

proofpoint[>]

Defend Email. Protect Data.



Defend
Prevent
Analyze
Encrypt



July 20, 2008

Best Practices for Email Security and Data Loss Prevention



- > Messaging Security**
 - Trends: Email, Spam and Data Loss**
 - Why Accuracy Matters**
 - Virtualization**
 - Data Loss Prevention**
 - Proofpoint Introduction**

What is Messaging Security?



Security threats have always been a problem to enterprises

“Inbound” Threats Came First

“Outbound” Threats Followed

Spam

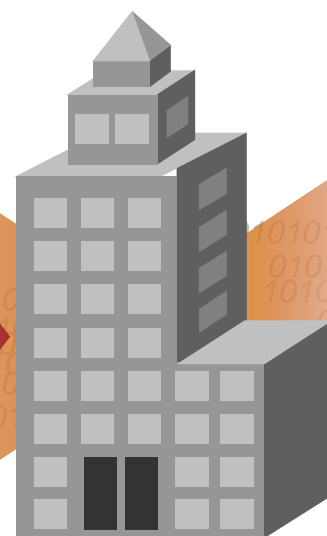
Viruses

Phishing

Denial of service

Botnets

Directory harvest



Enterprise

SMTP, HTTP and FTP services

Corporate governance

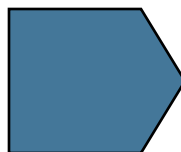
Security, privacy and compliance

Intellectual property

3 Major Email Trends

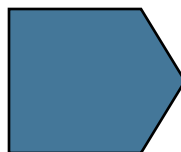


➤ **Email traffic doubling every year**



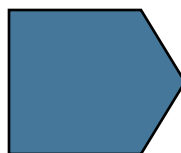
➤ **End users and corporate networks are overwhelmed**

➤ **Average message size has tripled**



➤ **Additional spending required to manage infrastructure demands**

➤ **80% of corporate information and data is stored in email**

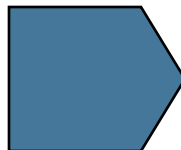


➤ **Email is the most critical application for most companies**

3 Major Spam Trends

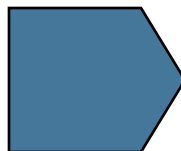


➤ **Rise in spam volumes**



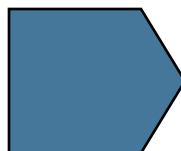
➤ **End users believe effectiveness has declined**

➤ **Rise of botnets**



➤ **Shorter, more intense, spam attacks**

➤ **Rise of new spam (PDF, Images)**



➤ **Spam circumvents filters, *drops* true effectiveness**

Spam continues to be a problem facing organizations

3 Major Corporate Data Loss Trends in '07



> **26% leaked sensitive data**



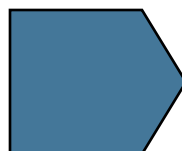
> **PR and financial nightmare**

> **20% subpoenaed for email records**



> **Costly business interruption**

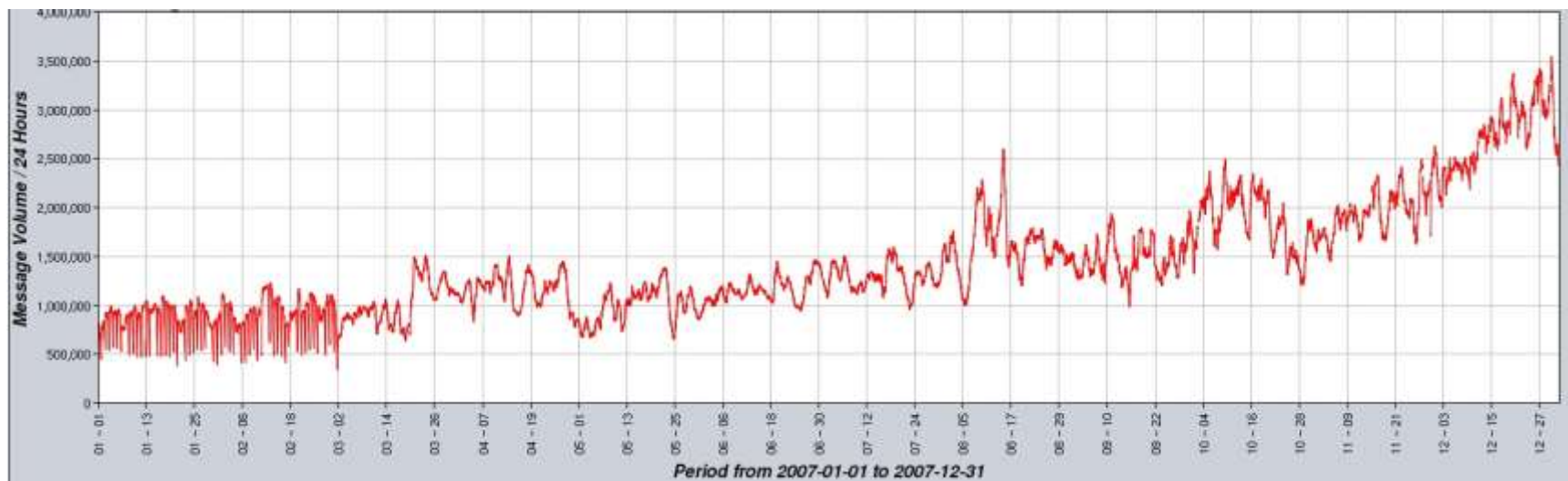
> **20% outgoing emails contained content that posed legal, financial or regulatory risk**



> **Companies are increasingly at risk**

Data Loss Prevention is a rapidly growing business risk that email security groups must face

2007 Spam Volume Trends



- **Proofpoint continually monitors spam levels and trends throughout the world**
- **Spam increased by 4x in 2007**
 - Doubled in the last 2 months alone

Recent Increases in Spam Volume



SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

SC Newswire
MAGAZINE

Pump-and-dump scam spikes spam by 445 percent

Illena Armstrong

Related Articles

[Storm worm still raging, now with new fake news stories](#)

[Email security vendors see PDF spam spike](#)

Spammers, hoping to score thousands of dollars in stock they've flimflammed targets into purchasing, have flooded email boxes with one of the largest pump-and-dump scams in history.

The attack likely has been spawned from another larger virus blitz that has been in the works since July, which has already been called the largest blended assault on end-users in two years —

the ultimate goal being the expansion of the "Storm Worm" botnet.

