for Accuracy – management overhead ?





# Websense Detection Techniques – Accuracy is crucial



# Common Objections

I don't know what data I need to protect

I don't know where my valuable data is

I need to do data classification first

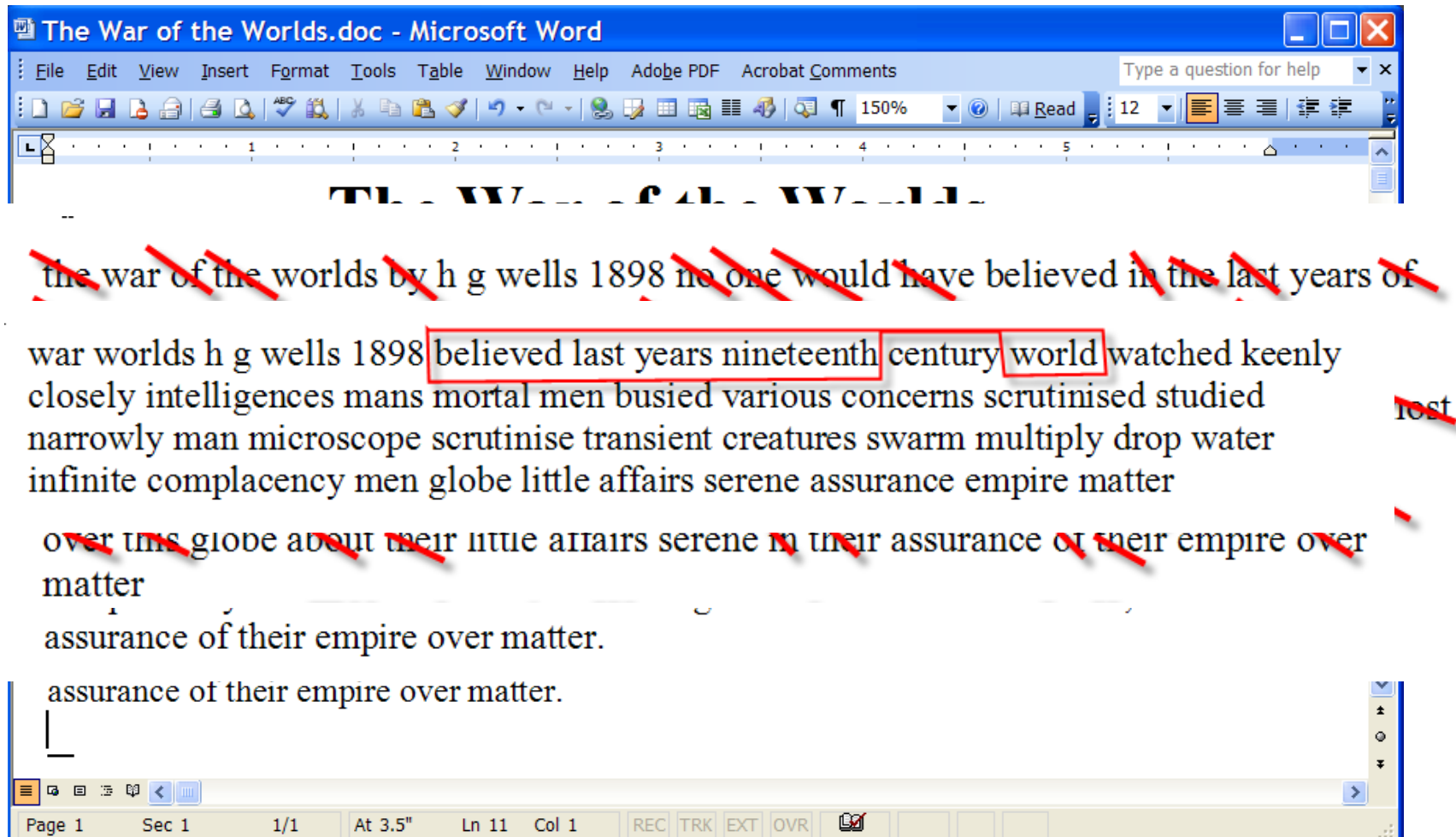
I am blocking all USB devices

I am going to use full disk encryption

I have mail encryption already

What if user uses Steganography

# File Fingerprint



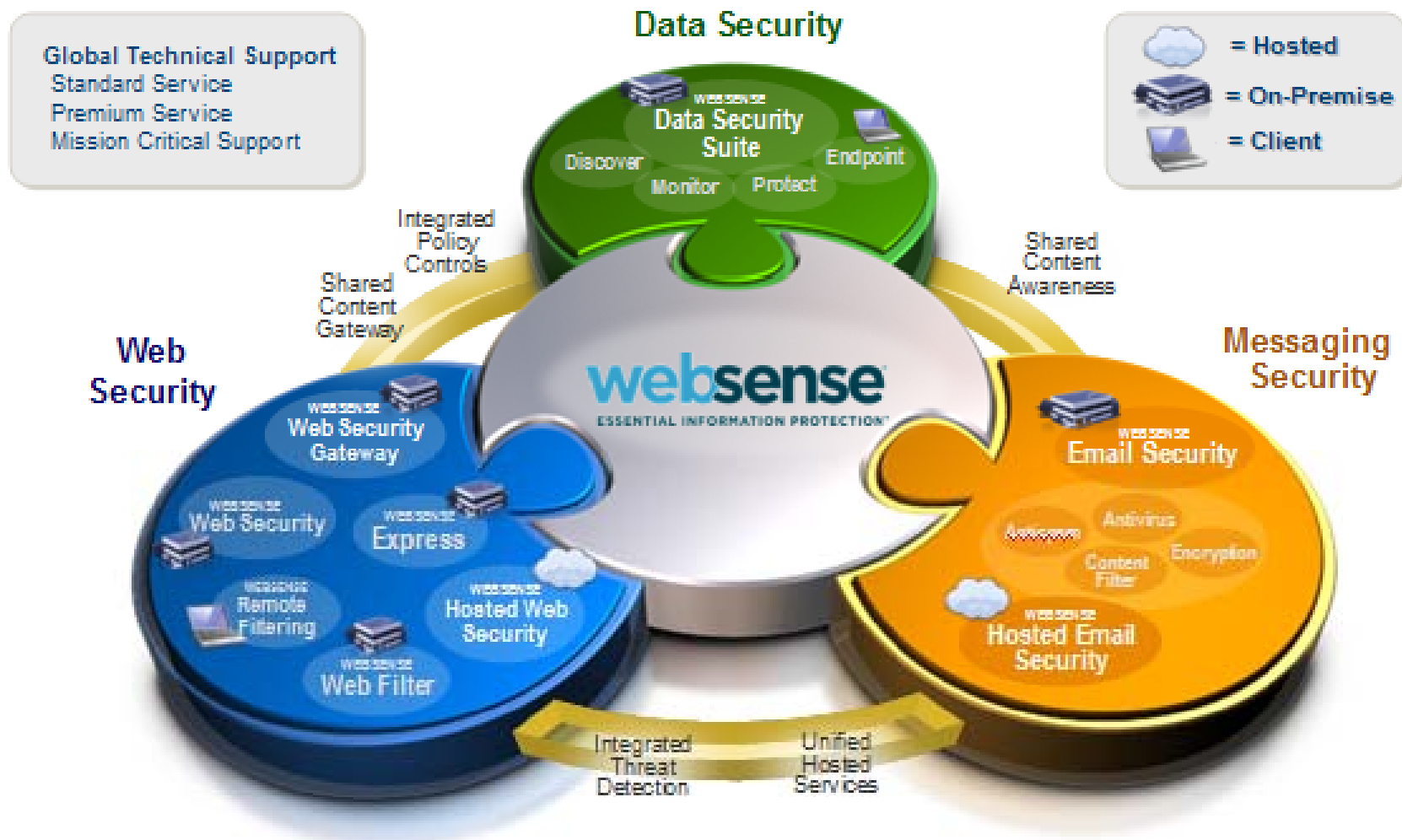
# DATABASE Fingerprint

	C	D	E	F	G	H	I	J
1	FIRST	LAST	ACCOUNT NUMBER	PASSWORD	DRIVERS LICENSE	PHONE NUMBER	EMAIL_ADDRESS	POSTAL CODE
2	RAUL	PASHAL	4684451986499930	dOleNxBJcB	B00089820	(930)750-0791	pashal_6358824@homestead.com	53395-9820
3	ORA	LEISURE	4132673384929420	ZEUtdKPkNj	G00698233	(293)561-7807	leisure_1100713@hotmail.com	29795-8233
4	JAMES	HINTZ	4803331697819540	keLcCstij	D00451340	(714)803-9738	hintz_6682080@homestead.com	03706-1340
5	GOLDIE	PURVIS	4409094843938080	HwbwUgKGqD	E00907590	(693)473-0722	purvis_1446362@hotmail.com	15222-7590
6	SUSAN	WILLIAMS	4083121379497770	JiqEjDXMJk	E00623438	(860)399-6891	williams_8414781@homestead.com	18142-3438
