The Application Usage and Risk Report

An Analysis of End User Application Trends in the Enterprise

Spring 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 (Spring Edition, 2009), from Palo Alto Networks provides a view into enterprise application usage by summarizing application traffic assessments from more than 60 large organizations across financial services, manufacturing, healthcare, government, retail and education. The assessments were conducted between August 2008 and December 2008, representing the behavior of nearly 900,000 users. The report supports the position that application controls within enterprises are failing. Applications have standard features to evade controls automatically, employees use applications to evade control mechanisms purposefully, and most current control mechanisms are ill-equipped to regain visibility and control.

Applications are designed for accessibility.

- More than half (57%) of the 494 applications found can bypass security infrastructure – hopping from port to port, using port 80 or port 443. Some examples of these applications include Microsoft SharePoint, Microsoft Groove and a host of software update services (Microsoft Update, Apple Update, Adobe Update), along with end-user applications such as Pandora and Yoics!

Applications that enable users to circumvent security controls are common.

- Proxies that are typically not endorsed by corporate IT (CGIProxy, PHProxy, Hopster) and remote desktop access applications (LogMeIn!, RDP, PCAnywhere) were found 81% and 95% of time, respectively. Encrypted tunnel applications such as SSH, TOR, GPass, Gbridge, and SwIPe were also found.

File sharing usage is rampant.

- P2P was found 92% of the time, with BitTorrent and Gnutella as the most common of 21 variants found. Browser-based file sharing was found 76% of the time with YouSendit! and MediaFire among the most common of the 22 variants.

Applications continue to consume bandwidth at a voracious rate.

- More than half (51%) of the bandwidth is being consumed by a little more than a quarter (28%) of the applications, most of which are consumer-oriented (media, social networking, P2P and browser-based file sharing, web-browsing and toolbars).

Enterprises are spending heavily to protect their networks – yet they cannot control the applications on the network.

- Collectively, enterprises spend more than $6 billion annually on firewall, IPS, proxy and URL filtering products. All of these products claim to perform some level of application control. The analysis showed that 100% of the organizations had firewalls and 87% **also** had one or more of these firewall helpers (a proxy, an IPS, URL filtering) – yet they were unable to exercise control over the application traffic traversing the network.

The data included in this analysis was generated from Palo Alto Networks next-generation firewalls that were deployed in the line of traffic for as long as a week, providing visibility into an average of 156 applications traversing each of the organization networks, with the highest number of applications detected at 305. The traditional tools that IT managers have at their disposal cannot see the applications traversing the network, or can see only a fraction of these applications. Applications themselves are designed to bypass the infrastructure tools, or employees actively bypass them using a range of applications. While blindly blocking all the applications is an unreasonable response, the risks that many of these applications represent are too significant to ignore.

INTRODUCTION

Regardless of the amount of money spent on firewalls, IPS's, proxies and URL filtering, employees are using their favorite applications whenever they want. Some of these applications make employees more productive, while others have absolutely no business value. Where the task of determining value becomes more difficult is when applications fall in between the two poles. There are some very clear delineations between those applications that enable business(Oracle, SharePoint, Exchange, etc) and those that do not enable the business (Xunlei, TOR, Hamachi, UltraSurf). An application such as Zoho Writer may allow an employee to finish a key document while MegaUpload will enable a non-technical user unfamiliar with FTP to transfer a large graphics file to a designer. Yet Zoho and MegaUpload introduce possible business risks (e.g., lack of compliance) and security risks (e.g., threat propagation) and as such, are not likely to be corporate-supported.

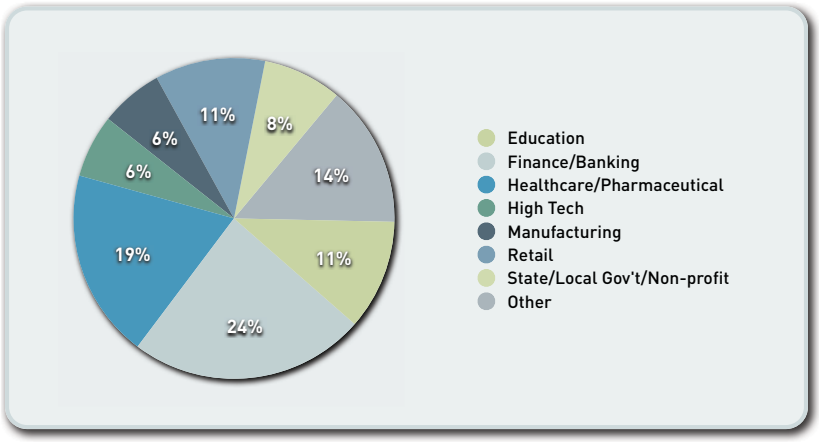


Figure 1: Demographic breakdown of the participating organizations.

The data analyzed in this report was generated using a Palo Alto Networks next-generation firewall deployed where it monitors the application traffic traversing the Internet gateway. Data is collected and analyzed with the organization receiving an in-depth report on the findings. For more information on the methodology, please review Appendix 2.

WHO CARES WHICH APPLICATIONS EMPLOYEES USE?

Everyone should care. The migration towards electronic storage of everything personal is well on its way. For example, many people have electronic versions of their tax returns on their hard drive. Not surprisingly, tax returns are a very commonly found document on P2P networks and it is unlikely that the user intentionally filed their return on the a P2P network.

The same can be said about health care records. A recent Computerworld article published in January of 2009 highlighted the fact that it was very easy to find patient details on P2P networks. The article mentions that, *"using common search terms, the author was able to gain access to a 1,718-page document containing Social Security numbers, dates of birth, insurance information, treatment codes and other health care data belonging to about 9,000 patients at a medical testing laboratory."*

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

In another highly publicized example, a contractor error led to the publishing of the blueprints for Marine One, the helicopter that transports President Obama and his family. This MSNBC article points out that the blueprints were found on a desktop with an IP address in Iran and by tracking backwards, the user was found to be a defense contractor with P2P on their PC. Undoubtedly the contractor had no intention of placing the files on a P2P network.

Assume for a moment that there security controls and policies are in place to combat the use of P2P. How would an employee who is accustomed to using P2P at work bypass the controls? One way would be to use one of the many encrypted tunnel applications and login to a home PC where file sharing can occur while safely ensconced in an encrypted tunnel, free from any security controls. Common variants of these applications include SSH, TOR and UltraSurf. Alternatively, a user can offload the "fun applications" to their home machine, accessing it with a remote desktop access application such as MS-RDP, LogMeIn! or Yoics!

For those who want to share files with a more limited set of users, there are more than 20 variants of browser-based file sharing applications, a new class of application that can act as a vector through which confidential data can pass with ease. These applications are not nearly as sneaky or as hard to configure correctly as P2P, but they do pass through security infrastructure with ease because they are all browser-based, using Port 80 or Port 443. Angry at being laid off? Or moving to a competitor? Launch YouSendIt! and transfer the customer database or the next-generation product plans to an online archive like BoxNet with ease. These applications are rapidly gaining popularity, appearing in 76% of the organizations, an increase of almost 100% over the previous two reports.

