# Side Effects of End-User Applications

*An Analysis of Application Traffic and Associated Risks in Healthcare Environments*

February 2010

**Palo Alto Networks**
232 East Java Dr.
Sunnyvale, CA 94089
Sales 866.320.4788
408.738.7700
www.paloaltonetworks.com

## Table of Contents

## KEY FINDINGS

Over the last 24 months, Palo Alto Networks has performed traffic assessments for 41 different healthcare organizations around the world. These assessments are an integral component of the proof-of-concept process whereby a Palo Alto Networks next-generation firewall is deployed on their network, monitoring traffic for up to a week. At the end of the collection period, an Application Visibility and Risk Report that summarizes the findings is generated to and presented to management (see Appendix 1 for more information on the methodology). A roll up of all 41 assessments shows that 506 unique applications were detected, consuming more than 25 terabytes of data. The key findings are summarized below:

**Applications that enable users to bypass controls are in use.**

- Applications that enable employees to bypass security or policy controls were found with relatively high frequency[1]. Specifically, external proxies were found on 80% of the networks while remote desktop access and encrypted tunnel applications were found 98% and 34% of the time respectively.

**Peer-to-peer file sharing applications were found in more than 90% of the organizations.**

- Eighteen peer-to-peer (P2P) applications were found across 33 of the 41 networks (93%) with an average of 5 P2P variants found on each network.
- The use of P2P applications increases the risk of inadvertent healthcare records transfer and adding to these risks, a new threat—Mariposa—is spreading rapidly across nine commonly used P2P networks.

**Browser-based file sharing applications show significant usage.**

- An average of 7 browser-based file sharing application variants were found across 31 of the 41 participating healthcare organizations (76%). While not as common as P2P, these applications simplify the transfer of large files via the web.

**Healthcare employees keep themselves entertained.**

- Out of the 506 applications found, 32% (161) of them qualify as entertainment oriented (social networking, media, file sharing and web browsing). Bandwidth consumed by these applications was approximately 44% of the total bandwidth consumed (11 terabytes).

**Application accessibility features make visibility and control difficult.**

- Of the 506 applications found, 57% (289) of them can use port 80, port 443, or hop ports as a means of enabling user access. Accessibility features make an application easier to use, but at the same time, can introduce business and security risks because traditional port-based offerings cannot see or control these applications.

The findings highlight the wide range of applications—business, custom healthcare and end-user oriented—that are commonly found on healthcare networks. The diversity of the applications is equaled by the diversity of the user population that is more computer savvy than ever which introduces a wide range of business and security risks.

[1] The frequency that an application is found is based on how often it appears on the network – the number of users is not a factor in frequency.

## INTRODUCTION

Healthcare organizations around the world are faced with a long list of challenges, not the least of which is saving lives. Today's network users are more computer savvy than ever before, using a wide range of applications for getting their jobs done as well as socializing and staying entertained at work. More often than not, these users make the assumption that they are entitled to use any application they desire, without taking into account the possible business and security risks. The risk exposure is not trivial.

- Risks to business continuity and electronic records privacy brought on by propagation of malware and/or application vulnerability exploits that are introduced to the network by a "click first and think later" mentality.
- Loss of patient data through unmonitored and/or unauthorized use of file transfer applications and/or features.
- Regulatory compliance violations (PCI, HIPAA, N3, etc.)[2] through the use applications that may jeopardize the network and the privacy of patient data.
- Operational cost increases from higher bandwidth consumption and lost user productivity, and added IT expenses for desktop cleanup.

The analysis of the 41 healthcare networks shows a wide range of work and non-work related applications. Those that are clearly non-work related, providing no business value whatsoever, such as Hulu Networks, Pandora and Gpass, KProxy, CGIProxy were found along with those that are clearly work related (Oracle, SharePoint, SAP). Also found in nearly all of the organizations were those that span the work/non-work gap (Flash, YouTube, Gmail, Google Docs).

The breadth of applications found during the analysis, along with the diversity of users highlights the challenges that IT departments face. On one hand, they are asked to enable network access for a demanding set of users, while on the other, they are required to protect the network and a wide range of patient data including health (last physical, recent test results), personal (social security number, age, address), and financial information (credit card numbers, bank accounts, income). As the drive towards electronic medical records (EMR) accelerates, the magnitude of this challenge is only amplified by the fact that many of these applications can easily evade detection and therefore are uncontrollable by existing firewall, IPS, Proxy or URL filtering solutions.

[2] Payment Card Industry Digital Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), N3 Network Security Initiative (N3)

## CIRCUMVENTION IS A COMMON PRACTICE

Our analysis showed that external proxies, encrypted, tunnel and remote desktop control applications were being used with surprisingly high frequency. External proxies, those that are not endorsed by IT were found, as were encrypted tunnels that are not VPN connectivity related. Both of these application groups require user effort and knowledge to deploy, indicating a level of purposeful circumvention over and above the casual user. Remote desktop applications are commonly used by IT but are also now being used by end-users as a way to login to their home machines and quite possibly bypass security.

## EXTERNAL PROXIES

There are two types of proxies that can be used for the purposes of bypassing security controls. The first is a private proxy that is installed on a server and is used by a single user. In this case, the proxy is installed on a machine at home, or somewhere outside of the healthcare network. The user will then browse to the external proxy as an unmonitored means to browse the web. Common private proxy variants include PHproxy, CGIproxy and Kproxy.

