



Understanding and Selecting a DLP Solution

FINANCIAL

Rich Mogull Securosis



No Wonder We're Confused

- Data Loss Prevention
- Data Leak Prevention
- Data Loss Protection
- Information Leak Prevention
- Extrusion Prevention
- Content Monitoring and Filtering
- Content Monitoring and Protection





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

FINANCIAL

-Rich Mogull





Feature vs. Product

Includes some of the detection and enforcement of DLP products, but are not dedicated to the task of protecting content and data. Centralized management, policy creation, and enforcement workflow dedicated to the monitoring and protection of content and data.



Financial Services Uses

• Protect customer PII from leakage

- Support PCI, GLBA, and breach notification compliance
- Identify locations of PII/ account information in storage
- Automatically encrypt outbound customer communications with account information
- Scan employee laptops for unprotected account information
- Stop transfer of financial information to portable storage





In Motion At Rest In Use



	000 =:=		1	11	0
0	8	1)	1	0
Ĩ	£		1		ľ





Content Awareness

 Context scanning is different from content scanning

- You want both
- Understand the different between simple metadata and business context





INFORMATION SECURITY DECISIONS

Rules

Regular expressions, keywords, and other basic pattern matching techniques best suited for basic structured data. $\label{eq:2.1} $$ $ (?:(?<Visa>4\d{3})|(?<Mastercard>5[1-5]\d{2})|(?<Discover>6011)|(?<DinersClub>(?:3[68]\d{2})|(?: 30[0-5]\d))|(?<AmericanExpress>3[47]\d{2}))([-]?)(?(DinersClub)(?:\d{6}\1\d{4})|(?(AmericanExpress)(?:\d{6}\1\d{4})))$$

Credit Card Numbers

^(?!000)(?!666)(?<SSN3>[0-6]\d{2}|7(?:[0-6]\d|7[012]))([-]?)(?!00)(?<SSN2>\d\d)\1(?!0000)(?<SSN4>\d{4})\$

Social Security Numbers

Regular expressions from: Jerry Schmersahl at http://regexlib.com/DisplayPatterns.aspx?cattabindex=3&categoryId=4





Database Fingerprinting

FINANCIAL

 Searching for exact matches to data loaded from a database, which can include multiplefield combinations.







Exact File Matching Binary Hash



Partial Document Matching

- Cyclical hashing, sometimes with additional linguistic analysis
- Eliminate whitespace, hash a range, offset, hash again







INFORMATION SECURITY DECISIONS

Statistical Analysis

 Bayesian, machine learning, and other statistical techniques that analyze a corpus of content to recognize other content that may be similar.







Conceptual/Lexicon

 A combination of dictionaries, rules, and other analysis to protect loosely defined ideas.







INFORMATION SECURITY DECISIONS

Categories

 Pre-built categories with rules and dictionaries for common types of sensitive data.







Technical Architecture





Data In Motion







Data In Motion







Data In Motion







Blocking

Bridge, Proxy, or Inject





Content Discovery





FINANCIAL



Endpoint

Storage

Application/Server





Content Discovery







Content Discovery







Content Discovery







Enforcement Actions

- Alert/Report
- Warn the User
- Quarantine- Move
- Quarantine- Encrypt
- Quarantine- Access Controls
- Remove/Delete





Endpoint Priorities

- Portable Storage
- Unmanaged Networks
- Data in Use







Endpoint Layers











Central Management





INFORMATION SECURITY DECISIONS

Directory Integration







Hierarchical Management

FINANCIAL

Corporate HQ





Role Based Administration

- System Administrator
- Policy Creator
- Incident Handler
- Investigator
- Business Unit Manager
- Supervisor