COMPUTERWORLD
Security

100 BEST PLACES TO WORK IN IT 2007 VIEW NOW

JUMP TO

Record-breaking 'Storm' linked to spam surge

Biggest, baddest e-mail malware ever, says researcher

Gregg Keizer [Today's Top Stories](#) or [Other Security Stories](#)

Comments (2) Recommendations: 31 — [Recommend this article](#)

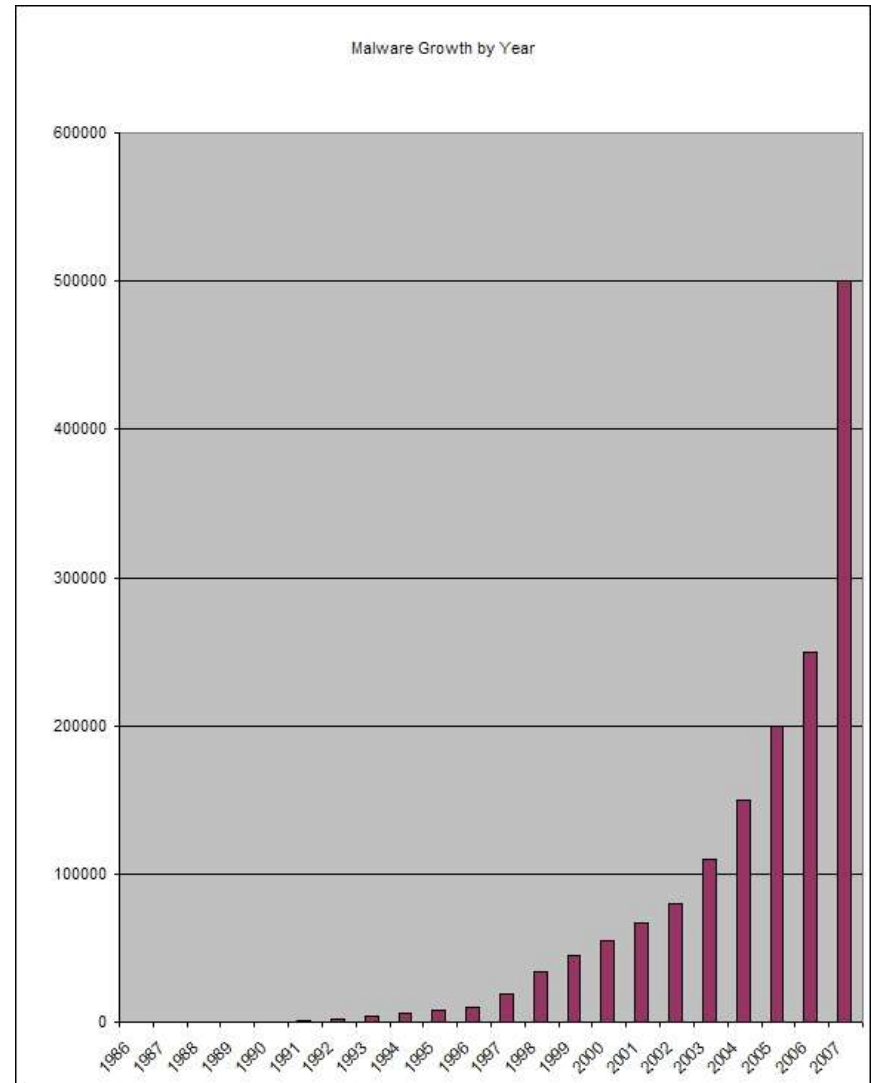
August 14, 2007 (Computerworld) — Storm, the Trojan horse that collects PCs into hacker-controlled botnets, roared back into life last month in several waves, security researchers said Monday, and has blown by 2005's Sober to become the most prolific e-mail-borne malware ever.

- Recent spam attacks have raised baseline spam volume
- Trend expected to continue in 2008

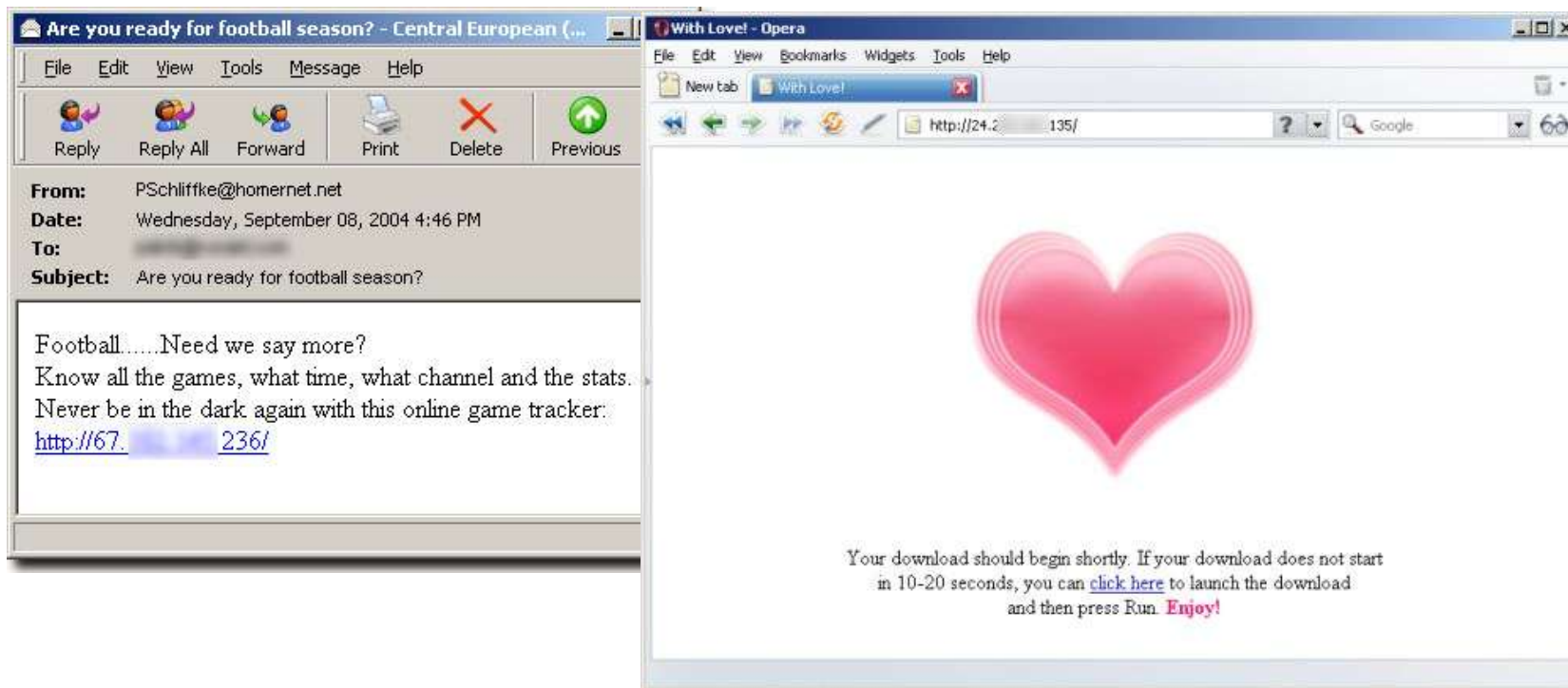
Malware Growth



- > **As many new malware samples detected in 2007 as in the prior 20 years combined**



Spammers Use Social Engineering



➤ Emails contain content about current hot topics

- Encourage users to download related app such as video codec
- When users click on URL, malware download is initiated

Spam Leverages Current Events



PCWorld Search PC World

Home News Hardware Reviews Software Reviews

Holiday Spirit Spread Malware

The Storm worm network nearly doubled in size over the Christmas holidays.