The last point to consider on the subject of why we should all care about application usage is the threat aspect. Malware writers are aware of the ease with which applications can traverse security infrastructures and they are taking full advantage of this to plant data-stealing executables like those that were used to steal millions of credit card numbers at Heartland Corporation this year and Hannaford Super Markets last year. How these threats were able to penetrate the security infrastructure is not 100% clear, but a case could be made that an end-user inadvertently clicked on something they should not have, or possibly did nothing but surf the web, and was targeted by a "drive-by" threat. Uncontrolled use of applications can affect everyone - employers, employees, and customers - in a number of different ways.

- Data loss such as credit card info is an inconvenience and possible credit hit for the victim. Loss of confidential data is costly in terms of clean up and reputation for both the employee and employer.
- Lost employee productivity as a result of non-work related application usage increases operational costs which are then transferred to possible price increases or reduced profit margins.
- Continual bandwidth upgrades brought on by streaming high-definition video and file sharing applications add unnecessary cost burdens to corporate infrastructure, which in turn affects corporate earnings.
- Continued lack of compliance with external regulations can result in fines or elevated charges per transaction. Again, making a direct impact on the bottom line.

The organizations that participated in the generation of this report are now more aware of the applications on the network and the risks they pose. Working in partnership with Palo Alto Networks they are addressing the findings through updated policy controls.

FINDINGS AND TRENDS

As outlined in both of the previous *Application Usage and Risk Reports (Spring 2008 and Fall 2008),* enterprise policies for appropriate application usage are inconsistent. Policies may exist but they are unenforced or merely given lip service. More often than not, the answer to the question of application usage policy is "what policy?" This is not to say that security teams do not want policy control – they do. Successful companies are transforming the IT department, known commonly as business inhibitors, into business enablers by asking them to usher in the use of these new applications. The problem is, the tools required to implement this transformation are inadequate. While every organization varied in terms of scope of application usage, there were several common themes.

- **Applications are designed for accessibility.**
- **Applications that enable users to circumvent security controls are common.**
- **File sharing usage is rampant.**
- **Applications continue to consume bandwidth at a voracious rate.**
- **Enterprises cannot control the applications on the network.**

Enterprises are rapidly becoming more aware that they have to address their growing application visibility and control problem. And they are looking for ways to positively enable application usage, as opposed to blindly blocking everything. The web 2.0 application that may not be "approved" may in fact be helping the company bottom line. So if IT can enable the application in a secure manner by allowing it and inspecting it for threats, then it is a win-win scenario. The employee is empowered, and IT is viewed as a business enabler as opposed to a business impediment.

APPLICATIONS ARE DESIGNED FOR ACCESSIBILITY

For purposes of this discussion, applications that have been designed for accessibility are defined as those that have been developed to use port 80 and port 443, and hop from port to port or can use a combination thereof. In this analysis, 57% of the 494 applications found can use port 80, port 443, or hop from port to port. As a feature, accessibility is not necessarily a bad thing and in fact, some of the first applications to be developed to take advantage of the "allow port 80" firewall rules were the desktop antivirus applications and the software update services. Trend, Kaspersky, Microsoft Update, Apple Update and Adobe Update all fall into the same category. The benefit of using port 80 is that it helps eliminate some of the IT effort required to deliver updates to desktops.

Every application, particularly those that traverse the firewall, represent risks, but blindly blocking these applications is not an option because doing so may impede business. For example, Microsoft SharePoint, Microsoft Groove and a host of software update services (Microsoft Update, Apple Update, Adobe Update) all fall into this category, so blocking them may block business use. On the other hand, applications such as BitTorrent, Pandora, Yoics!, and Gadu Gadu were also found and each of these applications introduces some level of business and security risk. Exercising some level of control over these applications may be desirable.

The majority of the "easy access" applications are consumer-oriented, indicating that accessibility goes beyond the business benefits. For example, collaborative applications found include social networking (14), email (28), instant messaging (33), VoIP (15), web posting (14) and conferencing (7). Of these 111 collaborative applications, it is safe to say that the majority are not endorsed by corporate IT, yet they may indeed provide some business benefit. The business value become less

clear when looking at the high number of media applications, which includes audio (13), photo-video (33) and gaming (8).

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.

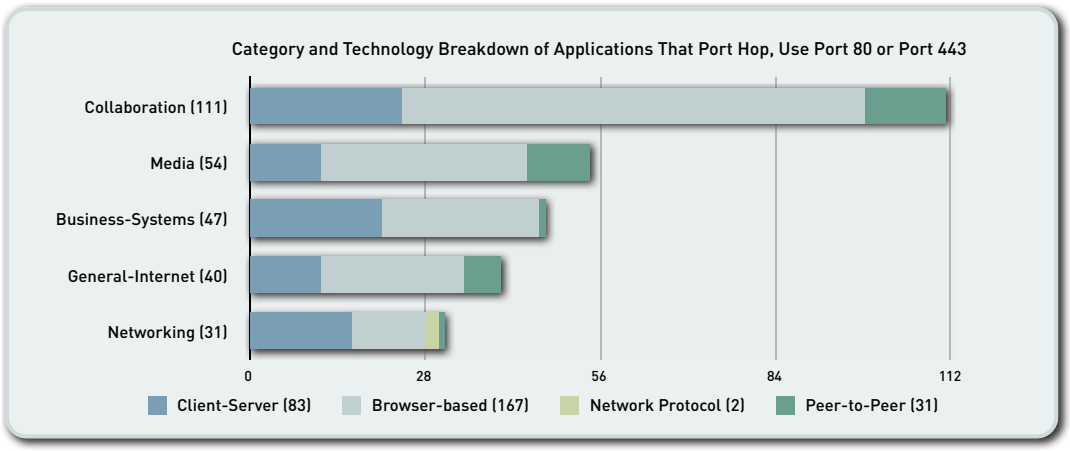


Figure 2: Breakdown of applications, by category and underlying technology, that use port 80, port 443 or hop ports as a means of simplifying access.

The process of determining the business value of the applications can be displayed by looking more closely at Yoics!, Microsoft SharePoint and Microsoft Groove as three examples. Yoics! is a client/server application that falls into the remote desktop access category. It uses port 80 or can hop from port to port (dynamic). Remote desktop access tools can be invaluable for IT support personnel. However, Yoics is not targeted at the IT professional – it is targeted at the end-user (consumer) as a means of accessing or sharing computing resources. From their website:

> *"Yoics is a powerful network solution that transforms any computer or network attached device instantly into an easily accessible and shareable internet resource. Featuring an intuitive user interface, remote access and sharing has just gotten as easy as using instant messaging."*

Yoics! uses VNC (Virtual Network Computing) to enable device sharing with other users. VNC is not a very secure tool so Yoics! sets up a secure connection between the two peers which is encrypted with a new random 160bit key for each connection established. Over that secure connection, a user can share their desktop, a folder, or a camera. Using the Yoics! NOW proxy, a user can also access internal network resources.

