The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

Fall Edition 2009

Palo Alto Networks
232 East Java Dr.
Sunnyvale, CA 94089
Sales: 866.207.0077
www.paloaltonetworks.com

Table of Contents

EXECUTIVE SUMMARY

The *Application Usage and Risk Report (Fall Edition, 2009)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing application traffic assessments conducted between March and September of 2009. This version of the report focuses on a group of applications that are top of mind for executives and IT managers alike: Enterprise 2.0 applications. Messaging of all types, social networking, cloud-based productivity, collaboration, blogging and wikis, are just a few of the types of applications that fall within this definition and not coincidently showed significant increases in usage when compared to the *Application Usage and Risk Report (Spring Edition, 2009)*.

Enterprise 2.0 adoption – embraced or resisted – is in full swing.

- More than a third (38%) of the 651 unique applications found fall within the Enterprise 2.0 definition described above. Compared to the *Application Usage and Risk Report (Spring Edition, 2009),* many of the Enterprise 2.0 applications showed significant increases in usage from several different perspectives. For example, SharePoint, Facebook, Twitter, and blog posting all showed double and triple digit increases in how frequently they were found as well as their overall resource consumption (sessions and bytes used).

Enterprise 2.0 benefits are no longer elusive – companies are improving communications and ability to respond while reducing costs.

- Research from McKinsey & Company and the Association for Information and Image Management (AIIM) shows that companies are seeing measurable benefits from the use of Enterprise 2.0 applications and technologies[1]. Specific benefits include an increased ability to share ideas, more rapid access to knowledge experts, and a reduction in travel, operations, and communications costs.

Traditional business and technology distinctions are meaningless.

- Enterprise 2.0 applications highlight the dissolution of the traditional distinctions between business and personal use. More often than not, the same applications used for social interaction are being used for work-related purposes. Irrespective of personal or work related usage, the dominant underlying technology is the browser (72% of research sample). Examples include the chat and email extensions for Facebook, which have rapidly been adopted and are now both ranked 4th in terms of frequency in their respective categories.

Applications are not threats – yet they carry risks.

- The adoption of Enterprise 2.0 applications is being driven by users, not by IT. The ease with which they can be accessed, combined with the fact that newer (younger) employees are accustomed to using them, points toward a continuation of this trend. The somewhat disconcerting fact is that many of the users do not take into account the business and security risks that these applications present. Looking at the 202 Enterprise 2.0 applications found, 70% can transfer files, 28% are known to propagate malware, and 64% have known vulnerabilities. Organizations are scrambling to determine policies, address security issues, and enable appropriate use. These applications are delivering business value – they are rapidly becoming part of "how business gets done" – but the risks are not being weighed by users.

The data within this report shows some significant increases in usage patterns that indicates, albeit somewhat loosely, that the applications are being used for more than entertainment and socializing. The indication is that the use is "how business gets done."

[1] Work Meets Play or the Future of Business (May 2009). McKinsey Global Survey Results: How Companies are Benefitting From Web 2.0 (June 2009). Association for Information and Image Management (AIIM) Industry Watch: Collaboration and Enterprise 2.0.

INTRODUCTION

It was not long ago that instant messaging (IM) made the cross over from personal use to corporate use as a means of enhancing existing communications. IM is easy to use and it lends itself well to textual conversations, thereby making it an ideal way to reach out to a colleague, or collaborate while on a conference call with a customer. At a high level, IM was able to accelerate key aspects of the business. It helped employees get their jobs done.

Fast forward to 2009 and similar criteria can be applied to a wide range of Web 2.0/Internet applications that fall within the Enterprise 2.0 definition. Social networking, blogging/micro-blogging, cloud-based productivity and collaborative applications are just a few of the applications that are making the cross over from personal to corporate use as a means of improving productivity. This report shows that the use of these applications is commonplace across a worldwide sample of more than 200 organizations in a wide range of industries.

From a global view, the traffic analysis showed remarkable consistency in terms of application usage. Categorically, there were no dramatic differences in terms of the types of applications used within the geographic regions. File sharing, IM, email, photo, video, audio, and social networking all showed consistency in terms of how frequently they were found on the network. A few instances of application-specific geographic preferences appeared, however the differences were not significant enough to skew the data one way or another.

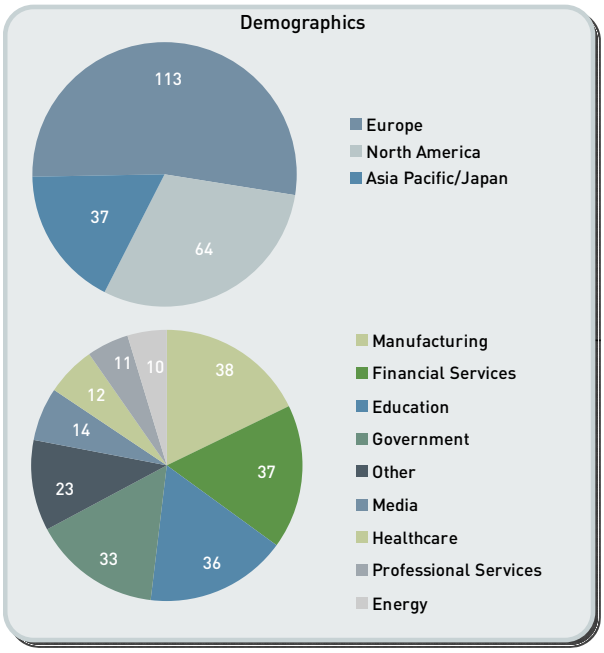

Figure 1: Geographic and industry breakdown of participating organizations.

ENTERPRISE 2.0 APPLICATION USAGE

Full-fledged adoption by IT and management may take quite a while, but Enterprise 2.0 applications are being used for business purposes. The increased frequency with which they were found and the increases in resource consumption, combined with the McKinsey and AIIM surveys, support this assertion. As stated previously, Enterprise 2.0 applications are loosely defined as Web 2.0 / Internet-based applications and technologies used for business purposes. Examples include messaging of all types, social networking, cloud-based productivity, collaboration, and conferencing. Based on this definition, 38% (255) of the 651 applications found during this analysis can be considered Enterprise 2.0.