Robert McMillan, IDG News Service
Saturday, January 12, 2008 11:00 AM PST

PRINT E-MAIL COMMENT RSS

SLASHDOT IT DIGG THIS DEL.ICIO.US NEWSVINE

Recommend this story? Yes 13 Votes No 0 Votes

Some clever, sexy Christmas-themed spam and a long holiday season helped the criminals behind the notorious Storm Worm more than double their network of infected PCs over the past few weeks, security experts say.

Storm kicked off its holiday spam-and-malware campaign on the day before Christmas, sending off a flurry of e-mail that invited victims to visit a Christmas-themed strip show on Web sites such as Merrychristmasdude.com. Victims who downloaded the strip show found their PCs attacked by malicious software.

NETWORKWORLD

Mortgage misery a boon for spammers

Submitted by [Paul McNamara](#) on Wed, 01/30/2008 - 9:39am.

There's at least one group for whom the mortgage crisis and refinancing activity is nothing but a shady business opportunity: spammers.

And they're making life even more miserable for legitimate e-mail users, especially those who have no choice but to use language that spam filters flag and snag.

➤ More examples of spam leveraging current events

Google “I’m Feeling Lucky” Spam



From: "Peoples, Wayne" <Wayne.Peoples@theperfectinterview.com>
Subject: JANUARY 85 % OFF!
Mon, 7 Jan 2008 02:33:27 -0100

<http://www.google.co.uk///search?hl=en&q=inurl%3Athereseason.com+V6J+5C6&btnl=745>



Spammers now abusing search engines

- Spammers include link to Google search in email
- URL includes string which triggers the “I’m Feeling Lucky” features
- Users click link and are redirected to spammer page

Spear Phishing Attack Targets Students

Spear phishers target US students

Attacks disguised as 'database update'

Written by Shaun Nichols in California
vnunet.com, 04 Feb 2008

Print  Discuss  Send to a friend  Share 

A new spear phishing attack is targeting the email accounts of US university students.

Researchers at [Sans Institute](#) said that the attacks are disguised as messages from administrators performing a 'database update'.

The messages state that in order to keep their [email accounts](#), the students must 'verify' the accounts by replying to the message with details such as user names, passwords and date of birth.

- Spear phishing on the rise
- Recent attack directed at students attempting to solicit access to email accounts
 - Email states that user's account will be deleted unless they respond

What Else is New?



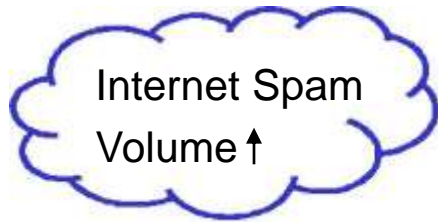
- Mp3 spam
- “3D image spam”
- Zip spam
- .xls/.doc spam
- Extreme obfuscation

- **MLX will continue to evolve to stay ahead of emerging threats**



H*E,R E WE GO AGAIN_!
'H_E B_I'G O,N_E BE+FORE T,H*E SEPTEMBER'+.RALLY!
T'H_E MARK ET IS ABOU+T TO P+O+P., A_N+D SO IS E+X,M_T+!
Fi+rm: EXCHA'N,GE M_OBILE T_E L+E (O-ther O_T+C : EXM T.PK)
Ti_ck: E+X-M-T
A-s'k*: 0 .'0,8
5-da,y p'ot.ential: 0+..4_0
T'h'i*s a g+reat oppo_rtuni_ty to at le-ast doub,le up!
N,o't o+n,l+y d.o e_s t'h.i_s f+i_r_m h,a+v+e gre.at funda-ment,als, b u't
gettin g t+h*i-s op+portun ity at t.h,e right ti'me, righ+t befo*re t'h*e
rall_y is w+h.a+t ma kes t'h.i*s d.e_a+l so swee_t!
Watc-h it s,o,a*r'!

3 Steps for Handling Volume Growth



Step 1:

Goal:

Improve Bandwidth Utilization
"Less traffic. More efficient processing."

Solution:

Connection management
(local or global reputation)

Proofpoint Solution:

Dynamic Reputation with netMLX
Proofpoint on Demand
Recipient Verification

Step 2:

Goal:

Limit amount of spam getting through.
"Best accuracy."

Solution:

Best filter effectiveness

Proofpoint Solution:

99.8% accuracy with MLX

Step 3:

Goal:

Boost Gateway Capacity
"More computing resources."

Solution:

More servers (physical or virtual)
Capacity Planning

Proofpoint Solution:

Master/Agent Architecture
Virtual Edition

Why Effectiveness Matters



	<i>2007</i>
<i>Volume (msg/day)</i>	500 Thousand
<i>Effectiveness</i>	94%
<i>Spam hitting Exchange</i>	30,000
<i># Users</i>	20,000
<i>Spam/User</i>	1.5 spams

Why Effectiveness Matters



	2007	2008
Volume (msg/day)	500 Thousand	2 Million
Effectiveness	94%	95%
Spam hitting Exchange	30,000	100,000
# Users	20,000	25,000
Spam/User	1.5 spams	4 spams

Why Effectiveness Matters



	2007	2008	
Volume (msg/day)	500 Thousand	2 Million	2 Million
Effectiveness	94%	95%	<u>99%</u>
Spam hitting Exchange	30,000	100,000	20,000
# Users	20,000	25,000	25,000
Spam/User	1.5 spams	4 spams	<u>0.8 spams</u>

Better effectiveness = Better load on mail servers (Exchange, Notes) =
Less spam in users' Inbox = fewer Help Desk calls

Why Are Some Solutions Failing?



Competitors offer “static” technologies

- Relying on exact matches of spam senders and content
- New spam is dynamic in nature – IPs, images, content
- Permutations are endless!

