The Application Usage and Risk Report

End User Application Trends in the Enterprise - Country Specific Findings

December 2011

Palo Alto Networks
3300 Olcott Street
Santa Clara, CA 95054
www.paloaltonetworks.com

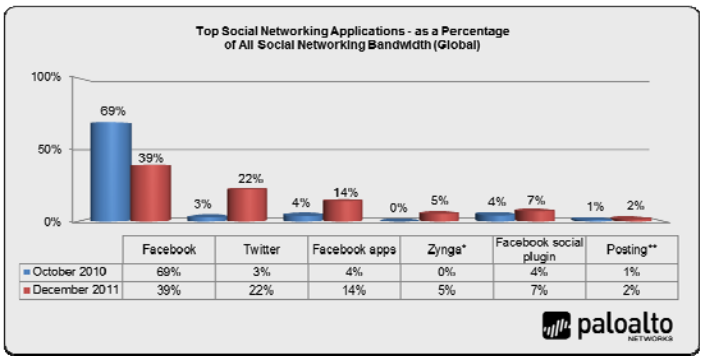
Table of Contents

Executive Summary

The *Application Usage and Risk Report (8th Edition, December 2011)* from Palo Alto Networks provides a global view into enterprise application usage by summarizing network traffic assessments conducted in 1,636 organizations worldwide between April 2011 and November 2011. The key findings and observations both globally and by specific countries are outlined below. To view the global findings, please download the *Application Usage and Risk Report (8th Edition, December 2011)* here.

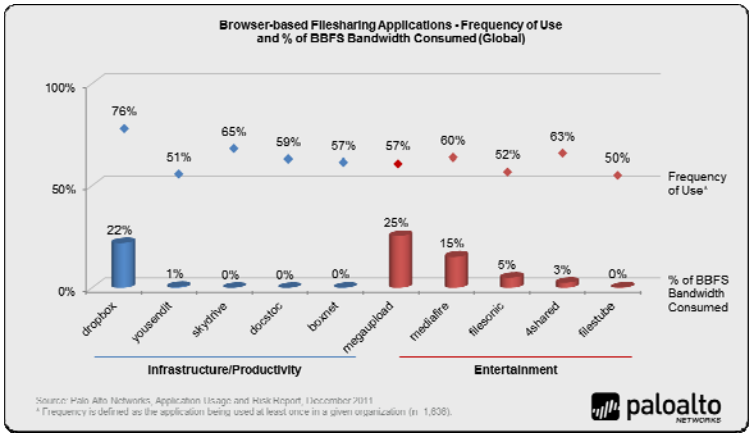
Social networking usage becomes more active.

- Active usage of social networking applications (Facebook-apps, games, social-plugins and posting) more than tripled, going from a cumulative 9% (October 2010) to 28% (December 2011) when measured as a percentage of total social networking bandwidth.



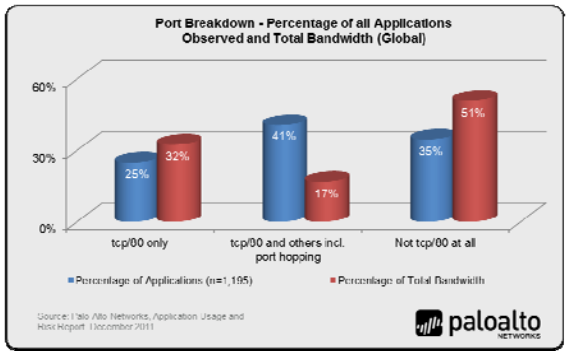
Browser-based filesharing use cases: work vs. entertainment.

- With 65 different browser-based filesharing variants found and an average of 13 being used in each of the participating organizations, two clear use cases are emerging within the browser-based filesharing market: work and entertainment. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. The analysis shows that 51% of the bandwidth consumed by 35% of the applications do not use tcp/80. In contrast, the 297 applications that use only tcp/80, and no other port by default, represent a mere 25% of the applications and 32% of the bandwidth observed.

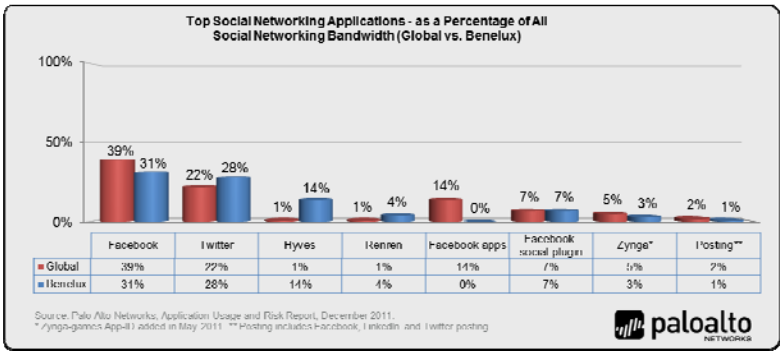


Country Specific Findings – Europe

Benelux (Belgium, Luxembourg, Netherlands)

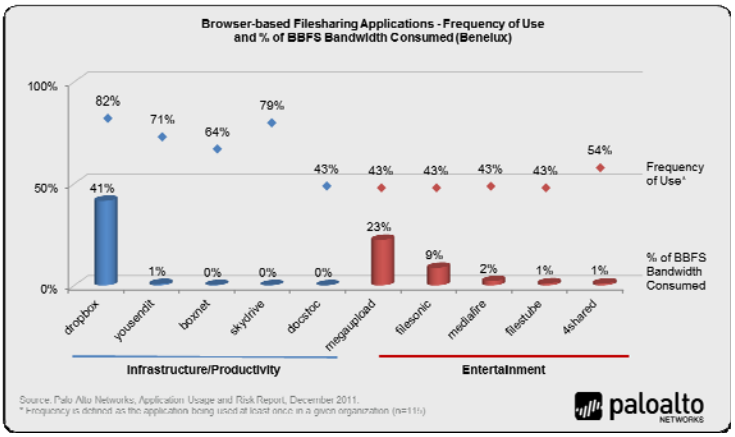
The Benelux sample encompassed 115 organizations with 973 applications detected. Key findings include:

Social networking usage becomes more active.



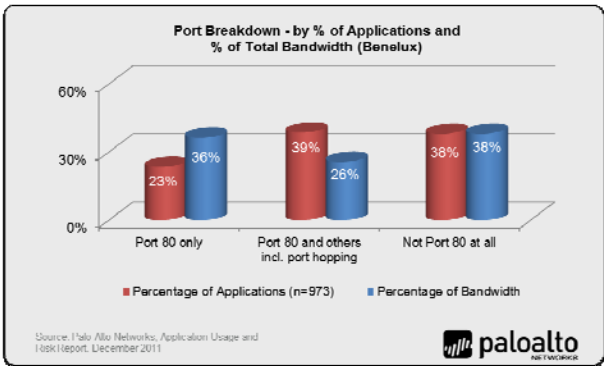
- Active social networking application (games, plugins, posting) usage is similar to global usage patterns. Hyves holds its own against most heavily used Facebook and Twitter. Interestingly, Renren, a Chinese social networking application appears at 4% - which is somewhat odd. A total of 62 different social networking applications were found in 99% of the participating organizations. An average of 14 were found on each network.

Browser-based filesharing use cases: work vs. entertainment.



- There were 52 different browser-based filesharing applications found across 96% of the 115 organizations observed in Benelux. Each organization had an average of 10 different variants on their network with Dropbox and Megaupload most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.

Securing port 80 is not securing the network.



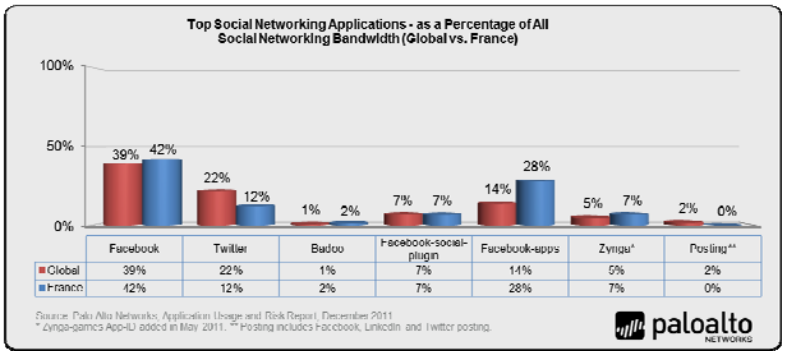
- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 973 applications found, 38% (370) of the applications do not use port 80 at all and those applications are consuming 38% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

France

The French sample encompassed 85 organizations with 867 applications detected. Key findings include:

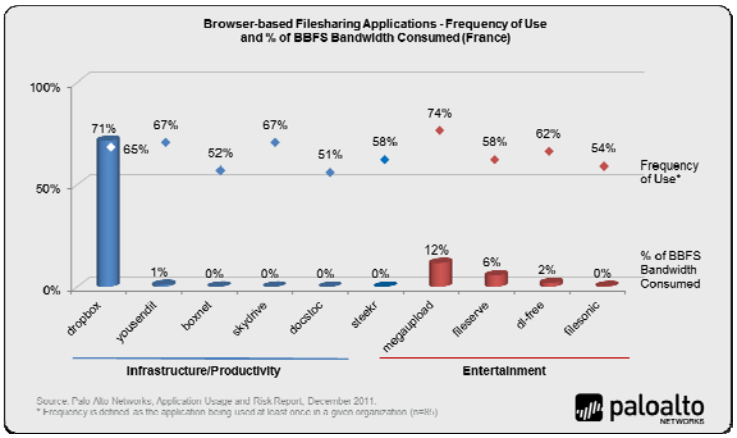
Social networking usage becomes more active.

