Application Visibility and Risk Report

Prepared for: Customer ABC

Prepared by: Palo Alto Networks

[date goes here]

Why Palo Alto Networks?

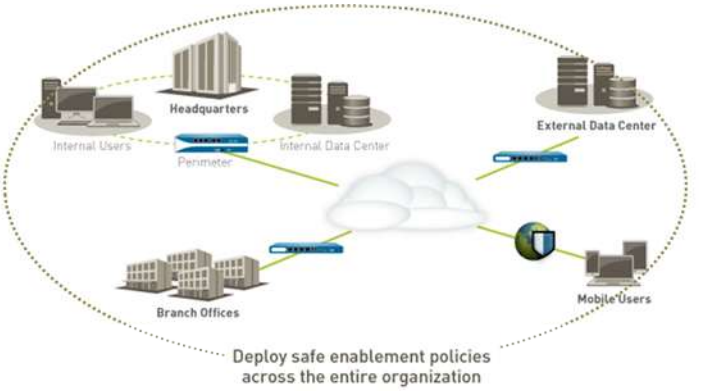
Fundamental shifts in the application and threat landscape, user behavior, and network infrastructure have steadily eroded the security that traditional port-based firewalls once provided. Users are accessing all types of applications, using a range of device types, often times to get their job done. Datacenter expansion, virtualization, mobility, and cloud-based initiatives are forcing organizations to re-think how to enable application access yet protect the network. Palo Alto Networks next-generation firewalls can help organizations safely enable applications, for all users, regardless of location, resulting in a reduction in the associated business and security risks.

Classifying all applications, across all ports, all the time. App-ID applies multiple classification mechanisms to the traffic stream, as soon as the firewall sees it, to determine the exact identity of application, regardless of port, encryption (SSL or SSH) or evasive technique employed. The knowledge of exactly which applications are traversing the network, not just the port and protocol, becomes the basis for all security policy decisions. Unidentified applications, typically a small percentage of traffic, yet high in potential risk, are automatically categorized for systematic management – which can include policy control and inspection, threat forensics, creation of a custom App-ID, or a packet capture for Palo Alto Networks App-ID development.

Tying users and devices, not just IP addresses, to policies. Security policies that are based on the application and the user identity, regardless of device or location, are a more effective means of protecting the network than relying solely on port and IP address. Integration with a wide range of enterprise user repositories provides the identity of the Microsoft Windows, Mac OS X, Linux, Android, or iOS user accessing the application. Users who are traveling or working remotely are seamlessly protected with the same, consistent policies that are in use on the local, or corporate network. The combined visibility and control over a user's application activity means organizations can safely enable the use of Oracle, BitTorrent, or Gmail, or any other application traversing your network, no matter where or how the user is accessing it.

Prevent against all threats, both known and unknown. Coordinated threat prevention can be applied to known malware sites, vulnerability exploits, viruses, spyware and malicious DNS queries can all be blocked in a single pass while custom or otherwise unknown malware is actively analyzed and identified by executing the unknown files and directly observing more than 100 malicious behaviors in a virtualized sandbox environment. When new malware is discovered, a signature for the infecting file and related malware traffic is automatically generated and delivered. All threat prevention analysis uses full application and protocol context, ensuring that threats are caught even if they attempt to hide from security in tunnels, compressed content or on non-standard ports.

Safe application enablement policies can help organizations improve their security posture, in the following ways. At the perimeter, the threat footprint can be reduced by blocking unwanted applications and then inspecting the allowed applications for both known and unknown threats. In the traditional or virtualized datacenter, application enablement translates to ensuring only datacenter applications are in use by authorized users, protecting the content from threats and addressing security challenges introduced by the dynamic nature of the virtual infrastructure. Enterprise branch offices and remote user enablement policies can be extensions of the same policies deployed at the headquarters location, thereby ensuring policy consistency.



Summary and Key Findings

Palo Alto Networks conducted an application visibility and risk analysis for Customer ABC using the Palo Alto Networks next-generation firewall. This report summarizes the Customer ABC analysis beginning with key findings and an overall business risk assessment; it then discusses the applications and types of content found, closing with a summary and recommended actions.

Key findings that should be addressed by Customer ABC:

Personal applications are being installed and used on the network.
End-users are installing and using a variety of non-work related applications that can elevate business and security risks.

Applications that can be used to conceal activity were found.
IT savvy employees are using applications that can conceal their activity. Examples of these types of applications include external proxies, remote desktop access and non-VPN related encrypted tunnel. Visibility into who is using these applications, and for what purpose should be investigated.

