

E-Mail Systems Report

Powered by Congruity Technologies'



Network Quality Assurance Software

Documents Email system usage statistics for stakeholder planning and management event and for independent verification of regulatory compliance efforts

Prepared for: Sample Compliance Report

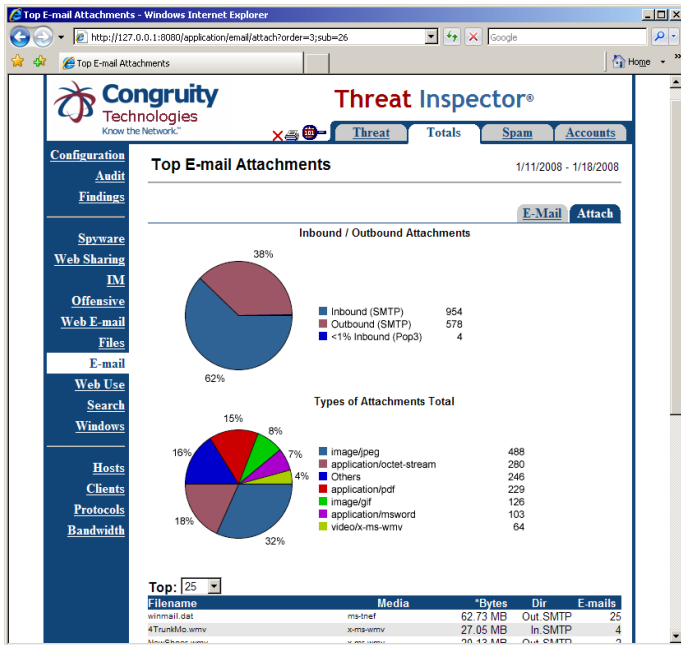
Contents:

- Introduction 3**
- E-mail (SMTP and POP3) 4**
 - Top E-mail Senders 5
 - Top E-mail Receivers 6
 - Internal POP3 Accounts 7
- Attachments (SMTP and POP3) 8**
 - Unsafe Attachments 10
- Estimated Spam (SMTP and POP3) 12**
- Web-based E-mail 14**
- Network information 19**
 - SMTP traffic (tcp-25) 20
 - POP3 traffic (tcp-110) 23

The Threat Inspector interactive report interface enables drill-down review and data manipulation to investigate and troubleshoot with ease

Email File Attachment Summary

Individual User Email Detail



Matched documents	Words
19 -adding	15-normal
4 -purchase	4-section
3 -times	3-place
2 -blue	2-job
2 -total	2-unit
2 -regards	2-###?####?####
1 -buyer	1-days
1 -definitions	1-discount
1 -item	1-medium
1 -part	1-personal
1 -receive	1-reference
	5-office
	3-page
	3-ryan
	2-price
	2-word
	1-malto
	1-dean
	1-format
	1-glass
	1-message
	1-number
	1-phone
	1-road
	1-tax

Detail includes: To; From; CC; BCC; Subject; Attachments/File Name; Mime-type; Size; Content analysis: Identifies phone #s; credit card #s; social security #s

Introduction

E-mail is a mission-critical application and a vital part of the electronic communications infrastructure for today's businesses. It is used to send and receive critical information, close deals, and solicit new business. It can also carry extremely valuable and confidential information. To protect the security of this information, it is important to understand what e-mail technologies are in use and how they function within your organization.

Use this report to:

- Document e-mail technologies in use. (SMTP, POP3, POP3S, Web-based e-mail)
- Evaluate the effectiveness of your e-mail security policies.
- Identify e-mail use that may circumvent or reduce the effectiveness of other security measures.
- Understand how your organization is choosing to use e-mail.



**Threat Inspector offers
device-independent
reporting & verification of
Email system (SMTP)
configuration & overall use**

E-mail (SMTP and POP3)

**Comprehensive
Summary of all
Email Activity**

E-Mail Totals

Inbound E-Mail		Outbound E-Mail	
E-Mails	2598	E-Mails	2147
Attachments	957	Attachments	575
Total size of E-Mails	596.97 MB	Total size of E-Mails	446.79 MB

SMTP E-Mail

Received		Sent	
E-Mails	2592	E-Mails	2147
Attachments	953	Attachments	575
Total size of E-Mails	596.75 MB	Total size of E-Mails	446.79 MB

POP3 E-Mail

Read by Internal Accounts		Served to External Accounts	
E-Mails	6	E-Mails	0
Attachments	4	Attachments	0
Total size of E-Mails	228.12 KB	Total size of E-Mails	0 B

Top E-mail Senders

Mailbox	*Sent	Spam	Attach	Bytes
npham@mycol.com	159	0	17	4.92 MB
dwilkinson@mycol.com	132	0	4	1.23 MB
bcampbell@mycol.com	116	0	4	2.28 MB
garyt@mycol.com	113	0	22	9.57 MB
tdelany@mycol.com	87	0	50	7.21 MB
klansford@mycol.com	83	0	0	2.83 MB
wbryan@mycol.com	81	0	35	2.08 MB
jratto@mycol.com	69	0	6	10.76 MB
dmangum@mycol.com	67	0	5	639.28 KB
jsopczak@mycol.com	66	0	4	6.24 MB
debmoore@mycol.com	63	0	6	24.79 MB
joni@mycolleg.com	61	0	0	725.76 KB
pcerda@mycol.com	59	0	23	5.45 MB
jlittlefield@mycol.com	49	0	19	58.82 MB
mburke@mycol.com	48	0	16	28.36 MB
leroyw@mycol.com	47	0	11	13.95 MB
lnunez@mycol.com	47	0	0	668.99 KB
mheinz@mycol.com	45	0	7	24.16 MB
kkingsbury@mycol.com	45	0	17	11.17 MB
kschatz@mycol.com	43	0	3	7.64 MB
chrisv@mycol.com	42	0	8	2.58 MB
estory@mycol.com	34	0	9	2.32 MB
jtchandler@mycol.com	33	0	17	6.17 MB
kevarts@mycol.com	31	0	24	73.56 MB
dbooker@mycol.com	29	0	5	658.68 KB
jdavis@mycol.com	26	0	45	37.05 MB
bbradley@mycol.com	25	0	8	2.55 MB
mrivas@mycol.com	23	0	7	375.60 KB
ddean@mycol.com	23	0	4	538.66 KB
sales@mycolleg.com	23	0	9	2.62 MB
bst-pb-l-zoll@mycol.com	22	0	29	4.25 MB
gsmith@mycol.com	20	0	0	177.22 KB
armin.quaschner@mycol.com	19	0	21	2.07 MB
robert.rico@mycol.com	18	0	1	393.10 KB
gtempleton@mycol.com	16	0	0	83.90 KB
Sub Totals: 35	1864	0 (%)	436	358.78 MB
Percent: 23%	87%	0	76%	80%
Totals: 153	2147	0 (%)	575	446.79 MB