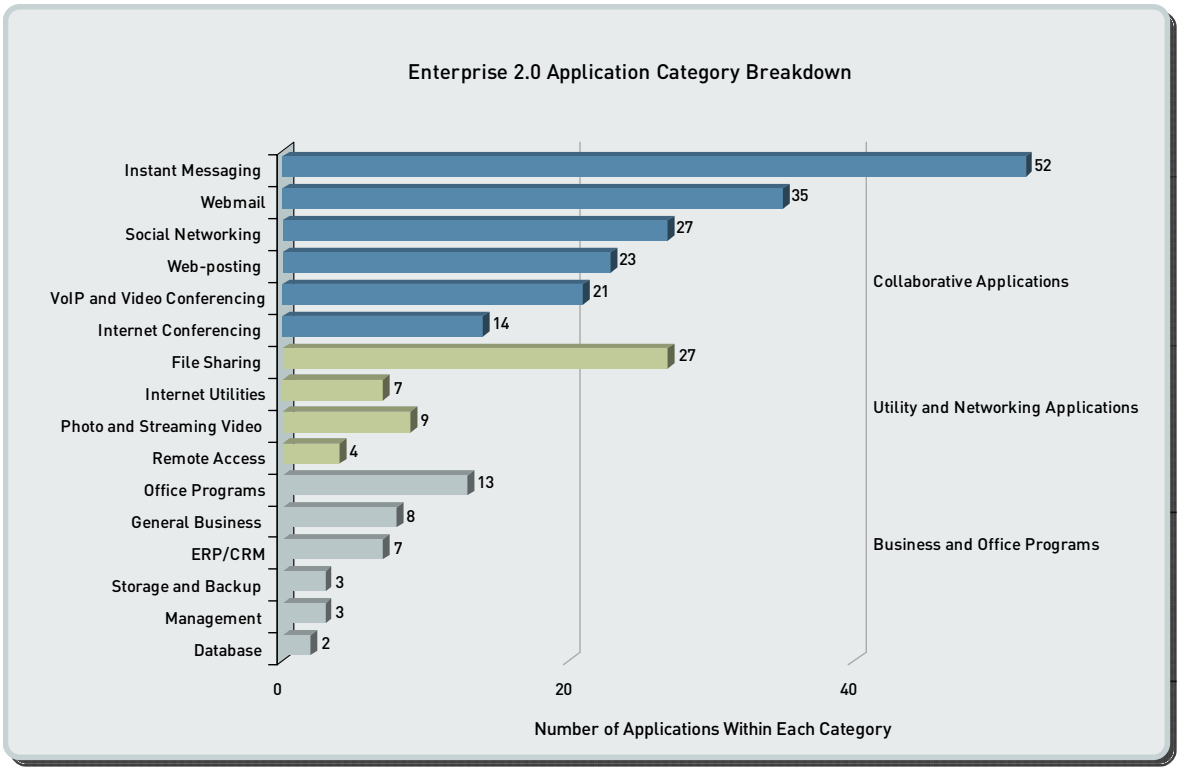

Figure 2: Number of Enterprise 2.0 applications found within each category.

Figure 2 shows that the number of applications found is heavily weighted toward those that are collaborative in nature. This data point supports the underlying premise that Enterprise 2.0 applications are based on a design whereby users and contributors are often one and the same. Many of the applications within the collaborative grouping were first used for personal purposes, expanding later to be used as a business productivity tool. Co-workers used to commonly ask if you are on IM, now, they will ask are you on Facebook or Twitter.

The remaining categories show fewer applications but the breadth of coverage indicates that even those applications are embracing the concepts behind Enterprise 2.0 – examples include productivity and ERP tools from Google and Zoho, as well as backup applications such as Mozy, DotMac and MobileMe. When compared to the *Application Usage and Risk Report (Spring Edition, 2009)*, specific examples of increased Enterprise 2.0 usage abound.

SHAREPOINT USAGE CONTINUES ITS RAPID GROWTH

Gartner estimates that SharePoint is 3rd in collaboration market share with 20%, behind Oracle Collaboration Suite and IBM Lotus Notes, yet year over year growth is a staggering 48% compared to 11% and 12% for the other two vendors[2].

- The analysis showed that 91% of the participating organizations were using SharePoint. This is a significant increase when compared to the *Application Usage and Risk Report (Spring Edition, 2009)*, where SharePoint was found 37% of the time.
- Overall, the average session and bandwidth consumption was flat, with the exception of SharePoint Documents which showed a17-fold increase in bandwidth consumed and a 4-fold increase in session consumption on a per organization basis.

WATCH OUT MICROSOFT, HERE COMES GOOGLE

- Google Docs demonstrated a relatively strong increase in frequency, showing up in 82% of the organizations, compared to 33% in the *Application Usage and Risk Report (Spring Edition, 2009)*.
- Not only was the Google Docs application found more frequently, both the sessions and bandwidth consumed per organization increased approximately 290% from the *Application Usage and Risk Report (Spring Edition, 2009)*, indicating more intense usage.

WEBEX COMPETITORS SHOW INCREASED USAGE

- Of the 14 Internet conferencing applications found, WebEx is the most well known, but not the most commonly used. Adobe-Connect was found 82% of the time, up from 35% in the previous analysis, while WebEx was found 59% of the time, up from 33%.
- WebEx consumed the highest amount of bandwidth per organization (229 MB) when compared to Adobe-Connect (15.4MB) and LiveMeeting (18.5MB). This usage pattern may indicate that WebEx is used for the corporate-focused, structured presentations, while the other tools are for more ad hoc, employee-driven presentations and meetings.

TWITTER RISES FROM NOWHERE

- Twitter is being used heavily and was the most popular instant messaging application (89%), up from 35% in the *Application Usage and Risk Report (Spring Edition, 2009)*.
- The sessions consumed per organization by Twitter users increased 252%, indicating more frequent periods of use, while bandwidth consumed jumped 775% to 184 MB per organization. Even if image transfer is taken into account, this increased usage is significant, given that Twitter communications are limited to a mere 140 characters.

[2] Gartner, Microsoft Continues to Expand Its Portal, Content and Collaboration Market Presence, March 2009

FACEBOOK EXPANDS ITS DOMINANCE

- The frequency with which Facebook was detected grew from 37% to 94% over the past six months. The sessions consumed per organization by Facebook users increased 192% while bandwidth consumed jumped 294% to 6.3 GB per organization, indicating more frequent or longer periods of use.
- For comparisons sake, LinkedIn was found 89% of the time, up from 35% in the *Application Usage and Risk Report (Spring Edition, 2009)*. Interestingly, the bandwidth and session consumption per organization declined 42% and 22%, respectively.
- Perhaps most interesting is the rapidity with which the Facebook Mail and Facebook Chat applications have become the 4th most commonly detected applications within their respective categories. Note that Facebook Chat was released in April 2008, and in a mere 18 months, it has become more widely used than Yahoo! IM and AIM (within this sample).