The second proxy variant is a public proxy or proxy service. These are merely implementations of the aforementioned proxy software applications that are made available to the public. For example, a healthcare employee who wants to browse the web anonymously can visit www.proxy.org and select from many thousands of proxies that have been established by well-meaning Internet citizens. Users can also sign up for an email update that notifies them of the new proxy sites made available on a daily basis. In either of these two cases, the traffic looks like normal web browsing and most security policies allow this type of traffic to pass unfettered. The result is that users are bypassing any control efforts including threat inspection, exposing the healthcare network to unnecessary risks. The risks that external proxies present to healthcare networks range from operational (bandwidth consumption and productivity loss) to business continuity (propagation of threats via anonymous proxies) to possible data loss.

The analysis discovered 14 different proxies, excluding HTTP proxy which might be endorsed by the IT organization. Excluding HTTP proxy from the discussion, external proxies were detected in 80% of the organizations with an average of 3 found in each. As shown in figure 1, the most commonly detected proxies are PHProxy and CGIProxy.

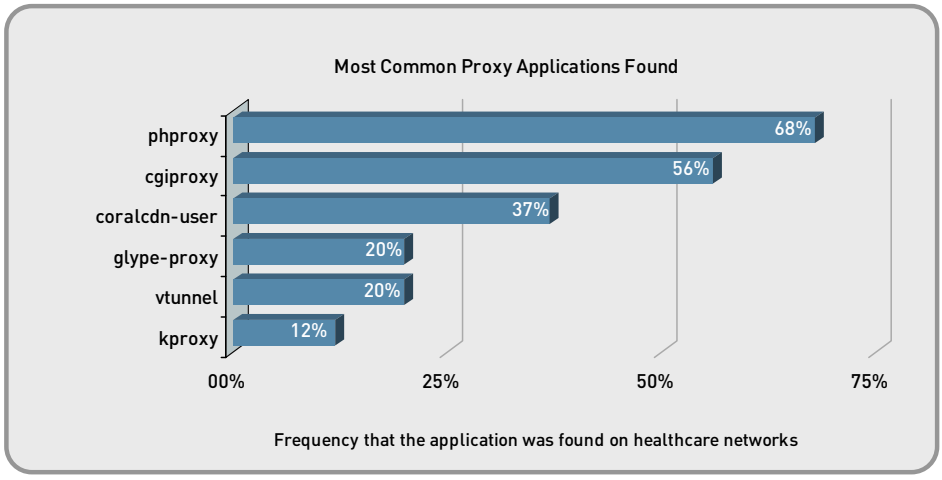



*Figure 1: The most commonly detected proxies found across the participating organizations.*

## ENCRYPTED TUNNEL APPLICATIONS

Whereas a proxy is used primarily to bypass web filtering controls, encrypted tunnel applications go one step further, enabling users to hide their activity within an encrypted tunnel. There are two primary reasons that these applications are in use on healthcare networks.

There are two types of encrypted tunnel applications: those that are endorsed by the organization (IPSec, IKE, ESP, Secure Access, SSH, SSL) and those that are not endorsed (Hamachi, TOR, UltraSurf, Gpass). Given that SSL is commonly used to protect data on healthcare networks, it was not surprising to find it in 100% of the organizations. SSH, found 85% of the time, is frequently used by IT to manage remote systems. Unfortunately, savvy network users have discovered that SSH can be used to establish a protected connection to another machine to bypass existing controls. Excluding the VPN connectivity applications and SSH, we found 7 encrypted tunnel applications across 34% of healthcare networks.

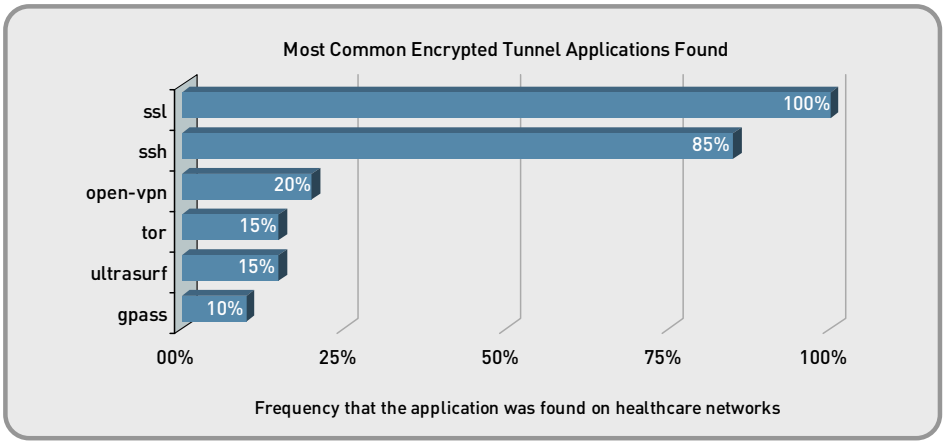



*Figure 2: The most commonly detected encrypted tunnel applications found.*

Of the other encrypted tunnel applications, TOR (The Onion Router) and UltraSurf warrant some added discussion as they are designed for the sole purpose of hiding activity. TOR is an encrypted tunnel that was developed by the U.S. Military as a means of secure communications over the early version of the Internet known as DARPA.NET. TOR is the recommended method of communications for corporate whistle-blowers and the Electronic Frontier Foundation (EFF) also recommends it as a mechanism for maintaining civil liberties online. TOR is a client/server application where the client is installed on the end-user's machine and is used to connect to the intended site through a series of TOR nodes. The data in the message is distributed such that no one node holds the entire message. Privacy is further ensured by the use of proprietary encryption. The final message comes back together when it is received by the intended recipient. Like TOR, Ultrasurf requires the installation of client software which establishes a secure connection for private use. TOR and UltraSurf are applications that have been developed as applications with the explicit purpose of bypassing security.