While Yoics! is a client/server application, yoics.net allows users to access their machine through a web browser. When using Yoics.net, the connection is tunneled over SSL to simplify remote, browser-based access to desktop resources. Yoics! uses SSL because it always works, even behind high security corporate firewalls. And it works with no software installed on the host computer. So if a user is at a friend's house, they won't need to install Yoics! to remotely access their desktop – they can just go to Yoics.net and access it. The second and third examples of applications that have features to enable them to bypass the firewall are **Microsoft SharePoint** and **Microsoft Groove**.

SharePoint is a browser-based collaboration tool from Microsoft that was found in 55 of the 63 organizations (87%). SharePoint can be used to host web sites, termed SharePoint Portals, which in turn, can provide access to shared workspaces and documents, as well as specialized applications such as wikis and blogs, from within a browser. SharePoint functionality is exposed as web parts, which are components that implement a certain functionality, such as a task list, or discussion pane.

These web parts are then composed into web pages, which are then hosted in the SharePoint portal. SharePoint sites are actually ASP.NET applications, which are served using Microsoft IIS and use a Microsoft SQL Server database as data storage backend.

The risks that SharePoint represent appear to be limited because it is a business application that is typically supported by IT. In reality, recent research by Neil MacDonald at Gartner shows that as many as 30% of the SharePoint deployments are rogue. A rogue SharePoint deployment is similar to the rogue wireless deployments of years ago. An improperly configured SharePoint deployment can provide an avenue for outbound data leakage and inbound threats or hackers.

Microsoft Groove is a collaboration tool that helps teams work together dynamically and effectively, even if team members work for different organizations, work remotely, or work offline. Groove works in conjunction with Microsoft SharePoint in either an online or offline mode. The offline mode targets teams with members who are usually off-line or who do not all share the same network security clearance. One interesting fact about Groove is that its underlying technology is peer-to-peer, which, in this case, is a positive use of a very powerful technology that has a very bad reputation due to its use for file-sharing of copyrighted materials. Microsoft Groove is a peer-to-peer application that uses either port 80 or port 2492 to pass through the firewall. Groove was originally developed by Groove Networks of Beverly, Massachusetts, and was acquired by Microsoft in March 2005.

The three examples outlined above highlight the wide range of applications that are capable of passing through the existing security infrastructure as a standard feature. One of the applications, Yoics!, has questionable value on a corporate network. It may be used by as a support tool by IT, but in all likelihood, it is an intrepid user accessing their home machine. The other two applications are clearly both business oriented and they too utilize commonly open ports to simplify access.

APPLICATIONS THAT ENABLE SECURITY CIRCUMVENTION

One of the clearest indications that employees will take whatever steps are necessary to use whichever applications they want is shown by the number of proxies, encrypted tunnel and remote desktop applications found. In the list of the most common examples of these applications found, one could argue that only a few are endorsed by the IT organization. The discovery of these applications highlights several key issues that IT managers must face every day. If employees want to use their favorite application for whatever reason, then there are a series of readily available tools that will facilitate bypassing whatever controls exist.

PRIVATE AND PUBLIC PROXIES

For the purposes of bypassing corporate control mechanisms, proxies (found across 81% of the organizations) are available in several variants. The first is a private proxy, which is a software application that is installed on a server and is used by a single user. In this case, the employee will install the software on a machine at home, or somewhere outside of the corporate network. While at work, the employee will use the browser to access the home machine as an unmonitored means to browse the web. The most commonly detected proxies that fall into this category are CGIProxy and PHProxy, which were detected in 57% and 51% of the accounts respectively.

The second proxy variant is a public proxy or a proxy service. These are merely implementations of the aforementioned proxy software applications that are made available to the public. For example, an employee that wants to browse the web anonymously can visit www.proxy.org and select from one of 7,700+ proxies that have been established by well meaning Internet citizens. Users can also sign up for an email update that notifies them of the 10 or so new proxy sites made available on a daily basis.

In either case, the employee is able to bypass existing controls, such as a firewall and URL filtering, and corporate implemented proxies. The reasons are simple – the traffic looks like normal web browsing and most corporate security policies allow this type of traffic to pass unfettered. An argument could be made that URL filtering could block public proxies, but in fact they are unable to keep up with an average of 10 new proxy services enabled every day. Overall, proxies that are typically not supported or endorsed by corporate IT were found in 81% of the organizations.

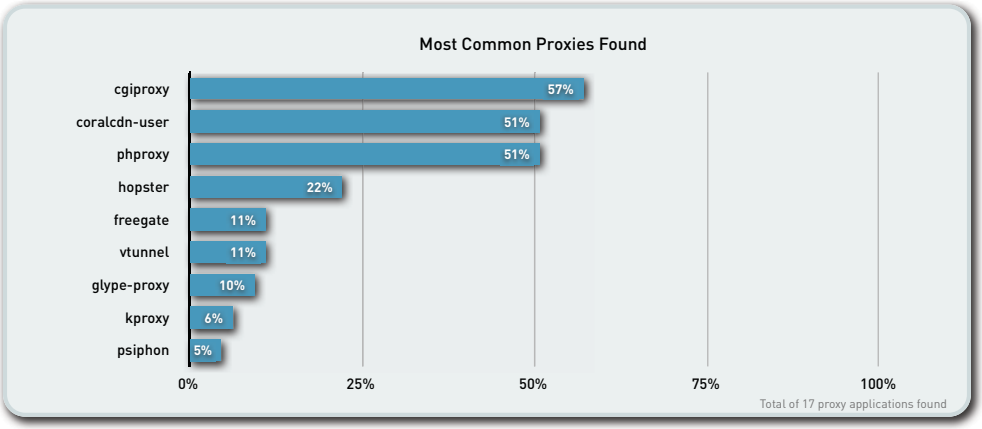


Figure 3: The most commonly detected proxies found across the participating organizations.

ENCRYPTED TUNNEL APPLICATIONS

Employees that want to use any application they want while at work can do so with an encrypted tunnel application that enables users to bypass security controls in an encrypted manner. Known examples of these types of applications include TOR, Hamachi, and UltraSurf. All three of these applications require the installation of client software which connects to a network of servers on the Internet. From there, the traffic is routed to its destination. Encrypted tunnel applications such as SSL and SSH were found in 100% and 89% of the organizations respectfully, while other, more clandestine applications, such as TOR, were found less frequently.

These applications fall into several different categories – those that are explicitly designed to bypass security such as TOR and Gbridge; and tools commonly user by IT that enable similar actions such as SSH and RDP. TOR (the onion router) is an interesting example of a privacy tool that was originally developed by the U.S. Military as a means of secure communications over the early version of the internet known as DARPA. TOR is the recommended method of communications for whistle-blowers. The Electronic Frontier Foundation (EFF) also recommends it as a mechanism for maintaining civil liberties online.

TOR is a client server application where the client is installed on the end-users machine and is used to connect to the intended site through a series of TOR nodes. The data in the message is distributed such that no one node holds the entire message. Privacy is further ensured by the use of proprietary encryption. The final message comes back together when it is received by the intended recipient.