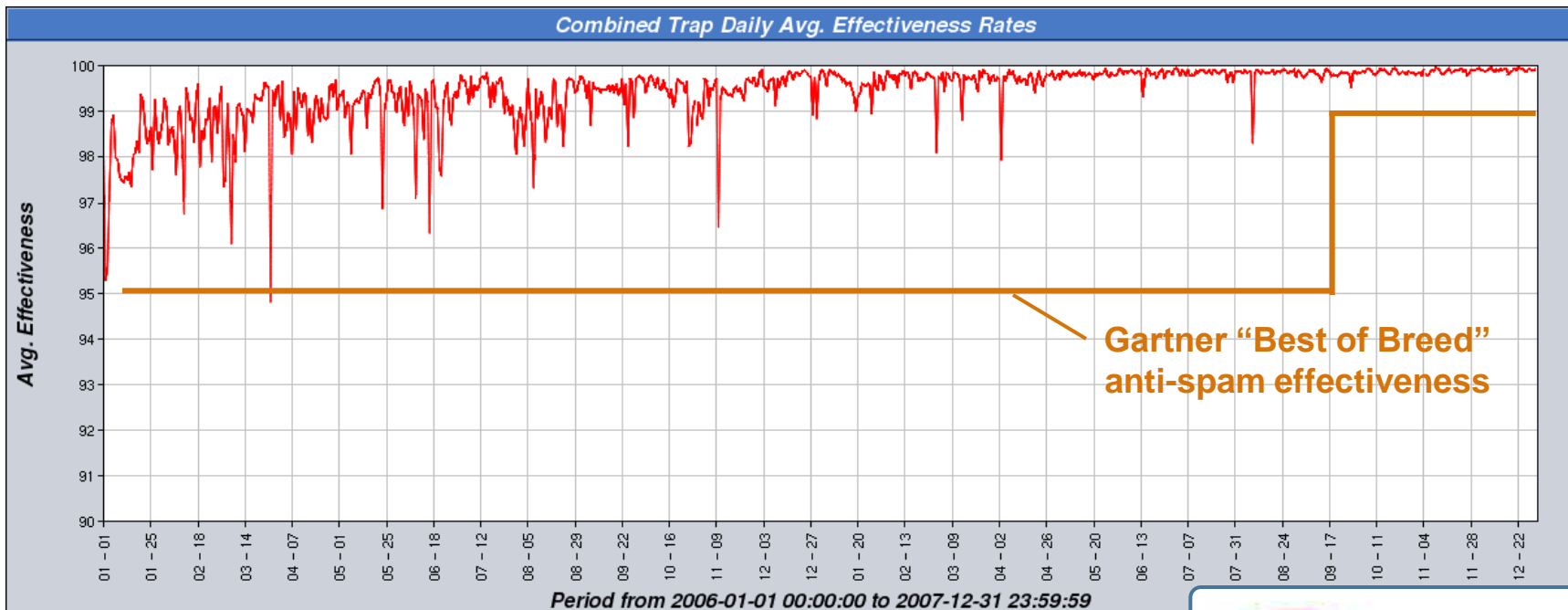
- Reputation
 - *How*: Match sending IP addresses and rules
 - *Problem*: Image-based spam comes from botnets, with rotating IPs.

- Signature
 - *How*: Match copy of email (or partial copy) against database
 - *Problem*: Image-based spam’s random images & text; endless permutations

Proofpoint’s MLX technology is dynamic and well-suited to the dynamic nature of spam

Accuracy Consistently >99.5%

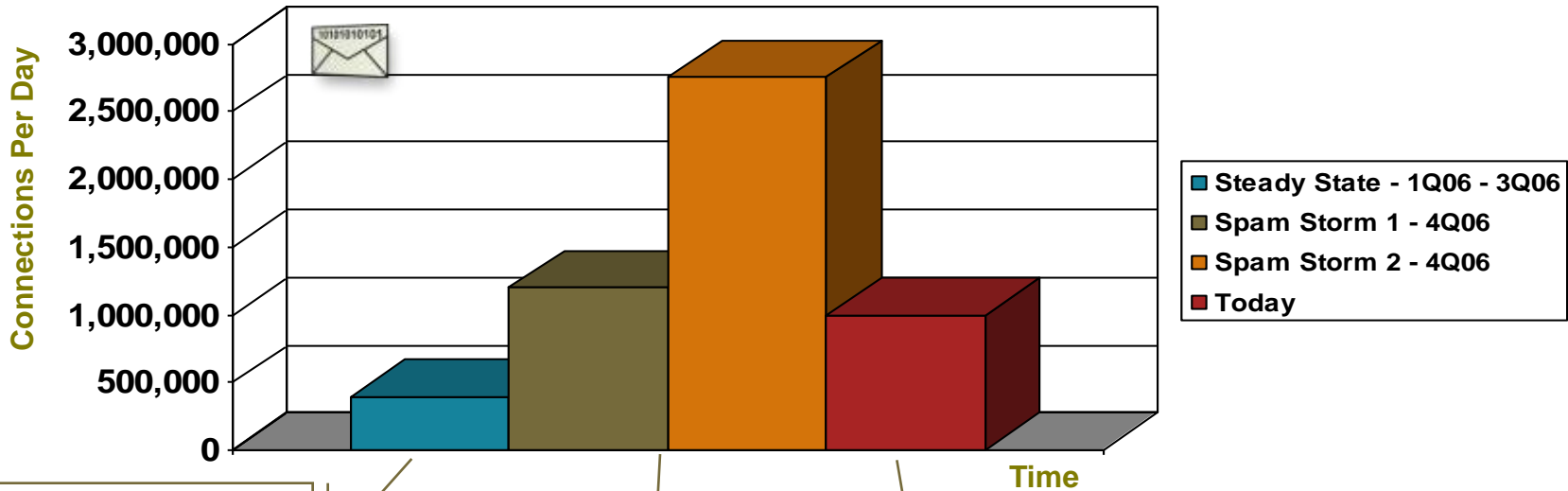
Less Spam = More Satisfied Users & Reduced Load on Mail Servers



"We reduced spam with a 99.998% effectiveness rate overnight. There was not a single false positive"

Proofpoint automatically adapts to new spam techniques

Case Study: Cincinnati Bell's Email Volume Growth and Dynamic Capacity Planning via Virtualization