The use of encrypted tunnel applications that are not VPN connectivity related represents another set of tools that can bypass security mechanisms, thereby exposing healthcare networks to a wide range of security risks such as the transfer of patient records and the introduction of malware.

## REMOTE DESKTOP CONTROL APPLICATIONS

Remote desktop control applications are similar to SSH in that they are commonly used by IT or support to help rectify PC or server problems remotely. Without question, these applications, like SSH, are invaluable tools for support and IT departments, but end-users are fully capable of using them to login to a remote machine and mask their network activity. We found a total of 21 variants, with an average of 6 per organization.

Some of the applications such as pcAnywhere and GoToMyPC are commercially-supported, while others such as RDP and telnet are part of the common operating system IT toolset. RDP is a client/server application that uses port 3389 by default but is also capable of hopping from port to port. RDP is a standard feature in Windows XP Professional, enabling users to access their computers across the Internet from virtually any computer. Once connected, Remote Desktop provides full mouse and keyboard control over the computer while displaying everything that's happening on the screen.

The target users for tools such as RDP historically have been IT-oriented but the sophistication of end-users has advanced to the point where this is no longer the case. With RDP, an employee can configure their PC to connect to an external PC to bypass security and run any application they desire, listen to music or surf the web.

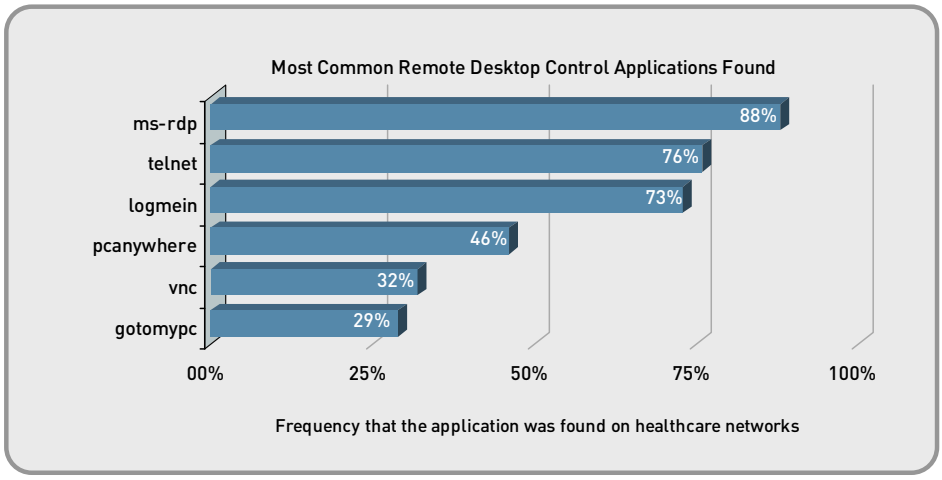



*Figure 3: Most commonly detected remote desktop access applications found.*

The risks that the unchecked use of remote desktop management applications pose is highlighted in a paper by Trustwave where these applications were viewed as the top source for data breaches. The paper states that by themselves, remote desktop applications were not responsible for the breach; they are typically used in conjunction with other attack vectors. When remote access applications are used in an uncontrolled manner, they are displaying bits of information that can be used by attackers to learn more about the network and assemble their attack methodology.

## P2P FILE SHARING USAGE IS HIGH

We found eighteen peer-to-peer (P2P) file sharing application variants across 33 of the 41 (93%) healthcare networks. On average, each of the 34 networks had 5 P2P variants, indicating relatively high usage. The most commonly found variants are shown in the graphic below.

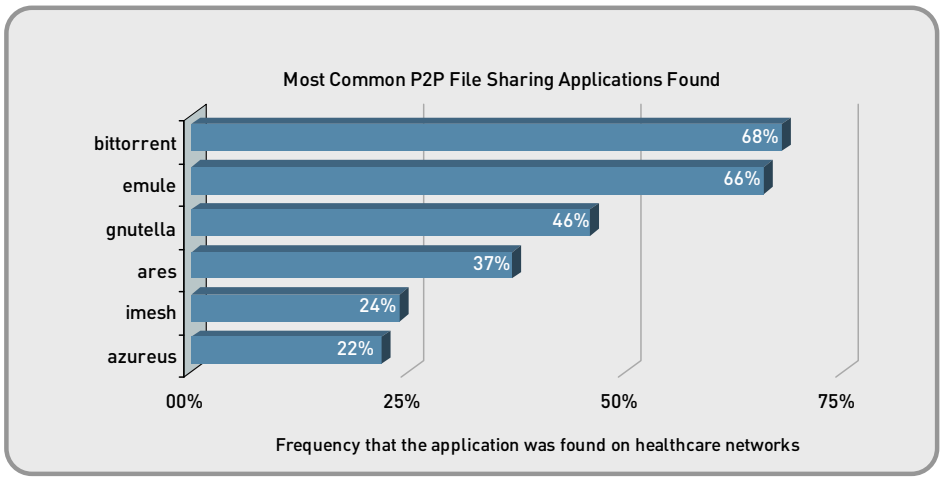



*Figure 4: The most commonly detected P2P-based file sharing applications found.*

P2P applications use a variety of techniques to pass through the firewall including port hopping and masquerading as HTTP. As security administrators developed ad hoc techniques to detect these applications, some P2P developers modified the application to use proprietary encryption as a means of bypassing the firewall, and signature based detection mechanisms. For example, µTorrent, the official BitTorrent client, uses proprietary encryption to evade detection.