Dashboard

ecutive Sun	imary Report	t														
Filter																
Incidents	by Action Tak ts by Action 1	ken and by Urg Taken	Jency					Incidents	s by Urgency =							
Incluen	Audited	Plackod		remented	Delease	a	Total	Inclucio	Cultical	_	Forloug	1-1	todovato		Tatal	
Incidents	Audiceu	39	324	icrypteu	n Release	.u 0	363	Incidents		4	= senous	58	nouerace	301	TUCAI	36
Inclusiones		22	001		2	2	000	Including	-	-				001	-	00
Top Incide	nts by Chann	nel														
Channel						Inciden	ts									
SMTP Ma	l .					1				224	4.1%					
ICAP										87	1.1%					
SMTP Ma	y Ly									28	14%			1.1	SMTP N	Mail
e msnms										4	1.5%				ICAP	
Show all w	7									-	24.000				FTP Pro	oxy
SHOW AIL											24.0%				SMTP N	Mail .
														61.7%	 msnms 	
Top Policy	Category															
Top Policy Policy Cat	Category 2gory		Erit	ical	= Serio	IS	⊒Mo	oderate	Total		Number of	Incidents				
Top Policy Policy Cate	Category egory		Ecrit	ical	<mark>≓</mark> Seriou Q	IS	1 Me	oderate	226	227	Number of	Incidents			Crit	itical
Top Policy Policy Cate OLPTT Acceptable I	Category egory		= Crit	ical	Seriou	15	1 10	oderate	226 38	<u>227</u> 50	Number of 200	Incidents			Crit	itical
Top Policy Policy Cate OLPTT Acceptable I Malicious Co	Category egory Jse ncealm		E Crit	ical	Serio	IS	1 10 44	oderate	Total 226 38 0	227 50 45	Number of 200	Incidents			E Crit Ser No	itical erious oderati
Top Policy Policy Cate OLPTT Acceptable I Malicious Co Social Securi Eactory Tec	Category egory Jse ncealm ty Nu		E Crit	ical	■ Seriou 0 2 1 0	15	1 10 44 0	oderate	Total 226 38 0 7 6	227 50 45 7	Number of 200	Incidents			Crit Set Mo	itical erious oderate
Top Policy Policy Cate OLPTT Acceptable I Malicious Co Social Securi Factory Tes	Category egory Jse ncealm ty Nu is		= Crit	ical	<pre></pre>	15	10 44 0	oderate	226 38 0 7 6	227 50 45 7 6	Number of 200				Crit Ser Mo	itical erious oderat
Top Policy Policy Cate OLPTT Acceptable I Malicious Co Social Securi Factory Test Show All»	Category egory Jse ncealm ty Nu s		E Crit	ical	2 2 1 0 0	15	10 10 14 0 0	oderate	226 36 0 7 6	227 50 45 7 6	Number of 200	Incidents			Crit Ser No	itical erious oderat
Top Policy Policy Cate OLPTT Acceptable I Malicious Co Social Securi Factory Tesl Show All»	Category 2gory Jse ncealm ty Nu s		Crit	ical	<pre></pre>	15	10 10 14 0 0	oderate	226 38 0 7 2 6	227 50 45 7 6	Number of 200	Incidents			Crit Ser Ndo	itical erious oderat
Top Policy Policy Cab OLPTT Acceptable I Malicious Co Social Securi Factory Tesl Show All»	Category 2gory Jse ncealm ty Nu s		E Crit	ical	0 2 1 0 0	15	10 10 44 0 0	oderate	226 38 0 7 5	227 50 45 7 6	Number of 200 150 50 0				Crit Ser Mo	itical erious oderat
Top Policy Policy Cab OLPTT Acceptable I Malicious Co Social Securi Factory Tesl Show All»	Category 2gory Jse ncealm ty Nu 5		E Crit	ical	2 2 1 0 0	15	10 10 44 0	oderate	Total 226 38 0 7 6	227 50 45 7 6	Number of 200 150 50 0 0	Incidents	Con south south	ay 16616	Crit Ser No	itical erious oderal