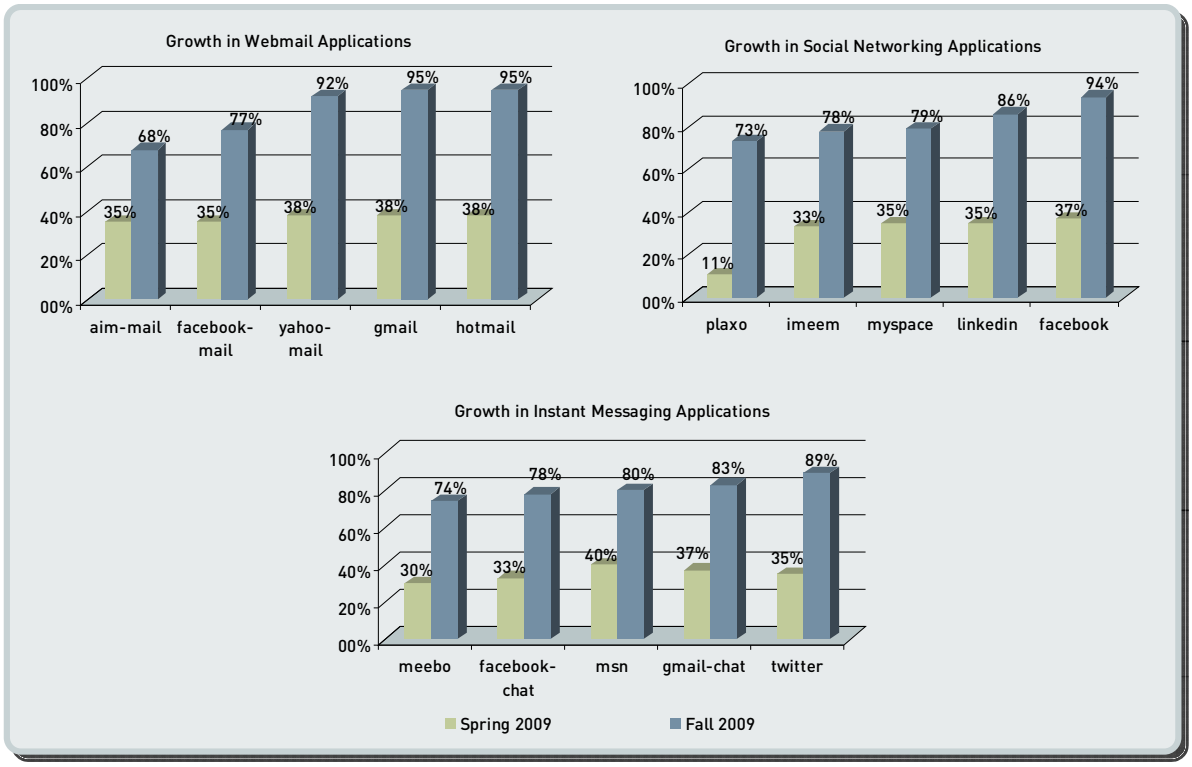

Figure 3: Changes in growth for top 5 social networking, webmail and instant messaging applications.

EMPLOYEES ARE ACTIVE CONTRIBUTORS

Not so long ago, a dictionary was the main resource to discover what the meaning of a word. Now, even though the Merriam Webster dictionary is online (www.m-w.com), it is more likely that a user will use Wikipedia (or Google, which will likely include a Wikipedia reference). This usage pattern points to two items relative to the Enterprise 2.0 discussion.

The first is obvious – the Internet is the fastest, most effective way to access to a wealth of information. The second point is that all of the content on Wikipedia is generated, vetted, edited, and defended by users. There is a Wikipedia moderator but most often, they remain in the background. User-generated content is one of the key tenets of the Enterprise 2.0 world. More accurately, users, consumers and contributors are often one and the same.

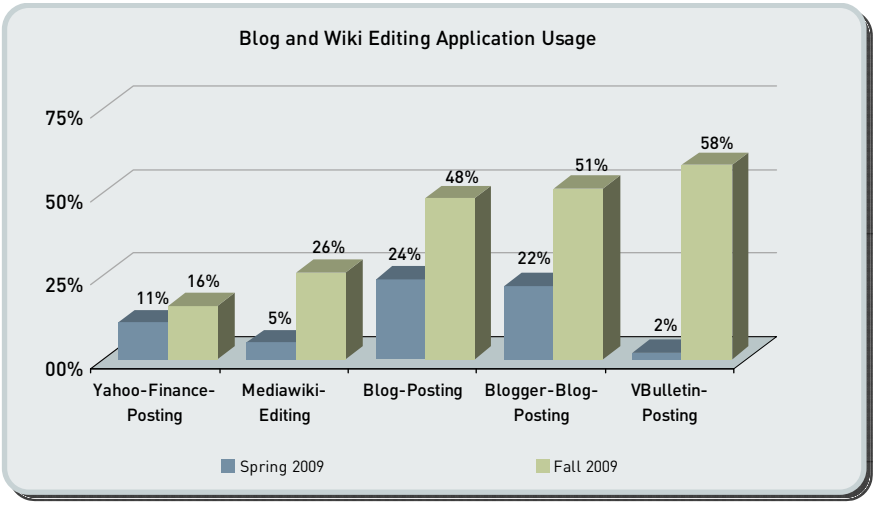

Figure 4: Frequency that top blog/wiki editing applications were found.

Looking now at the applications found during this analysis, the statistics show that users were significantly more active in their blogging and posting activity when compared to the *Application Usage and Risk Report (Spring Edition, 2009)*. In addition to the frequency with which these applications were found, overall activity increased from several perspectives.

- The number of application variants found more than doubled to 23, up from 11.
- Total session activity increased by a factor of 39 while total bandwidth consumed increased by a factor of 48.

The dramatic increases in blog/wiki activity fully supports one of the key tenets around Enterprise 2.0 applications, which is that users, consumers and contributors are often the same person.

ENTERPRISE 2.0 BENEFITS ARE NO LONGER ELUSIVE

A key difference between Enterprise 2.0 applications and the more "traditional" corporate applications is who is driving the adoption. A traditional application such as Microsoft Word or an Oracle Database is almost always driven from the top down, by management or corporate edict. Enterprise 2.0 applications on the other hand are often driven from the bottom up, by end-users. Three examples that support this observation are Google Docs, SharePoint and Facebook.