It is important to point out that peer-to-peer technology by itself is a very powerful tool, leveraging shared computing resources for efficiency. There are two reasons why P2P file sharing applications have garnered a negative reputation. First, they are being used to share copyrighted materials and second, they have been at the heart of several significant data breaches where personal information has been shared—including healthcare records.

A Computerworld article highlighted the fact that it was very easy to find patient details on P2P networks. The article mentions that, *"using common search terms, the author was able to gain access to a 1,718-page document containing Social Security numbers, dates of birth, insurance information, treatment codes and other health care data belonging to about 9,000 patients at a medical testing laboratory."*

The data that can be found on P2P networks is there because someone has put it there or, in the case of the inadvertent breaches, the application was not configured correctly. The discovery of health care records on P2P networks may or may not slow the momentum for moving all medical records to a consistent electronic format in the US that has been generated by the passage of the $18 billion healthcare reform package. The benefits of electronic storage are clear, as outlined in this US News and World Report article – easy to access, transfer, send and receive. But the risks are great given employees' penchant for ignoring the rules and convincing themselves that they won't infect the network or inadvertently share all of the files on their hard drive (and possibly shared drives on the network).

In the event that the possible inadvertent sharing of patient records is not sufficient to deter the use of these applications, healthcare organizations now must worry about a serious threat being propagated via P2P: the Mariposa threat (also known as Butterfly, Delf, Autorun, and Pilleuz). Mariposa manifests itself as a botnet, arbitrarily downloading executable programs on command. This allows the bot master to infinitely extend the functionality of the malicious software beyond what is implemented during the initial compromise.

The most common Mariposa delivery mechanism are P2P applications, including Ares, Bearshare, Direct Connect, eMule, iMesh, Kazaa, Gnutella, BitTorrent (via LimeWire client), and Shareaza. In addition to spreading via P2P, Mariposa can also spread through IM messages with links to infect other hosts, and via USB drives. Based on the usage of P2P applications within healthcare organizations, nearly every organization assessed is exposed to the Mariposa threat.

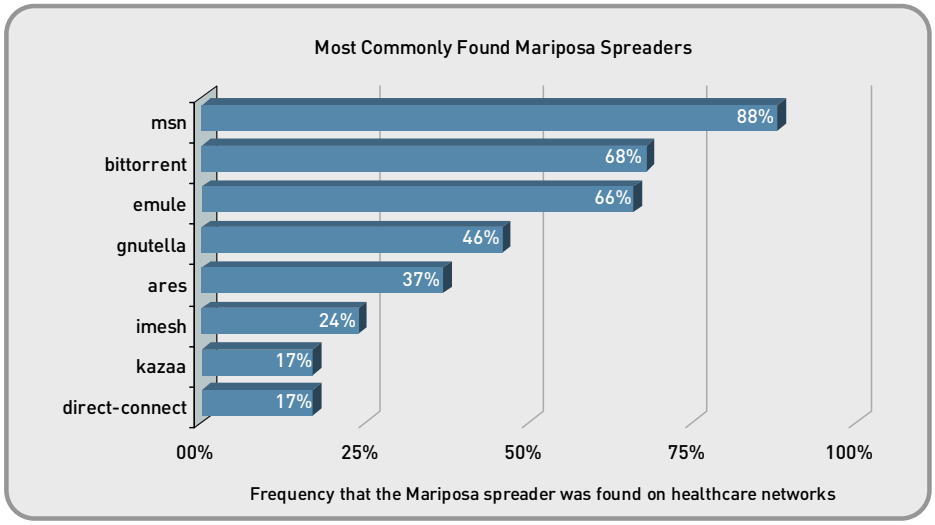



*Figure 5: The most common Mariposa spreaders found across the participating healthcare organizations.*

## BROWSER-BASED FILE SHARING GAINS IN POPULARITY

While not as broadcast-oriented nor as well known as P2P, we found browser-based file sharing applications on 76% of the healthcare networks. We define browser-based file sharing applications as those that provide file transfer (e.g., YouSendit!, MegaUpload), provide file backup (e.g., BoxNet), and public domain publishing (e.g., DocStoc).

In total, we found 22 different browser-based file sharing variants with an average of 7 variants detected on each of the 41 healthcare networks. The most common use for this up and coming class of application is to simplify the transfer of large files through port 80 or port 443 where they look like normal web traffic. The business benefits are significant. Moving x-ray or image files that are too big for email is easily done through a browser which means that users will no longer struggle with how to use ftp.

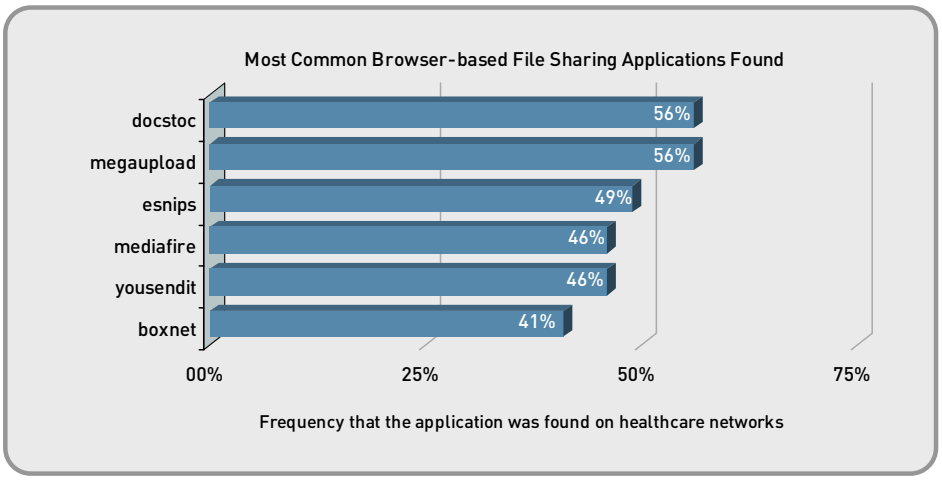



*Figure 6: The most commonly detected browser-based file sharing applications found.*