Note: If present the <>@<>sender, represents e-mail sent by the SMTP server with no return address. SMTP servers use this to send rejection and confirmation messages. A rejection message may be sent because of an invalid e-mail address, virus detection or SPAM filering.

Top E-mail Receivers

Mailbox	*Received	Spam	Attach	Bytes
npham@mycol.com	298	21 (7%)	79	16.64 MB
bcampbell@mycol.com	235	79 (34%)	44	42.61 MB
klansford@mycol.com	147	47 (32%)	21	61.82 MB
dwilkinson@mycol.com	147	26 (18%)	90	26.17 MB
garyt@mycol.com	122	16 (13%)	79	46.76 MB
mburke@mycol.com	120	29 (24%)	81	38.53 MB
dmangum@mycol.com	117	31 (26%)	72	18.01 MB
leroyw@mycol.com	112	24 (21%)	65	35.23 MB
tdelany@mycol.com	112	55 (49%)	45	19.69 MB
wbryan@mycol.com	109	13 (12%)	76	11.98 MB
pabco@mycol.com	100	56 (56%)	33	9.41 MB
jratto@mycol.com	99	37 (37%)	10	27.49 MB
chrisv@mycol.com	92	31 (34%)	57	8.42 MB
mrivas@mycol.com	79	10 (13%)	57	20.15 MB
lnunez@mycol.com	74	19 (26%)	9	8.65 MB
pcerda@mycol.com	72	17 (24%)	10	30.05 MB
kkingsbury@mycol.com	70	19 (27%)	29	9.35 MB
kschatz@mycol.com	70	19 (27%)	17	7.63 MB
gdean@mycol.com	69	11 (16%)	63	13.01 MB
jlittlefield@mycol.com	67	18 (27%)	88	44.20 MB
dolores@mycol.com	65	21 (32%)	45	4.26 MB
gsmith@mycol.com	61	16 (26%)	24	15.44 MB
jtchandler@mycol.com	55	18 (33%)	38	7.80 MB
manny@mycol.com	52	24 (46%)	13	4.95 MB
debmoore@mycol.com	50	11 (22%)	4	6.65 MB
jsopcza@mycol.com	45	14 (31%)	69	23.51 MB
estory@mycol.com	44	14 (32%)	7	7.65 MB
dbooker@mycol.com	42	10 (24%)	21	2.89 MB
mheinz@mycol.com	41	15 (37%)	13	23.47 MB
hstelzig@mycol.com	37	11 (30%)	2	471.48 KB
wwaite@mycol.com	34	15 (44%)	3	4.49 MB
markus@mycol.com	30	4 (13%)	16	4.94 MB
kevarts@mycol.com	29	16 (55%)	42	46.06 MB
bbradley@mycol.com	28	4 (14%)	13	5.77 MB
gtempleton@mycol.com	25	1 (4%)	1	5.34 MB
Sub Totals: 35	2949	772 (26%)	1336	659.49 MB
Percent: 47%	95%	94%	95%	97%
Totals: 74	3119	817 (26%)	1403	679.54 MB

Note: The total number of e-mails, attachments, and bytes may not match summary totals because an e-mail received by a SMTP server may be addressed to multiple receivers.

Internal POP3 Accounts

Internal users are accessing external POP3 servers for e-mail. This use represents an additional inbound e-mail channel and circumvents corporate investment in anti-virus, anti-Spam, encryption, and content filtering. Use of this technology may pose significant security challenges and exposure.

Things to consider:

- POP3 is unencrypted. Account names, passwords and contents are transmitted in the clear.
- POP3 use circumvents investments in e-mail gateway security technologies such as anti-virus, anti-Spam, encryption, content filtering and monitoring.
- Regulated industries may need to comply with logging requirements or provide content filtering control. Use of private unmonitored e-mail can easily breach the customer information confidentiality requirements of the Gramm-Leach-Bliley act, the SEC's Books and Recording keeping retention requirements or HIPAA regulations.

Accounts

Client IP	Account	*Received	Spam	Attach	Bytes
Internal clients accessing external servers.					
192.168.10.138	brarry450	6	5 (83%)	4	228.12 KB
Totals: 1		6	5 (83%)	4	228.12 KB

Web Report offers Email drill-down detail

Including individual user' mailbox & email drill-down detail

The screenshot shows the 'Top E-mail Senders' report in Threat Inspector. The report lists various email senders with columns for Mailbox, Sent, Spam, Attach, and Bytes. The top sender is npham@leco.com with 159 sent emails and 4.92 MB of data.