- Google Docs: In some ways, Google Docs epitomize Enterprise 2.0 applications. They are collaborative, they are easily accessible, and they help users get their jobs done. Users introduced these applications to the enterprise world and over time IT and management have begun to view them as a viable alternative. Many of the more progressive organizations are offering them as an alternative to the desktop-based productivity applications. In an online survey done by industry analyst firm IDC, the use of Google Docs is expected to grow from 19.5% to 27.1% in 12 months[3]. The same poll showed that Microsoft Office use would remain flat at the rate of 96.9%.

- SharePoint: In most cases, SharePoint is being deployed by management, in a top down manner, but according to Gartner[4], there is evidence that approximately 30% of the deployments are rogue , meaning that end-users or business groups saw a need to be more collaborative and deployed a tool they had at their disposal. Microsoft has made deploying SharePoint relatively easy. A standalone version of SharePoint is included for free as part of the Windows Server Services (WSS) package. WSS integrates with Microsoft Office (Word, PowerPoint, Access, Excel, and Outlook) and when documents or content changes, RSS feeds can notify users as needed.

- Social Networking: The increased usage patterns of Facebook and LinkedIn shown earlier, coupled with data points from AIIM and McKinsey, indicate that these applications are being used for business purposes. The McKinsey report indicates that Facebook enables viral marketing to a specific set of users while the AIIM report shows that users are more likely to have a LinkedIn account for business purposes and a Facebook account for personal use.

Irrespective of who is driving the adoption of Enterprise 2.0 applications, the quantification of the business benefits has historically been elusive. This is no longer the case as shown in two industry reports by McKinsey Consulting and the non-profit group Association for Information and Image Management (AIIM). The results from recent surveys by both of these groups show that respondents are seeing measurable benefits from the use of these tools[5].

- The McKinsey Report on Web 2.0: Approximately 69% of the companies surveyed have gained measurable benefits – innovation, more effective marketing, more rapid access to information, lower costs and higher revenues. Respondents saw an increased ability to share ideas, more rapid access to knowledge experts, and a reduction in costs for travel, operations and communications. Quantitatively, benefits ranged from a 10% reduction in operational costs to a 30% increase in the speed to access knowledge experts.

- AIIM: More than 50% of those surveyed consider the use of Enterprise 2.0 applications to be important or very important. The top three business benefits were knowledge sharing at nearly 60%; reduced effort in information gathering (nearly 50%), and improved efficiency/speed of delivery (35%).

[3] IDC Office QuickPoll Online Survey, July 2009
[4] Gartner, Neil MacDonald, The Phantom Security Menace Rogue SharePoint Sites http://blogs.gartner.com/neil_macdonald/2009/03/24/the-phantom-security-menace-rouge-sharepoint-sites/
[5] Association for Information and Image Management (AIIM) Industry Watch: Collaboration and Enterprise 2.0.

The benefits around the adoption of Enterprise 2.0 will continue to gain momentum as users and business managers figure out new ways of using these tools. The question is, what are the risks and how can they be effectively managed? The answer is to develop new application usage policies that enable the use of these applications while maintaining an appropriate security posture.

USAGE PATTERNS INDICATE BOTTOMS UP ADOPTION

No one would argue that the adoption of Enterprise 2.0 applications is being driven by end-users. Many data points exist to support this fact. The applications themselves—Facebook, LinkedIn, Gmail, Yahoo! IM, Twitter—all began as personal use applications. Many of these applications are becoming, or have already become, a vital part of the users' lives. This trend, good or bad, will only accelerate as younger people move into the workforce.

The rapid growth in usage makes sense – there are no barriers to entry for many of these tools for users to register and start sharing, collaborating and communicating. The underlying technology helps continue the accelerated use with the vast majority (72%) of them being browser-based. Of the 51 client-server applications on the list, 80% of them use port 80, port 443, or can hop ports as a means of simplifying access, showing once again that reducing the barriers to entry can help increase the usage.

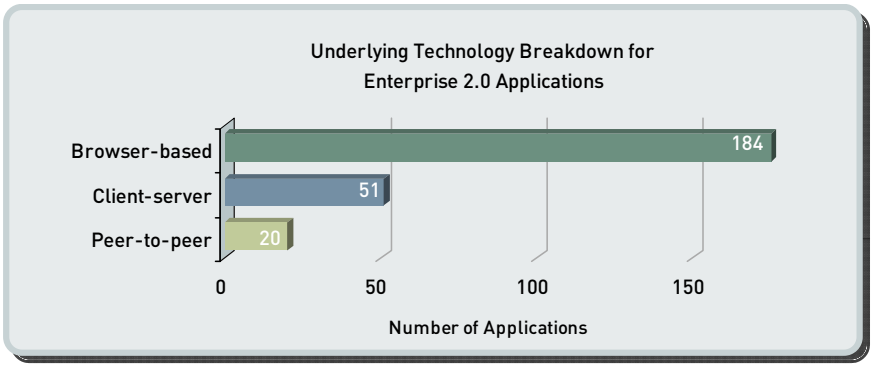

Figure 5: Breakdown of underlying technology for the 255 Enterprise 2.0 applications.

APPLICATIONS ARE NOT THREATS

Yet applications do indeed carry risks. This is a key point and possibly the most significant consideration that organizations must take into account as they look at embracing and deploying Enterprise 2.0 applications. The fact that many of these applications cross the work-versus-play boundary and are web-based makes controlling their use in a secure manner difficult.

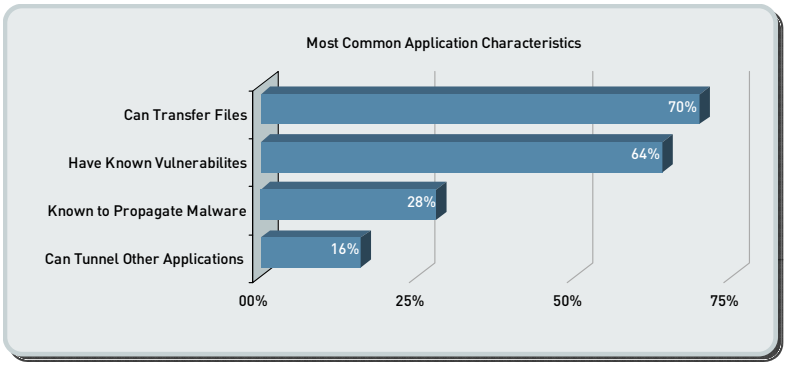

Figure 6: Application behavioral characteristics that represent business and security risks.