7	MARTHA	CAHILL	4830782323949940	DHaNHERKoc	A00925521	(795)656-8906	cahill_1162450@who.org	35020-5521
8	MEI	TOKAR	4915759347313980	KlssvmSnob	H00658334	(503)627-1556	tokar_3650942@who.org	54724-8334
9	DANIEL	SMITH	4718214769659850	vjqstGEan	F00557274	(288)878-2616	smith_4913955@homestead.com	52330-7274
10	HAZEL	HANSEN	4836195836003030	ExrcVlkyUT	G00259934	(751)998-8949	hansen_9424180@yahoo.com	46561-9934
11	JOSEPH	NICHOLS	4468381105299690	BxUsvEZkAe	A00186262	(463)501-6809	nichols_1162318@ebay.com	22348-6262
12	VIRGINIA	CAMACHO	4855420530088610	JHYkcHEhJs	A00024172	(792)972-1880	camacho_121975@hotmail.com	90980-4172
13	JOHN	THOMPSON	4501523428889320	kvJGGusOfP	E00580064	(278)469-6181	thompson_1266229@yahoo.com	41334-0064
14	PETER	CLARK	4608121971967830	ucaTOWOLHY	B00296024	(936)554-4464	clark_6388088@homestead.com	48795-6024
15	OSCAR	FERGUSON	4029460039835530	uBEckPdYim	A00805757	(964)205-1884	ferguson_9125936@ebay.com	99656-5757
16	BESSIE	HOLZHAUER	4270959499061360	sqyWwsjqJU	E00826559	(472)947-8236	holzhauser_486822@who.org	27894-6559
17	JAMES	CARRINGTON	4876941172142800	fiPeJypyAe	B00202312	(419)984-7186	carrington_1408617@msn.com	93059-2312