Browser-based file sharing applications do not pose the same level of risk as P2P file sharing applications, but the risks that do exist cannot be ignored. The significant differences in usage (purposeful file sharing) , application configuration complexity and the many-to-many distribution model indicate that P2P risks are higher. However, in a healthcare environment, browser-based file sharing applications could easily be used to transfer copyrighted materials and sensitive data from research labs in a relatively deliberate manner. In addition, these applications provide a vector for the delivery of threats either directly from someone pulling down an infected file or indirectly through malware-infested advertising (a known delivery mechanism) as part of the application providers' business model.

## HEALTHCARE EMPLOYEES STAY ENTERTAINED

As the cost of bandwidth continues to drop, healthcare organizations are able to increase the size of their Internet connection to deploy more online offerings, improve end-user experience and provide guest networking access to visitors. Unfortunately, high-speed connectivity also means the network users can easily access increased amounts of online content that may not be healthcare in nature and in so doing, adversely affect the business applications.

Out of the 506 applications we found, 32% (161) of them can be categorized as web browsing, media, social networking, or file sharing. Bandwidth consumed by these applications was approximately 45% of the total bandwidth consumed (11 terabytes). A category breakdown of the applications is shown below.

- Web browsing and internet utilities: 24 applications consumed 6.7 terabytes of data (26%)
- Media: 53 photo and video applications including Flash and 23 audio streaming applications consumed 4.3 terabytes of bandwidth (~17%).
- Social networking: 21 applications consumed 135 gigabytes (3%)
- File sharing: 18 P2P and 22 browser-based file sharing applications consumed 52 gigabytes (1%)

In many cases, the use of these applications is purely for entertainment—either the employee or a guest network user. For example, Hulu Networks and Pandora are both entertainment delivery applications and they provide no business value. They do pass the time for a hospital visitor, making it a difficult decision to block the application. Flash and YouTube both span the entertainment and work use as does social networking, depending on the organization policies. As shown below, Flash, if broken out of the photo and streaming video category, represents approximately 7% of bandwidth consumption.

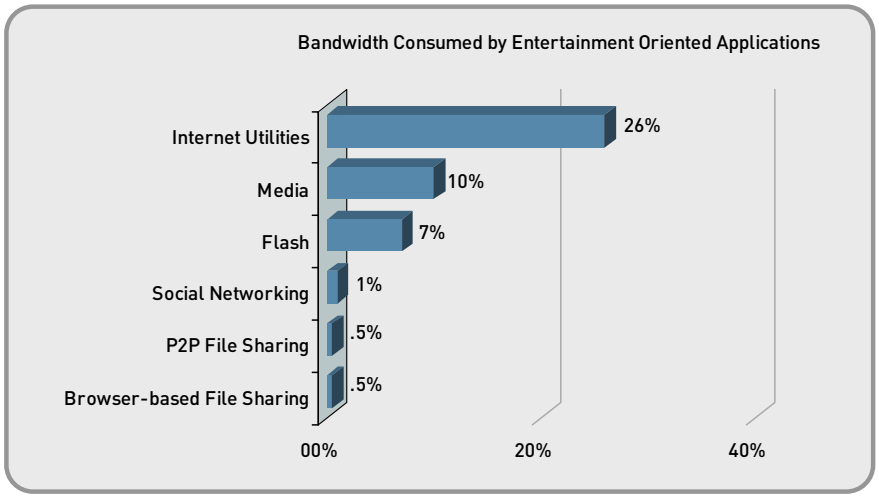



*Figure 7: Breakdown of bandwidth consumption by entertainment oriented application categories.*

New applications that may not be healthcare oriented seem to be made available weekly making the bandwidth management challenge for healthcare organizations that much more significant. Blindly blocking them is not really an option, given the volume, the effort involved and the value presented to guest users. Possibly a more viable alternative is identifying the largest bandwidth hogs based on the application and then allowing them while scanning them for threats and applying QoS to them so that research and business applications are not bandwidth deprived.

## ACCESSIBILITY FEATURES INTRODUCE RISK

Applications that have been designed for accessibility are defined as those that have been developed to use port 80 and port 443, and hop from port to port or can use a combination thereof. As a feature, accessibility is not necessarily a bad thing and in fact, some of the first applications to be developed to take advantage of the "allow port 80" firewall rules were the desktop antivirus applications and the software update services. The benefit of using port 80 is that it helps eliminate some of the IT effort required to deliver updates to desktops.