Applications that can lead to data loss were detected.
File transfer applications (peer-to-peer and/or browser-based) are in use, exposing Customer ABC to significant security, data loss, compliance and possible copyright infringement risks.

Applications used for personal communications were found.
Employees are using a variety of applications that enable personal communications. Examples include instant messaging, webmail, and VoIP/video conferencing. These types of applications can introduce productivity loss, compliance and business continuity risks.

Bandwidth hogging, time consuming applications are in use.
Media and social networking applications were found. Both of these types of applications are known to consume corporate bandwidth and employee time.

Business Risks Introduced by High Risk Application Traffic

The potential business risks that can be introduced by the applications traversing the network are determined by looking at the behavioral characteristics of the high risk applications (those that carry a risk rating of 4 or 5 on a scale of 1-5). Each of the behavioral characteristics can introduce business risks. Application file transfer can lead to data leakage; ability to evade detection or tunnel other applications can lead to compliance risks; high bandwidth consumption equates to increased operational costs and applications that are prone to malware or vulnerabilities can introduce business continuity risks. Identifying the risks an application poses to is the first step towards effectively managing the related business risks.

A summary of the business risk calculation is shown in figure 1. Appendix A has a complete description of the business risks.

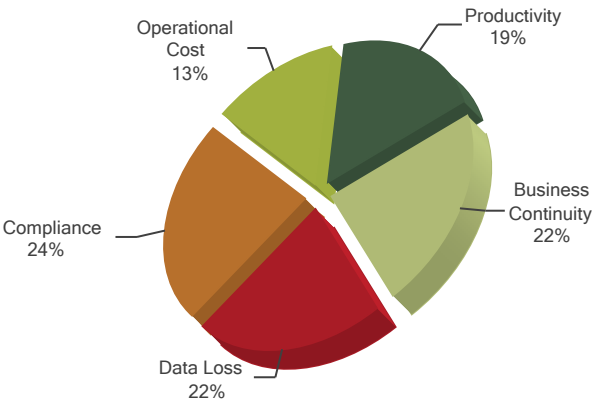


Figure 1: Business risk breakdown of Top High Risk Applications

Top High Risk Applications in Use

The high risk applications (risk rating of 4 or 5) sorted by category, subcategory and bytes consumed are shown below. The ability to view the application along with its respective category, subcategory and technology can be useful when discussing the business value and the potential risks that the applications pose with the respective users or groups of users.

Key observations on the 149 high risk applications:

Activity Concealment:
Proxy (8) and remote access (4) applications were found. In addition, non-VPN related encrypted tunnel applications were detected. IT savvy employees are using these applications with increasing frequency to conceal activity and in so doing, can expose Customer ABC to compliance and data loss risks.

File transfer/data loss/copyright infringement:
P2P applications (16) and browser-based file sharing applications (20) were found. These applications expose Customer ABC to data loss, possible copyright infringement, compliance risks and can act as a threat vector.

Personal communications:
A variety of applications that are commonly used for personal communications were found including instant messaging (10), webmail (16), and VoIP/video (4) conferencing. These types of applications expose Customer ABC to possible productivity loss, compliance and business continuity risks.

Bandwidth hogging:
Applications that are known to consume excessive bandwidth including photo/video (25), audio (2) and social networking (15) were detected. These types of applications represent an employee productivity drain and can consume excessive amounts of bandwidth and can act as potential threat vectors.