18	ERIK	ALEXANDER	4864185642094010	SUQPawKtCU	B00313732	(609)272-0273	alexander_8064120@who.org	59928-3732
19	CATHERINE	WISCH	4522434791230970	JGeZXRUMCB	B00675067	(934)213-7206	wisch_1318262@bbc.uk.co	85752-5067
20	PHILLIS	MIDGLEY	4862476652529070	uUHKdcqPLK	H00745588	(279)542-5762	midgley_4395431@ustreas.gov	19616-5588
21	GUSTAVO	KELIPIO	4986780881554850	GgvPcgDKHM	B00816053	(296)279-8118	kelipio_7570691@homestead.com	64423-6053
22	KENT	ADAMS	4535123969225290	FljsPvXFme	A00391715	(428)508-9503	adams_2527354@bbc.uk.co	95076-1715
23	JONATHAN	SIEGEL	4588441012817760	CbtNKuNvBH	C00513836	(276)705-7671	siegel_7551343@homestead.com	03515-3836
24	CHRISTINE	JOHNSTON	4642237228057940	CIUCTaVeFe	F00599458	(991)634-0906	johnston_159644@ebay.com	05841-9458
25	DANIEL	NADAL	4720281953201620	VvDvZbDkyZ	H00686586	(344)537-2104	nadal_4209741@bbc.uk.co	05140-6586
26	JACLYN	PARKER	4638423565936630	VClpZsAdnf	D00227336	(926)958-4510	parker_3671846@homestead.com	13510-7336
27	REGINA	YEE	4793822578900930	BBYJlsCivc	A00273437	(705)729-2870	hgh_8790919@acme.com	41248-3437
28	ANNA	GARNER	4721433709799330	EhPQMZsGIX	H00781736	(937)778-1260	garner_7564867@hotmail.com	68451-1736