- Social networking games and plugins are used more heavily in France than they are globally Facebook is a clear dominant player with 39% of the bandwidth consumed. On average, 16 social networking applications per organization were found across 98% of the organizations observed. In total, 63 different social networking applications were found in France.



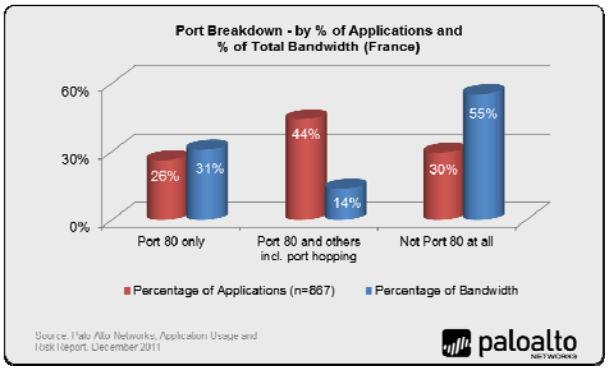
Browser-based filesharing use cases: work vs. entertainment.

- There were 54 different browser-based filesharing applications found across 94% of the 85 organizations observed in France. Each organization had an average of 15 different variants on their network with Dropbox being most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of the 867 applications found, 30% of them do not use port 80 at all and those applications are consuming 55% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

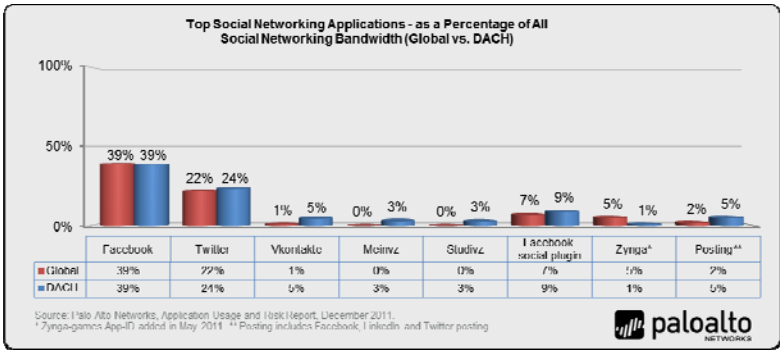


DACH (Germany, Switzerland and Austria)

The sample in DACH encompassed 62 organizations with 833 applications detected. Key findings include:

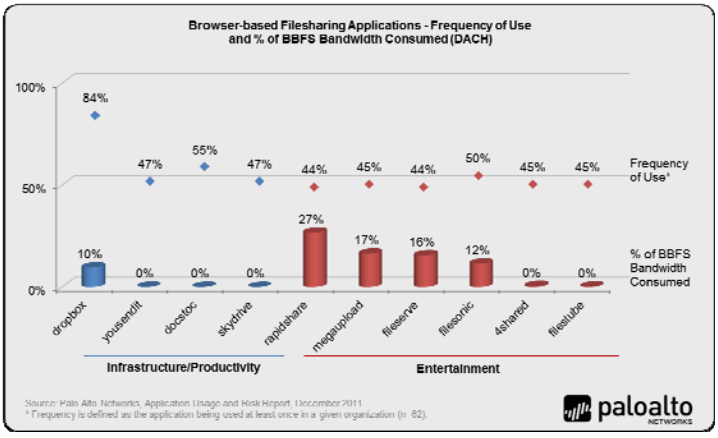
Social networking usage becomes more active.

- Several local social networking applications are in use while active social networking applications (games, posting, plugins, apps) usage is similar to the global usage patterns. on average, 19 social networking applications per organization were found across 97% of the 62 DACH organizations observed. A total of 62 social networking applications were found.



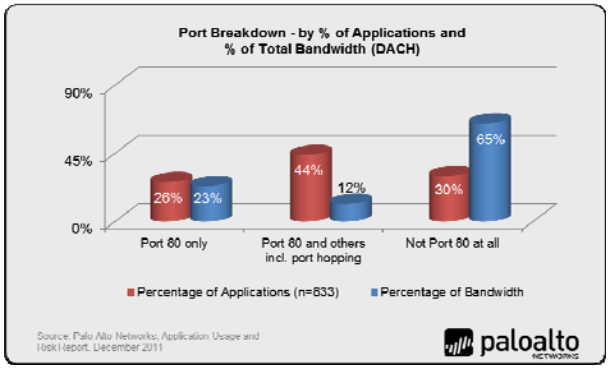
Browser-based filesharing use cases: work vs. entertainment.

- There were 48 different browser-based filesharing applications found across 90% of the 62 organizations observed. Each organization had an average of 13 different variants on their network with Rapidshare being used most heavily. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 833 applications found in the 62 organizations observed, 30% of them do not use port 80 at all and those applications are consuming 65% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

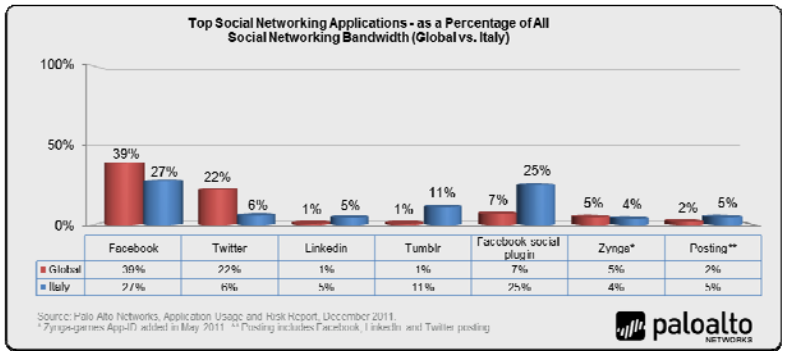


Italy

The Italian sample encompassed 51 organizations with 725 applications detected. Key findings include:

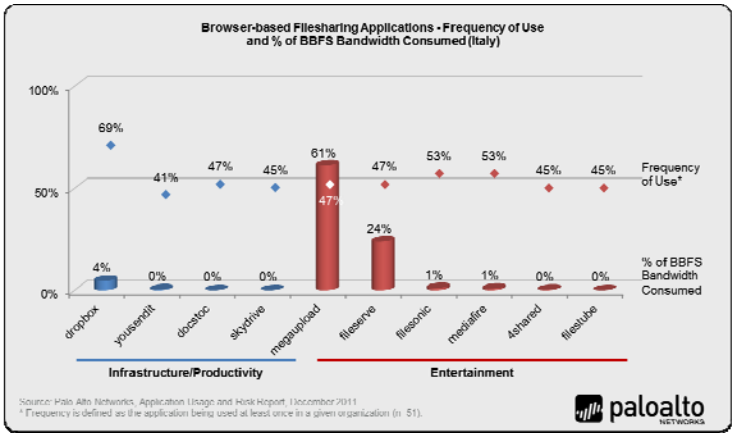
Social networking usage becomes more active.

- In Italy, Facebook social plugins consumed 25% of the bandwidth - nearly as much as Facebook itself (24%) while Twitter consumed a mere 6% of the overall social networking bandwidth. An average of 13 social networking applications per organization were found across 96% of the 51 Italian organizations observed. In total, 53 variants were found.



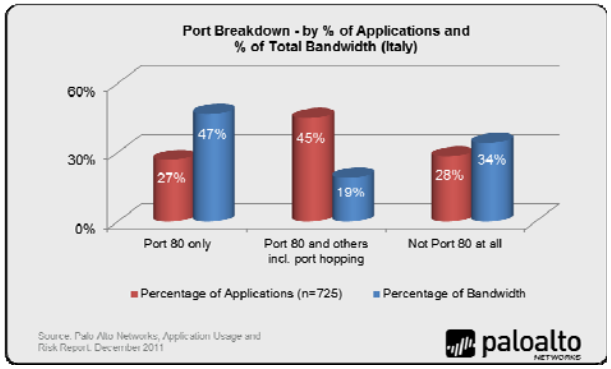
Browser-based filesharing use cases: work vs. entertainment.