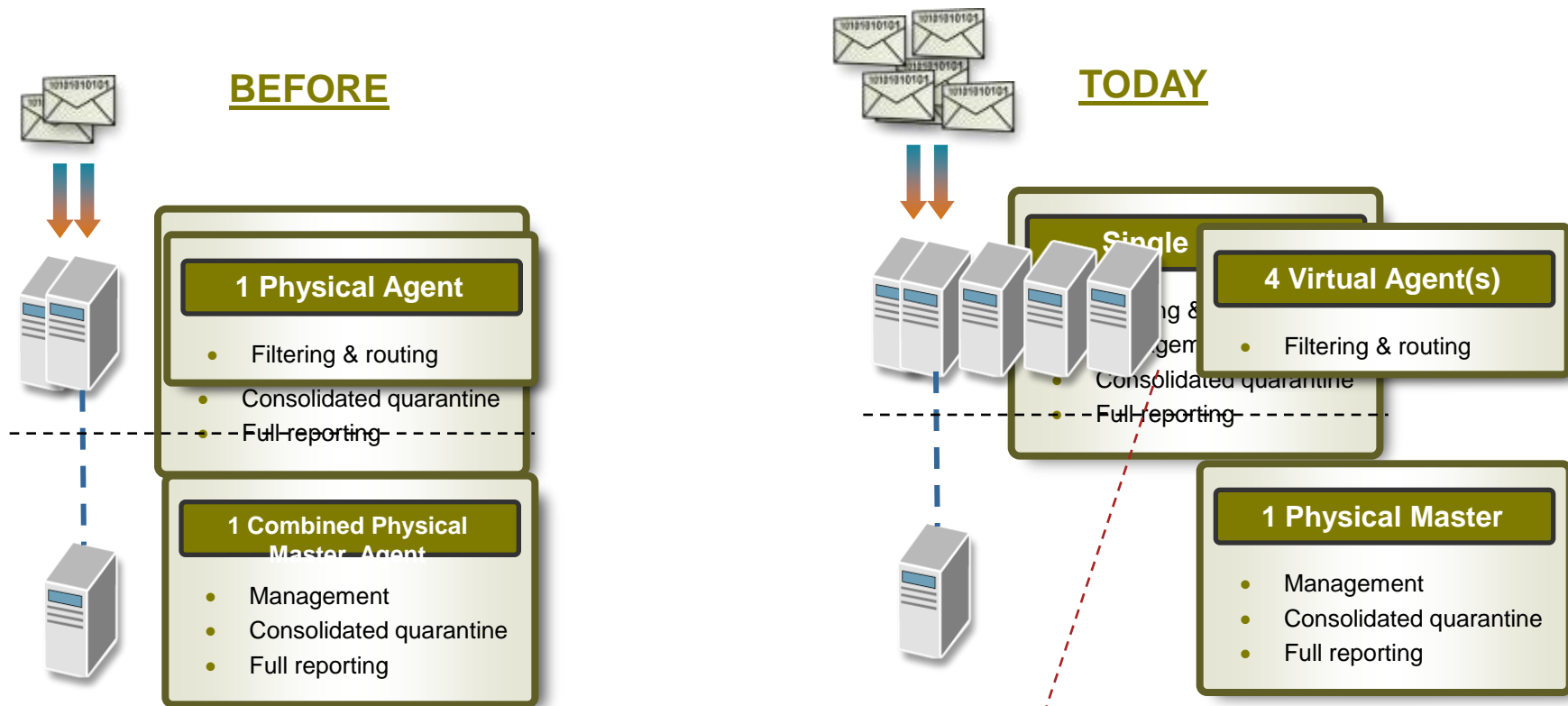


Appliances Needed: 2
Physical Appliances Used: 2

During spam storm, needed new appliances to handle load.
Added virtual appliances, but in the end retired physical appliances.

Appliances Needed: 5
Physical Appliances Used: 1
Virtual Appliances Used: 4

Proofpoint's Virtual Edition and Modular Architecture Allows Cincinnati Bell to Reap Benefits of Virtual Appliances



Can provision as many virtual agents as needed

Data Loss Prevention



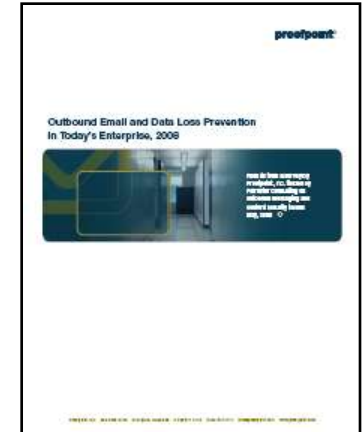
- **Protect information**
 - Structured: SSN, bank account, credit card, dictionaries/smart IDs
 - Unstructured: Financials, press releases, CAD drawings
- **Adhere to regulatory compliance**
 - HIPPA
 - GLBA
 - PCI
- **Integrated with content inspection and policy engine**



Forrester 2008 Email & Data Loss Prevention Survey 400+ Organizations

> Who was surveyed:

- Director Level to C-Level
- Public / Private
- Evenly distributed: 1000 to 20,000+ employees
- Participating companies in US, UK, France, Germany and Australia



> Real Business Risk

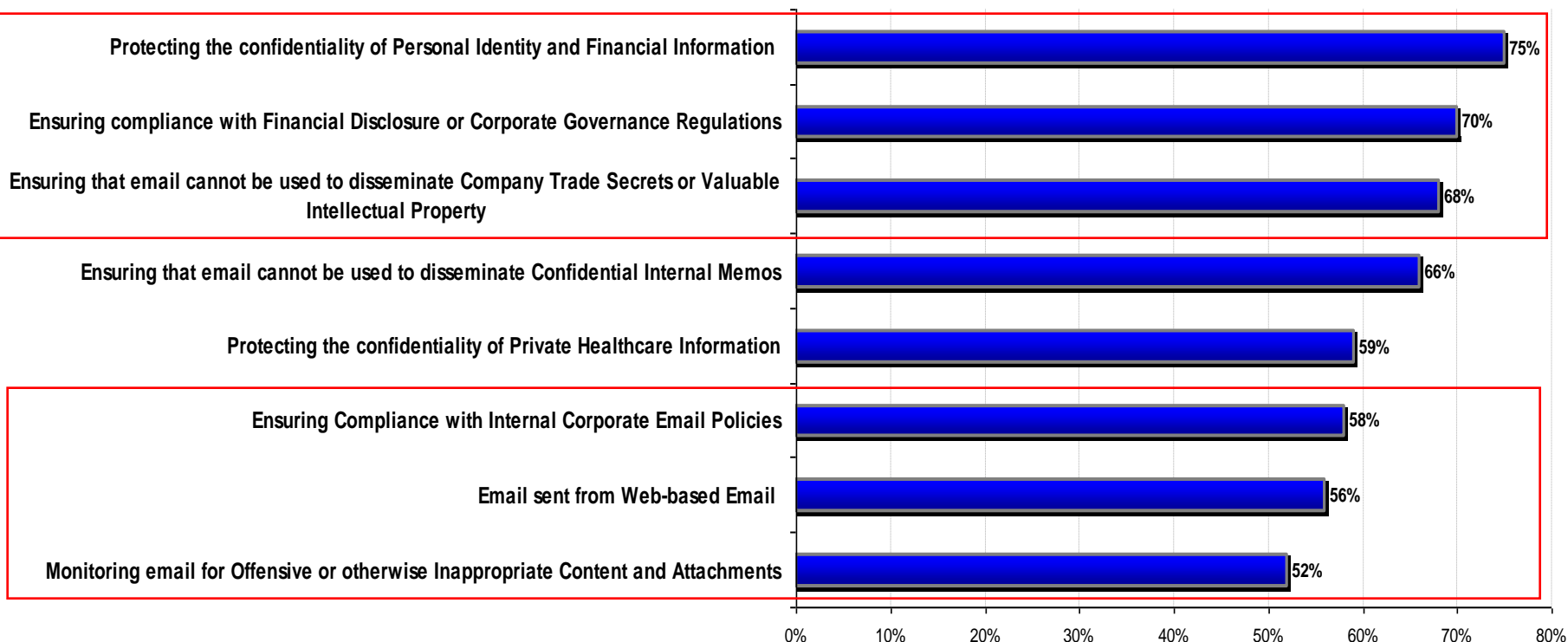
- 68%: At least 2 out of 3 are concerned with protecting the confidentiality of personal identity, financial info, trade secrets or intellectual property in outbound email
- 51%: More than half say it is important to reduce legal and financial risks associated with outbound/HTTP email
- 38%: More than 1 in 3 perform regular audits of outbound email content
- 27%: More than 1 in 4 investigated exposure of confidential sensitive or private information
- 23%: About 1 in 4 was impacted by the exposure of sensitive or embarrassing information in the last 12 months