Gbridge enables privacy by establishing a VPN tunnel inside of a Google Gtalk instant messaging session (note that Gbridge is not a Google application – it is an extension written by another developer). A Gbridge user can then connect to multiple PCs (outside the firewall) that are logged in under the same Gtalk user account. Gbridge can also be extended to Gtalk friends based on invitation, enabling them to perform such popular functions as folder synchronization, remote desktop share (VNC), automatic backup, live browsing and chat, etc. – all in an encrypted manner. To most security devices, Gbridge will pass undetected, looking like HTTP traffic, or at most instant messaging traffic, which may or may not pose a risk to the enterprise. Unbeknownst to the security team, hidden inside of the IM session is an encrypted connection that may be performing unauthorized file sharing or acting as a completely hidden inbound threat vector.

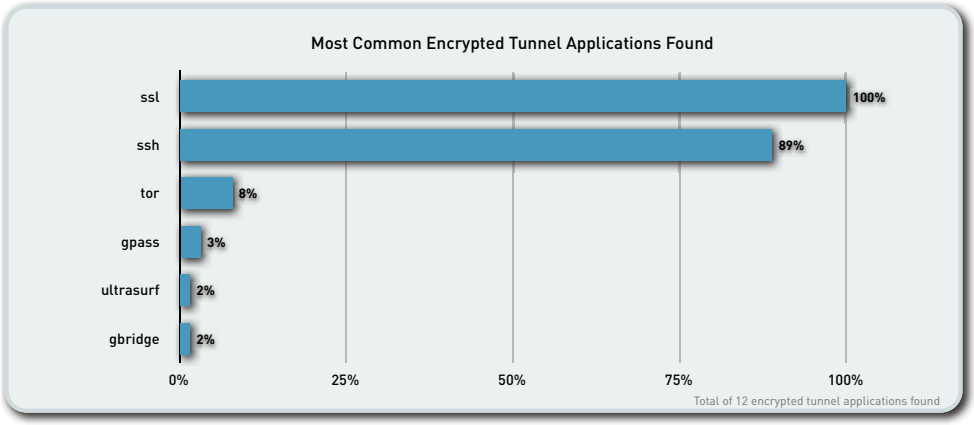


Figure 4: The most commonly detected encrypted tunnel applications found across the participating organizations.

The last example of encrypted tunnel applications that enable proactive security evasion is SSH. Whereas TOR and Gbridge are applications that have been developed as applications with the explicit purpose of bypassing security, SSH is commonly used by IT to establish a protected connection to another corporate machine for purposes of remote management. Detected on 89% of the networks in this study, SSH has been known to be used by knowledgeable end-users to access their home machines (or other machines) and use those remote machines for non-work related activities. To be fair, SSH is a commonly-used IT tool and it is difficult to determine how it is being used in every organization. However, there are known instances within this set of organizations where SSH control policies were in place, yet sophisticated users were violating the policy. With SSH, a user can easily bypass existing controls in an encrypted tunnel.

REMOTE DESKTOP CONTROL APPLICATIONS

The third group of applications that employees commonly use to circumvent security controls is remote desktop access applications, found across 95% of the organizations. In the hands of an IT or support person, these tools help rectify PC or server problems remotely. Without question, these applications are invaluable tools, however, with more that 20 different variants found, the use of these applications clearly extends to employees outside of traditional IT/support roles.

Some of the applications such as pcAnywhere and GoToMyPC are commercially-supported, while others such as RDP and VNC are part of the common IT toolset. Remote desktop access applications were found 95% of the time, with remote desktop protocol (RDP) and LogMeIn! the most commonly detected at 86% and 51% respectively.

Earlier in the paper, a description of the remote desktop access application, Yoics! was provided as an application that contains built-in features that enable it to bypass the firewall. It is a safe assessment that Yoics! is targeted at the end-user who wants access a PC outside of the work environment.

The target users for tools such as RDP and Virtual Network Computing (VNC) historically have been IT oriented but are no longer as clearly defined. RDP is a client/server application that uses port 3389 by default but is also capable of hopping from port to port. RDP is a standard feature in Windows XP Professional, enabling users to access their computers across the Internet from virtually any computer, Pocket PC, or smartphone. Once connected, Remote Desktop provides full mouse and keyboard control over the computer while displaying everything that's happening on the screen. With Remote Desktop, users can leave their computer at the office without losing access to files, applications, and e-mail.

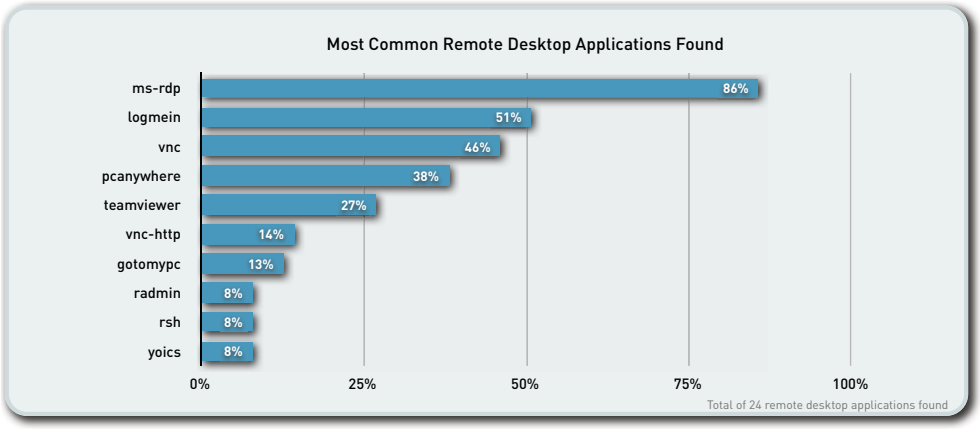


Figure 5: The most commonly detected remote desktop access applications found across the participating organizations.

With RDP, an employee can easily configure their work PC to connect to their home PC and from there can, run any application they desire – swap files, run a P2P application, listen to music, surf the web – all in a tunnel that can be encrypted with RC4, although it is known to be susceptible to man-in-the middle vulnerabilities. VNC, like RDP is an IT-oriented tool for remote access to another computer. VNC is a client server application where the client is the machine accessing the remote PC (server). VNC uses several ports 5900 through 5906, with each port corresponding to a separate screen. VNC is not the most secure application, although it can be tunneled over SSH or a VPN connection to provide privacy. One of the more valuable VNC features is that it is cross-platform, enabling control over Windows, Mac or UNIX machines.

Each of the applications discussed in this section can be used for work-related purposes, primarily in the IT department as a means of remotely managing PCs and servers. They can also be used by employees to access PCs or servers outside of work. The problem is that the IT department is unable to distinguish clearly between the two because of a lack of visibility – so the policy is, more often than not, allow VNC and RDP to be used by anyone.