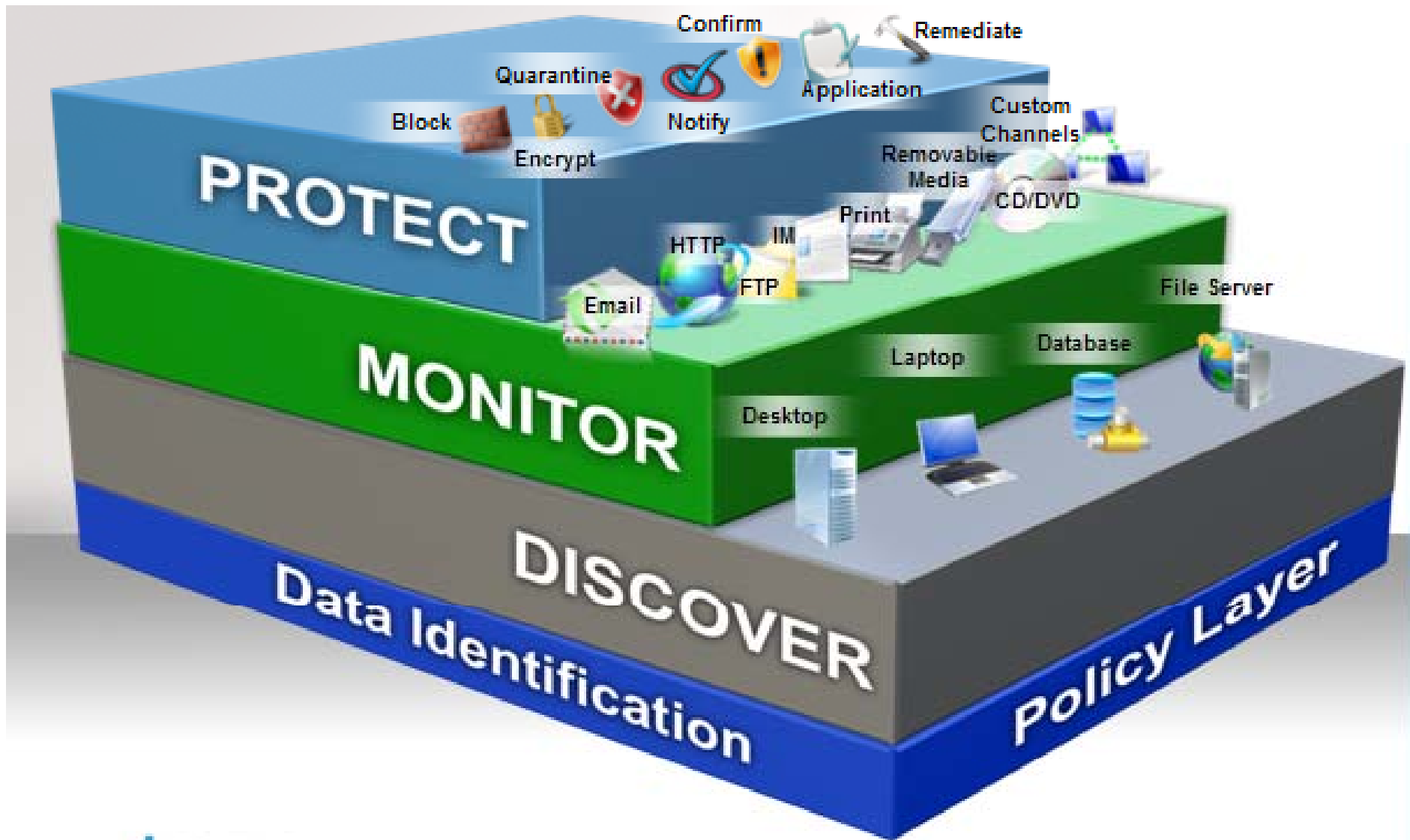
# WebSense Essential Information Protection