- There were 44 different browser-based filesharing applications found across 90% of the 51 organizations observed. Each organization had an average of 13 different variants on their network with Megaupload being used most heavily. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

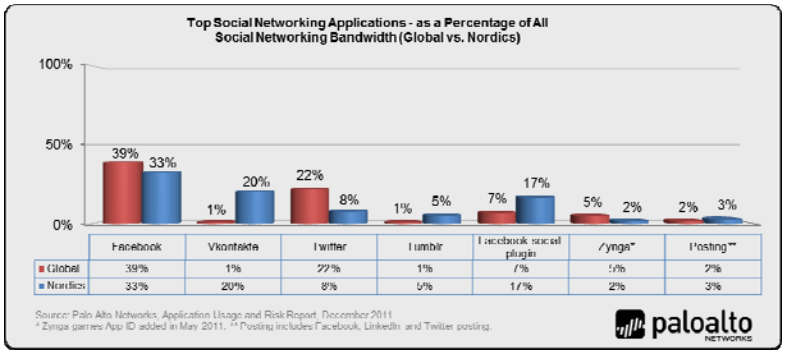
- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 725 applications observed, 28% of them do not use port 80 at all and those applications are consuming 34% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.



Nordics (Denmark, Finland, Norway, Sweden)

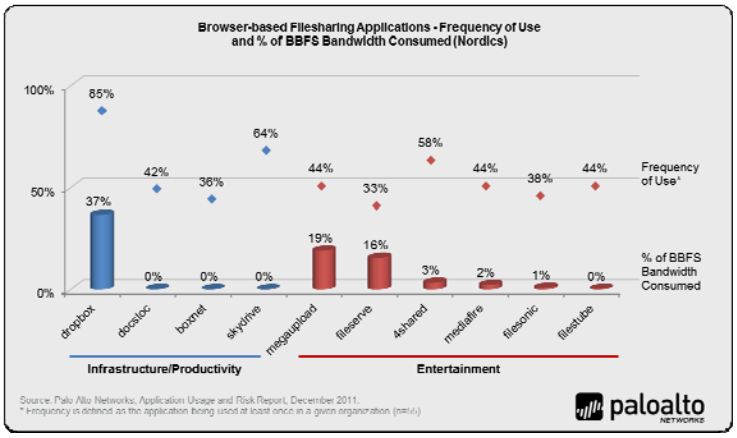
The Nordics sample encompassed 55 organizations with 785 applications detected. Key findings include:

Social networking usage becomes more active.



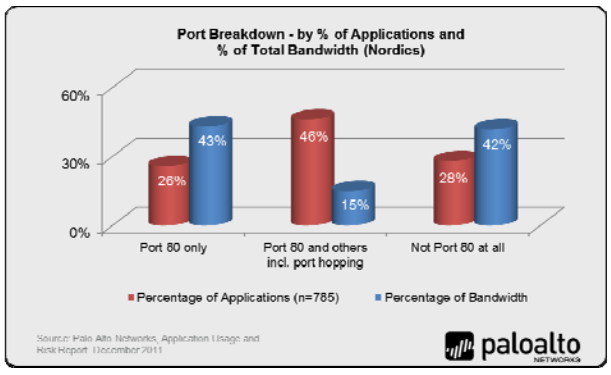
- Interestingly, Vkontakte, originally a Russian only site, now in 67 languages, consumed 20% of the bandwidth while Twitter consumed only 8%. Part of the bandwidth consumption may be related Vkontakte's integration with filesharing torrents. On average, 15 social networking applications per organization were found across 87% of the 55 organizations observed in the Nordics. A total of 63 different social networking applications were found.

Browser-based filesharing use cases: work vs. entertainment.



- There were 42 different browser-based filesharing applications found across 78% of the 55 organizations observed. Each organization had an average of 10 different variants on their network with Dropbox and Megaupload being most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.

Securing port 80 is not securing the network.



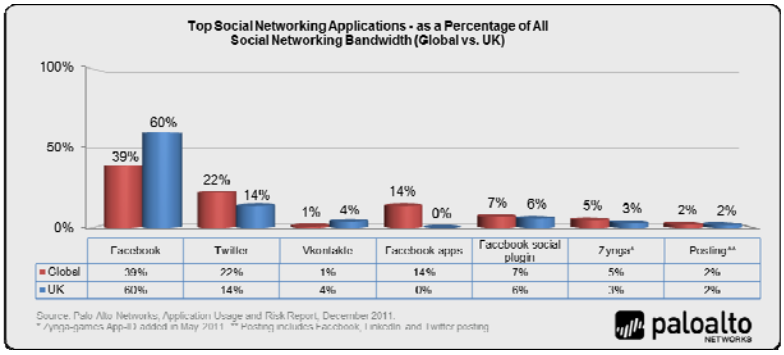
- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 935 applications found, 28% of them do not use port 80 at all and those applications are consuming 42% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

UK

The UK sample encompassed 70 organizations with 812 applications detected. Key findings include:

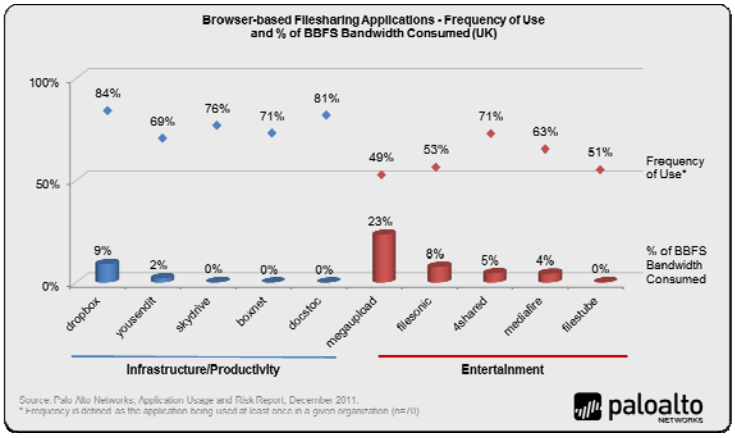
Social networking usage becomes more active.

- In the UK, active social networking applications (games, posting, plugins, apps) usage patterns are similar to those seen globally. On average, 17 social networking applications per organization were found across 100% of the 70 organizations observed. A total of 68 different social networking applications were found.



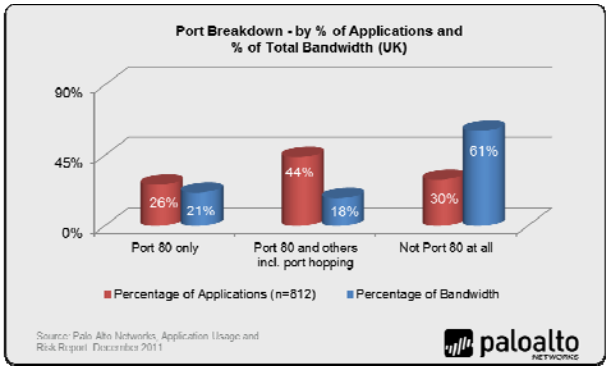
Browser-based filesharing use cases: work vs. entertainment.

- There were 42 different browser-based filesharing applications found across 96% of the organizations observed. Each organization had an average of 13 different variants on their network with Dropbox being most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

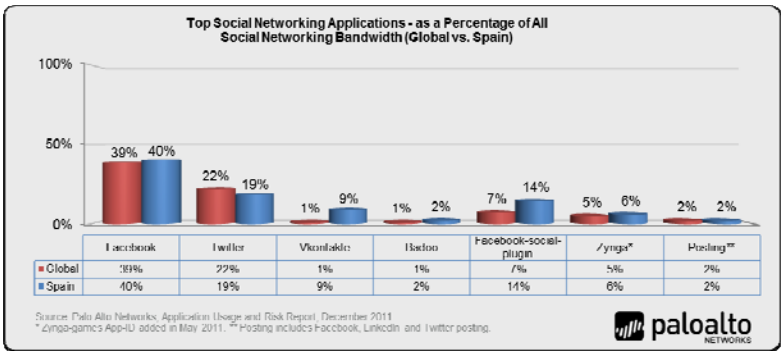
- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 812 applications found, 30% of them do not use port 80 at all and those 214 applications are consuming 61% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.



Spain

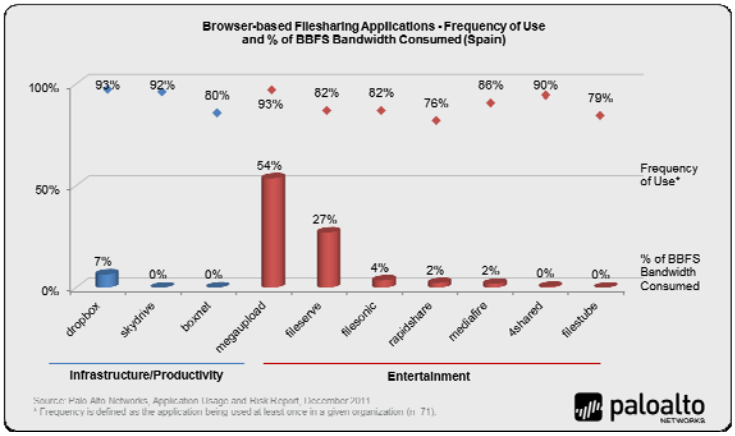
The sample in Spain encompassed 71 organizations with 935 applications detected. Key findings include:

Social networking usage becomes more active.