P2P FILE SHARING USAGE IS RAMPANT

The recent discovery of Marine One blueprints and healthcare records on a P2P network, along with the fact that P2P filesharing was found 92% of the time in this study, demonstrates that P2P is not just a problem for higher education environments. The continued high usage of peer-to-peer applications within enterprises adds an exclamation point to the assertion that employees use whatever application they want. It is commonly understood that using P2P at work is not a corporate

supported application, yet in 9 out of 10 organizations, an average of six P2P variants were found, and in one case, as many as 17 variants were found.

The most common P2P applications found were BitTorrent and Gnutella – both at 68%. In terms of bandwidth consumed, P2P file sharing increased dramatically (92%) over the previous report, chewing through 2.3 terabytes or 5% of the total bandwidth viewed across all organizations. From a bandwidth perspective, BitTorrent was the most voracious.

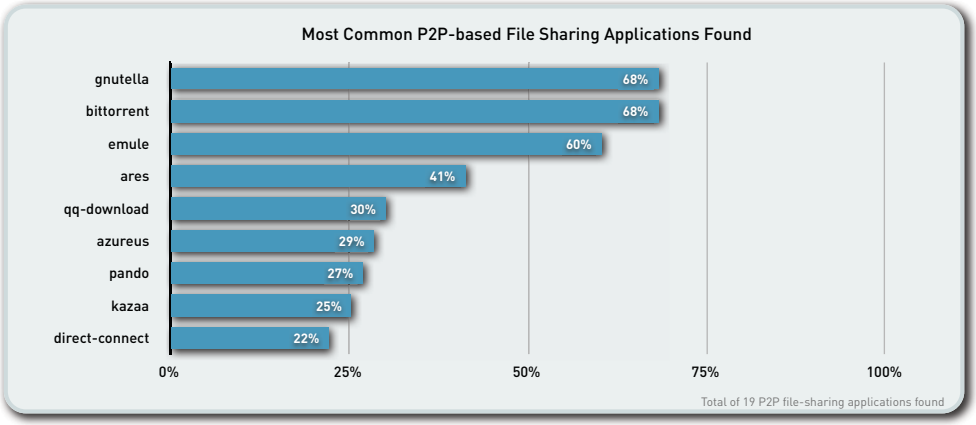


Figure 6: The most commonly detected P2P-based file sharing applications found across the participating organizations.

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

It is important to point out that peer-to-peer technology by itself is a very powerful tool, leveraging shared computing resources for efficiency. The negative reputation that P2P technology has received is due to the end result of the use of P2P, not the technology itself. The data that can be found P2P networks is there because someone has put it there or, in the case of the inadvertent breaches, the application was not configured correctly.

BROWSER-BASED FILE SHARING GAINS IN POPULARITY

While not as broadcast oriented as P2P, browser-based file sharing applications showed continued growth with an average of five variants discovered in 76% of the organizations with YouSendit! and MediaFire the most common of the 22 variants detected. This up and coming class of application represents another area of high risk for enterprises in that these applications can bypass controls (port 80 or port 443), acting as an avenue of data leakage, as well as an inbound threat vector. Browser-based file sharing applications include those that provide file transfer (e.g., YouSendit!), backup (e.g., BoxNet), and publishing (e.g., DocStoc) capabilities.

Currently, there are at least 29 different applications that fall into this category with more being added almost weekly. All but one of these applications use either port 80 and/or port 443 as a means of passing through the firewall. Fs2you has an optional client that can use tcp port 3128 or udp port 3128 in addition to its default use of port 80.

The business value for these applications is clear for anyone who has tried and failed to move a large PowerPoint, graphics or multimedia file over email. Login to **YouSendIt!**, the most popular browser-based application found (57%), upload the file, send the URL to the recipient and the task is complete. No more asking the IT guy to help ftp it, or trying to chop it up or compress it.

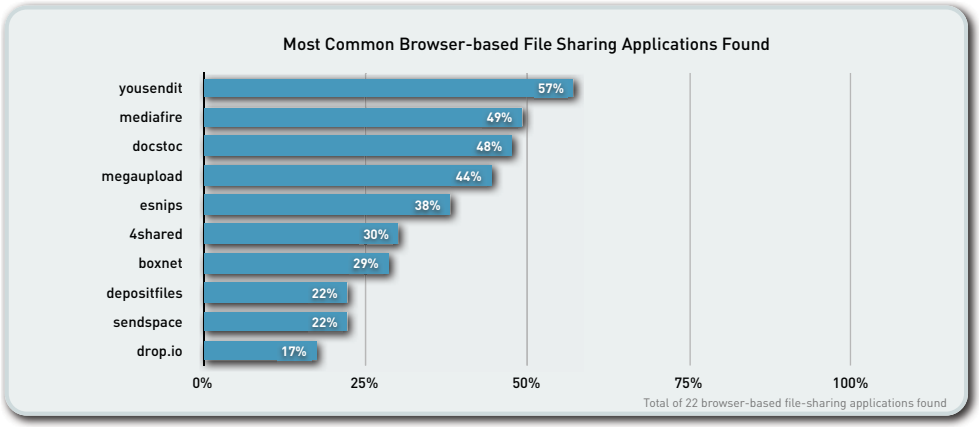


Figure 7: The most commonly detected browser-based file sharing applications found across the participating organizations.

YouSendIt! has several different applications – all of which are focused on file transfer across either port 80 or port 443. The four applications are Lite (free), Pro, Business Plus and Corporate Suite – the differences are advanced features such as file size, branding and file expiration dates. Billed as a way to easily move large graphics files, YouSendIt! is making a concerted effort to attract corporate users with a series of plugins for applications such as PhotoShop, Outlook and CoralDRAW. YouSendIt! takes security more seriously than other applications in this category by using SSL to encrypt the transfer of files. As another example of their desire for corporate support, YouSendIt! defines their application as firewall-friendly, "using port 80 and port 443, which are always open, eliminating the use of other non-standard firewall ports".

MediaFire is another example of a browser-based file sharing application that uses port 80, looking innocently like other web traffic, bypassing any possible port 80 controls that are in place. MediaFire is available for free and allows users to upload files as large as 100 MB. The user is then supplied with a unique URL, which locates the file and enables anyone with whom the uploader shares it to download the file. Currently there is no time limit on how long uploaded files will be stored. There are two levels of security for stored files – mark them private and password protect them. Marking them private means that the file can't be shared with other people and no one except the file owner can download it. It does not appear that the files are encrypted during the upload, storage or download process.

It would be inaccurate to say that browser-based file sharing poses the same level of risks as P2P applications pose. There have been no known errant distributions of confidential files. This is because the user is required to take action to deliver or receive the file, and the audience tends to be limited in scope. These applications do however 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.

THE UNCONTROLLABLE BANDWIDTH HOGS

As the cost of bandwidth continues to drop, organizations are able to increase the size of their Internet connection to deploy more online service offerings, and provide their employees/customers with an improved end-user experience. The allure of high-speed connectivity, the desire to use whatever application they want and the melding of personal and work life means that there is a strong likelihood that many of the applications leveraging increased speeds are not business-related.