Top Policy Policy Cate OLPTT Acceptable I Małcious Co Social Securi Factory Tesl Show All»	Category 2gory Jse ncealm ty Nu 5		Crit	ical	2 2 1 0 0	15	1 10 44 0 0	oderate	226 38 0 2 5	227 50 <u>45</u> 7 6	Number of 200 150 50 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Incidents	Con. Social Securi	ary Testis	Crit Set	itical erious oderat
Top Policy Policy Cate OLPTT Acceptable I Malcious Co Social Securi Factory Tesl Show All »	Category 2gory Jse ncealm ty Nu is	Phing		ical	0 2 1 0 0	15	1 10 44 0 0	oderate	Total 226 38 0 2 5	227 50 45 7 6	Number of 200	Incidents	Con. Securi- Social Facti	ary Tests	Crit	itical erious oderat
Top Policy Policy Cat OLPTT Acceptable Malcious Co Social Securi Factory Tesl Show All >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Category 2gory Jse ncealm by Nu is es and Destin	vations		ical	Seriou Q Q Q Q Q Q	15	10 10 14 0 0	Destination	Total 226 38 0 7 5	227 50 45 7 6	Number of 200 160 100 50 000 ¹⁰⁷ Pcost	Incidents	Con Social Securit	ay 16515	Crit Set	itical erious oderat
Top Policy Policy Cate OLPTT Acceptable Malicious Co Social Securi Factory Tes Show All & Top Source Sources	Eategory :gory lise mceahin ty Nu s	nations ≣Critica	al j	Serious		is ite	10 10 44 0 0	Destination	Total 226 38 0 7 5 5	227 50 45 7 6	Number of 200 160 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ncidents	Con Social Secon Fact	ay 10 ⁵¹⁵	Crit Sec No	itical erious aderati
Top Policy Policy Catr OLPTT Acceptable I Malicious Co Social Security Factory Tesi Show All>	Eategory sgory Jse meadm ty Nu s es and Destin sstoa.com	Nations	al a	ical		15 16 16 16 15	■ Me 10 44 0 0 1117 101 1117 101	Destination sbesser@gma	Total 226 38 0 0 7 5 5 s s	227 50 45 7 6	Number of 200 150 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	r Sable Use National Serious	Con Social Security Fact	ay 16515 derate	Crit Set hko 154 85	tical tal
Top Policy Policy Cat OLPTT Acceptable I Malicious Co Social Securi Factory Tesi Show All » Top Source Sources demo-uno joseph.v@bf firefox@tesi	Eategory egory Jse Ise Nu s es and Destin estpa.com pa.com	nations ≡Critica	al a	ical		is ate <u>96</u> 84	1 10 14 0 0 0	Destination sbesser@gma 62.90.5.163 sharon@websa	Total 226 38 0 2 1 2 1 2 1 2 1 2	227 50 45 7 6	Number of 200 150 100 50 0 0 0 0 0 0 0 0 0 0 0 0 0	Table Use Nations	Con Securi- Social Feat	a) To ^{sto} derate	Crit Set Mo Tot 154 13	itical odera
Top Policy Cate OLPTT Acceptable I Malicious Co Social Securi Factory Tes Show All & Cop Sources demo-uno joseph. v@tc firefor@tes lam@testpa	Category ggry Jse ceah s s es and Destin estpa.com pa.com	tations ≡Critica	al =	ical	■ Serior 0 2 1 0 0 0 0 0 0 0 0 0 0 0 0 0	15 ate 96 84 84 12	1 10 44 0 2 2 Total 117 101 100 14	Destination sbesser@gma 62.90.5.163 sharon.besser	Total 226 38 9 0 2 5 2 5 - s - - energyabo - -	2227 500 45 ₹ 2 6	Number of 200 - 160 - 100 - 60 - 0 - ritical = 2 0 2 0 0 2 0 2 0 0	Landon Use Mandous	Con. Social Fraction 18 18 1	ar) Te ^{ste} derate	Crit Set No 154 85 13 3	tal