Forrester 2008 Email and DLP Survey

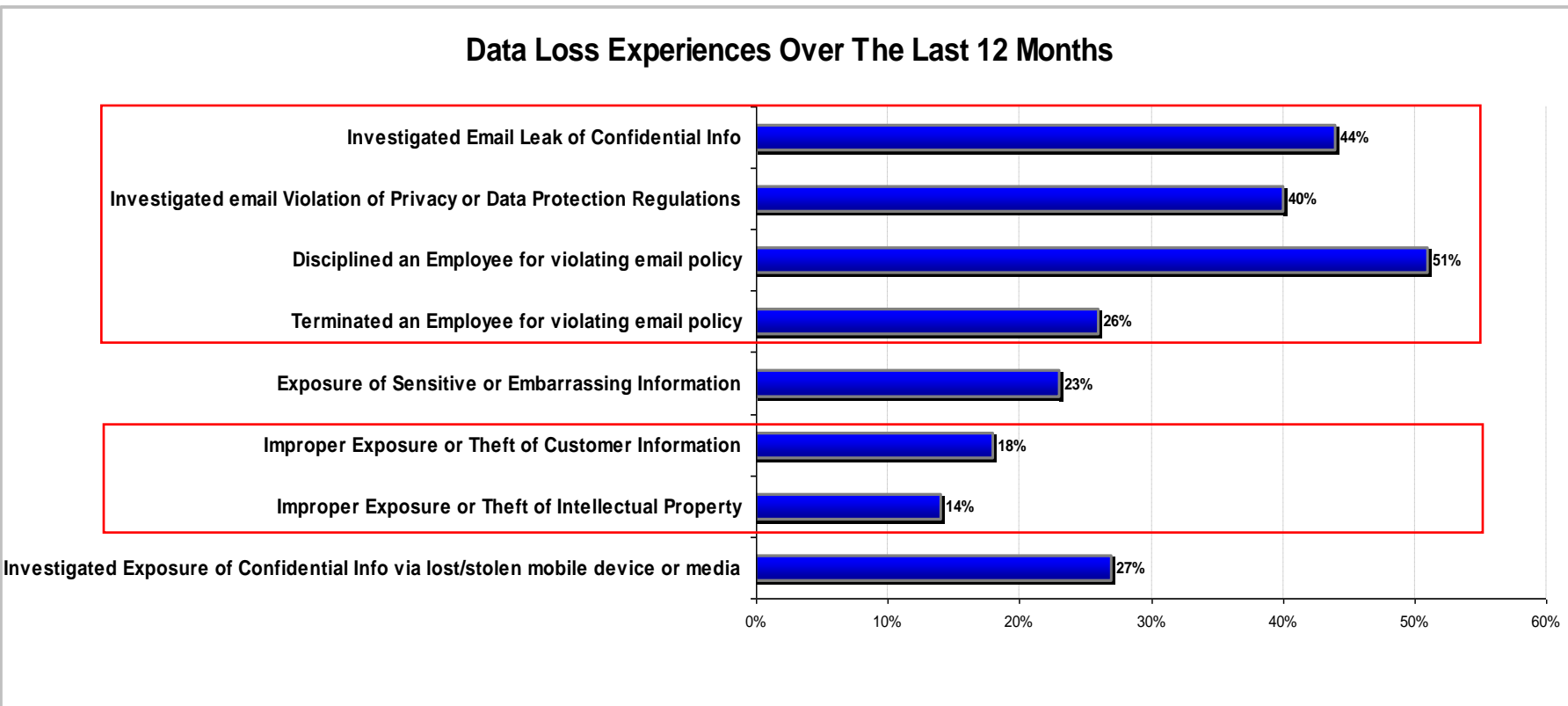
Outbound Email Concerns



Outbound Email Concerns 2008



Forrester 2008 Email and DLP Survey Data Loss Experiences

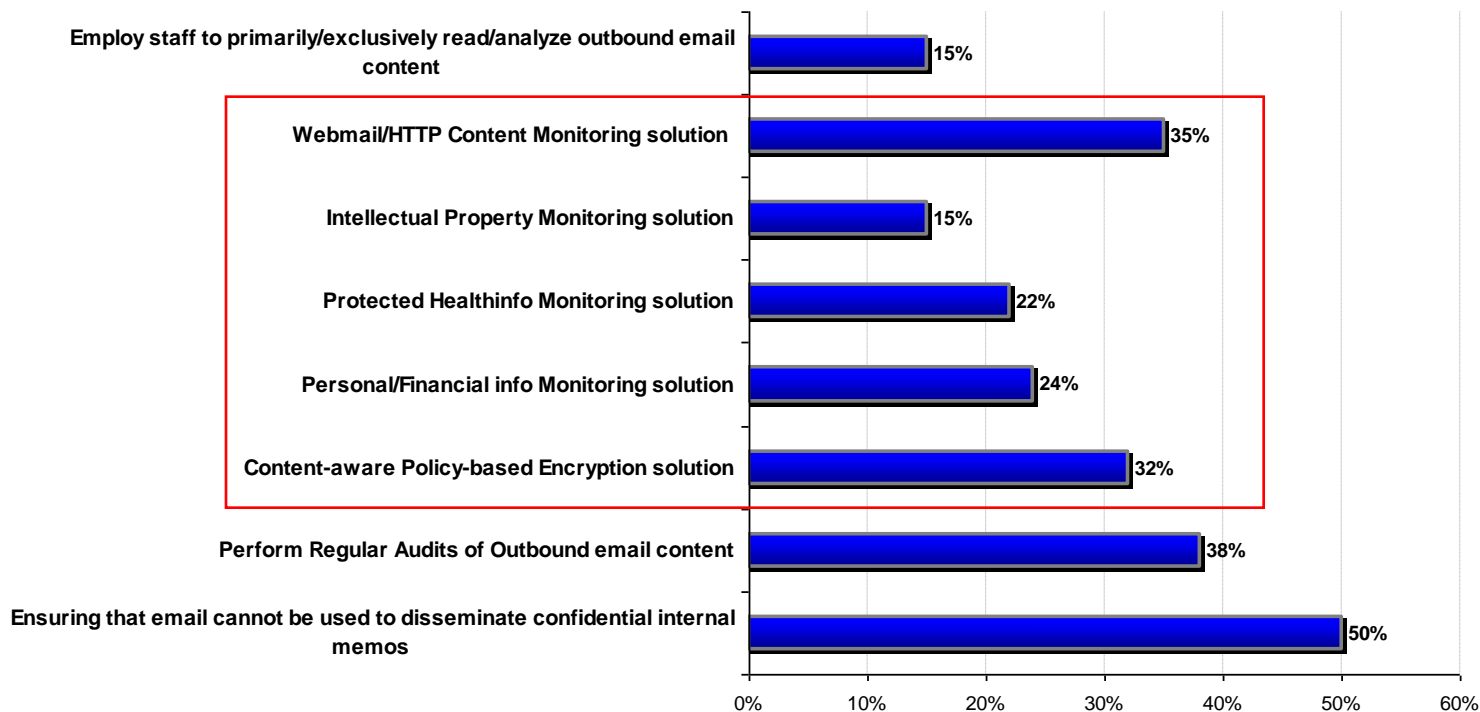


Almost of 1/3 of Companies “Don’t Know” the % of outbound email that poses Legal, Financial or Regulatory Risk