Each application that Palo Alto Networks identifies includes data on the behavioral characteristics which is used by administrators to learn more about the application and in turn, make a more informed business decision on how to treat the application. Based on the behavioral characteristics of the applications within the analysis, the most significant risk is leakage/loss of personal and corporate data brought on by file transfer capabilities (70%) within the application. Applications that have known vulnerabilities (64%) or can propagate or be used by malware (28%) pose a risk to the network in terms of business continuity and the subsequent increased operational costs from desktop clean up and forensics efforts.

Most users will not be fully aware of the specific application behaviors and the risks that they pose, much less the specific threats that target an application. Cyber-criminals are not dumb – they look for a target-rich environment such as Microsoft applications because they represent the vast majority of the PC installed base. Depending on the configuration, SharePoint uses MS-SQL, IIS and ASP.Net—all of which have known vulnerabilities that are used by cyber criminals to achieve their monetary goals.

Social networking users represent an equally target-rich environment—millions of users exchanging images, links and documents at a breakneck pace with a "click now, think later" mentality. KoobFace, Fbaction, and Boface are just a few examples of the threats that are propagated via a URL from a social networking site that invites a recipient to join the network or view a photo. These threats take advantage of the implied trust that social networking users have with each other.

- Koobface: this threat (the anagram of Facebook) is multi-faceted, targeting MySpace, Twitter, Facebook and other sites. Users are prompted to click on a URL and a worm is downloaded to the PC which looks for personal data.
- Fbaction: Another Facebook phishing attack that encourages users to sign up for fbaction.net using their Facebook credentials. Those credentials are then used to hijack the Facebook account.
- Boface: Convinces users to click on a link pointing to a video resulting in a download. Shortly after the download is complete, the user's Facebook account will be hijacked and used as a means of spamming (and propagating a worm) all their friends.

According to the AIIM report mentioned previously, only 30% of the companies surveyed have policies around the use of Enterprise 2.0 applications, compared with 88% who have policies around the use of email. Interestingly, in the same report, security risks as an impediment to deployment ranked 6th behind items such as lack of understanding, corporate culture, priority, costs and ROI[6].

[6] Association for Information and Image Management (AIIM) Industry Watch: Collaboration and Enterprise 2.0.

ONGOING TRENDS IN USAGE

The *Application Usage and Risk Report*, now in its fourth iteration, provides a view into longer-term trends around application activity. One of those trends is the rapid ascension of browser-based file sharing, which now exceeds peer-to-peer file sharing in frequency. In addition to the shift in file sharing usage, an analysis of the applications that are built for accessibility through the inclusion of port 80, port 443, or port hopping features continues to expand while users continue to stay entertained at work, consuming massive amounts of bandwidth.

A SUBTLE SHIFT IN FILE SHARING USAGE: P2P VS. BROWSER-BASED

Since the inaugural *Application Usage and Risk Report (Spring Edition, 2008)*, browser-based file-sharing usage in terms of frequency has steadily increased to the point where the frequency with which it was found now exceeds that of peer-to-peer file sharing. A portion of the initial growth from Spring 2009 to Fall 2009 can be attributed to the addition of new applications to the database.

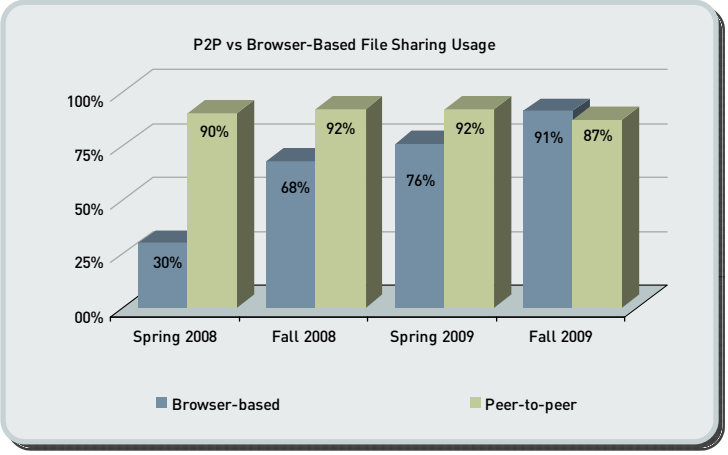

Figure 7: Comparative growth of browser-based file sharing usage.

It is no surprise that browser-based file sharing usage is on the rise. It is a useful tool that simplifies the transfer of large files; it enables centralized storage for mobile users; and it allows all users to backup their data in an easily accessible location. A comparison of resource consumption and the number of variants found is shown in the table below.

	Browser-Based File Sharing	Peer-to-Peer File Sharing
Frequency that the application type was found	91%	87%
Total bandwidth consumed	2.98 TB	15.95 TB
Total sessions used	5.1 Million	561 Million
Megabytes per session	0.58 MB/Session	0.03 MB/Session
Number of application variants found	23	22
Average number of application variants per organization	8	5
Most frequently detected application	Skydrive (66%)	BitTorrent (61%)
Most bandwidth intensive application	RapidShare (2 TB)	BitTorrent (13.1 TB)

It would be inaccurate to say that browser-based file sharing pose the same level of risks that peer-to-peer applications pose. There have been no known errant distributions of confidential files through browser-based file sharing, possibly because they are user-to-user focused as opposed to the broadcast focus for P2P.

The benefit to browser-based file-sharing applications is they make if very easy to move large files such as a presentation or a graphic. Users are no longer forced to split a file up or take other steps to get around the email attachment limitations. However, browser-based file sharing applications do pose some risks because they represent an avenue for purposeful transfer of confidential data. In addition to the potential data leakage risks, 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.

USE OF APPLICATIONS WITH ACCESSIBILITY FEATURES CONTINUES

The Spring 2009 Application Usage and Risk Report introduced the analysis of applications that use port 80, port 443, or port hop as a feature in order to improve accessibility. To the application developer, accessibility makes the application easier to use, thereby increasing usage while decreasing user issues. For the end-user, it means the application can be used from anywhere, at anytime.

Out of the 651 unique applications found in this analysis, 59% were designed for accessibility. As displayed in figure 8, the majority of these applications appear to be consumer-oriented, but there are applications within the category that are indeed used for business. The collaborative applications group includes social networking (25), email (31), instant messaging (43), VoIP/video (14), web posting (21) and conferencing (7). Based on the data in earlier sections of this report, and on what is seen in research on a regular basis, it is safe to say that these applications may not be endorsed by corporate IT, yet they do provide some business benefit. The business value becomes less clear when looking at the high number of media applications (93), which includes streaming audio, photo-video, and gaming.