Mailbox	Sent	Spam	Attach	Bytes
npham@leco.com	159	0	17	4.92 MB
dwilkinson@leco.com	132	0	4	1.23 MB
bcarnsbell@leco.com	117	0	4	2.34 MB
garyt@leco.com	113	0	22	9.57 MB
tdelany@leco.com	87	0	50	7.21 MB
klansford@leco.com	83	0	0	2.83 MB
wryan@leco.com	81	0	35	2.08 MB
jratto@leco.com	71	0	7	12.55 MB
dmargus@leco.com	67	0	5	639.28 KB
jsoczak@leco.com	66	0	4	6.24 MB
debmore@leco.com	63	0	6	24.79 MB
jon@leco.com	61	0	0	725.76 KB
pcarda@leco.com	59	0	23	5.45 MB
jilliefield@leco.com	49	0	19	58.82 MB
mhurka@leco.com	48	0	16	28.36 MB
leryvu@leco.com	47	0	11	13.95 MB
lnunez@leco.com	47	0	0	668.99 KB
mheinz@leco.com	45	0	7	24.16 MB
kkingsbury@leco.com	45	0	17	11.17 MB
kschartz@leco.com	44	0	3	7.54 MB
chrisv@leco.com	43	0	8	2.64 MB
estory@leco.com	34	0	9	2.32 MB
ritchandler@leco.com	33	0	17	6.17 MB
kwarta@leco.com	31	0	24	73.56 MB
stooker@leco.com	29	0	5	658.69 KB
Sub Totals: 25	1654	0 (%)	313	310.72 MB
Percent: 16%	76%	0	54%	66%
Totals: 153	2170	0 (%)	578	469.07 MB

The screenshot shows the 'Mailbox : pcer@leco.com' report in Threat Inspector. It displays statistics for Received-In(SMTP) and Sent-Out(SMTP) emails, including counts for E-Mails, SPAM, and Attachments, along with total sizes. Below this is an 'Email listing' table with columns for Subject Line, Type, Attach, Spam?, Size, and Time.

Subject Line	Type	Attach	Spam?	Size	Time
HP SI 500	Out(SMTP)	1	0	2.32 MB	01/18/08 12 PM
FW: 4 Top Commercial	In(SMTP)	1	1	6.45 MB	01/18/08 12 PM
FW: RIDE™ EMI COWGIRLS	Out(SMTP)	0	0	16.95 KB	01/18/08 12 PM
*No Subject...	In(SMTP)	0	1	2.28 MB	01/18/08 11 AM
FW: RIDER™ EMI COWGIRLS	In(SMTP)	0	1	12.86 MB	01/18/08 11 AM
germhamer	Out(SMTP)	1	0	79.37 KB	01/18/08 10 AM
FW: D52-22	In(SMTP)	0	0	2.84 KB	01/18/08 09 AM
Re: MARTINETES	In(SMTP)	0	0	11.92 KB	01/18/08 09 AM
RE: lunch	Out(SMTP)	0	0	8.73 KB	01/18/08 09 AM
RE: lunch	In(SMTP)	0	0	6.86 KB	01/18/08 08 AM
RE: lunch	In(SMTP)	0	1	97.64 KB	01/18/08 04 AM

Attachments (SMTP and POP3)

Things to consider:

- Does your business require multimedia-type attachments? For example: jpeg, gif, wmv, avi, mpeg, wav, mp3... If not, a high percentage of multimedia content may be an indication of abuse and non-business-related activity.
- Do you have requirements to archive e-mail data? If so, multimedia attachments may have a large impact on the amount of storage space required.
- If blocking or limiting the size of attachments, be aware that many users migrate to personal e-mail systems such as POP3 and Web-based E-mail to avoid limitations.

Top Attachments

Filename	Media	*Bytes	Dir	E-mails
winmail.dat	ms-tnef	62.73 MB	Out.SMTP	25
4TrunkMo.wmv	x-ms-wmv	27.05 MB	In.SMTP	4
Power_Windows.wmv	x-ms-wmv	18.08 MB	Out.SMTP	5
freakoutnowhopper.wmv	x-ms-wmv	17.39 MB	Out.SMTP	3
Toot-tone2.wmv				
2008 annual meeting attendee list.doc				
2008 Annual Meeting Contractor List.xls				
SeasonsintheSun.pps				
BeachesofEurope.wmv				
Update for Mauer B-Phonic.pdf				
bg20h991_labv_mpc.tgz				
freakoutnowhopper.wmv				
tvafs_morlock.wmv				
image001.jpg	jpeg	10.12 MB	In.SMTP	50
image002.jpg	jpeg	9.85 MB	In.SMTP	22
Hey.wmv	x-ms-wmv	9.80 MB	In.SMTP	1
image003.jpg	jpeg	9.53 MB	In.SMTP	12
GoodMorningGuys.wmv	x-ms-wmv	9.01 MB	In.SMTP	1
image008.jpg	jpeg	8.93 MB	In.SMTP	7
image005.jpg	jpeg	8.76 MB	In.SMTP	8
image006.jpg	jpeg	8.76 MB	In.SMTP	8
Male_Priorities_003.wmv	x-ms-wmv	8.56 MB	Out.SMTP	2
WhatMenAreReallyThinking.wmv	x-ms-wmv	8.21 MB	In.SMTP	1
P1160017.JPG	jpeg	8.13 MB	Out.SMTP	1
P1160021.JPG	jpeg	8.13 MB	Out.SMTP	1
P1160019.JPG	jpeg	8.13 MB	Out.SMTP	1
P1160018.JPG	jpeg	8.13 MB	Out.SMTP	1
P1160016.JPG	jpeg	8.13 MB	Out.SMTP	1
P1160020.JPG	jpeg	8.13 MB	Out.SMTP	1
P1160015.JPG	jpeg	8.13 MB	Out.SMTP	1
SundiDitchSurfing.wmv	x-ms-wmv	8.12 MB	Out.SMTP	1

Non-business attachments consume bandwidth, disc storage and represent potentially embarrassing legal discovery/audit data