## The power of integration



# WebSense Data Security Suite

## Comprehensive Data Loss Prevention



# Data Security leverage other security technologies and Enables Business

•Can data be uploaded to this site



•URL  
•Filtering



•Can a specific user access this data



•Digital Vault/ DRM



•Can data be copied this device



•Device Control



•Is my data secured in the event it is lost



•Encryption



•  
**Websense  
Data Loss  
Prevention**

# Context VS. Content

## •People



- Who are your users?
- Who are the data stakeholders?
- Who should/not use your data?

## •Data



- What type of data do you have?
- Where is your data located?
- What is the value of your data?

## •Process



- What communication channels are in use?
- What are your data security policies?
- What are good/bad data processes?



# Business Intelligent Controls

## Data in Use/Motion



# Incident details

The screenshot displays the Websense Network & Endpoint management interface. On the left is a navigation sidebar with buttons for Overview, Incident Management, Reports, Status & Logs, Configuration, Administration, and Options. The main area is titled 'Network & Endpoint' and shows a list of incidents. Incident 13781 is selected and highlighted with a red box. Below the list, the 'Properties' tab is active, showing details for incident 13781. The details include the source (10.150.16.11), destination (72.14.247.83), and category (General Email). A list of violated policies is shown, with 'Social Security Numbers/SSN: delimited Social Sec...' and 'Social Security Numbers/SSN: Wide (1.3)' highlighted with red boxes. On the right, the 'Source Details' section is expanded, showing information about the user 'Doe, John' (jdoe) and their role 'Product Marketing Manager'.

**Overview**

**Incident Management**

- Network & Endpoint
- Discovery Overview

**Reports**

**Status & Logs**

**Configuration**

**Administration**

**Options**

**Network & Endpoint**

Assign... Release... More Actions Filter Favorites

Filter: All Incidents Number of Filtered Incidents: 266 Find ID: Go Clear

ID	Date & Time	Source	Policy Categories	Channel	Destination	Urgency	Action	Max Matches	Total Size
13781	14 Apr. 2009, 07:49:49 PM	10.150.16.11	Credit Cards; PCI; S...	ICAP	72.14.247.83	Moderate	Blocked, Notified, A...	16	3 KB
13772	14 Apr. 2009, 07:47:35 PM	10.150.16.11	Credit Cards; PCI; S...	ICAP	72.14.247.83	Moderate	Blocked, Notified, A...	1	53 B
13502	07 Apr. 2009, 04:19:51 PM	10.150.16.11	Credit Cards; PCI; S...	ICAP	205.178.152.58	Moderate	Blocked, Notified, A...	30	10 KB
13229	26 Mar. 2009, 05:39:18 AM	10.150.16.11	Credit Cards; PCI	ICAP	74.125.43.19	Moderate	Blocked, Notified, A...	1	109 B
13220	26 Mar. 2009, 05:37:51 AM	10.150.16.11	Credit Cards; PCI	ICAP	74.125.43.19	Moderate	Blocked, Notified, A...	1	53 B
13211	26 Mar. 2009, 05:35:01 AM	10.150.16.11	Credit Cards; PCI	ICAP	74.125.43.19	Moderate	Blocked, Notified, A...	1	57 B