Top Policy Policy Cate OLPTT Acceptable 1 Malcious Co Social Securi Factory Tes Show All>	Eategory ggory Jse cceam s s set and Destin astpa.com pa.com com	rations <mark>≡</mark> Critic	al E	ical	■ Seriot 0 2 1 0 0	15 ate <u>96</u> 84 84 12 3	1 10 44 0 0 0 70tal	Destination sbesser@gma 62.90.51w8 sharon@vses sharon_besse disk.drive on the	Total 226 38 0 2 2 6 3 6 4 2 5 4 4 2 6 4	2227 50 45 5 5 5 5 5 6 6	Number of 200 150 100 60 0,07 ⁷ Pco ⁸¹	Incidents	Con. Securit Social Securit 18 18 2 1 2	ay Teate Jerate	Crit Set No 164 85 13 2 0	itical erious oderat 18 <u>10</u> 1
Top Policy Policy Cate OLPTT Acceptable 1 Malcious Co Social Securi Factory Tesi Show All.» Top Sources demo-uno joseph. v@bt firefox@testpa kim@testpa	Category cgory Jse ceaem ty Nu s s sspa.com com com	rations ≡Critic	al s Q Q Q Q	ical	■ Serior 0 2 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	ste 96 84 84 12 3	10 10 10 10 11 10 10 10 10 14 14 14	Destination sbesser@pma 62.905.163 sharon@web sharon_bess disk.drive.on.to	Total 226 38 2 3 2 5 5 5	2227 50 45 7 6	Number of 200 150 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	function of the second	Con Social Securit Faction 18 18 2 1 2	ay Te ^{sts} derate	Crit Sec No Sec No	itical erious odera
Top Policy Policy Cati OLPTT Acceptable I Malcious Co Social Secur Factory Tesl Show All/w Top Sources demo-uno joseph.v@bt frefox@Restpa uno@testpa	Category egory lse nceam by Nu s es and Destin estpa.com pa.com .com	Nations	al = 2 0 0	ical		15 nte 96 84 84 12 2 3	10 10 14 0 0 0	Destination besser@gma 62,905.163 sharon_bess disk.drive on b Show Ally	Total 226 38 0 5 5 s s s s s s s s s s s s s	2277500 45 7 2 6	Number of 200 150 50 0,0 ⁴⁷ Rec ⁸¹	f Jable Use Matching	Con Social Fact 18 18 2 1 2	ay Te ^{sts}	Core See Ide	itical erious odera
Top Policy Policy Cat OLPTT Acceptable I Malcous Co Social Secur Factory Tes' Show All>	Category egory like ncceam by Nu s s es and Destin sstpa.com pa.com .com	nations Critica	al = Crit	ical	© 2 2 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	15 96 84 84 12 2 2	E Ma 1 1 1 1 1 1 1 1 1 1 1 1 1	Destination besser Opma 62.90.5.163 sharon Desse disk drive on Lesse disk drive on Lesse Show All>	Total 226 38 9 3 9 2 2 4 5 4 5 4 s 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5<	2277 500 45 Z 6	Number of 200 150 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Incidents	Con Social Sector Factor 18 18 2 1 2	ማ 16 ⁸¹⁵ derate	Core See Hob Hob See Hob See Hob See	itical erious oderat 18 10 1
Top Policy Policy Cat OLPTT Acceptable 1 Malcious Co Social Secur Factory Tesis Show All>	Category egory Jse coeam ty Nu es and Destin sepa.com .com .com .com .com	tations ■ Critic.	al = 2 0 0 0	ical Serious Destinatio		15 96 94 84 84 12 2 3	■ Ma 10 44 0 0 Total 117 101 100 14 4 14 117 100 14 4 14 117 100 14 14 10 14 10 10 10 10 10 10 10 10 10 10	Destination sbesser@gna 62,905,163 sheron_besser dsk.drive on t Show Alla Policy	Total 226 9 7 5 5 1.com %PyAb %Category	2277 50 45 7 5 6	Number of 200 00000000000000000000000000000000	Serious	Con. Social Fact 18 18 2 1 2	ल्भ 10 ⁵¹⁵ derate 1	Critical Control Contro Control Control Control Control Control Control Control Control C	itical erious oderat tal <u>18:</u> <u>10:</u> 11:





W	1 11 11		1	Adm	ninistrator	Logout Preferences H
ERICEPT	ome Reports Sear	ch Categories Policies	Workflow	Administration	Help	
Reports: Homepage						
Filters: Categories	🔽 🛛 Date Rang	e 🔽 Fi	ter			
Category - Last 7	days (by day)	Top Hosts - Last 7 days	(by day)		Protocol - I	Last 7 days (by day)
	100	Host	Count	15.0	4	
12.5 -		10.7.1.2	60	15.0 -	1	
		10.7.1.11	49	12.5 -	- \	A
10.0 -		10.7.1.12	44	10.0		
7.5 -		us.f638.mail.yahoo.com	27	7.5	•	\times
5.0 - 2.5 - 0.0 -		us.f636.mail.yahoo.com	4	5.0 2.5 0.0		
It, Jacobian Security Number Per	11, 14, 11, 10, 10, 10, 10, 10, 10, 10, 10, 10				41, 14, 200, ➡ HTTP	41,15, 14,10, 14,20, 14,10, 14,00, 14,00, 14,10, 14,00,00, 14,00,00,00, 14,00,00,00,00,00,00,00,00,000,000,000,0

Showing first 10 results. Show All

		Date/Time	Category	State	Match Count	To Hoet	Protocol
ą,	•	2007-11-05 17:51:49.0	Personal Information	NEW	53	10.7.1.2	smtp
ł,	→ D	2007-11-05 17:51:49.0	Personal Information	NEW	53	us.f638.mail.yahoo.com	www-post
ł	+	2007-11-05 17:51:49.0	Personal Information	NEW	42	10.7.1.11	рор
ł.	+	2007-11-05 17:51:49.0	Personal Information	NEW	53	10.7.1.2	smtp





System Administration

FINANCIAL

- Performance Monitoring
- Backup and Restore
- Import and Export
- Load Balancing/ Clustering

- Database Management
- Archiving
- Endpoint Agent
 Management
- Storage Scanning/Agent Management

• User Management

Internal Groups





Policy Creation







INFORMATION SECURITY DECISIONS

Non-Technical Wizards





INFORMATION SECURITY DECISIONS

Test Mode

 Evaluate policies in monitoring only mode separate from production incident queue to support tuning.







INFORMATION SECURITY DECISIONS

Policies Are Data



- Hash, encrypt, and restrict policies
- Business unit policies may need to be restricted from handlers





Websense

W Websense Policy Wizard	
Add/Remove Policies Adding/Removing policies using pre-defined templates	CONTENT PROTECTION SUITE
To add or remove a policy, click its checkbox. Select a policy to view its c:	intents.
Policy Templates:	Policy Contents:
Templates Federal and Industry Regulations GLBA - Advanced Policy GLBA - Advanced Policy GLBA - Advanced Policy GLBA - Advanced Policy GLBA - Express Policy HIPAA HIPAA FERPA FERPA FIPEDA FIPEDA FFIEC	Rule Name GLBA rules for regulated database fields
E	Details: Regulatory requirements and compliance rules for GLBA
Image: State Laws Image: State Laws <t< td=""><td>1</td></t<>	1
	< <u>B</u> ack <u>N</u> ext > Dancel





Incident Workflow





INFORMATION SECURITY DECISIONS

Incident Queue

ID	Time	Policy	Channel	Severity	User	Action	Status
1138	1625	PII	Email	1.2 M	rmogull	Blocked	Open
1139	1632	HIPAA	IM	2	jsmith	Notified	Assigned
1140	1702	PII	НТТР	1	192.168.0.213	None	Closed
1141	1712	R&D/Product X	USB	4	bgates	Notified	Assigned
1142	1730	Financials	Storage	4	192.168.1.94	Encrypt	Escalated
1143	12/1/08	Source Code	Cut/Paste	12	sjobs	Confirm	Open





	nt						
🔲 Filter: Default Filt	er					Sho	owing 180 Inc
ement 🔲 Incident Manager	ment List						
Action 🔻	Find ID:	Go				1	K (1 2 3
ID Date & Tir	ne v	Source	Policy Category	Status	Action Taken	Urgency	Channel
<u>327</u> 06 Jun. 200	7, 04:50:59 PM	Mark Twain	Intellectual Property	/ Check w/ HR	Audited	Moderate	SMTP
✓ <u>322</u> 06 Jun. 200	7, 04:21:21 PM	TECH\jlondon	PCI - Express Policy	In Process	Audited	∃ Moderate	HTTP
321 06 Jun. 200	7, 04:19:55 PM	TECH\jlondon	PCI - Express Policy	In Process	Audited	Moderate	🔁 FTP
320 06 Jun. 200	7, 04:19:54 PM	TECH\jlondon	Encrypted File: E	In Process	Audited	E Critical	🛃 FTP
319 06 Jun. 200	7, 04:19:51 PM	TECH\jlondon	HIPAA; PCI - Expre	In Process	Audited	E Critical	🔁 FTP
	tion						
Incident Informa Properties Urgency: Modera	tion Forensics (ite Action Ta	History ken: Audited	Channel: @HTTP A:	ssigned To: dorit	<u>(</u>	<u>(</u>	K (1D: 322
Incident Informa Properties Urgency: Modera Details: http:// Source: TE Destination: w4.me Violated Policies Policy Category	tion Forensics (te Action Ta (w4.media-convert. CH\jlondon tdia-convert.com, C Policy Name	History ken: Audited com/cgi-bin/mcuplo ategory: Dynamic	Channel: HTTP A: ad3.cgi?sid=6t6ccfukvnqbv .Content	ssigned To: dorit 37629g7ie9ukr≶=e Violation Trigger	n Severity	6 (Daterti	M ID: 322
	tion Forensics Action Ta Action Ta (w4.media-convert. CH\jlondon cdia-convert.com, C Policy Name DET. CON Dia	History ken: Audited com/cgi-bin/mcuplo ategory: Dynamic	Channel: HITTP A: ad3.cgi?sid=6t6ccfukvnqbv Content Policy Type	ssigned To: dorit 37629g7ie9ukr≶=e Violation Trigger	n Severity	% Detecti	M ID: 322