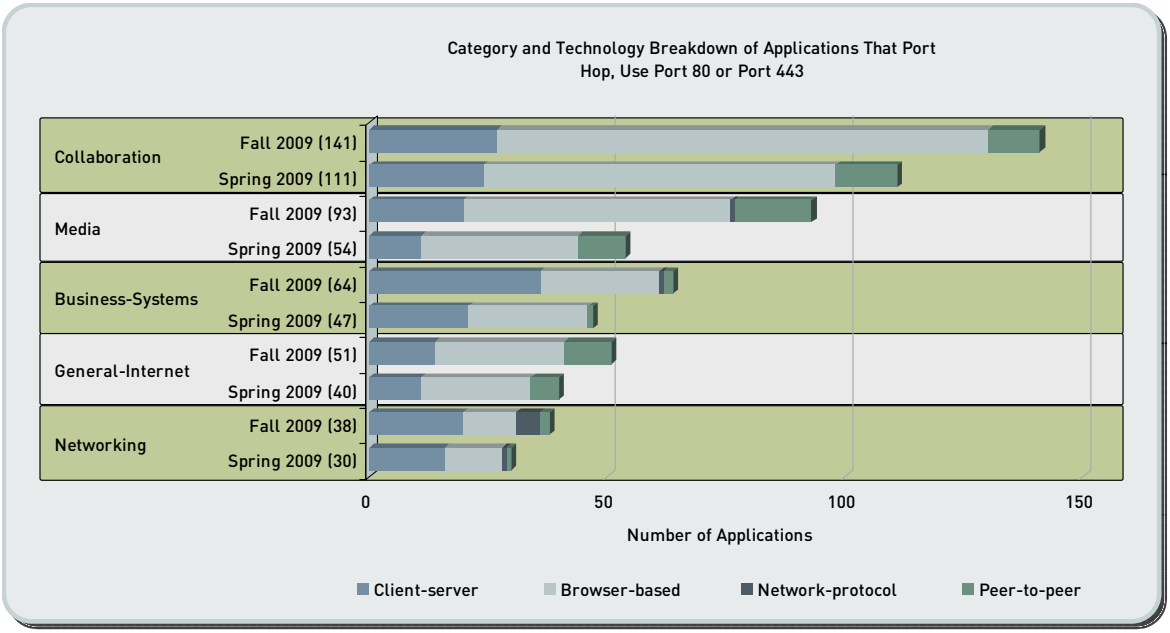

Figure 8: Comparative growth of applications with accessibility features.

A final takeaway within this group of applications is the underlying technology that is in use. The heavy use of client-server and peer-to-peer technology shows that the traffic traversing the firewall may look like HTTP, but it is not web browsing and in fact may not use the browser at all.

ENTERTAINMENT APPLICATIONS REMAIN VORACIOUS

The Spring 2009 Application Usage and Risk Report showed that a relatively small number of primarily entertainment focused applications (25%) were consuming more than half of the overall bandwidth. The Fall 2009 analysis shows that this trend is ongoing, with 29% of the applications (190) consuming 56% of the bandwidth (105 TB).

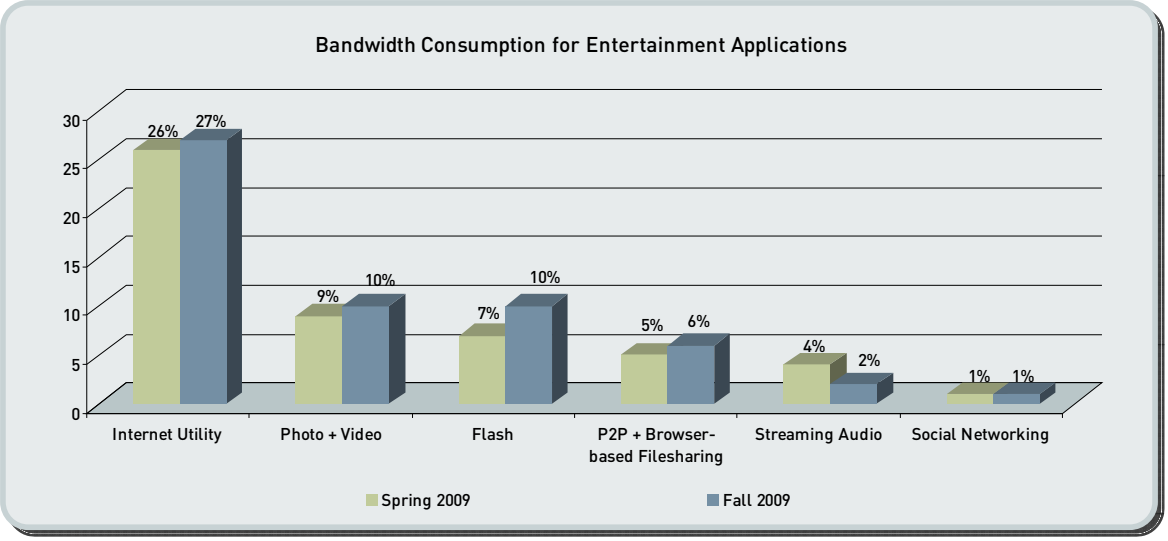

Figure 9: Bandwidth consumption for entertainment applications.

Of note is the fact that Flash, an application used extensively for both work and entertainment, was shown to consume 10% of the bandwidth; a massive 18TB.

SUMMARY

The bi-annual Application Usage and Risk Report has firmly established the fact that users are accessing nearly any application they want and at any time for both business and personal purposes. The Fall 2009 version Application Usage and Risk Report shows that Enterprise 2.0 applications are increasing in use. The reasons are relatively obvious as they enable viral marketing, more rapid information access, and cost reductions for travel and communications. However, in many cases, the rapid growth in usage is occurring without proper considerations for the associated business and security risks. Those that blindly allow the use expose themselves to significant business and security risks. Those the summarily block them all will force end-users to figure out a way to go around the control mechanisms. Organizations need to strike an appropriate balance between the business benefit and the associate security risks.

About Palo Alto Networks

Palo Alto Networks™ is the leader in next-generation firewalls, enabling unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 10Gbps with no performance degradation. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. Enterprises can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation. For more information, please visit http://www.paloaltonetworks.com.

APPENDIX 1: 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 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, usually up to seven days, an Application Visibility and Risk Report is generated 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.

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, Content-ID and User-ID.

App-ID: Using as many as four different traffic classification mechanisms, App-ID™ accurately identifies exactly which applications are running on networks – irrespective of port, protocol, SSL encryption or evasive tactic employed. App-ID gives administrators increased visibility into the actual identity of the application, allowing them to deploy comprehensive application usage control policies for both inbound and outbound network traffic.