Filename	Media	*Bytes	Dir	E-mails
SundiDitchSurfing2.wmv	x-ms-wmv	8.05 MB	Out.SMTP	1
SundiDitchSurfing2.wmv	x-ms-wmv	7.95 MB	In.SMTP	1
image004.jpg	jpeg	7.82 MB	In.SMTP	10
image007.jpg	jpeg	7.62 MB	In.SMTP	6
P1160028.JPG	jpeg	7.59 MB	Out.SMTP	1
P1160027.JPG	jpeg	7.59 MB	Out.SMTP	1
P1160025.JPG	jpeg	7.59 MB	Out.SMTP	1
P1160024.JPG	jpeg	7.59 MB	Out.SMTP	1
P1160023.JPG	jpeg	7.59 MB	Out.SMTP	1
P1160026.JPG	jpeg	7.59 MB	Out.SMTP	1
P1160022.JPG	jpeg	7.59 MB	Out.SMTP	1
Power_Windows.wmv	x-ms-wmv	7.05 MB	In.SMTP	2
IMGP3870.JPG	octet-stream	7.02 MB	In.SMTP	1
IMGP3869.JPG	octet-stream	7.02 MB	In.SMTP	1
BrightenYourDay.mpeg	mpeg	6.89 MB	Out.SMTP	1
4TrunkMo.wmv	x-ms-wmv	6.76 MB	Out.SMTP	1
P1160029.JPG	jpeg	6.74 MB	Out.SMTP	1
P1160030.JPG	jpeg	6.74 MB	Out.SMTP	1
P1160031.JPG	jpeg	6.74 MB	Out.SMTP	1
Sub-total: 50		530.2 MB		206
Percent: 5%		32%		13%
Totals: 1048		1.62 GB		1532

Unsafe Attachments

Unsafe attachments include files with extensions that are executable by users and are often used by viruses to infect workstations via e-mail. Attachments with extension types such as .exe, .com, .bas and many others should never be directly opened without first verifying who the sender is and scanning for viruses.

Unsafe Attachments

File Ext	Attached	Bytes	Direction
.pps	9	24.08 MB	Received
.pps	4	12.85 MB	Sent
.ppt	2	5.37 MB	Received
.mp3	1	1.56 MB	Sent
.mp3	1	1.54 MB	Received
Totals: 5	17	45.4 MB	

Note: Double clicking on any of the above attachments by a user could lead to a virus infection or security compromise.

E-mail received with executable attachments

E-mail Subject:			
File	Mime	Times	Bytes
[Fwd: i have a Remodeling job & i'm looking for a 'perfect' contractor !]			
HowToFindAPreferredCompplication/vnd.ms tractor.pps	application/vnd.ms-powerpoint	1	4.70 MB
Ad for Conexpo			
Conexpo flyer for Asia.ppt	application/octet-stream	1	3.96 MB
FW: Buying a new car- careful...			
Mercedes.pps	application/octet-stream	1	3.82 MB
Fw: "Our Generation"----Shot to hell!!			
SeasonsintheSun.pps	application/vnd.ms-powerpoint	1	3.77 MB
FW: Aging Gracefully			
SeasonsintheSun.pps	application/octet-stream	1	3.76 MB
FW: I want to rent this place! XX			
Beach_House_For_Rent.ppt	application/octet-stream	1	2.90 MB
Re: FW: This is cool!!			
DidYouKnow_1.pps	application/octet-stream	1	2.85 MB
Happy Anniversary!			
AnniversaryToastSong.mp3	audio/mpeg	1	1.54 MB
Executive Assistant			
The Perfect Fit.ppt	application/vnd.ms-powerpoint	1	1.40 MB
For the do-it your-selves, plumbers-electricians-HVAC			
HomeProjects.pps	application/vnd.ms-powerpoint	1	1.17 MB
FW: 1941 PHOTOS FOUND IN AN OLD			

E-mail Subject:			
File	Mime	Times	Bytes
BROWNIE CAMERA			
PearlHarbour.pps	application/octet-stream	1	798.98 KB
FW: INFORMATION			
softdrinksawareness.pps	application/vnd.ms-powerpoint	1	326.79 KB
Totals: 12		12	30.99 MB

E-mail sent with executable attachments

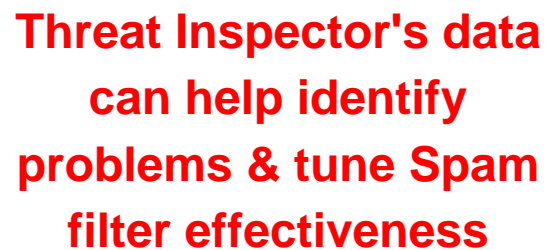
E-mail Subject:			
File	Mime	Times	Bytes
FW: "Our Generation"----Shot to hell!!			
SeasonsintheSun.pps	application/vnd.ms-powerpoint	1	3.91 MB
FW: Happy Anniversary!			
AnniversaryToastSong.mp3	audio/mpeg	1	1.56 MB
For the do-it your-selfers, plumbers-electricians-HVAC			
HomeProjects.pps	application/vnd.ms-powerpoint	1	1.19 MB
Totals: 5		5	14.41 MB

Estimated Spam (SMTP and POP3)

Spam is the widely accepted term for Internet junk e-mail such as advertisements and get-rich schemes that clutter e-mail inboxes. More technically, spam is classified as unsolicited commercial e-mails or unsolicited bulk e-mail. Threat Inspector uses an onboard dictionary to get an approximate estimation of the amount of spam received by your e-mail systems. This dictionary is comprised of words frequently used in the English language along with a number of words that identify offensive slang, hate speech, and which are commonly associated with spam.

Note: If spam filtering is in place on the SMTP server, the audit cannot tell how much spam gets through to end users, only the amount that is hitting the servers.