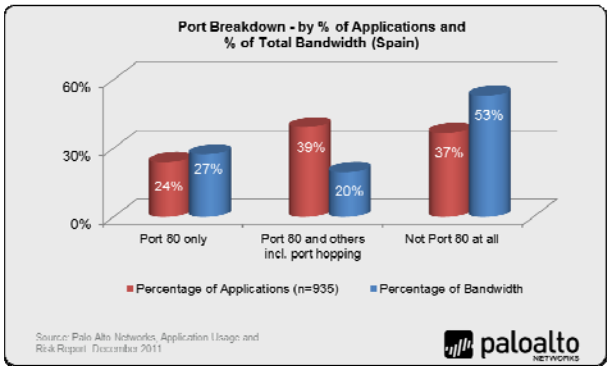
- In Spain, active social networking applications (games, posting, plugins, apps) are used a bit more heavily when compared to the global usage patterns. On average, 21 social networking applications per organization were found across 99% of the 71 organizations observed. A total of 63 different social networking applications were found.

Browser-based filesharing use cases: work vs. entertainment.



- There were 48 different browser-based filesharing applications found across 96% of the organizations observed. Each organization had an average of 21 different variants on their network with Megaupload being most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.

Securing port 80 is not securing the network.

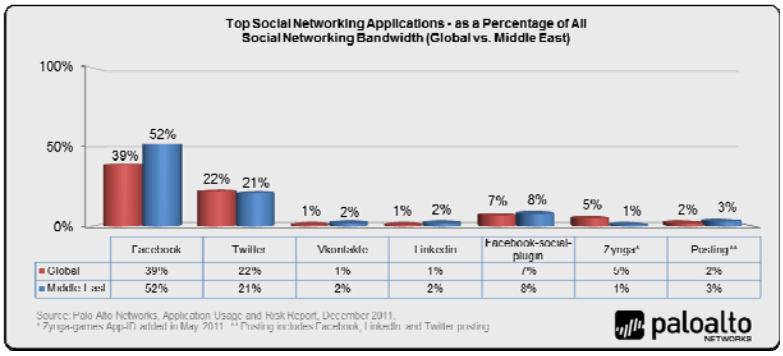


- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 935 applications found in the 71 organizations observed, 37% of them do not use port 80 at all and those applications are consuming 53% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

Middle East (Jordan, Kuwait, Oman, Qatar, Saudi Arabia, UAE)

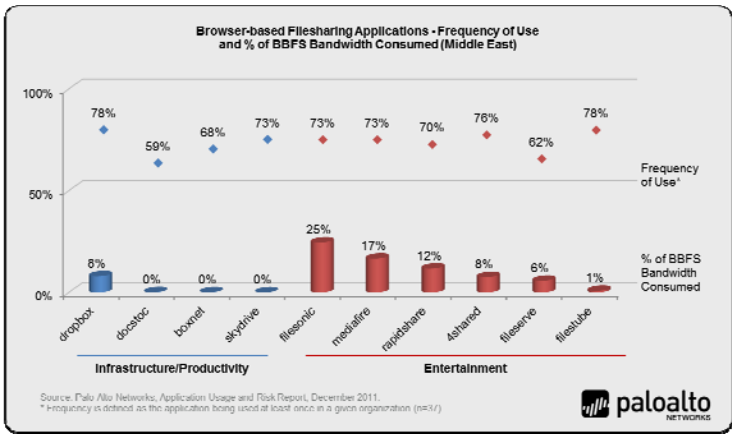
The sample in the middle east encompassed 37 organizations with 674 applications detected. Key findings include:

Social networking usage becomes more active.



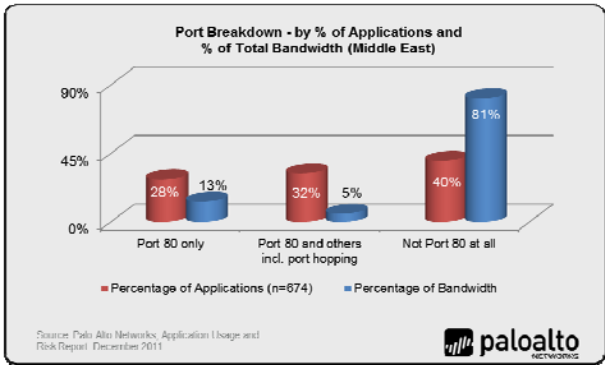
- Active social networking applications (games, posting, plugins, apps) are used a bit more heavily when compared to the global view. Facebook is a clear dominant player with 52% of bandwidth consumed. On average, 19 social networking applications per organization were found across 97% of the 37 organizations observed. A total of 55 different social networking applications were found.

Browser-based filesharing use cases: work vs. entertainment.



- There were 46 different browser-based filesharing applications found across 95% of the organizations observed. Each organization had an average of 18 different variants on their network with Filesonic being most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.

Securing port 80 is not securing the network.



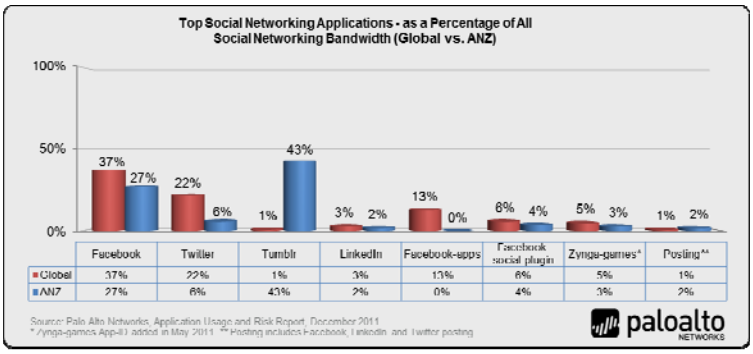
- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 674 applications, 40% of them do not use port 80 at all and those applications are consuming 81% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

Country Specific Findings – APAC

ANZ (Australia and New Zealand)

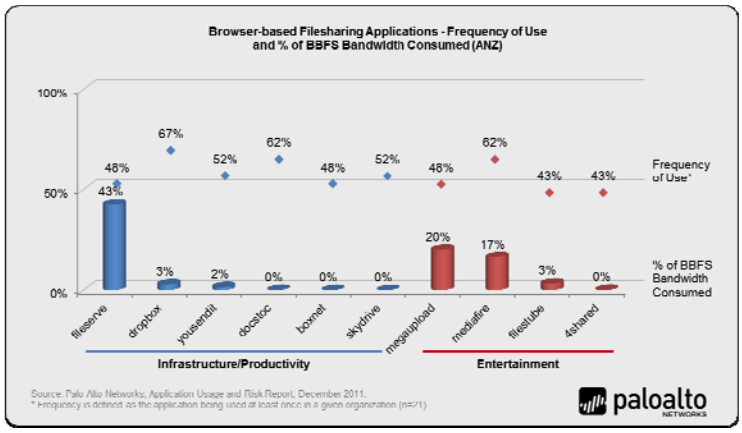
The ANZ sample encompassed 21 organizations with 566 applications. Key findings include:

Social networking usage becomes more active.



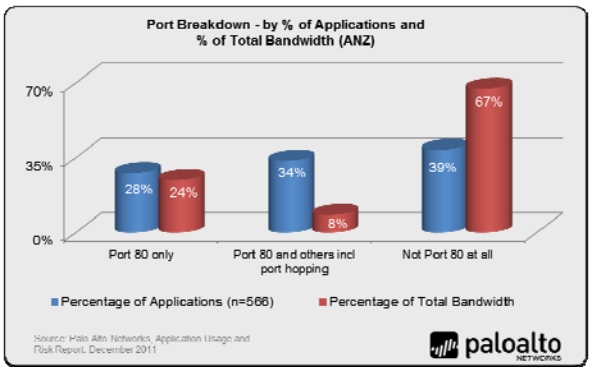
- Tumblr, a micro-blogging site based in NY city was used more heavily than any other social networking application. ANZ is the only geography where Tumblr was used so heavily and it highlights the fact that where the application is developed has little bearing on where it is popular. An average of 20 social networking applications per organization (and a total of 48) were found.

Browser-based filesharing use cases: work vs. entertainment.



- There were 34 different browser-based filesharing applications found across 81% of the 21 organizations observed. Each organization had an average of 12 different variants on their network. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.

Securing port 80 is not securing the network.