**Properties** Forensics History ID: 13781

**Details:** ICAP http://mail.google.com/mail/?ui=2&ik=544109603c&at=&view=up&act=sm&jsid=gsgvu6sjsjoa&...

**Source:** 10.150.16.11 Incidents by this Source

**Destination:** 72.14.247.83 **Category:** General Email

**Violated Policies**

- 5144 xxxx xxxx 1108, 5370 xxxx xxxx 3020...5299 xxxx xxxx 1938, 4916 xxxx xxxx 8111
- Social Security Numbers/SSN: delimited Social Sec...** (PreciseID Patterns) 15 Matches
- Social Security Numbers/SSN: Wide (1.3)** (PreciseID Patterns) 15 Matches
- Social Security Numbers/SSN: Wide - ICAP & Lotus ...** (PreciseID Patterns) 15 Matches
- Social Security Numbers/US SSN (NLP Policy)** (PreciseID Patterns) 14 Matches

**Action:** Blocked, Notified, Audited

**Assigned to:** Unassigned

**Channel:** ICAP

**Protocol:** HTTP

**Incident Tag:** N/A

**Date & Time:** 14 Apr. 2009, 7:49:49 PM

**Source Details**

Full Name: Doe, John

Username: jdoe

Email: jdoe@demo.websense.com

IP Address: 10.150.16.11

Title: Product Marketing Manager

Manager: Madoff, Bernard

Phone Number: +1 301 9292333

admin Superuser

# Business Intelligent Controls

## Data at Rest

Who	What	Where	How	Action
Human Resources	Source Code	Desktop	Word	Audit
Customer Service	Business Plans	Laptop	Excel	Block
Marketing	Patient Information	File Server	PowerPoint	Notify
Finance	M&A Plans	Database	Database	Remove
Accounting	Employee Information	Document Mgmt. System	PDF	Encrypt
Sales	Financial Statements	Email Repository	PST File	Quarantine
Legal	Customer Records	Personal Storage Device	Excel	Confirm
Technical Support	Technical Documentation			
Engineering	Competitive Information			

# Discovery incident details

Discovery Overview > **Discovery Incident Management**

Filter: Default Filter Number of Filtered Incidents: 3 Find ID: Go Clear

**Properties** History ID: 13722

File Name: \\demo-xp.demo.websense.com\C\$\sample-data.pdf

**Violated Policies**

Credit Card Numbers for Discovery/CCN - Default (Discovery) (1.2) (PreciseID Patterns)	30 Matches
5270 xxxx xxxx 5516, 5370 xxxx xxxx 3020...783, 4916 xxxx xxxx 6147, 3020xxxxxxx4838	
Sensitive and Private information for Discovery/Sensitive Private: US Credit C... (PreciseID Patterns)	30 Matches
5270 xxxx xxxx 5516, 5370 xxxx xxxx 3020...783, 4916 xxxx xxxx 6147, 3020xxxxxxx4838	

**More Details**

Local Date Detected: 14 Apr. 2009, 05:11:46 PM GMT-0400  
Analyzed by: Endpoint Server DEMO-DSS.demo.webser  
Action: Audited  
Assigned to: Unassigned  
Channel: Endpoint Discovery  
Incident Tag: N/A  
Discovery Task: N/A

**File Permissions**

LOCAL_SYSTEM	[RW]
BUILTIN_USERS	[RW]
BUILTIN_ADMINISTRATORS	[RW]
DEMO\JDoe	[RW]

**File Details**

File Size:	178 KB
Date Created:	07 Apr. 2009, 09:18:54 PM GMT-0400
Date Modified:	07 Apr. 2009, 09:18:55 PM GMT-0400
Date Accessed:	07 Apr. 2009, 09:18:55 PM GMT-0400
File Owner:	DEMO\JDoe