Totals						
Inbound E-mail	E-mails		Attachments		Bytes	
SMTP-Spam	777	30%	352	37%	443.13 MB	74%
POP3-Spam	5	%	0	%	73.52 KB	%
Spam-Totals:	782	30%	352	37%	443.2 MB	74%
Totals:	2598		957		596.97 MB	



**Threat Inspector's data
can help identify
problems & tune Spam
filter effectiveness**

Top SPAM

Subject:	Type	Attachments	Bytes	Time
25% Off Coupon Inside	In.SMTP	0	11.99 KB	01/17/08 03 AM
Footwear Sale, Huge Hunting Deals & Shipping Coupon from The Guide	In.SMTP	0	44.31 KB	01/11/08 11 PM
Houston Concert Update	In.SMTP	0	62.20 KB	01/16/08 07 PM
Houston Concert Update	In.SMTP	0	62.19 KB	01/16/08 07 PM
Guide Gear Northwoods Twill Parka under \$20... Coupon & More from The Guide	In.SMTP	0	18.16 KB	01/13/08 10 AM
This Week -- Coupons, 40% Off Six Book Club Favorites, More	In.SMTP	0	47.18 KB	01/16/08 03 AM
Guide Gear Cascade Jacket under \$18... Get More Cold Weather Deals from The Guide	In.SMTP	0	17.32 KB	01/16/08 06 PM
Good Luck at The Houston Marathon	In.SMTP	0	9.57 KB	01/12/08 07 PM
Tickets On Sale & Special Offers for the Week	In.SMTP	0	49.17 KB	01/11/08 06 PM
GIFTapolis.com SALE~OVER 700 ITEMS UP TO 80% OFF	In.SMTP	0	11.83 KB	01/14/08 04 PM
This weekend: sitewide savings + extra 25% off clearance!	In.SMTP	0	15.91 KB	01/17/08 10 AM
Tickets On Sale & Special Offers for the Week	In.SMTP	0	41.18 KB	01/18/08 08 AM
Tips of the Week!	In.SMTP	0	30.41 KB	01/17/08 12 PM
Free Overnight Shipping and Free Return Shipping from Endless.com Shoes & Handbags	In.SMTP	0	13.53 KB	01/17/08 06 AM
Save Big this Holiday Weekend!	In.SMTP	0	33.10 KB	01/17/08 01 PM
Tickets On Sale & Special Offers for the Week	In.SMTP	0	66.10 KB	01/11/08 05 PM
Your Dover Design Sampler - Plus Winter Sale Savings	In.SMTP	0	22.01 KB	01/16/08 11 AM
Extra 50% Off Fashion Clearance 2 Days Only	In.SMTP	0	11.74 KB	01/17/08 11 AM
Patriots now 17 and 0 after defeating the Jaguars 31 to 20 in AFC divisional playoff	In.SMTP	0	5.31 KB	01/12/08 10 PM
Tickets On Sale & Special Offers for the Week	In.SMTP	0	56.86 KB	01/18/08 08 AM
Sub-total: 20		0	630.07 KB	
Total: 782		352	443.2 MB	

Web-based E-mail

Web-based e-mail offers a flexible and convenient way to view and send e-mails from any Internet-connected computer. Many of these services are free, anonymous and are convenient for personal e-mail use. And they are unmonitored.

Organizations that allow users to access personal Web-based accounts from work may be seriously compromising network security. Web-based e-mail circumvents investment in SMTP e-mail security technologies such as anti-virus, anti-spam and content protection systems. As an undocumented information conduit it can be used to export confidential company information or exchange materials and personal views that are against company or regulatory policy. Additionally, while web-based e-mail offers its users some degree of identity protection, the same is not true for the organization. Web E-mails can contain web beacons, scripts, and executables that can be used to identify the organization, internal workstations and compromise systems.

Threats:

- Represents an undocumented conduit for exporting confidential information out of the organization.
- Regulated industries that allow employees to use personal e-mail tools, without retaining those messages, could face serious legal and regulatory trouble related to Sarbanes-Oxley compliance.
- Regulated healthcare industries that allow employees to use external e-mail services to exchange patient records could face serious legal and regulatory trouble related to HIPAA by exposing confidential healthcare information in a readable format over the Internet.
- Each use represents an undocumented remotely exploitable vulnerability and vector for attack.

Web-based E-mail providers

Types	Clients	Sites	Sessions	Failed	*Bytes
Yahoo! Mail	23	33	3243	2	57.95 MB
Google	4	4	1153	0	14.88 MB
Hotmail	14	11	107	0	632.33 KB
AOL-Web-Mail	3	5	25	0	347.03 KB
Totals: 4		53	4,528	2	73.79 MB

Top Web-based E-mail Clients

Client	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.101	2154	0	22.23 MB	19.02 MB	3.21 MB
192.168.10.140	267	0	9.75 MB	8.81 MB	962.88 KB
192.168.10.112	629	0	9.06 MB	5.1	
192.168.10.95	220	1	7.50 MB	6.7	
192.168.10.116	162	0	3.59 MB	3.2	
192.168.10.92	191	0	3.35 MB	2.8	
192.168.10.105	134	0	3.00 MB	2.5	
192.168.10.91	80	0	2.65 MB	2.0	
192.168.10.97	91	0	2.30 MB	2.0	
192.168.10.104	73	0	2.03 MB	1.8	
192.168.10.98	120	0	2.02 MB	1.6	
192.168.10.103	62	0	1.24 MB	1.1	
192.168.10.134	68	0	879.77 KB	511.	
192.168.10.127	56	1	864.23 KB	741.	
192.168.10.130	57	0	827.97 KB	700.	
192.168.10.131	34	0	467.03 KB	390.	
192.168.10.85	21	0	450.19 KB	386.	
192.168.10.82	33	0	431.44 KB	362.89 KB	68.55 KB
192.168.10.90	21	0	416.73 KB	248.77 KB	167.96 KB
192.168.10.94	6	0	343.16 KB	210.30 KB	132.86 KB
192.168.10.88	15	0	306.31 KB	271.19 KB	35.12 KB
192.168.10.117	16	0	99.42 KB	71.28 KB	28.14 KB
192.168.10.128	5	0	80.01 KB	67.36 KB	12.66 KB
192.168.10.138	2	0	11.91 KB	3.22 KB	8.68 KB
192.168.10.110	7	0	9.00 KB	4.36 KB	4.64 KB
192.168.10.86	1	0	3.63 KB	2.32 KB	1.31 KB
192.168.10.123	1	0	3.36 KB	2.43 KB	954.00 B
192.168.10.83	1	0	1.51 KB	915.00 B	629.00 B
192.168.10.136	1	0	1.19 KB	531.00 B	689.00 B
Sub-total: 29	4,528	2	73.79 MB	60.91 MB	12.88 MB
Percent: 100%	100%	100%	100%	100%	100%
Totals: 29	4,528	2	73.79 MB	60.91 MB	12.88 MB