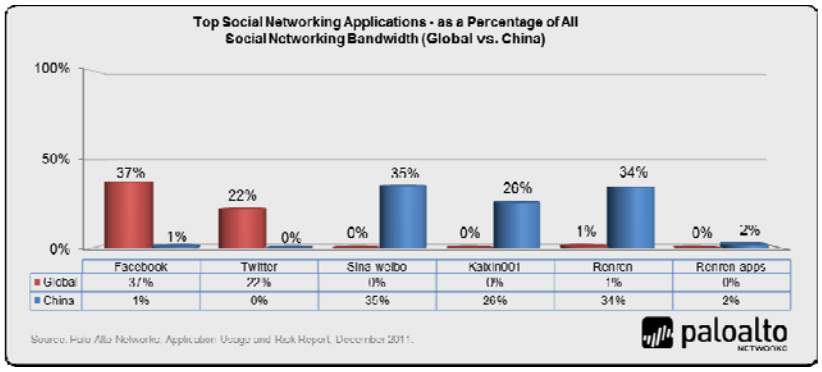
- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 566 applications found, 39% of them do not use port 80 at all and those 219 applications are consuming 67% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

China

The Chinese sample encompassed 18 organizations with 535 applications detected. Key findings include:

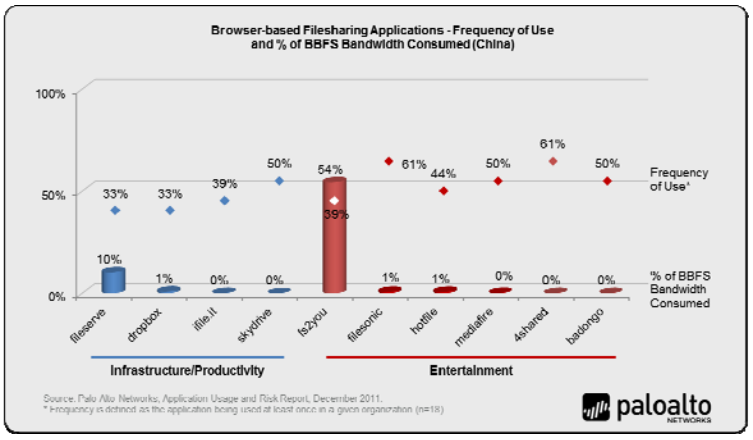
Social networking usage becomes more active.

- Localized social networking sites are more popular and are used more heavily than others. A total of 48 different social networking applications were found across 94% of the 18 organizations observed with an average of seven detected on each network (the lowest out of all geographies observed).



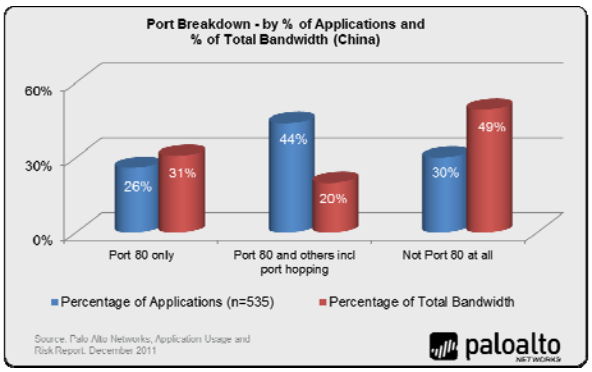
Browser-based filesharing use cases: work vs. entertainment.

- There were 30 different browser-based filesharing applications found across 89% of the organizations observed. Each organization had an average of eight different variants on their network with fs2you the most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of the 535 applications found in the 18 Chinese organizations observed, 30% of them do not use port 80 at all and those 161 applications are consuming 49% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

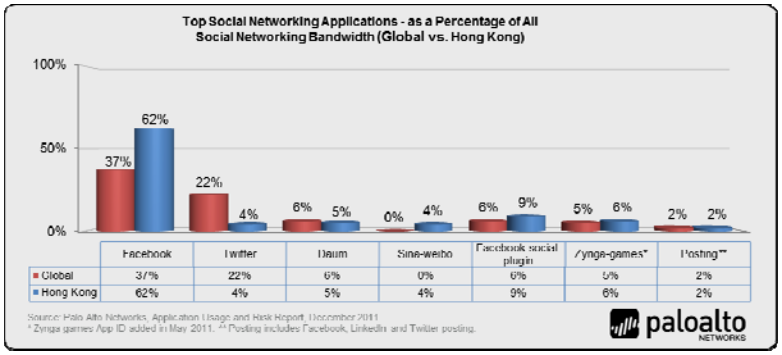


Hong Kong

The Hong Kong sample encompassed 46 organizations with 734 applications detected. Key findings include:

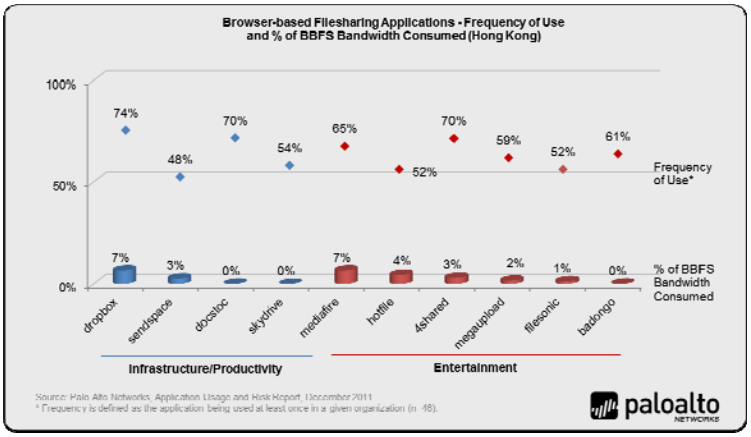
Social networking usage becomes more active.

- While Facebook dominates, some of the action oriented applications, (apps, plugins, games, posting) are used more heavily in Hong Kong than they are globally. On average, 14 social networking applications per organization were found across 98% of the 46 organizations observed. A total of 63 different social networking applications were found.



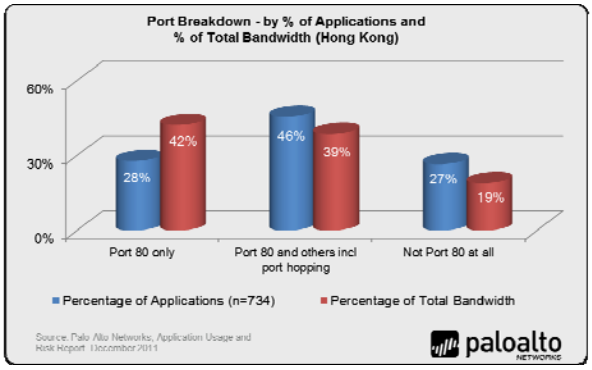
Browser-based filesharing use cases: work vs. entertainment.

- There were 41 different browser-based filesharing applications found across 100% of the organizations observed. Each organization had an average of 12 different variants on their network. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of 734 applications, 27% of them do not use port 80 at all and those 195 applications are consuming 19% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

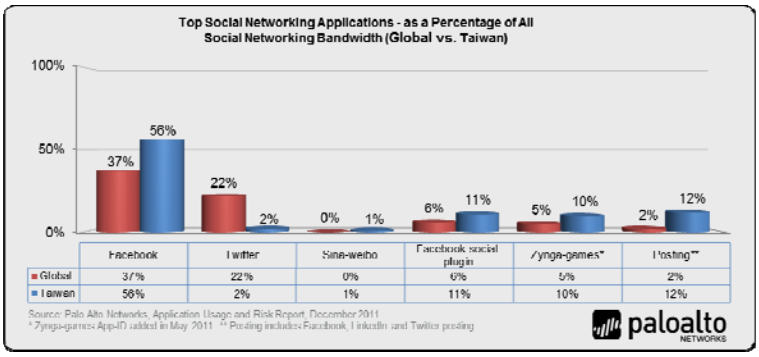


Taiwan

The Taiwan sample encompassed 148 organizations with 898 applications detected. Key findings include:

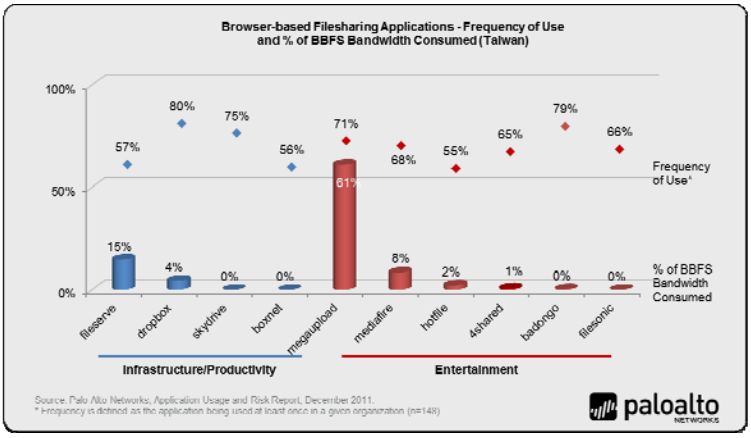
Social networking usage becomes more active.

- While Facebook dominates, the action oriented uses (apps, games, posting, and plugin) are all used more heavily in Taiwan then they are globally. An average of 12 social networking applications per organization (and a total of 61) were found across 99% of the 148 Taiwan organizations observed.