**Host**

Hostname:	demo-xp.demo.websense.com
IP Address:	10.150.16.11

**Endpoint Details**

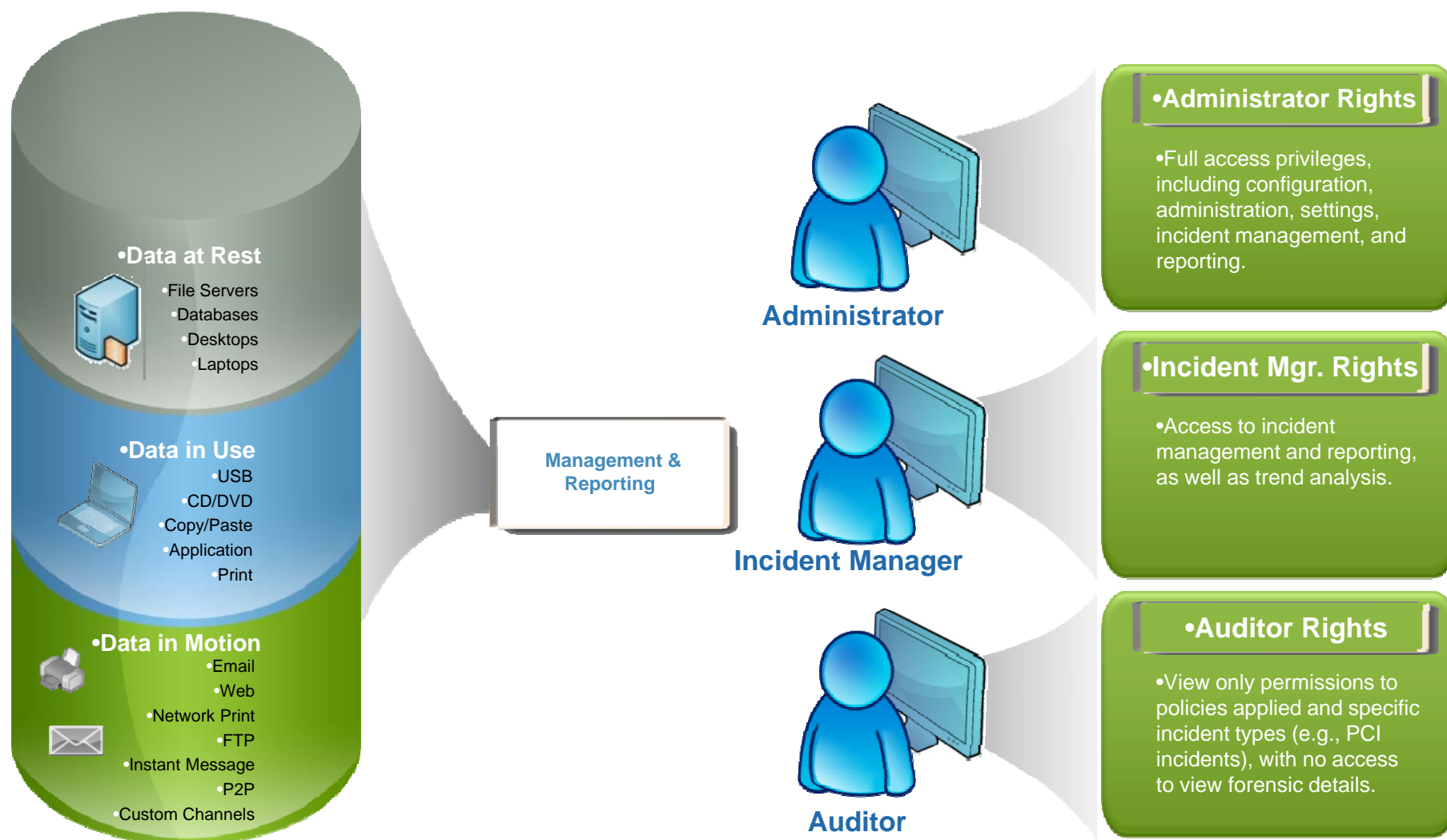
Endpoint Type:	Desktop
----------------	---------

**Other**

Run As User:	DEMO\JDoe
Checksum:	8050341179335465403
File Owner Name:	DEMO\JDoe
File Owner SID:	S-1-5-21-2301113347-732623881-...