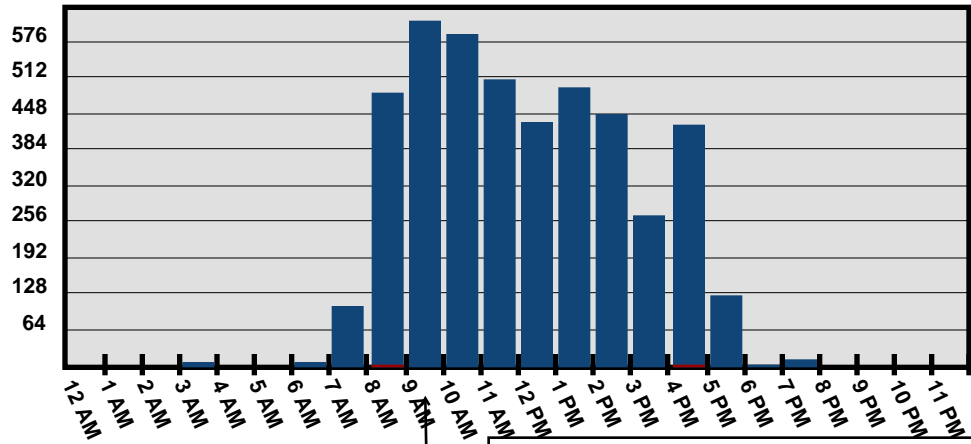
Over 20 MB of data sent via Web-mail representing a potentially serious data leakage problem

Top Client requests

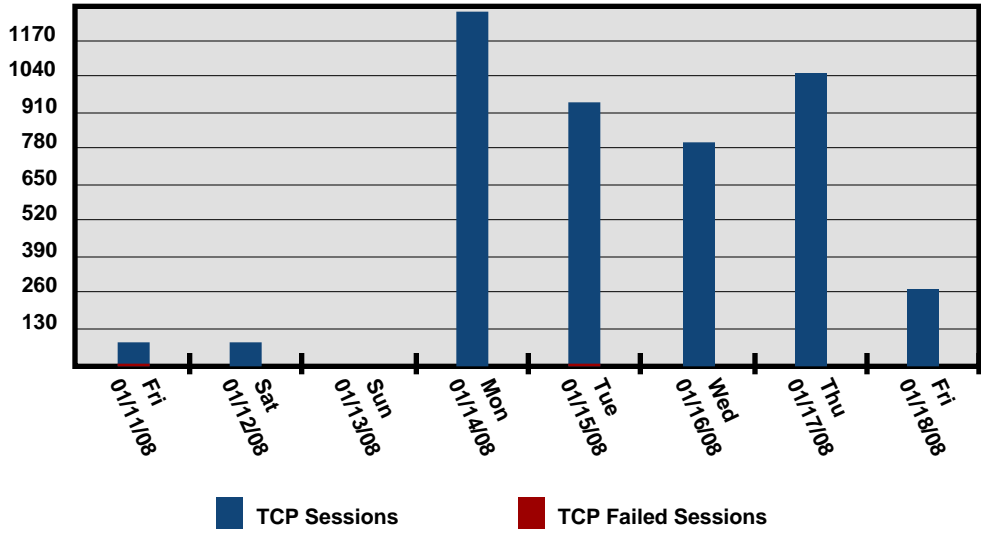
Filename	Requests	Method	Status	*Total Bytes	Mime Type Avg. Bytes
Directory Request					html
1511	Get	OK	20.27 MB	13.74 KB	
Directory Request					html
990	Post	OK	9.02 MB	9.33 KB	
login					html
318	Get	OK	5.56 MB	17.90 KB	
launch					html
206	Get	OK	4.27 MB	21.25 KB	
securedownload					octet-stream
2	Get	OK	2.64 MB	1.32 MB	
bind					html
132	Get	OK	2.63 MB	20.44 KB	
securedownload					jpeg
29	Get	OK	1.87 MB	66.17 KB	
Directory Request					javascript
505	Get	OK	1.82 MB	3.69 KB	
securedownload					gif
12	Get	OK	760.48 KB	63.37 KB	
Directory Request					html
1063	Get	Moved Temporarily	731.29 KB	704.46 B	
ShowLetter					html
22	Get	OK	584.72 KB	26.58 KB	
ShowFolder					html
18	Get	OK	359.27 KB	19.96 KB	
ShowLetter					html
110	Get	Moved Temporarily	276.69 KB	2.52 KB	
Directory Request					javascript
58	Post	OK	254.96 KB	4.40 KB	
Directory Request					jpeg
4	Get	OK	234.00 KB	58.50 KB	
Directory Request					plain
13	Get	OK	216.01 KB	16.62 KB	
_us.js					html
51	Get	Not Found	174.46 KB	3.42 KB	
securedownload					msword
3	Get	OK	162.05 KB	54.02 KB	
favicon.ico					x-icon
24	Get	OK	150.33 KB	6.26 KB	
toolbar1.gif					gif
1	Get	OK	144.67 KB	144.67 KB	
launch					html
206	Get	Moved Temporarily	138.45 KB	688.22 B	
Directory Request					html
1	Get	Not Modified	112.23 KB	112.23 KB	
rte.js					x-JavaScript
2	Get	OK	101.18 KB	50.59 KB	