Technical vs. Business

FINANCIAL

User interfaces and workflow should account for technical and nontechnical users





INFORMATION SECURITY DECISIONS

Single Incident View

WW .							Administrator	Logout Preference <u>s Help</u>
/ERICE	PT Home	Reports Se	earch Cate	gories Policies	Workflow	Administratio	n Help	
Events: Ev	ent Detail							
🖌 Actions 🖪	Back to Results 🕨 Fal	se Hit 🕨 Trai	nsfer to Self					[4 4 6 ▶ ▶]
Overview	Attributes Content	Highlight	Session Data	Workflow History	Attachment	ts		
Attributes		Matches					Workflow	
Severity:	<u>1</u> 4	ersonal custo	mer informatio	n 2. credit card nu	mbers 3. social s	ecurity numb	State:	NEW
Match Count:	40	ain just to sat	tisfy the buyer.	lastname firstnar	me address city s	state do	Priority:	1
Category:	VCPT/pcidss	to satisfy the	buyer lastna	me firstname addr	ess city state dol	o account#	Case:	2
Date/Time:	2007-11-21 08:00:07.0	ccount# date	lasttransaction	ssn creditcard # ex	pdate sheila walt	ters 19823 m	Organization	: Default
Protocol:	www-post	s.txt" content	-type: text/plai	n mastercard 5389	733663647952 5	243883980304	7 Reviewer:	unassigned
From Account:	2						Has Annotati	ons: false
To Account(s):	<u>v</u>							
From Host:	10.7.1.11							
To Host:	us.f638.mail.yahoo.com							
From IP:	10.7.1.11							
To IP:	69.147.97.199							
From Port:	1475							
To Port:	4							
Has Attachments:	true							
Log size:	0	. 1						





Ŵ	1 11 11	Administrator Logout Preferences He						
VERICEPT	me Reports Search Cat	egories Policies Workflow Administration Help						
Events: Event Detail								
Actions 🖪 Back to Results	False Hit Transfer to Self	4 4 10 } }						
Overview Attributes Lo	ntenti Higniight Session Data	WORKIOW HISTORY						
Content-type:text/html								
Yahoo! <u>My Yahoo! Mail</u> <u>Tutorial</u> Make Y! your home page	is More 🔻	Overview Attributes Content Highlight Session Data Workflow History						
Trate		Table of Matches						
XAHOO MAI	L	search job: 1 2 3						
		vour resume: <u>1</u> <u>2</u> <u>3</u>						
Mail 💌 Addresses 💌 O	Calendar 💌 Notepad 💌	post job: 1						
Check Mail Compose		cover letter: 1 2						
		Highlighted Content						
Vonage: 1 Free	<u>Previous Next Back to Messages</u>	http/1.0 200 ok server: microsoft-iis/6.0 content-length: 75648 content-type: text/html set-cookie:						
	Delete Reply 🔻 Forwa	ez=80201-80212%2b80214-80239%2b80241%2b80243-80244%2b80246%2b80248-80252%2b80254-80257%2b80259-80266%2b80270-80271%2b80273-80275%						
Folders [Add - Edit]	This massage is not flawed I at	expires=sat 12 apr 2008 19:43:16 gmt; patn=/; domain=.monster.com set-cookie: mnsnp9=1; expires=sat 15 mar 2008 21:43:16 gmt; patn=/; domain=www.monster.com; set-cookie: jsintabtest=a; expires=wed 14 nov 2007 19:43:16 gmt; patn=/; domain=monster.com; cache-control: max-age=826						
🛱 Inbox (1)	This message is not hagged. [Flag	date: mon 15 oct 2007 19:43:16 gmt connection: keep-alive < ldoctype html public "-//w3c//dtd html 4.01 transitional//en"						
🔍 Draft	Date: Sun, 8 Apr 2007 00:23:11	nttp://www.w3.org/tr/ntm4/loose.atd > find jobs, network, build a better career, monster works for me, monster.com looking for a job/ <a <br="" id="hdu2">href="http://mv.monster.com/" style="color: #639";>log in help looking to hire? post idb is search resumes my monster account resumes quickapply apply						
Sent Cont	From: "Lawrence Cole" <vrcptico< td=""><td colspan="7">history cover letter is questionnaires my profile (beta) my local forums jasper find jobs saved jobs job search agents company research (beta) diversity job</td></vrcptico<>	history cover letter is questionnaires my profile (beta) my local forums jasper find jobs saved jobs job search agents company research (beta) diversity job						
Bulk [Empty]	Subject: 🖉 Customer Confidentia	search iss feeds job search (beta) security center post resume build online copy & paste upload word (.doc) privacy plus security center resume writing services money credit insurance real estate retirement money management taxes education choose your career path select the right degree find the right school						
Garash [Empty]	To: 🛞 "Tammy Lee" <vrcpttle< td=""><td>pay for school manage your time job fair s calendar pre-register contact us for exhibitors career advice get the job on the job take a break in the spotlight</td></vrcpttle<>	pay for school manage your time job fair s calendar pre-register contact us for exhibitors career advice get the job on the job take a break in the spotlight						
		community monster blog monster services security center contact us job search : enter keywords (e.g. nurse sales) select category accounting/auditing						
		arts entertainment and media automotive/motor vehicle/parts banking biotechnology and pharmaceutical building and grounds maintenance business						
		opportunity/investment required career fairs computer services computers hardware computers software construction mining and trades consulting services						
		consumer products creative/design customer service and call center education training and library electronics employment placement agencies energy/utilities						