The analysis found that out of a total of 48.5 TB of data analyzed, 24.7 TB is being consumed by a little more than a quarter (28%) of the applications. Most of the applications are consumer-oriented, falling into the following categories: media, social networking, P2P and browser-based file sharing, web-browsing and toolbars. Some of the applications in this group highlight the dilemma that IT managers face. They may see YouTube as an application that consumes too much bandwidth, but cannot block it because the marketing department is using it for customer video testimonials. The same premise applies to Flash – an active consumer of bandwidth, and a known threat vector, but also a tool used across the enterprise. The challenge with these applications is twofold. On one hand, many may fall outside of the "approved list" of applications while on the other hand, they are indeed capable of providing business value, so summarily blocking them is not a viable option. However, identifying the application, who is using it, then controlling and inspecting it is a perfectly acceptable action.

Application Category	Number of Applications	Bandwidth Used	Percentage of Traffic
Social Networking	17	0.4 TB	2%
Streaming Audio	13	1.8 TB	7%
P2P + Browser-based File Sharing	41	2.3 TB	9%
Flash	1	3.3 TB	13%
Photo + Video	44	4.4 TB	18%
Internet Utility (Browsing & Toolbars)	21	12.5 TB	51%
Totals	137	24.7 TB	100%

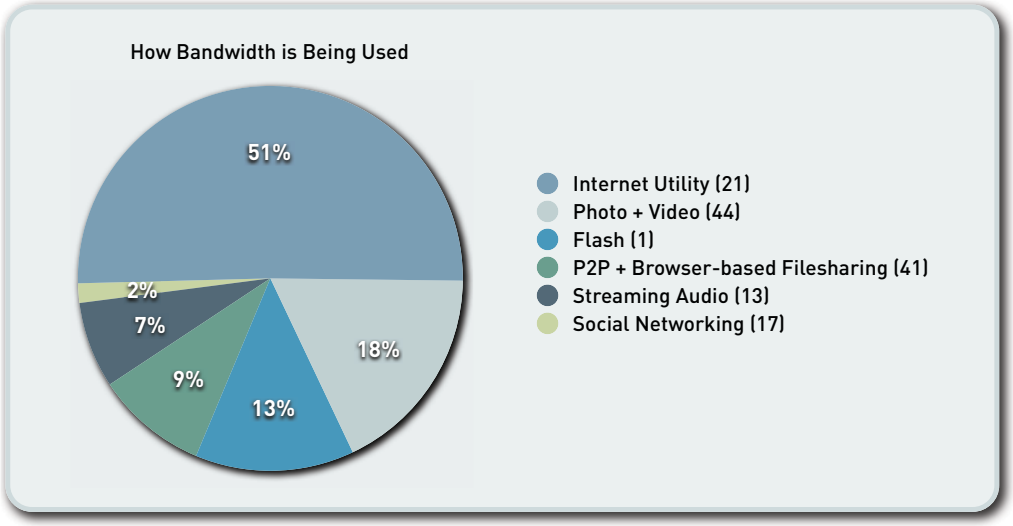


Figure 8: Analysis of how bandwidth is being used across largely consumer-oriented application categories.

As an example Flash, was found in 100% of the organizations and consumed 3.3 TB or 7% of the overall bandwidth observed. Commonly used for web site graphics, marketing elements and training videos, Flash is the "plumbing" for a wide range of streaming content. Clearly there are business and security risks associated with Flash, but can an IT manager impose a policy to block it? The answer is no because there is no way of knowing how it is being used, however, steps can be made to mitigate the impact of Flash on the network and users. Inspecting the content as it traverses the network and identifying the heaviest users for QoS controls are possible options, but wholesale blocking is not a viable alternative without crippling many mainstream sites.

Hulu Networks is a perfect example of an entertainment application used at work. Hulu, the self-proclaimed leader in cerebral gelatinizing high definition TV over the web was found 83% of the time and consumed an average of 3.86 GB of bandwidth in *each* of the organizations where it was detected. Hulu is categorized as a photo-video application, one of 44 different photo and video applications found during the analysis. Hulu uses Flash to deliver a limited set of movies along with TV and cable shows from NBC and Fox. Unlike applications such as YouTube, which can enable posting of work-related videos, Hulu is broadcast only – and as such, it is unlikely that it is being used for work. Users can however embed video clips into social networking sites and online communities, using code samples provided by Hulu. In terms of delineating Hulu content from generic Flash, Palo Alto Networks identifies the unique characteristics that Hulu exhibits, enabling administrators to set a policy that allows Flash yet controls Hulu and other video sites like it.

Whereas Flash clearly straddles the line between business and pleasure, the 13 different streaming audio applications such as iTunes, Pandora, and ShoutCast, found 86%, 68% and 57% of the time, respectively, are entertainment – pure and simple. The use of these three applications was exceeded only by generic HTTP audio streaming, yet they (iTunes, Pandora, ShoutCast) combined to consume 852 GB or 2% of overall traffic. Note that iTunes usage is a mix of listening and download/update traffic.

The most interesting application of the three is ShoutCast, which is a streaming portal owned by AOL. While not as well known as iTunes or Pandora, according to AccuStream iMedia Research, ShoutCast was the streaming provider for more than 50% of the 6.67 billion hours (22 hours for every single person in the U.S.) of Internet radio heard in 2008.

ShoutCast is a radio receiver for users to listen, but also enables a user to become a radio host. If a user is passionate about their music, or their political views, or just likes to talk, they can download the ShoutCast Radio Distributed Network Audio Software (DNAS), install it on an Internet connected server and begin broadcasting. Once installed, the radio host only needs to drop the music files into the appropriate folder and the streaming begins. ShoutCast DNAS defaults to tcp/8000 but can be configured to use any port. The DNAS software can also act as a relay, sending and receiving other radio stations. Because DNAS is installed on a freely available Internet connection and is accessible by tcp/80 (or other port), it is conceivable that an employee, taking advantage of high speed networking at work, can stream music to the world. Further exemplifying the interconnected nature of the Internet is the fact that listeners can access ShoutCast-based radio stations using Pandora, iTunes (Mac), or WinAmp (Windows) – all found frequently in this analysis.

New entertainment oriented applications seem to be made available weekly. With no end in sight, questioning the use of many of these applications is an absolute necessity, from a bandwidth perspective as well as a business and security risk perspective. It is unrealistic to try and block these applications because there are many cases where business value is provided. A more positive approach, might be to provide employees with entertainment application usage privileges. Assuming the cost is a manageable one and the risks are appropriately mitigated, there may be a tremendous morale and productivity enhancement.

EXISTING CONTROL MECHANISMS ARE FAILING

Based on published market share data, enterprises are spending more than $6 billion annually in FW, IPS, proxy and URL filtering products that all claim to perform some level of application control. The analysis showed that 100% of the organizations had firewalls and 87% **also** had one or more of these firewall helpers (a proxy, an IPS, or URL filtering). Despite the spending levels, the analysis shows that organizations are unable to control applications traffic.