Filename	Requests	Method	Status	*Total Bytes	Mime Type Avg. Bytes
test					html
	41	Get	OK	91.65 KB	2.24 KB
RPC.aspx					json
	19	Post	OK	81.16 KB	4.27 KB
bundle.js.aspx					javascript
	2	Get	OK	72.56 KB	36.28 KB
Directory Request					xml
	8	Get	OK	63.98 KB	8.00 KB
fc					html
	11	Get	OK	57.61 KB	5.24 KB
Static					html
	20	Get	OK	41.37 KB	2.07 KB
Directory Request					xml
	12	Post	OK	39.75 KB	3.31 KB
Light.js					x-JavaScript
	5	Get	OK	39.56 KB	7.91 KB
Header.js					x-JavaScript
	5	Get	OK	32.95 KB	6.59 KB
login					html
	23	Get	Moved Temporarily	31.66 KB	1.38 KB
formrpc					xml
	7	Get	OK	30.67 KB	4.38 KB
load.html					html
	13	Get	OK	26.63 KB	2.05 KB
Sub-total: 5447				52.99 MB	
Percent: 92%				98%	
Total: 5922				54.12 MB	

Access times



Daily usage levels may represent data leakage risk



Network information

The following sections show the networking activity underlying e-mail communications. All information presented here is based on the common ports for SMTP (tcp-25), POP3 (tcp-110) and POP3S (tcp-995) which are identified as the primary servers and clients that support these services along with amount activity and time of use.

Use this section to:

- Check for rogue or unexpected internal SMTP servers.
- Verify that user workstations are not sending or attempting to send e-mail to unauthorized external SMTP servers. This is a common indication that a workstation has been compromised and is being used to send spam. This activity could put your organization's IP addresses on various anti-spam block lists creating difficulties in sending corporate e-mail.
- Identify Internal and external POP3 clients and servers.
- Identify Internal and external POP3S clients and servers.

SMTP traffic (tcp-25)

Top Internal SMTP Servers

Internal Servers	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.6	2855	0	644.72 MB	626.70 MB	18.02 MB
Totals: 1	2,855		644.72 MB	626.7 MB	18.02 MB

Note: Only known servers should show up here. Any unexpected server should be investigated.

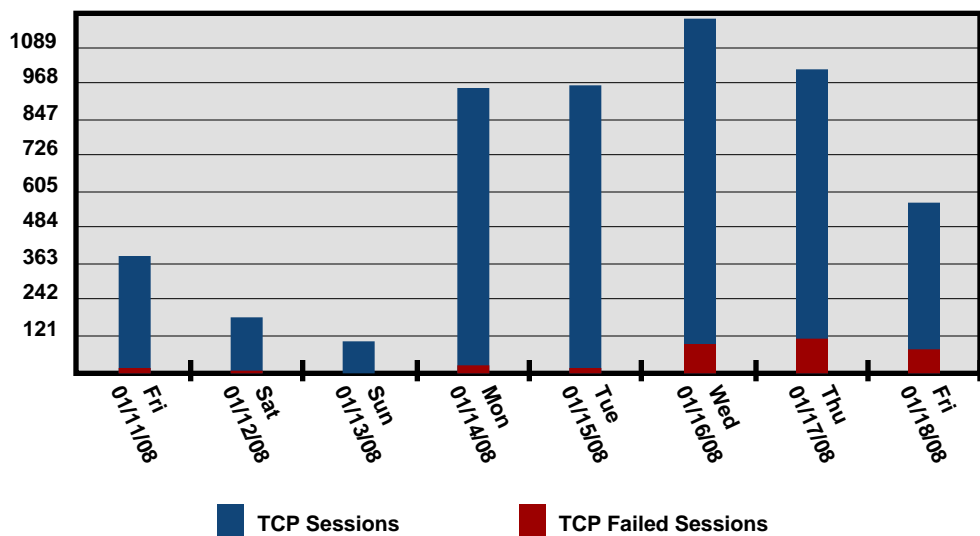
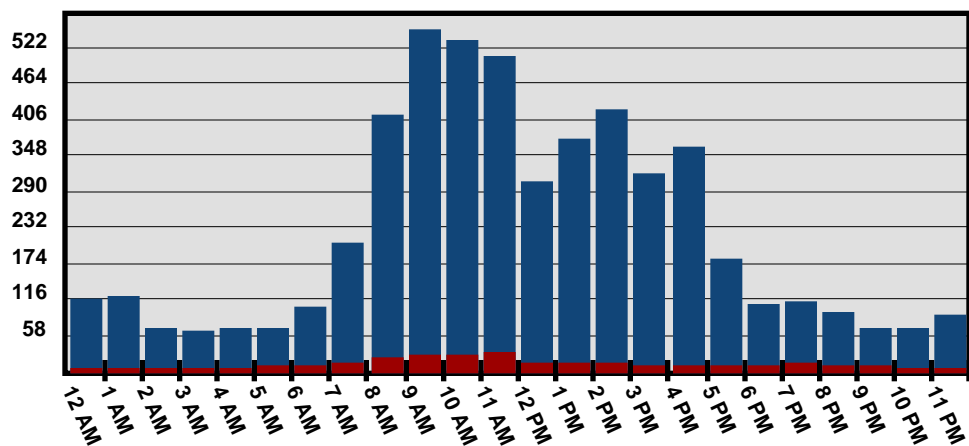
Top Internal SMTP Clients

Internal Clients	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.6	2509	332	479.05 MB	14.68 MB	464.37 MB
192.168.10.138	1	0	1.47 KB	885.00 B	616.00 B
Totals: 2	2,510	332	479.05 MB	14.68 MB	464.37 MB

Note: Only clients authorized to send SMTP e-mail directly to the Internet should be shown here. This should be your SMTP server(s). Individual workstations should not be able to send SMTP e-mail directly through the firewall. Workstations that are attempting or sending e-mail to unauthorized SMTP servers may be compromised.