Forrester 2008 Email and DLP Survey Mitigation Process & Technologies



Adoption of Technologies to Mitigate Outbound Risks



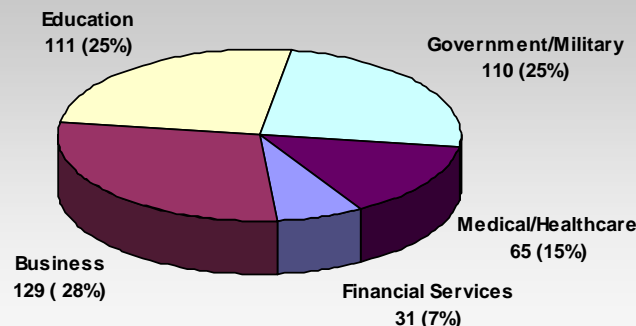
Data Breach Incidents



2007 (Published) Data Breaches

Total Breaches: 446

Exposed # of Records: 127,000,000



- Top documented 25 data breaches in 2007 resulted in 125,000,000 lost customer/private records
- 2008 tally (as of 5/1/08):
 - >140 incidents, > 10M records

Top Data Breaches (2006-2008)	Exposed No. of Records
TJX Corp	94,000,000
Dept of Veteran's Affair	28,000,000
Hannaford Bros. supermarket chain	4,200,000
Fidelity National Information Services	8,500,000
Georgia Dept. of Community Health	2,900,000
Chase Card Services	2,600,000
University of Miami	2,100,000
Texas Guaranteed Student Loan Corp	1,300,000
Chicago Board of Elections	1,300,000
SAIC (military contractor)	867,000
Gap Inc.	800,000
UCLA	800,000

Data Leakage Is A Huge Business Problem

Cost of Data Breach



> Damages

- Cost per record: \$197
- Average total cost per reporting company ~\$6.3M
- TJX severed ~\$500M - \$1B as a result of breach
- Lost business account for 65% of data breach costs

> Regulation Penalties

- PCI: Penalties up to \$500K or even losing privilege to process credit card transactions
 - Visa has begun levying fines of \$25K/month to Level I merchants for non-compliance
- GLBA: Civil and criminal penalties for noncompliance
 - Fines up to \$1M or 1% of total assets
 - Civil penalties up to \$100K and key officers up to \$10K per violation
- HIPAA: Civil and criminal penalties for noncompliance
 - Up to \$25K for multiple violations in a calendar year
 - Up to \$250K and/or imprisonment up to 10 years for known misuse of individually identifiable health information

Inadvertent/Unintentional Data Leakage Examples

- Insurance staff at a bank sending customer private data to insurance carriers
- Mortgage/escrow staff sending customer loan applications/data to title companies
- Hospital staff/doctors/patients communicating medical/personal information over email
- Staff members sending work files to personal email accounts to work at home
- Legal department sending sensitive corporate data to other legal entities
- Employees sending CEO/sensitive memos to friends & family or posting info to blogs/websites

“75% of US companies are concerned about protecting the confidentiality of personal identity and financial information in outbound email”

Forrester 2008 Outbound Email and DLP Survey

“63% of respondents stated that they send work documents to personal e-mail address so that they can access them from home”

RSA survey 2008

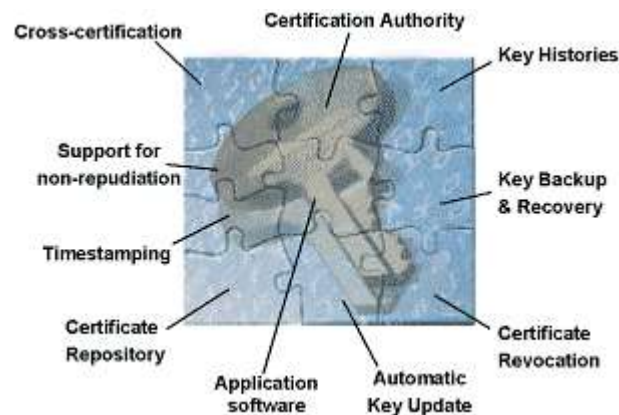
Encryption: Why Isn't All Email Secure?



- **The perpetual goal**
 - Provide secure email that is transparent to the user
- **The perpetual challenges**
 - Key management – PKI!
 - Requirement for client software
 - Complex
 - Expensive message storage
- **Why now?**
 - There are new mandates

“An estimate of 43% of outbound emails that should be encrypted are actually sent in encrypted form”

*Forrester 2008
Outbound Email and
DLP Survey*



Why Are Outbound Threats Occurring?



$$\text{no. of channels} \times \text{P(Data Loss)} = \text{data availability}$$

- **Email**
 - biggest thru 2010*
- **Blogs, FTP, HTTP, IM**
- **New Channels**



- **Email is everywhere**
 - 70% of corporate data lives in email
- **File Servers**
- **Desktops**
- **Laptops**
- **USB Thumb Drives**

Outbound Messaging Security Best Practice



> Define Policies

- Document
- Communicate
- Train

> Map Solution to Requirements

- Corporate governance content
- Structured
- Unstructured
- Auto-Encrypted

Implementation of Email-related Security Policies (All Companies, 2007)



Proofpoint Overview



- Unified email security and data loss prevention solutions
- 24x7 support
- Fastest-growing young technology company in North America

#1 on Deloitte's Fast 500 "Rising Star" List 2006

Focus On...