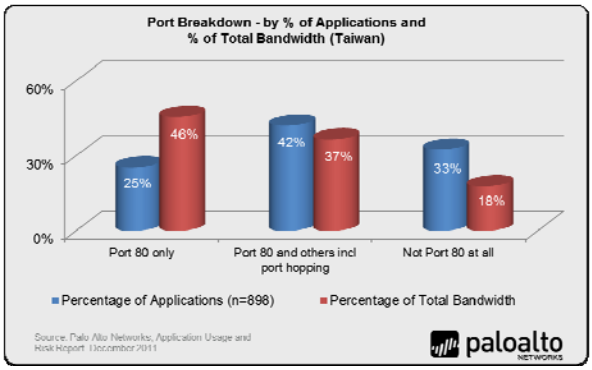
Browser-based filesharing use cases: work vs. entertainment.

- There were 53 different browser-based filesharing applications found across 97% of the organizations observed. Each organization had an average of 15 different variants on their network with Megaupload used most heavily. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of 898 applications found, 33% of them do not use port 80 at all and those 292 applications are consuming 18% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

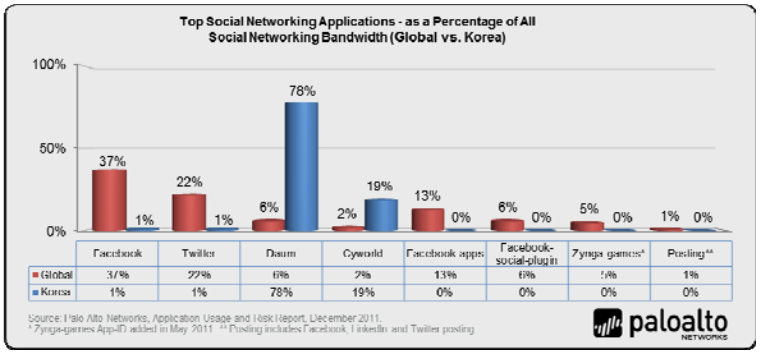


Korea

The Korean sample encompassed 35 organizations with 707 applications detected. Key findings include:

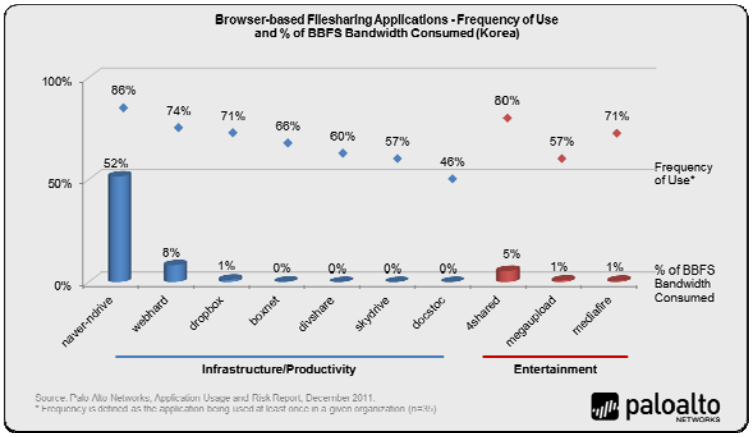
Social networking usage becomes more active.

- While Facebook dominates elsewhere, Daum and Cyworld both are used more heavily in Korea than anywhere else. An average of 20 social networking applications per organization (and a total of 57) were found across 96% of the organizations observed.



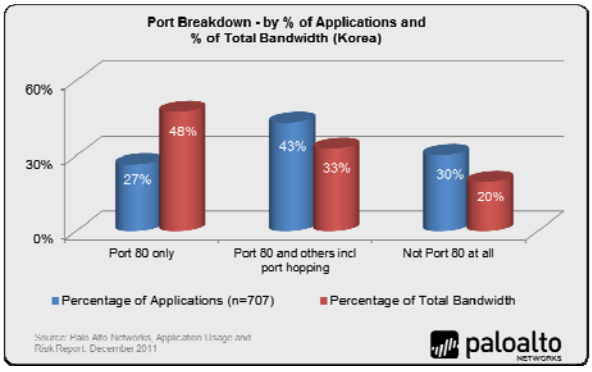
Browser-based filesharing use cases: work vs. entertainment.

- There were 55 different browser-based filesharing applications found across 86% of the organizations observed. Each organization had an average of 18 different variants on their network with Naver-ndrive used most heavily. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of the 707 applications found, 30% of them do not use port 80 at all and those 214 applications are consuming 20% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

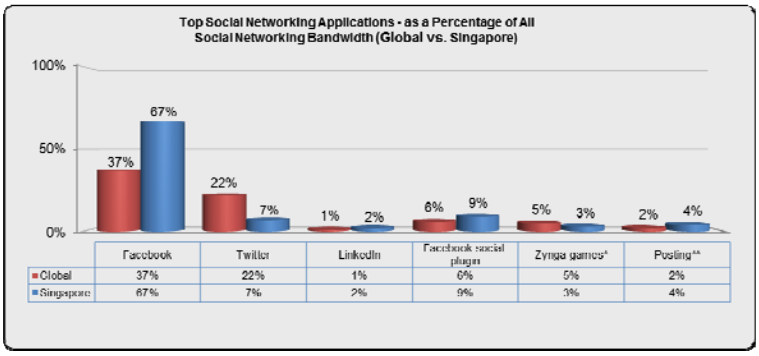


Singapore

The Singapore sample encompassed 65 organizations with 775 applications detected. Key findings include:

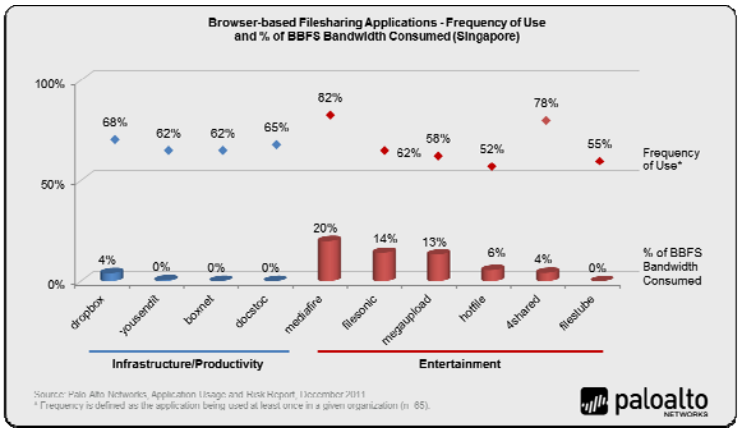
Social networking usage becomes more active.

- While Facebook dominates elsewhere, the action oriented uses (apps, games, posting, and plugin) are all used more heavily in Singapore then they are globally. An average of 16 social networking applications (and 64 in total) were found on 97% of the 65 participating organizations.



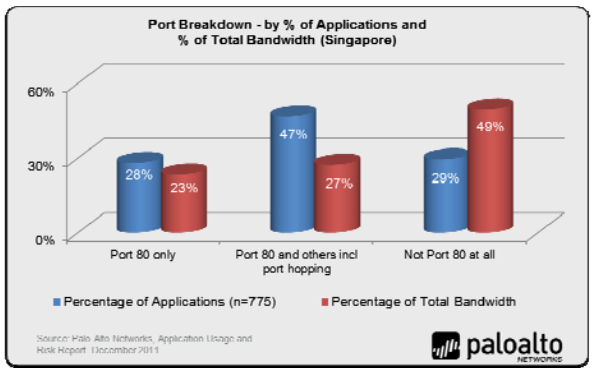
Browser-based filesharing use cases: work vs. entertainment.

- There were 47 different browser-based filesharing applications found across 92% of the organizations observed. Each organization had an average of 18 different variants on their network. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 775 applications found, 29% of them do not use port 80 at all and those 216 applications are consuming 49% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

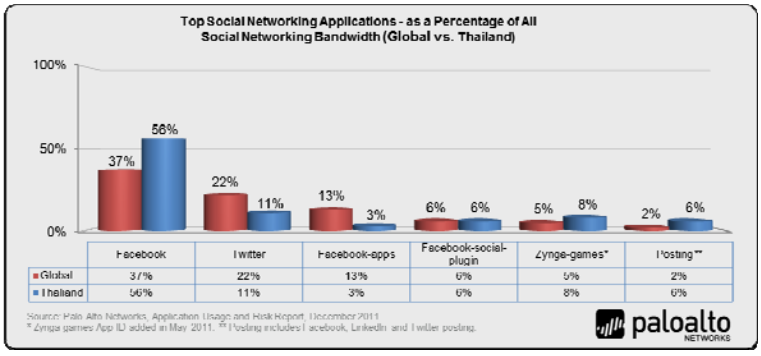


Thailand

The Thai sample encompassed 75 organizations with 759 applications detected. Key findings include:

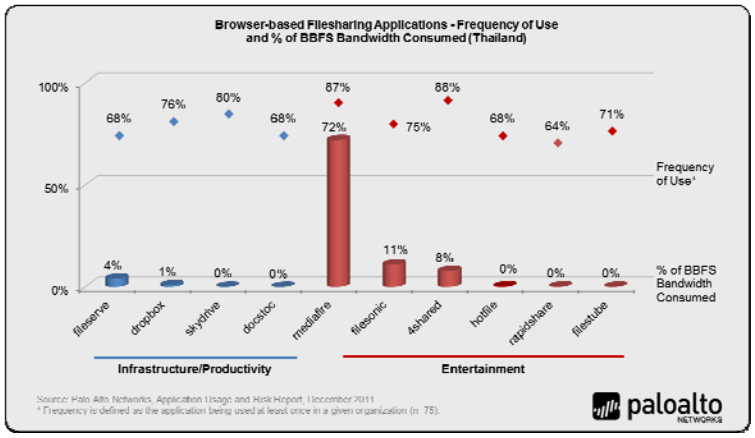
Social networking usage becomes more active.