Other Workflow Features

- Case management
- Incident correlation
- Hierarchical incident management
- Identity correlation
- Historical analysis
- Reporting





Top Five Features

- ✓ Content Analysis
 - **Technical Architecture**
- ✓ Central Management
- ✓ Policy Creation
- Incident Workflow



The 3-Step Selection Process

- Define scope and set expectations
- Formalize requirements
- Evaluate and select





Form Selection Committee

FINANCIAL

 The selection committee should represent key stakeholders from IT and business





Determine Protected Content Types

- PII/NPI
- Credit card numbers
- Social Security Numbers
- Healthcare data
- Engineering plans
- Chemical formulae
- Research documents
- Customer lists
- Corporate financials
- Source code
- Media files
- Legal documents





Define Protection Expectations

FINANCIAL

 Determine where you want to protect the data, how you want to protect it, and set appropriate expectations.







Outline Process Workflow





Formalize Requirements

- Issue a formal RFI
- Create a draft RFP
- Confirm requirements with selection committee





Evaluate and Select

- **1. Issue the RFI**
- 2. Perform paper evaluation
- **3.** Bring in 3 vendors for on-site presentations and risk assessment
- 4. Finalize RFP and issue to your short list

- **5.** Assess responses and begin deep testing
- 6. Select, Negotiate, Buy

How To Test

O SearchFinancialSecurity.com

- Compare products side by side
- Create a few representative policies
- View results in monitoring mode
- Test for false negatives
- Lab-test enforcement
- Lab-test integration

Financial Services Considerations

FINANCIAL

Focus on products with database fingerprinting

INFORMATION SECURITY DECISIONS

- Test carefully, and confirm exchange method meets your security requirements
- Bad or test data can interfere with enforcement
- Don't forget to use discovery

O SearchFinancialSecurity.com

 FS is the primary market for these tools, so they tend to be well suited for your environment





Key Testing Criteria

Policy creation and content analysis.

- Email integration.
- Incident workflow- with real handlers.
- Directory integration.
- Storage integration on major platforms to test performance and compatibility for dataat-rest protection.
- Endpoint functionality on your standard image.
- Network performance- not just bandwidth, but any requirements to integrate the product on your network and tune it. Do you need to pre-filter traffic? Do you need to specify port and protocol combinations?
- Network gateway integration.



Navigating the Maze

- Understand your needs first, then start the selection process
- Focus on policy creation, workflow, and integration with your infrastructure

- Point solutions can solve part of the problem, but broad suites provide more flexibility
- Test products head to head





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

FINANCIAL

-Rich Mogull





Rich Mogull Securosis, L.L.C.

FINANCIAL

rmogull@securosis.com
http://securosis.com
AIM: securosis
Skype: rmogull