# Unified Management and Reporting – Use DSS as part of your business process



## Application Awareness and Control

- Pre-classified and categorized applications
- Data and user policy controls for individual or categorized applications

The screenshot shows the 'Application Selection' tab of the Windows Firewall rule configuration. The 'Single Application' radio button is selected. The 'Application Name' field contains 'Yahoo Messenger' and the 'Executable Name' field contains 'YAHOOM'. The 'Application Group' dropdown menu is open, showing '--- Select Group ---'. The 'Operation Selection' section is partially visible, showing 'Apply the following settings:' and a list of operations with their status: Print (Block Operation), Cut/Copy (Allow Operation), Paste (Apply Content Policies), File Access (Apply Content Policies), and Screen Capture (Allow Operation). The 'Anywhere' radio button is selected under the 'When connected to corporate network' section.

**Applications > Edit Application**

Define a new application, select an existing one or select a group of applications from the list:

**Application Selection**

☒ Single Application

Application Name:  [Select Application](#)

Executable Name:

☐ Application Group:  ▼

**Operation Selection**

Apply the following settings:

Print	<input type="text" value="Block Operation"/> ▼
Cut/Copy	<input type="text" value="Allow Operation"/> ▼
Paste	<input type="text" value="Apply Content Policies"/> ▼
File Access	<input type="text" value="Apply Content Policies"/> ▼
Screen Capture	<input type="text" value="Allow Operation"/> ▼

When connected to corporate network:

☒ Anywhere

☐ When connected to corporate network

☐ When NOT connected to corporate network

Application Group

--- Select Group ---

--- Select Group ---

Collaboration

**Instant Messaging**

P2P File Sharing

Telephony, Conferencing, ..

Web Browsers

CRM

Data Warehousing, Analyti..

Contact Managers

ERP, SCM

Word Processing

Spreadsheets

Project Managers

Email

Database

Presentation

**Applications**

☒ Enabled

Operations can be limited per application.  
Add applications and specify operation limitations.

Name	Location Based Enforcement	Print	Copy	Paste	Save	Run
<input type="checkbox"/> Notepad (NOTEPAD)	Always					
<input type="checkbox"/> Microsoft Word (winword)	Always					
<input type="checkbox"/> Yahoo Messenger (YAHOOM)	Always					
<input type="checkbox"/> Default NOT Connected	NOT Connected					
<input type="checkbox"/> Default Connected	Connected					

**Add...** **Remove**

**Legend:** Allow Operation Block Operation Apply Content Policies

- **Automated vs. Manual Policy Application**
- **Websense has pre-categorized applications**
  - Use Case Example: Apply Content Policies for AOL, but Block ALL other IM

# Websense = Superior Value

- Vendor Consolidation
  - Web Security Email Security and Data Loss Prevention, all from Websense
- Hardware Consolidation
  - Integrated components and flexible architecture
  - Support for virtualization
- Built-in Proxy
  - Websense can inspect HTTP/S traffic without a third party solution.
  - Others may require the purchase of another proxy at each site for HTTP/S traffic analysis. Integration will not provide destination awareness and control.
- Long Term Fit
  - Websense supports open integrations and co-existence
  - Websense is highly scalable and distributable – will grow with your business
- Consolidated Platform
  - Network and Endpoint Data Loss Prevention
  - Data Loss Prevention and Web Security

# Customers Who Trust Websense

## Global Coverage and Support

- Over 50,000 customers worldwide
- Over 41 million subscription seats
- 5,000 value-added resellers
- Award-winning global support and services

### Financial Services



### Healthcare - Insurance



### Government



### Technology



### Telecommunications



### Transportation - Energy



### Manufacturing



### Retail



### Media





# Q&A