- Facebook is consuming the most bandwidth but games and posting are all used more heavily in Thailand then than they are globally. On average, 16 social networking applications per organization (and 60 in total) were found across 97% of the 75 organizations observed.



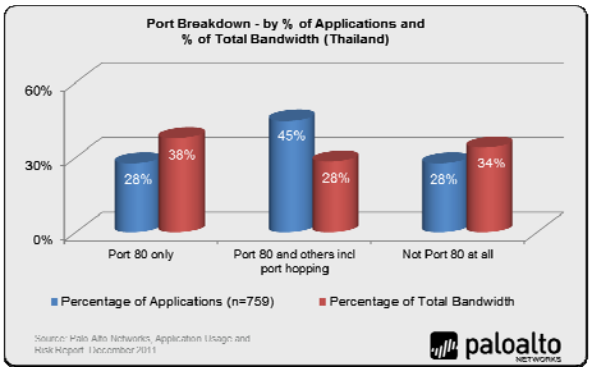
Browser-based filesharing use cases: work vs. entertainment.

- There were 48 different browser-based filesharing applications found across 95% of the organizations observed. Each organization had an average of 16 different variants on their network with Mediafire being the most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of the 759 applications observed in the analysis for Thailand, 28% of the applications do not use port 80 at all and those 210 applications are consuming 34% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

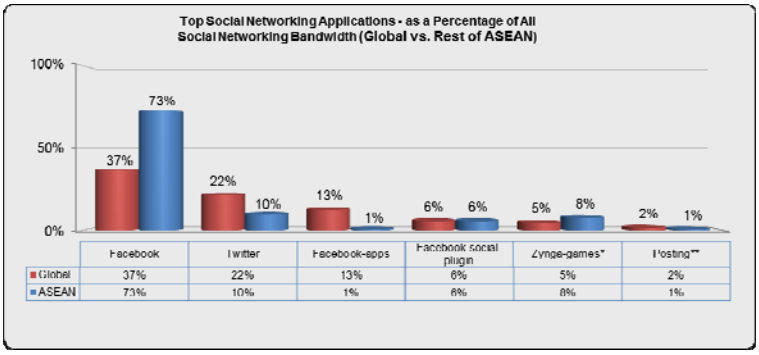


Rest of ASEAN (Malaysia, Indonesia, Philippines, Vietnam)

The rest of ASEAN sample encompassed 23 organizations with 657 applications detected. Key findings include:

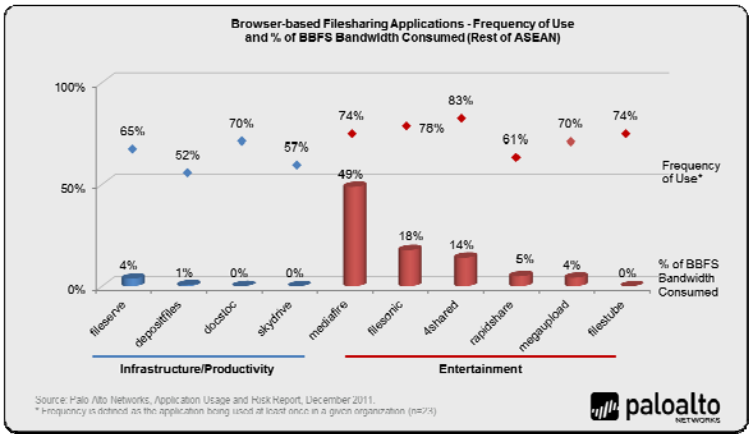
Social networking usage becomes more active.

- Facebook is consuming the most bandwidth, but some of the action oriented uses, mainly Zynga games, are used more heavily in ASEAN than they are globally. On average, 20 social networking applications (and 50 in total) were found across 83% of the organizations observed.



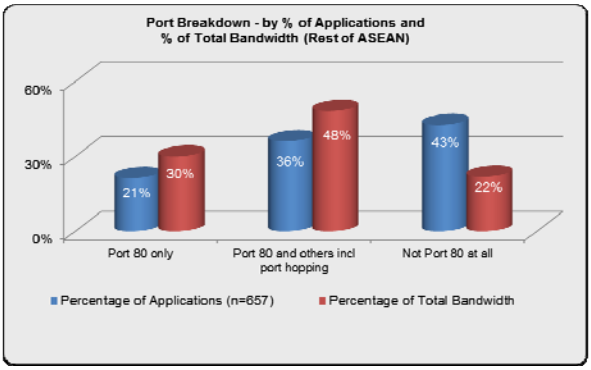
Browser-based filesharing use cases: work vs. entertainment.

- There were 32 different browser-based filesharing applications found across 83% of the organizations observed. Each organization had an average of 18 different variants on their network with Mediafire being the most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of 657 applications found in the organizations observed, 43% of the applications do not use port 80 at all and those 280 applications are consuming 22% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

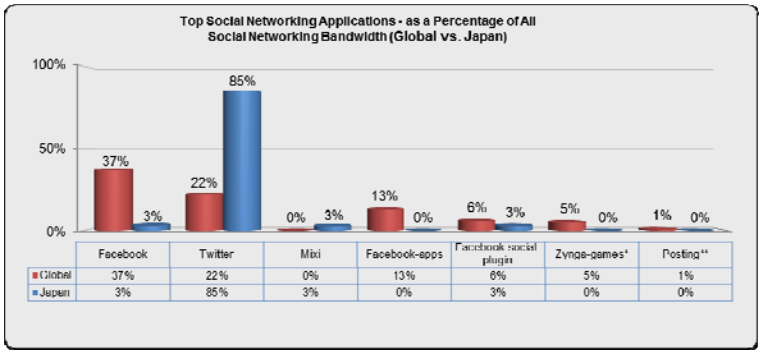


Country Specific Findings – Japan

The Japanese sample encompassed 89 organizations with 923 applications detected. Key findings include:

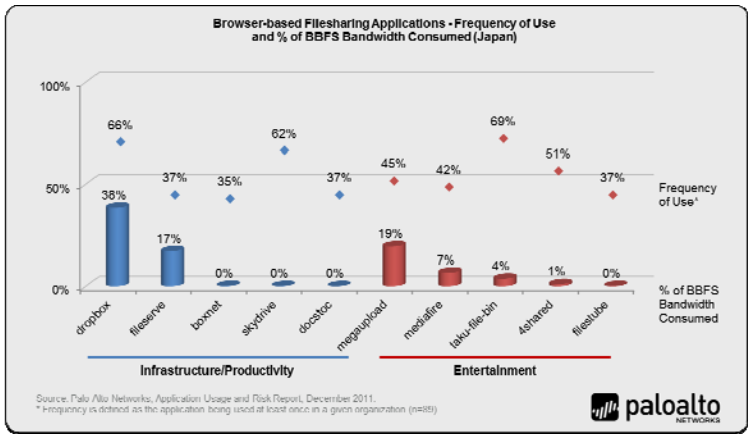
Social networking usage becomes more active.

- Twitter usage is consuming 85% of the social networking bandwidth, leaving only 15% for the other 71 social networking applications. How will they all survive? On average, 91% of the 89 Japanese organizations had 15 different social networking applications in use.



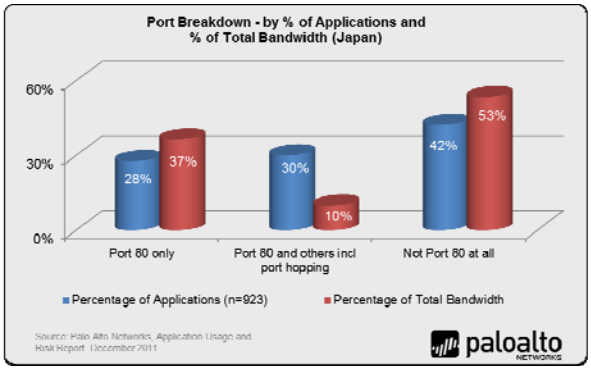
Browser-based filesharing use cases: work vs. entertainment.

- There were 65 different browser-based filesharing applications found across 89% of the organizations observed. An average of 12 browser-based filesharing applications were found each participating organizations with Dropbox being the most heavily used. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. In fact, out of 923 applications found, 42% of them do not use port 80 at all and those 390 applications are consuming 53% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.