Note: In some cases, workstations may be configured to send SMTP e-mail to an authorized upstream service provider. In this case, the top workstation will show up here. The use of authorized upstream providers can be verified via Threat Inspector's user Interface. If the firewall is properly configured, a compromised workstation may be detected and identified by a high failed session count due to workstation traffic being blocked at the firewall.

SMTP Access Times



POP3 traffic (tcp-110)

External POP3 Servers

External Servers	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
218.176.95.140 - US	9	0	257.49 KB	245.51 KB	11.99 KB
128.185.42.242 - US	544	544	98.81 KB	0.00 B	98.81 KB
Totals: 2	553	544	356.3 KB	245.51 KB	110.8 KB

Note: Access or attempted access to external POP3 servers may be for personal e-mail and its use should be carefully considered.

Internal POP3 Clients

Internal Clients	Outbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.138	9	0	257.49 KB	245.51 KB	11.99 KB
192.168.10.117	544	544	98.81 KB	0.00 B	98.81 KB
Totals: 2	553	544	356.3 KB	245.51 KB	110.8 KB

Internal POP3 Servers

Internal Servers	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
192.168.10.6	623	0	283.22 KB	155.54 KB	127.68 KB
Totals: 1	623		283.22 KB	155.54 KB	127.68 KB

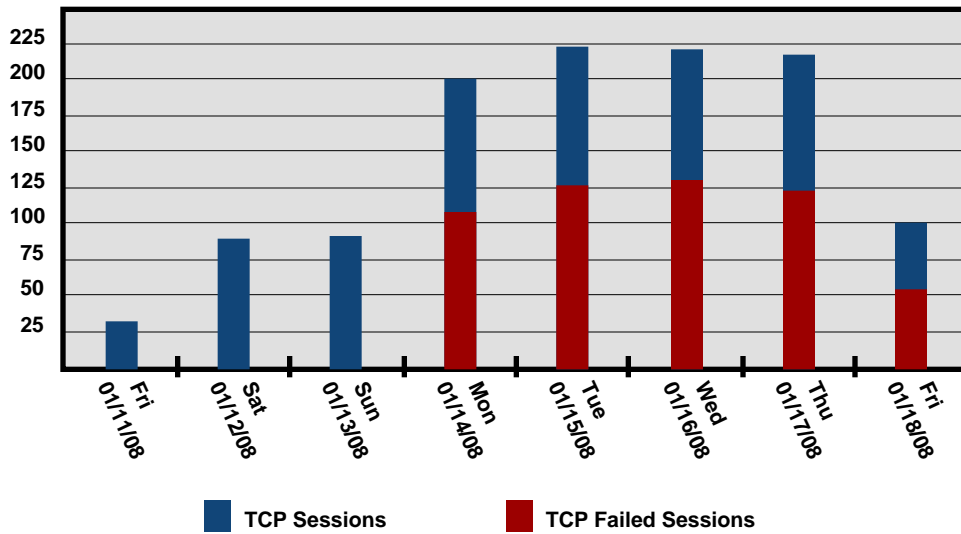
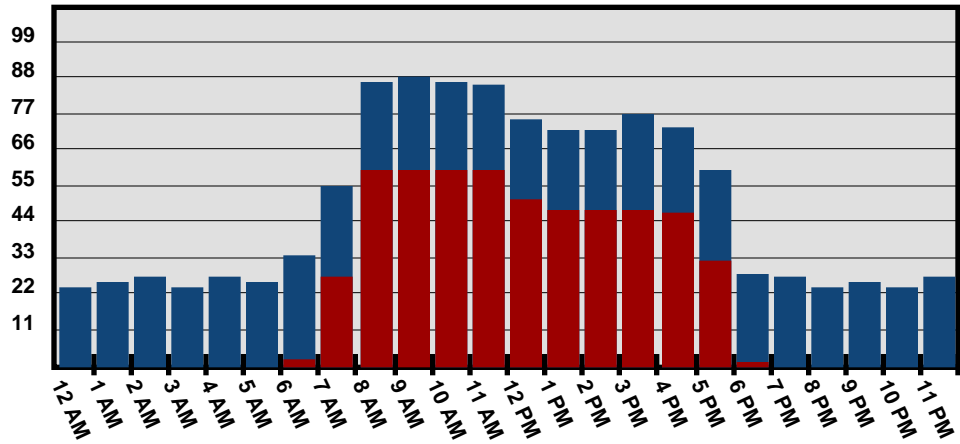
Note: Only known servers should show up here. Any unexpected server should be investigated.

External POP3 Clients

External Networks	Inbound		*Total	Bytes	
	Sessions	Failed		Inbound	Outbound
218.34.91.0 - US	393	0	178.61 KB	98.01 KB	80.60 KB
64.0.0.0 - US	227	0	103.37 KB	56.82 KB	46.55 KB
218.146.64.0 - US	3	0	1.24 KB	726.00 B	546.00 B
Totals: 3	623		283.22 KB	155.54 KB	127.68 KB

Note: POP3 is not secure! Access to your internal e-mail system via POP3 from un-trusted networks can be monitored and this includes account names and passwords.

POP3 Access Times



■ TCP Sessions
 ■ TCP Failed Sessions