The reasons for the loss of control are straightforward. Existing firewalls see only ports and protocols and 57% of the applications found can bypass what is considered to be the most strategic point in the security infrastructure – the firewall. Adding IPS (UTM) does not address the problem because the firewall still relies on port and protocol to initially classify the traffic. IPS is a negative enforcement model so an administrator must tell it which applications to block. Proxies control a very limited number of applications and they tend to "break" other applications. Finally, URL filtering is merely a database of websites, and applications are far more than a mere URL.

SUMMARY

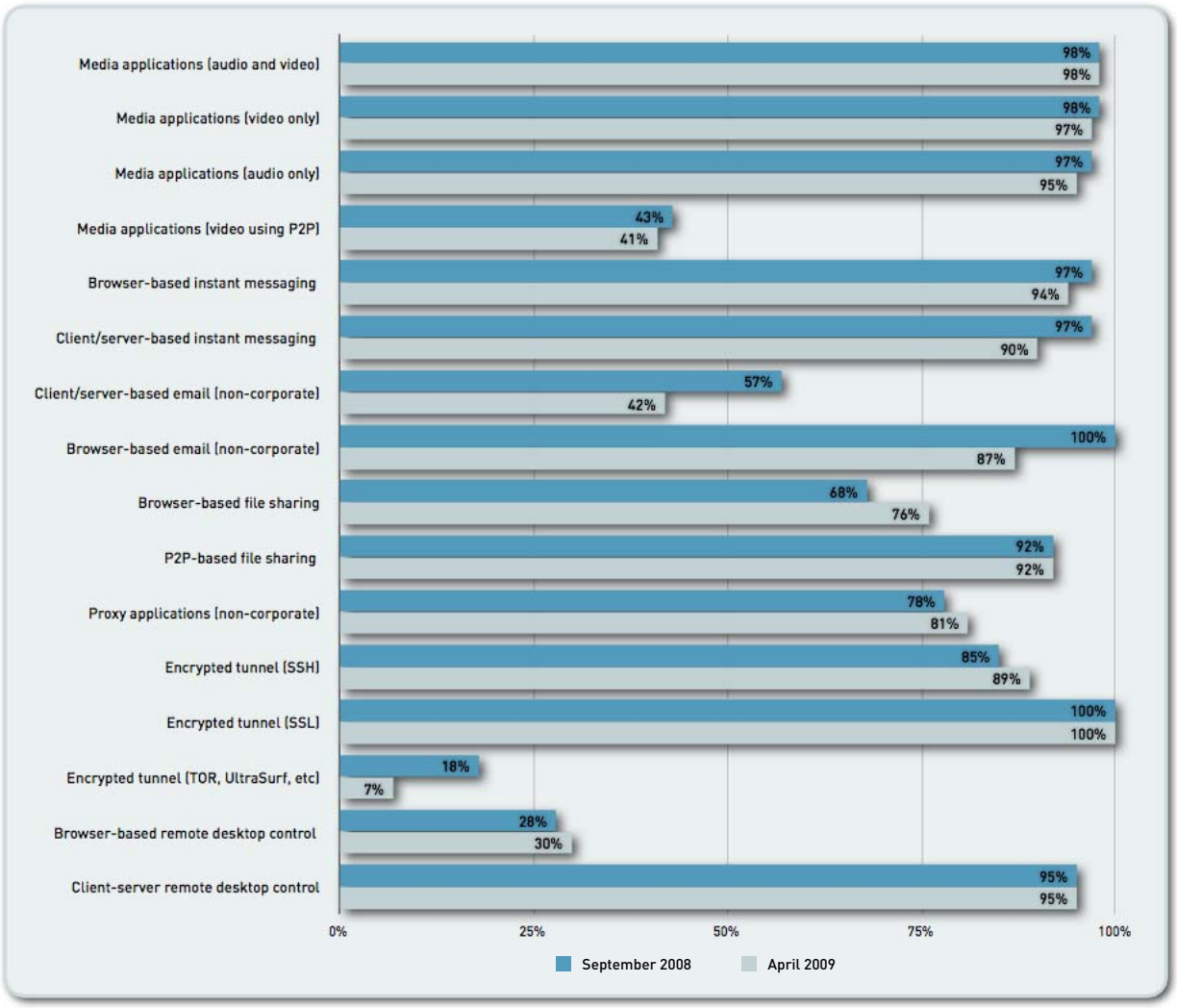
In the process of establishing and maintaining network security, many IT organizations have earned the unwarranted reputation of impeding the business. When a business unit asks for permission to use a new application, they are told “No.” The reputation is not IT groups’ fault. The findings in this report show that the application developers and users alike have figured out ways around the IT department. Built-in features to pass through the firewall. Proxies, encrypted tunnels and remote desktop access pass through tougher controls. All as a means for employees to use what ever application they want, regardless of security risk, business benefit or amount of bandwidth consumed. In order for IT organizations to transform from business impediments to business enablers, they need to deploy solutions that provide visibility and control over applications (not ports or protocols), users (not IP addresses) and content.

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, visit www.paloaltonetworks.com.

APPENDIX 1: SUMMARY OF CHANGES FROM PREVIOUS REPORT

A summary of the changes between the Application Usage and Risk Report, Fall 2008 and Spring 2009 is shown below.



APPENDIX 2: 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 one 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

The application visibility that Palo Alto Networks next-generation firewalls provides is delivered by a patent-pending technology called App-ID. Designed to address security evasion tactics commonly used in many of today's new applications, App-ID uses as many as four identification techniques to determine the exact identity of applications flowing in and out of the network.

Application visibility does not stop with application identity. If it did, the application identity would not help the administrator make more informed decisions about how to treat the application. Presented with the name of an application never before seen on the network, of which there may be many, an administrator may be inclined to block it. It is not about telling an administrator that an application is "bad" and should be blocked. The more effective approach is to present a complete picture of what the application is and how it is being used. With the Palo Alto Networks solution, administrators are presented with the application name, a description, its characteristics and its underlying technology, allowing administrators to make much more informed security policy decisions.

To facilitate the decision making process on how to treat an application, Palo Alto Networks provides additional background for more than 800 applications including a detailed description, alternative sources of information and which port(s) are commonly used. To help keep administrators more informed, eight different application characteristics are provided including:

The accurate identification of the application by App-ID solves only part of the visibility and control challenge that IT departments face with today's Internet-centric environment. Inspecting permitted application traffic becomes the next significant challenge and one that is addressed by Content-ID.

Content-ID melds stream-based scanning, a uniform threat signature format, and a comprehensive URL database with elements of application visibility to limit unauthorized file transfers, detect and block a wide range of threats and control non-work related web surfing. Content-ID works in concert with App-ID, leveraging the application identity to help make the content inspection process more efficient and more accurate.