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 transfer of files and sensitive data (CC# and SSN), 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 Microsoft Active Directory links the IP address to specific user and group information, enabling IT organizations to monitor applications and content based on the employee information stored within Active Directory. User-ID allows administrators to leverage user and group data for application visibility, policy creation, logging and reporting.

Purpose-Built Platform: Designed specifically to manage enterprise traffic flows using function-specific processing for networking, security, threat prevention and management, all of which are connected by a 10 Gbps data plane to eliminate potential bottlenecks. The physical separation of control and data plane ensures that management access is always available, irrespective of the traffic load.

To view details on more than 900 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/

APPENDIX 2: APPLICATIONS FOUND

The highest number of applications found on any one network was 402 with the average being 165. The complete list of the 615 unique applications found, ranked in terms of frequency are listed below. To view details on the entire list of 900+ 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%

1. web-browsing
2. ssl
3. dns
4. icmp
5. ntp
6. flash
7. netbios-ns
8. ms-update
9. ftp
10. youtube
11. google-analytics
12. soap
13. snmp
14. google-safebrowsing
15. rss
16. http-audio
17. hotmail
18. gmail
19. http-proxy
20. facebook
21. smtp
22. http-video
23. google-toolbar
24. rtmpt
25. yahoo-mail
26. photobucket
27. ldap
28. sharepoint
29. netbios-dg
30. limelight
31. adobe-update
32. atom
33. twitter
34. google-video
35. msrpc
36. google-calendar
37. yahoo-toolbar
38. webdav
39. dailymotion
40. asf-streaming
41. linkedin
42. flickr
43. apple-update
44. google-desktop
45. flexnet-installanywhere
46. silverlight
47. ms-rdp
48. ms-ds-smb
49. gmail-chat
50. google-docs
51. adobe-connect
52. google-picasa
53. rtmp
54. msn
55. ssh
56. myspace
57. skype
58. kerberos
59. imeem
60. itunes
61. facebook-chat
62. metacafe

75%

63. facebook-mail
64. web-crawler
65. myspace-video
66. meebo
67. google-earth
68. plaxo
69. yahoo-webmessenger
70. yahoo-im
71. netbios-ss
72. napster
73. webshots
74. telnet
75. outlook-web
76. mssql-mon
77. spark
78. reuters-data-service
79. ms-netlogon
80. stumbleupon
81. mobile-me
82. hulu
83. dhcp
84. ike
85. flixster
86. aim-mail
87. active-directory
88. skype-probe
89. salesforce
90. skydrive
91. last.fm
92. stun
93. squirrelmail
94. friendfeed
95. livejournal
96. office-live
97. msn-file-transfer
98. google-talk-gadget
99. pop3
100. orkut
101. ipsec-esp-udp
102. msn-voice
103. ustream
104. msn-toolbar
105. logmein
106. citrix
107. rapidshare
108. google-lively
109. syslog
110. bittorrent
111. mssql-db
112. babylon
113. shoutcast
114. rtsp
115. webex
116. docstoc
117. vbulletin-posting
118. megavideo
119. aim-express
120. yousendit
121. nintendo-wfc
122. ms-sms
123. mediafire
124. justin.tv
125. aim
126. lotus-notes
127. backweb
128. friendster
129. blackboard
130. slp
131. megaupload
132. blogger-blog-posting
133. snmp-trap
134. sharepoint-admin
135. myspace-mail
136. ebuddy
137. hp-jetdirect
138. esnips
139. emule
140. phproxy
141. mogulus
142. ooyala

50%

143. zango
144. 4shared
145. gnutella
146. blog-posting
147. msn-webmessenger
148. horde
149. bbc-iplayer
150. ms-exchange
151. meebome
152. yourminis
153. gotomeeting
154. deezer
155. live365
156. hi5
157. boxnet
158. depositfiles
159. ares
160. google-talk
161. yahoo-voice

162. symantec-av-update
163. zimbra
164. rtp
165. sip
166. pandora
167. oracle
168. citrix-jedi
169. gadu-gadu
170. dropbox
171. radius
172. norton-av-broadcast
173. vnc
174. time
175. teamviewer
176. bebo
177. clearspace
178. cgiproxy
179. tftp
180. sendspace
181. outblaze-mail
182. ciscovpn
183. pogo
184. jabber
185. filestube
186. mail.com
187. teredo
188. imap
189. twig
190. blackberry
191. myspace-im
192. coralcdn-user
193. veohtv
194. xobni
195. worldofwarcraft
196. stickam
197. portmapper
198. logitech-webcam
199. jango
200. bugzilla
201. yum
202. rdt
203. mms
204. sharepoint-documents
205. roundcube
206. xing
207. ssdp
208. yandex-mail
209. open-vpn
210. lwapp
211. azureus
212. second-life
213. lpd
214. trendmicro
215. secureserver-mail
216. qvod
217. live-meeting
218. classmates
219. playstation-network
220. ping
221. mail.ru
222. irc
223. netsuite
224. gre
225. youku
226. mediawiki-editing
227. ipsec-esp
228. ppstream
229. yahoo-douga
230. tvu
231. soribada
232. grooveshark

25%

233. netvmg-traceroute
234. evernote
235. echo
236. dealio-toolbar
237. netspoke
238. mysql
239. msn-video
240. hyves
241. iloveim
242. flumotion
243. qq-mail
244. pptp
245. kaspersky
246. pando
247. ms-groove
248. icq
249. upnp
250. socialtv
251. oovoo
252. diino
253. yourfilehost
254. xunlei
255. tudou
256. imvu
257. netflow
258. h.323
259. glype-proxy
260. drop.io
261. subversion
262. subspace
263. libero-video
264. daytime
265. tidaltv
266. rpc
267. 2ch
268. yahoo-file-transfer
269. pcanywhere
270. netease-mail
271. move-networks
272. kontiki
273. ipv6
274. h.245
275. gotomypc
276. seeqpod
277. qq-download
278. qq
279. jaspersoft
280. ipp
281. gpass
282. vmware
283. imesh
284. corba
285. yahoo-webcam
286. sharepoint-calendar
287. seesmic
288. yahoo-finance-posting
289. rsvp
290. nfs
291. messengerfx
292. kazaa
293. blin
294. streamaudio
295. steam
296. nntp
297. eatlime
298. mozy
299. generic-p2p
300. xm-radio
301. tuenti
302. source-engine
303. rtcp
304. open-webmail
305. vtunnel
306. sophos-update
307. rhapsody
308. neonet
309. ichat-av
310. autobahn
311. filemaker-pro
312. fastmail
313. userplane
314. secure-access
315. rip
316. octoshape
317. dotmac
318. winamp-remote
319. websense
320. symantec-syst-center
321. sightspeed
322. pandora-tv
323. orb
324. sap
325. kugoo
326. cox-webmail
327. zoho-im
328. tor
329. jira
330. imo
331. direct-connect
332. whois
333. tacacs-plus
334. optimum-webmail
335. livelink
336. carbonite
337. webex-weboffice
338. tagoo
339. sybase
340. qqlive
341. pplive
342. wins
343. rsync
344. mount
345. medium-im
346. l2tp
347. h.225
348. sopcast
349. editgrid
350. cups
351. apple-airport
352. ultrasurf
353. tivoli-storage-manager
354. ncp
355. ms-win-dns
356. msn-money-posting