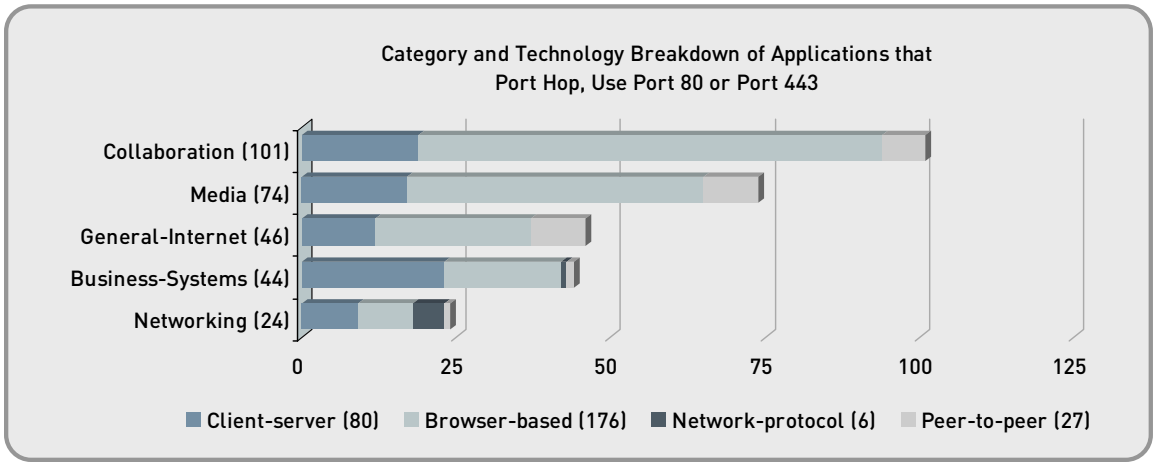



*Figure 8: Breakdown of applications, by category and underlying technology, that use port 80, port 443 or hop ports as a means of simplifying access.*

In this analysis, 60% of the 589 applications we found can use port 80, port 443, or hop from port to port. Every application, particularly those that traverse the firewall, represent risks. The discussion of applications with accessibility features highlights the fact that they may not be what they seem to be. As shown in figure 8, many of them use client/server and peer-to-peer technology, which means that that the traffic traversing the firewall may look like HTTP, but is not web browsing, nor is it a browser-based application. The risks that these applications pose to healthcare organizations is that they are essentially invisible to port-based security solutions, which places patient information at risk.

Blindly blocking these applications is not an option because doing so may be stopping a legitimate use. For example, Microsoft SharePoint, Microsoft Groove, and a host of software update services (Microsoft Update, Apple Update, Adobe Update) all fall into this category, and blocking them will only increase the IT burden. On the other hand, applications such as BitTorrent, Pandora, and YouSendIt! also fall into this category and each of these applications introduces a level of risk that dictates some level of control.

## SUMMARY

The analysis shows that there is wide spread use of applications that span both work and non-work usage patterns which is common on most any network. Surprisingly, applications that enable users to mask their activities are being used regularly as are those that have accessibility features to enable them to bypass the firewall. In order maintain protection of electronic medical records and patient data, comply with governmental regulations (PCI, HIPAA, N3, etc.)[3], and enable guest network access, healthcare organizations need to regain visibility into what users are doing by deploying solutions that provide a view of the applications (not ports or protocols) on the network and then block the known bad applications and control others where appropriate.

## METHODOLOGY

The data in this report is generated via the Palo Alto Networks Application Visibility and Risk assessment process where a Palo Alto Networks next-generation firewall is deployed within the healthcare network, in either tap mode or virtual wire mode, where it monitors traffic traversing the Internet gateway. At the end of the data collection period, up to seven days worth of data is extracted (with permission from the organization) and used to generate an Application Visibility and Risk Report that presents the findings along with the associated business risks, and a more accurate picture of how the network is being used. The data from each of the AVR Reports is then aggregated and analyzed, resulting in The Application Usage and Risk Report.

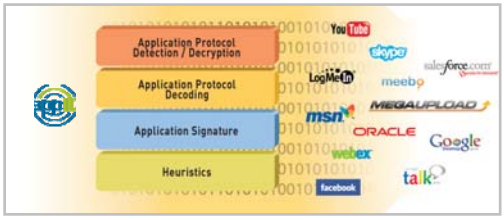
To view details on all applications currently identified by Palo Alto Networks, including their characteristics and the underlying technology in use, please visit the Applipedia (encyclopedia of applications) at the following URL: http://ww2.paloaltonetworks.com/applipedia/

[3] Payment Card Industry Digital Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), N3 Network Security Initiative (N3).

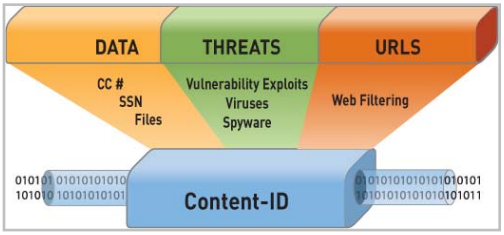
## APPENDIX 1: ABOUT PALO ALTO NETWORKS

Delivered as a purpose-built platform, Palo Alto Networks next-generation firewalls bring visibility and control over applications, users and content back to the IT department using three identification technologies: App-ID, User-ID and Content-ID.

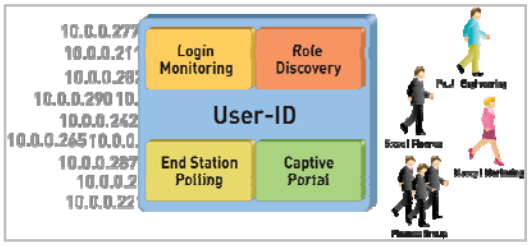
**App-ID™:** The first firewall traffic classification engine to use as many as four different mechanisms to accurately identify exactly which applications are running on the network, irrespective of port, protocol, SSL encryption, or evasive tactic employed. The determination of the application identity is the first task performed by the firewall and that information is then used as the basis for all firewall policy decisions.