- Research and innovation
- Messaging security
- Customers

Customers



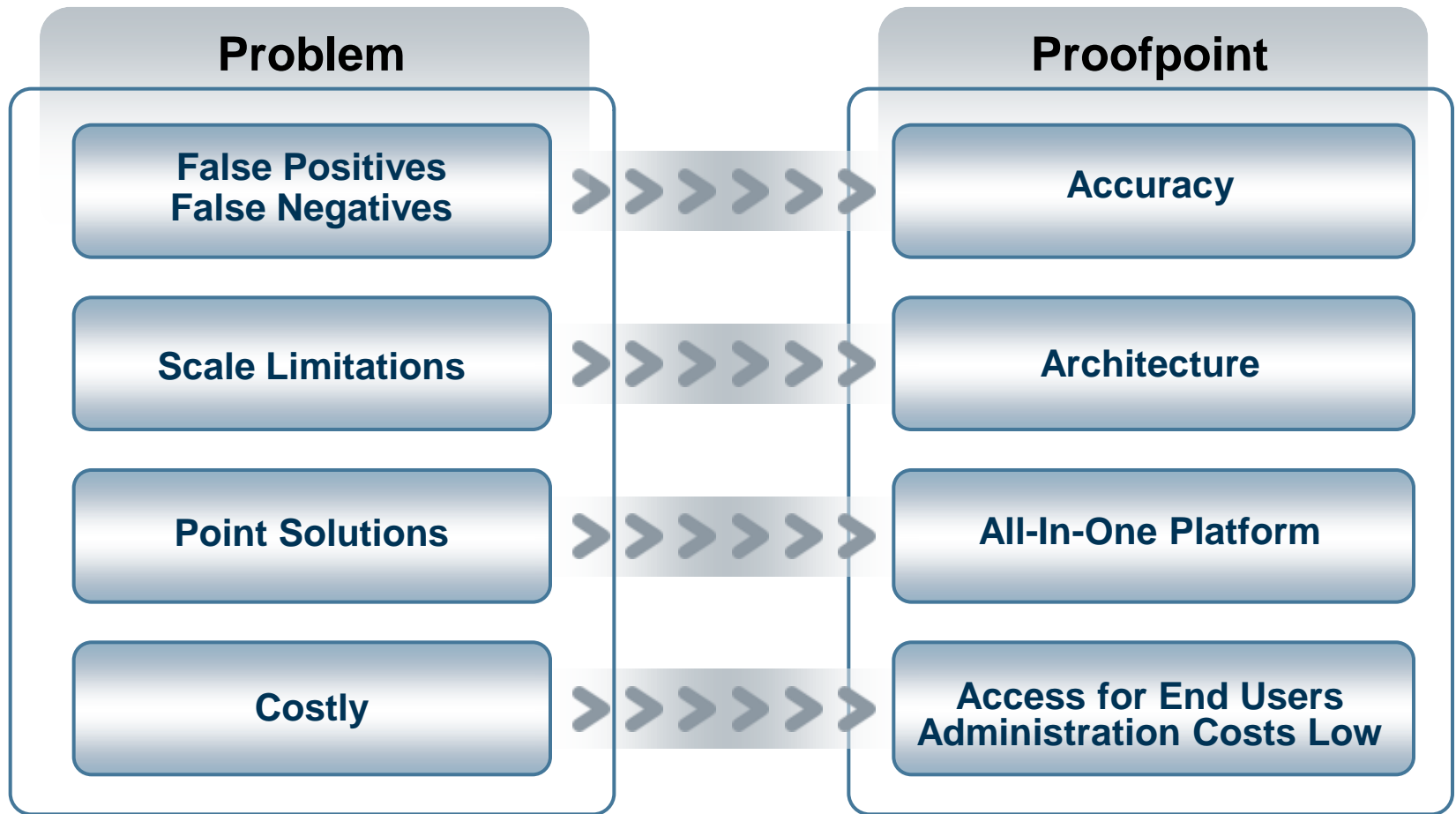
Partners



Validation



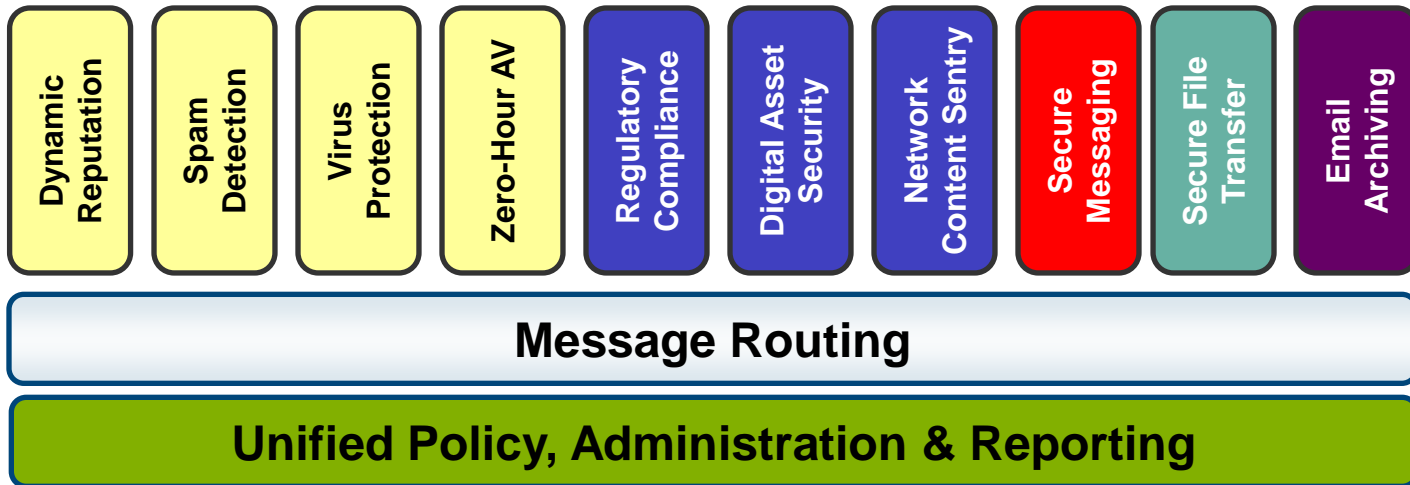
Proofpoint Summary



Complete Platform For Email Security & Compliance



Proofpoint Attack Response Center



Proofpoint helps you:

- Defend against inbound threats
- Prevent leaks of information
- Encrypt sensitive information
- Archive email securely



We Partner with Patriot Technologies



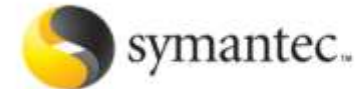
- **Our Mission:** to be the trusted, go-to source for comprehensive IT security solutions
- **Our Customers:** 1000s of commercial and government organizations worldwide
- **Our Partners:** best-of-breed security technology providers

Client Overview

Federal Government







Commercial



Our Solutions

A comprehensive suite of security solutions:

- Security Tools 
- Professional Services 
- Security Appliance Manufacturing 




Contract Vehicles



- **GSA #GS-35F-4363D**
- **Consulting and Technical Services (CATS) Contract MD CATS Contract #050R5800338**
- **DLA BPA# SP4700-02-A-0005**
- **ESI BPA# FA8771-06-A-0303 (Securify)**
- **ESI BPA# W91QUZ-07-A-0003 (BigFix)**
- **NIH BPA# HHSN 263999900685B**
- **BPA# W91QUZ-06-A-0005 (Websense)**
- **Federal ID #52-1957100**
- **CAGE Code: 07FD4**
- **DUNS: 933945248**
- **GSA Agent and Teaming Programs Available**

Why Patriot?

- **A single source for all IT security needs**
- **Objective analyses based on security best practices**
- **A proven track record of success**
- **Our team**
 - Seasoned, certified security professionals
 - Experts on regulatory requirements and best practices

Thank You



For questions about this presentation or
for general information about Proofpoint, contact us at:

info@proofpoint.com

408-517-4710

www.proofpoint.com