357. babelgum
358. radmin
359. poker-stars
360. fotki
361. folding-at-home
362. camfrog
363. veetle
364. send-to-phone
365. livestation
366. gnunet
367. discard
368. cooltalk
369. backup-exec
370. zoho-writer
371. wolfenstein
372. verizon-wsync
373. socks
374. radiusim
375. postgres
376. mixi
377. filedropper
378. concur
379. computrace
380. netop-remote-control
381. freeetv
382. zoho-show
383. scps
384. lotus-sametime
385. koolim
386. instan-t-file-transfer
387. zoho-sheet
388. uusee
389. sccp
390. live-mesh
391. joost
392. hopster
393. gtalk-file-transfer
394. aim-file-transfer
395. acronis-snapdeploy
396. x11
397. netviewer
398. ms-wins
399. manolito
400. lokalisten
401. finger
402. xdmcp
403. tikiwiki-editing
404. sling
405. pownce
406. miro
407. mcafee
408. ibm-director
409. hushmail
410. hotspot-shield
411. garena
412. gamespy
413. ebay-desktop
414. db2
415. cpq-wbem
416. comcast-webmail
417. bebo-mail
418. zelune
419. vnc-http
420. twitpic
421. spotify
422. rsh
423. rping
424. packetix-vpn
425. ospfigp
426. niconico-douga
427. netmeeting
428. ms-iis
429. kproxy
430. iheartradio
431. icq2go
432. doof
433. zoho-wiki
434. yoics
435. timbuktu
436. soulseek
437. rpc-over-http
438. ndmp
439. mcafee-epo-admin
440. glide
441. git
442. battlefield2
443. xbox-live
444. wikispaces-editing
445. sugar-crm
446. simplify
447. rlogin
448. razor
449. mediamax
450. kino
451. ilohamail
452. groupwise
453. cvs
454. youseemore
455. xfire
456. wetpaint-editing
457. tcp-over-dns
458. pim
459. peerguardian
460. ms-scheduler
461. igp
462. gizmo
463. gds-db
464. foxy
465. feidian
466. elluminate
467. dabbledb
468. cisco-nac
469. circumventor
470. bacnet
471. yuuguu
472. ypserv
473. yahoo-blog-posting
474. webconnect
475. wccp
476. t.120
477. ms-dtc
478. fs2you
479. freegate
480. eigrp
481. zenbe
482. yammer
483. writeboard
484. wiiconnect24
485. tvants
486. sky-player
487. rtmpe
488. noteworthy-admin
489. ms-ocs
490. meevee
491. imhaha
492. iccp
493. gtalk-voice
494. genesys
495. forticlient-update
496. avaya-phone-ping
497. wixi
498. usermin
499. unassigned-ip-prot
500. thinkfree
501. sosbackup
502. siebel-crm
503. qqmusic
504. party-poker
505. meebo-file-transfer
506. jap
507. informix
508. igmp
509. hopopt
510. big-brother
511. zoho-planner
512. zoho-mail
513. zoho-crm
514. yugma
515. web-de-mail
516. taku-file-bin
517. seven-email
518. ovation
519. noteworthy
520. netbotz
521. megaproxy
522. meabox
523. ip-in-ip
524. innovative
525. inforeach
526. http-tunnel
527. graboid-video
528. gmail-drive
529. g.ho.st
530. fortiguard-webfilter
531. foldershare
532. flashget
533. esignal
534. earthcam
535. dimdim
536. crossloop
537. cddb
538. asterisk-iax
539. apc-powerchute
540. 2ch-posting
541. 100bao
542. zoho-share
543. zoho-meeting
544. zoho-db
545. tokbox
546. pna
547. mgcp
548. magicjack
549. lotus-notes-admin
550. jxta
551. ip-messenger
552. google-finance-posting

553. google-app-engine
554. filemaker-anouncement
555. egp
556. camo-proxy
557. bypassthat
558. bomberclone
559. altiris
560. zoho-people
561. zoho-notebook
562. x-font-server
563. webqq
564. vsee
565. vmtp
566. ventrilo
567. trinoo
568. t-online-mail
569. tacacs
570. spark-im
571. sharepoint-wiki
572. ruckus
573. rstatd
574. private-enc
575. pingfu
576. msn2go
577. modbus
578. meetro
579. laconica
580. ipv6-icmp
581. howardforums-posting
582. hamachi
583. gyao
584. gmx-mail
585. fluxiom
586. dnp3
587. cvsup
588. zwiki-editing
589. xtp
590. xns-idp
591. wlccp
592. wikidot-editing
593. war-rock
594. viadeo
595. vakaka
596. tvtonic
597. trunk-1
598. trendmicro-earthagent
599. surrogafier
600. sun-nd
601. spirent
602. socialtext-editing
603. snp
604. secure-access-sync
605. rusers
606. r-services
607. r-exec
608. reliable-data
609. rediffbol-audio-video
610. rediffbol
611. realtunnel
612. pup
613. psiphon
614. privax
615. pnni
616. pipe
617. openft
618. nimbuzz
619. narp
620. ms-frs
621. motleyfool-posting
622. moinmoin-editing
623. mekusharim
624. lifecam
625. lan
626. iso-ip
627. ipsec-ah
628. ipcomp
629. instan-t-webmessenger
630. i-nlsp
631. ibackup
632. httport
633. ghostsurf
634. gbridge
635. firephoenix
636. fc2-blog-posting
637. evony
638. etherip
639. emcon
640. drda
641. desktoptwo
642. dameware-mini-remote
643. clarizen
644. cbt
645. campfire
646. bgp
647. beinsync
648. backpack-editing
649. ariel
650. ameba-blog-posting
651. activesync