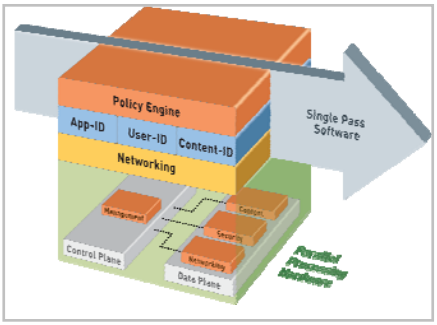

**Content-ID:** A stream-based scanning engine that uses a uniform threat signature format detects and blocks a wide range of threats and limits unauthorized file transfers while a comprehensive URL database controls non-work related web surfing. The application visibility and control delivered by App-ID, combined with the comprehensive threat prevention enabled by Content-ID means that IT departments can regain control over application and related threat traffic.




**User-ID:** Seamless integration with enterprise directory services such as Active Directory, eDirectory, LDAP, and Citrix is unique to Palo Alto Networks and enables administrators to view and control application usage based on individual users and groups of users, as opposed to just IP addresses. User information is pervasive across all features including application and threat visibility, policy creation, forensic investigation, and reporting.




**Purpose-built Platform:** Multi-Gbps throughput is enabled through function-specific processing for networking, security, threat prevention and management, which are tightly integrated with a single pass software engine to maximize throughput. A 10Gbps data plane smoothes traffic flow between processors while the physical separation of control and data plane ensures that management access is always available, irrespective of traffic load.



## APPENDIX 2: APPLICATIONS FOUND

The complete list of the 506 unique applications found, ranked in terms of frequency are listed below. To view details on the entire list of 950+ applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications at http://ww2.paloaltonetworks.com/applipedia/

**100% Frequency**

1. ldap
2. yahoo-mail
3. ssl
4. ntp
5. dns
6. netbios-ns
7. flash
8. web-browsing
9. icmp
10. snmp
11. ms-update
12. http-audio
13. gmail
14. hotmail
15. smtp
16. ftp
17. soap
18. netbios-dg
19. google-safebrowsing
20. rss
21. yahoo-toolbar
22. youtube
23. webdav
24. google-calendar
25. http-video
26. facebook
27. aim-mail
28. sharepoint
29. google-analytics
30. google-toolbar
31. rtmp
32. rtmpt
33. msrpc
34. aim-express
35. yahoo-webmessenger
36. adobe-connect
37. atom
38. google-docs
39. http-proxy
40. myspace
41. apple-update
42. ms-ds-smb
43. msn
44. google-desktop
45. google-picasa
46. ms-rdp
47. spark
48. flexnet-installanywhere
49. itunes
50. outlook-web
51. ipsec-esp-udp
52. ssh
53. google-earth
54. metacafe
55. stumbleupon
56. ike
57. netbios-ss
58. stun
59. gmail-chat
60. kerberos
61. mssql-mon
62. yahoo-im
63. orkut
64. squirrelmail
65. twitter
66. web-crawler
67. hulu
68. rtsp
69. reuters-data-service
70. aim
71. msn-toolbar
72. telnet
73. livejournal

**75% Frequency**

74. live365
75. pandora
76. ms-netlogon
77. backweb
78. dhcp
79. photobucket
80. logmein
81. imeem
82. webshots
83. skype
84. ms-exchange
85. meebo
86. meebome
87. limelight
88. myspace-video
89. citrix
90. active-directory
91. myspace-mail
92. pop3
93. bittorrent
94. webex
95. snmp-trap
96. phproxy
97. linkedin
98. mobile-me
99. emule
100. blackboard
101. citrix-jedi
102. syslog
103. dailymotion
104. skype-probe
105. mssql-db
106. facebook-mail
107. norton-av-broadcast
108. friendfeed
109. yahoo-voice
110. salesforce
111. sharepoint-admin
112. facebook-chat
113. silverlight
114. adobe-update
115. shoutcast
116. pogo
117. live-meeting
118. asf-streaming
119. flixster
120. msn-voice
121. radius
122. zimbra
123. docstoc
124. megaupload
125. google-lively
126. rtp
127. cgiproxy
128. comcast-webmail
129. secureserver-mail
130. msn-file-transfer
131. mms
132. blogger-blog-posting
133. ciscovpn
134. zango
135. slp
136. ms-sms
137. flickr
138. ooyala
139. ustream
140. friendster

**50% Frequency**

141. napster
142. xm-radio
143. mail.com
144. esnips
145. worldofwarcraft
146. move-networks
147. blog-posting
148. gnutella
149. mediafire
150. yousendit
151. portmapper
152. myspace-im
153. hp-jetdirect
154. pcanywhere
155. classmates
156. imap
157. twig
158. msn-webmessenger
159. gotomeeting
160. bbc-iplayer
161. mogulus
162. hi5
163. streamaudio
164. horde
165. boxnet
166. tftp
167. lwapp
168. google-talk
169. lpd
170. time
171. gre
172. lotus-notes
173. outblaze-mail
174. ipsec-esp
175. ebuddy
176. teredo
177. logitech-webcam
178. sip
179. last.fm
180. 4shared
181. ares
182. nintendo-wfc
183. google-video
184. rdt
185. veohtv
186. coralcdn-user
187. bebo
188. plaxo
189. trendmicro
190. blackberry
191. netsuite
192. rapidshare
193. gadu-gadu
194. google-talk-gadget
195. evernote
196. justin.tv
197. vbulletin-posting
198. cox-webmail
199. office-live
200. netspoke
201. yum
202. pptp
203. vnc
204. depositfiles
205. skydrive
206. second-life
207. subspace
208. irc
209. nntp
210. netflow
211. babylon
212. megavideo
213. tidaltv
214. gotomypc
215. stickam
216. yahoo-webcam
217. msn-money-posting
218. oracle
219. optimum-webmail
220. sharepoint-documents
221. ssdp
222. upnp
223. jabber
224. dealio-toolbar
225. ms-groove
226. webex-weboffice
227. mediawiki-editing