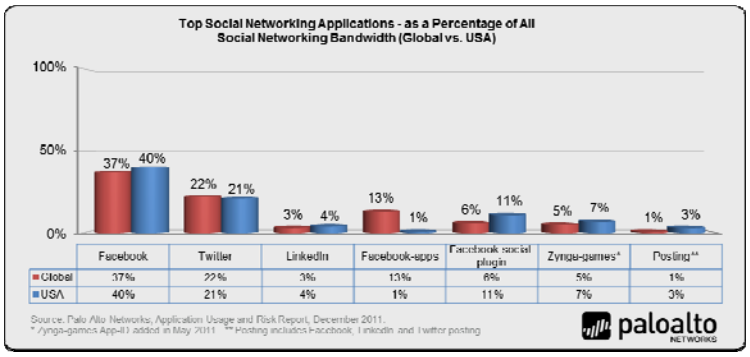
Country Specific Findings – North America

USA

The USA sample size encompassed 395 organizations with 1,121 applications detected. Key findings include:

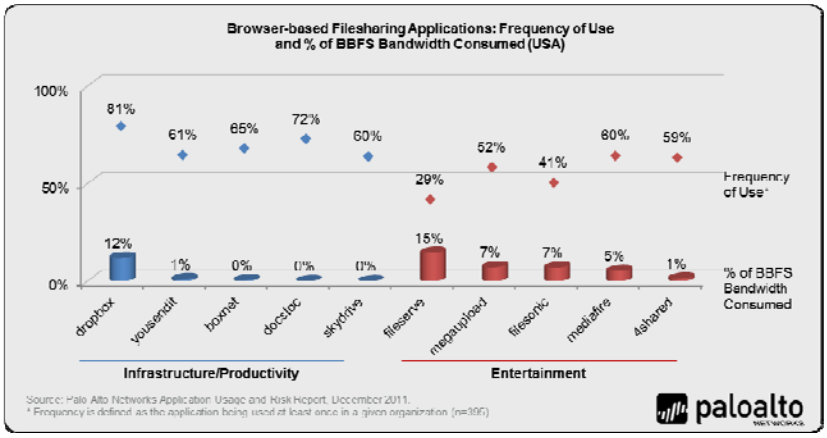
Social networking usage becomes more active.

- Action-oriented social networking applications (games, plugins, posting) are used more heavily in the USA than they are globally. There were 69 different social networking applications found across 96% of the 395 organizations. On average, there were 15 different social networking applications in use.



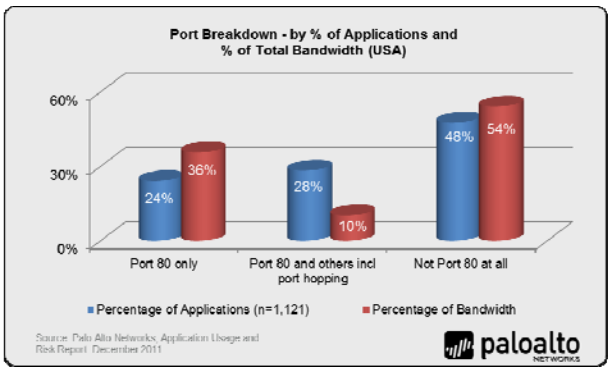
Browser-based filesharing use cases: work vs. entertainment.

- There were 55 different browser-based filesharing applications found with across 95% of the organizations observed and an average of 11 were found on each network. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of 1,121 applications found, 48% of them do not use port 80 at all and those 534 applications are consuming 54% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.

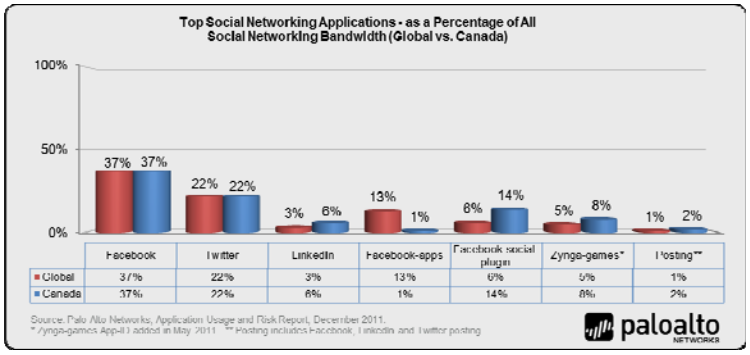


Canada

The Canadian sample encompassed 49 organizations with 703 applications detected.

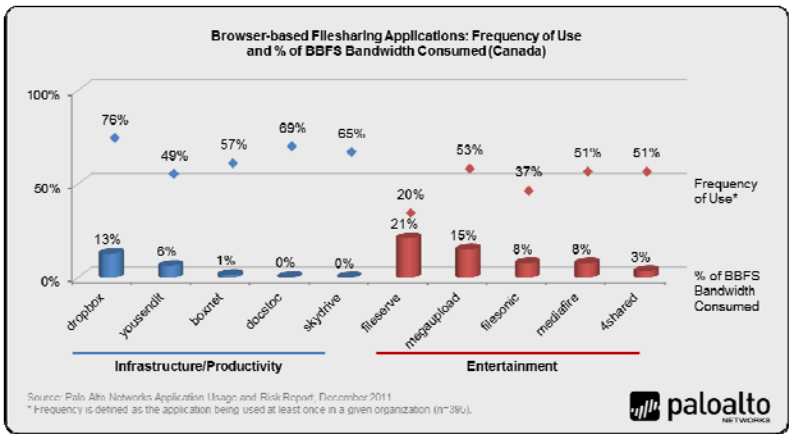
Social networking usage becomes more active.

- In Canada, active social networking applications (games, plugins, posting) are used more heavily than they are globally. There were 58 different social networking applications found with an average of 15 detected on 94% of the 49 participating organizations.



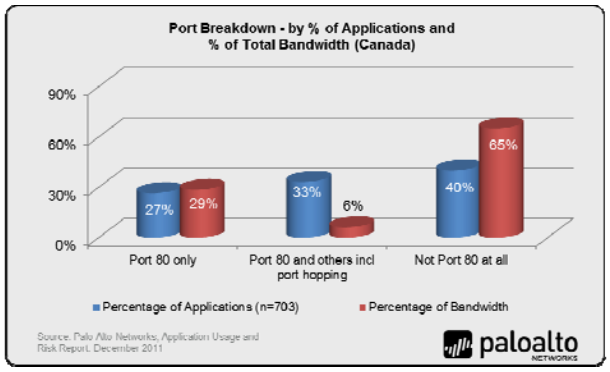
Browser-based filesharing use cases: work vs. entertainment.

- There were 36 different browser-based filesharing applications found across 94% of the organizations observed and an average of 10 were found on each network. Regardless of how they are used, the risks associated with browser-based filesharing applications are significant; they are an unchecked set of applications flowing across most firewalls – using tcp/80, sometimes SSL and others hopping ports.



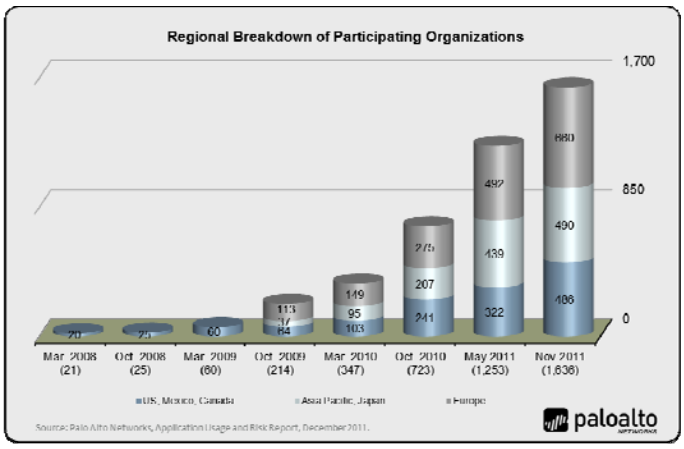
Securing port 80 is not securing the network.

- Conventional wisdom suggests that most of an organization's traffic is going through tcp/80. Out of the 703 applications found in the Canadian organizations observed, 40% of them do not use port 80 at all and those 282 applications are consuming 65% of the bandwidth. A focus on tcp/80 is a security requirement, without a doubt, but too much focus may introduce significant risks.



Appendix 1: Demographics and Methodology

The data in this report is generated from 1,636 traffic assessments 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 enterprise directory services (Microsoft Active Directory, LDAP, eDirectory) 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, eDirectory, LDAP or a range of terminal services solutions. 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 20 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 than1,400 applications currently identified by Palo Alto Networks, including their characteristics and the underlying technology in use, please visit Applipedia, the Palo Alto Networks encyclopedia of applications

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its next-generation firewalls enable unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 20Gbps 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. Most recently, Palo Alto Networks has enabled enterprises to extend this same network security to remote users with the release of GlobalProtect™ and to combat targeted malware with its WildFire™ service. For more information, visit www.paloaltonetworks.com.