To view details on more than 800 applications currently identified by Palo Alto Networks, including their characteristics and the underlying technology in use, please visit the Applipedia (encyclopedia of applications) located here http://ww2.paloaltonetworks.com/applipedia/

APPENDIX 3: MOST COMMON APPLICATIONS FOUND

Listed below the 494 different applications found across the more than 60 organizations, ranked in terms of frequency and sorted alphabetically. Note that there is a mix of consumer or end-user oriented applications along with a wide range of business and networking applications. To view details on the 800+ applications, including their characteristics and the underlying technology in use, please check Palo Alto Networks encyclopedia of applications located here http://ww2.paloaltonetworks.com/applipedia/

web-browsing (100%)
ssl
ntp
netbios-ns
icmp
dns
snmp
smtp
ms-update
flash
soap
netbios-dg
ldap
ftp
http-audio
youtube
webdav
rss
http-proxy
facebook
yahoo-mail
hotmail
gmail
msrpc
google-safebrowsing
google-calendar
google-analytics
ssh
photobucket
msn
kerberos
http-video
apple-update
sharepoint
rtmpt
gmail-chat
aim-mail
yahoo-webmessenger
rtmp
ms-rdp
itunes
dhcp
adobe-connect
stumbleupon
myspace
ms-ds-smb
linkedin
google-toolbar
google-desktop
yahoo-toolbar
twitter
soribada
ms-exchange
limelight
hulu
flexnet-installanywhere
aim-express
spark
google-picasa
google-docs
myspace-video
mssql-mon
dailymotion
atom
stun
rtsp
myspace-mail
imeem
reuters-data-service
metacafe
netbios-ss (75%)
ms-netlogon
facebook-mail
snmp-trap
ike
facebook-chat
comcast-webmail
skype-probe
ms-sms
msn-toolbar
ipsec-esp-udp
active-directory
syslog
pop3
orkut
livejournal
google-earth
blackboard
yahoo-im
telnet
pandora
outlook-web
mobile-me
gnutella
bittorrent
squirrelmail
aim
yahoo-voice
silverlight
mssql-db
google-lively
pogo
backweb
skype
friendster
friendfeed
webshots
webex
emule
ebuddy
web-crawler
hp-jetdirect
citrix-jedi
yousendit
slp
sip
shoutcast
sharepoint-admin
secureserver-mail
salesforce
cgiproxy
xm-radio
ustream
move-networks
live365
citrix
tftp
msn-voice
zimbra
zango
norton-av-broadcast
meebome
phproxy
myspace-im
mms
logmein
coralcdn-user
blog-posting (50%)
worldofwarcraft
time
rtp
radius
netflow
msn-file-transfer
mediafire
lwapp
imap
blogger-blog-posting
meebo
live-meeting
google-talk
docstoc
vnc
ooyala
adobe-update
rdt
megaupload
horde
jabber
flixster
classmates
ciscovpn
ssdp
portmapper
msn-money-posting
blackberry
ares
yum
mogulus
logitech-webcam
trendmicro
teredo
pcanywhere
meevee
esnips
bbc-iplayer
asf-streaming
xobni
twig
second-life
mail.com
ipsec-esp
hi5
cox-webmail
gre
stickam
open-webmail
ms-groove
ichat-av
veohtv
streamaudio
socialtv
oracle
gadu-gadu
dealio-toolbar
upnp
rpc
qq-download
msn-webmessenger
mediawiki-editing
lpd
justin.tv
bebo
4shared
subspace
daytime
boxnet
azureus
autobahn
yahoo-file-transfer
websense
teamviewer
send-to-phone
pando
optimum-webmail
netease-mail
irc
tacacs-plus (25%)
rip
netspoke
lotus-notes
kazaa
gtalk-voice
roundcube
pptp
aim-file-transfer
webex-weboffice
verizon-wsync
sharepoint-documents
sendspace
qq-mail
outblaze-mail
nntp
nfs
hopster
direct-connect
depositfiles
corba
yandex-mail
yahoo-webcam
symantec-syst-center
sharepoint-calendar
seven-email
qq
orb
l2tp
icq
gnunet
fastmail
discard
apple-airport
xunlei

x11
tvu
ppstream
netvmg-traceroute
netmeeting
ipv6
h.323
h.245
echo
whois
sybase
ncp
napster
ms-win-dns
ipp
gtalk-file-transfer
drop.io
cups
carbonite
pplive
neonet
mysql
mcafee
livelink
imesh
editgrid
blin
zoho-wiki
youseemore
yourfilehost
vnc-http
vmware
sling
rapidshare
ms-wins
jaspersoft
inforeach
flickr
ebay-desktop
concur
clearspace
bomberclone
backup-exec
yahoo-finance-posting
subversion
steam
sopcast
sccp
ruckus
mount
gotomypc
gotomeeting
eigrp
bugzilla
vtunnel
source-engine
ndmp
msn-video
ms-iis
ms-dtc
iloveim
groupwise
freegate
folding-at-home
foldershare
filemaker-pro
filedropper
evernote
dotmac
db2
big-brother
xdrive
xdmcp
winamp-remote
userplane
t.120
socks
sightspeed
rsvp
radiusim
pownce
postgres
oovoo
noteworthy-admin
medium-im
lotus-sametime
joost
igp
glype-proxy
fileswire
eatlime
zenbe
yoics
wins
unassigned-ip-prot
tor
secure-access
rsh
radmin
poker-stars
mozy
mediamax
hushmail
camfrog
zoho-writer
zoho-sheet
yugma
yahoo-douga
writeboard
wolfenstein
uusee
tvants
scps
rsync
rping
pna
noteworthy
ms-scheduler
ms-ocs
meebo-file-transfer
kproxy
jira
imvu
finger
cvs
cooltalk
100bao
zoho-im
wlccp
wikispaces-editing
wetpaint-editing
tvtonic
tivoli-storage-manager
tikiwiki-editing
tidaltv
soulseek
sophos-update
sap
rlogin
psiphon
pim
pbwiki-editing
party-poker
ospfigp
ms-frs
manolito
koolim
kaspersky
ip-in-ip
ibackup
google-finance-posting
fs2you
etherip
elluminate
doof
cpq-wbem
apc-powerchute
altiris
airaim
zoho-show
xfire
xbox-live
wixi
war-rock
unyte
trinoo
thinkfree
sugar-crm
srp
rvd
pingfu
perforce
miro
messengerfx
meeting-maker
mcafee-epo-admin
kugoo
ipsec-ah
idrp
icq2go
http-tunnel
gpass
glide
gizmo
fire
drda
dabbledb
crossloop
zoho-notebook
zoho-crm
zelune
ypserv
x-font-server
wikidot-editing
webconnect
wccp
vsee
veetle
usermin
ultrasurf
tokbox
tagoo
swipe
swapper
sun-nd
sosbackup
siebel-crm
r-exec
reserved
ragingbull-posting
privax
netviewer
ms-ocs-file-transfer
ms-ocs-audio
motleyfool-posting
mobile
mail.ru
lotus-notes-admin
livestation
instan-t-file-transfer
informix
imhaha
ilohamail
iccp
hopopt
hmp
generic-p2p
gbridge
freeetv
fluxiom
flumotion
filemaker-anouncement
fastviewer
egp
dynamicintranet
dropboks
circumventor
backpack-editing
babelgum
avaya-phone-ping
aim-video
aim-audio (2%)