**25% Frequency**

228. deezer
229. jango
230. imesh
231. ipv6
232. tvu
233. teamviewer
234. xobni
235. websense
236. h.323
237. grooveshark
238. tacacs-plus
239. mysql
240. open-webmail
241. verizon-wsync
242. bugzilla
243. azureus
244. drop.io
245. corba
246. rpc
247. daytime
248. meevee
249. ppstream
250. socialtv
251. symantec-av-update
252. tivoli-storage-manager
253. h.245
254. ichat-av
255. msn-video
256. filemaker-pro
257. fastmail
258. roundcube
259. open-vpn
260. secure-access

261. dropbox
262. pando
263. imvu
264. yahoo-file-transfer
265. yourminis
266. sopcast
267. glype-proxy
268. vtunnel
269. clearspace
270. mozy
271. sybase
272. yandex-mail
273. direct-connect
274. filestube
275. kazaa
276. sendspace
277. xunlei
278. concur
279. icq
280. userplane
281. cups
282. ipp
283. ncp
284. rtcp
285. rip
286. cooltalk
287. yahoo-finance-posting
288. netease-mail
289. seven-email
290. tor
291. filedropper
292. qq-download
293. yourfilehost
294. sharepoint-calendar
295. youseemore
296. netvmg-traceroute
297. qq
298. autobahn
299. discard
300. zoho-sheet
301. yahoo-douga
302. youku
303. ultrasurf
304. mcafee
305. carbonite
306. nfs
307. gnunet
308. bomberclone
309. playstation-network
310. steam
311. jira
312. livelink
313. subversion
314. iloveim
315. medium-im
316. folding-at-home
317. ping
318. rsvp
319. scps
320. jaspersoft
321. kproxy
322. x11
323. 2ch
324. backup-exec
325. dotmac
326. oovoo
327. orb
328. rhapsody
329. seeqpod
330. tagoo
331. db2
332. hushmail
333. mail.ru
334. qq-mail
335. send-to-phone
336. gpass
337. foldershare
338. neonet
339. poker-stars
340. wolfenstein
341. aim-file-transfer
342. zoho-im
343. finger
344. whois
345. etherip
346. symantec-syst-center
347. vmware
348. babelgum
349. kontiki
350. pplive
351. qvod
352. tudou
353. igp
354. ospfigp
355. xing
356. kaspersky
357. h.225
358. netmeeting
359. sccp
360. seesmic
361. sightspeed
362. winamp-remote
363. bebo-mail
364. groupwise
365. inforeach
366. eatlime
367. generic-p2p
368. live-mesh
369. mediamax
370. apc-powerchute
371. computrace
372. ms-win-dns
373. rpc-over-http
374. koolim
375. radiusim
376. elluminate
377. ebay-desktop
378. echo
379. ibm-director
380. ms-iis
381. noteworthy-admin
382. sophos-update
383. blin
384. fotki
385. joost
386. pna
387. sling
388. tvants
389. uusee
390. freegate
391. hopster
392. zelune
393. l2tp
394. rsh
395. yoics
396. eigrp
397. ndmp
398. gtalk-voice
399. zoho-wiki
400. octoshape
401. pandora-tv
402. cvs
403. 100bao
404. fs2you
405. kugoo
406. manolito
407. xdrive
408. doof
409. source-engine
410. apple-airport
411. mount
412. wins
413. ypserv
414. airaim
415. gtalk-file-transfer
416. imo
417. lotus-sametime
418. messengerfx
419. pownce
420. yugma
421. razor
422. avaya-phone-ping
423. bacnet
424. cpq-wbem
425. ms-dtc
426. wlccp
427. editgrid
428. zoho-notebook
429. zoho-writer
430. earthcam
431. livestation
432. pingfu
433. socks
434. glide
435. radmin
436. rlogin
437. vnc-http
438. hyves
439. rsync
440. sosbackup
441. tikiwiki-editing
442. wetpaint-editing
443. daap
444. iheartradio
445. simplify
446. spotify
447. cisco-nac
448. filemaker-anouncement
449. postgres
450. ilohamail
451. lotus-notes-admin
452. noteworthy
453. zenbe
454. gbridge
455. hotspot-shield
456. ipsec-ah
457. tcp-over-dns
458. innovative
459. sap
460. sugar-crm
461. zoho-crm
462. dropboks
463. fileswire
464. git
465. perforce
466. webconnect
467. fortiguard-webfilter
468. iccp
469. modbus
470. ms-wins
471. t.120
472. icq2go
473. spark-im
474. swapper
475. twitpic
476. campfire
477. dimdim
478. timbuktu
479. yuuguu
480. zoho-meeting
481. host
482. ip-in-ip
483. narp
484. nvp-ii
485. srp
486. unassigned-ip-prot
487. altiris
488. big-brother
489. ms-scheduler
490. netbotz
491. ariel
492. meeting-maker
493. libero-video
494. rtmpe
495. sky-player
496. http-tunnel
497. psiphon
498. r-exec
499. r-services
500. xdmcp
501. bgp
502. hopopt
503. pim
504. rping
505. camfrog
506. wikispaces-editing