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
4	concur	business-systems	general-business	browser-based	25,510,321	651
5	google-docs-base	business-systems	office-programs	browser-based	41,633,763,580	14,895
4	ms-groove	business-systems	office-programs	peer-to-peer	8,694,941	55
5	google-docs-enterprise	business-systems	office-programs	browser-based	32,856	4
4	ms-update	business-systems	software-update	client-server	24,395,025,867	85,182
4	egnyte	business-systems	storage-backup	browser-based	30,215,234	465
4	sosbackup	business-systems	storage-backup	client-server	115,240	2
4	ms-exchange	collaboration	email	client-server	90,489,681,905	838,610
5	smtp	collaboration	email	client-server	52,324,415,049	229,232
4	gmail-base	collaboration	email	browser-based	19,770,419,222	266,309
4	hotmail	collaboration	email	browser-based	6,866,089,186	219,156
4	lotus-notes-base	collaboration	email	client-server	3,790,633,781	91,208
4	aim-mail	collaboration	email	browser-based	2,491,264,136	43,312
4	daum-mail	collaboration	email	browser-based	489,740,012	98
5	horde	collaboration	email	browser-based	169,785,104	5,701
4	netease-mail	collaboration	email	browser-based	153,522,284	3,922
4	squirrelmail	collaboration	email	browser-based	151,349,028	4,311
4	qq-mail	collaboration	email	browser-based	25,783,996	1,420
4	gmail-enterprise	collaboration	email	browser-based	7,152,024	61
4	outlook-web	collaboration	email	browser-based	4,528,330	196
4	mail.ru-mail	collaboration	email	browser-based	2,024,370	108
4	yandex-mail	collaboration	email	browser-based	1,846,624	19
4	blackberry	collaboration	email	client-server	1,286,040	415
4	imap	collaboration	email	client-server	1,190,047	943
4	roundcube	collaboration	email	browser-based	1,134,478	74
4	telenet-webmail	collaboration	email	browser-based	509,056	40
4	gmx-mail	collaboration	email	browser-based	489,832	96
4	pop3	collaboration	email	client-server	58,248	28
4	web-de-mail	collaboration	email	browser-based	44,616	5
4	yahoo-im-base	collaboration	instant-messaging	client-server	874,050,333	100,797
4	imo	collaboration	instant-messaging	browser-based	547,815,233	31,610
4	google-talk-base	collaboration	instant-messaging	client-server	13,515,765	1,211
5	ebuddy	collaboration	instant-messaging	browser-based	11,074,451	584
4	aim-express-base	collaboration	instant-messaging	browser-based	10,097,763	1,181
4	qq-base	collaboration	instant-messaging	client-server	4,804,698	430
5	jabber	collaboration	instant-messaging	client-server	466,698	3
4	gadu-gadu	collaboration	instant-messaging	client-server	136,596	12
4	msn-base	collaboration	instant-messaging	client-server	65,323	47
4	mibbit	collaboration	instant-messaging	browser-based	19,242	6
4	live-meeting	collaboration	internet-conferencing	client-server	2,317,397,820	13,829
4	genesys-base	collaboration	internet-conferencing	client-server	260,804,441	4,902
4	att-connect	collaboration	internet-conferencing	client-server	136,964,816	4,220
4	facebook-base	collaboration	social-networking	browser-based	13,506,875,716	959,886
5	netlog	collaboration	social-networking	browser-based	636,715,936	8,801
4	sina-weibo-base	collaboration	social-networking	browser-based	397,538,146	27,239
4	orkut	collaboration	social-networking	browser-based	45,790,011	229
4	facebook-posting	collaboration	social-networking	browser-based	33,596,924	319
4	odnoklassniki-base	collaboration	social-networking	browser-based	32,705,456	1,526
4	vkontakte-base	collaboration	social-networking	browser-based	24,921,858	763
5	stumbleupon	collaboration	social-networking	browser-based	23,888,840	7,939
4	plaxo	collaboration	social-networking	browser-based	20,220,672	1,899
4	myspace-base	collaboration	social-networking	browser-based	5,410,291	220
4	facebook-apps	collaboration	social-networking	browser-based	3,977,542	100
4	cyworld	collaboration	social-networking	browser-based	2,896,214	191

4	me2day	collaboration	social-networking	browser-based	1,401,729	222
4	ameba-now-base	collaboration	social-networking	browser-based	916,096	27
4	twitter-posting	collaboration	social-networking	browser-based	144,134	28
5	skype	collaboration	voip-video	peer-to-peer	3,211,862,084	67,576
4	sip	collaboration	voip-video	peer-to-peer	975,071	6,703
4	msn-voice	collaboration	voip-video	peer-to-peer	382,664	268
4	yahoo-voice	collaboration	voip-video	peer-to-peer	10,479	2
4	blog-posting	collaboration	web-posting	browser-based	24,221,436	1,265
4	dropbox	general-internet	file-sharing	client-server	71,306,108,068	49,057
4	sharefile	general-internet	file-sharing	browser-based	28,965,723,195	329
4	skydrive-base	general-internet	file-sharing	browser-based	12,051,827,913	42,611
4	yousendit-base	general-internet	file-sharing	browser-based	3,169,186,574	3,309
5	ftp	general-internet	file-sharing	client-server	2,972,890,312	159,576
5	webdav	general-internet	file-sharing	browser-based	2,374,813,805	743,167
4	rapidshare	general-internet	file-sharing	browser-based	2,229,394,510	4,674
4	4shared	general-internet	file-sharing	browser-based	895,149,103	3,335
5	dl-free	general-internet	file-sharing	browser-based	314,531,348	16
4	sendspace	general-internet	file-sharing	browser-based	196,068,719	39
4	google-drive-web	general-internet	file-sharing	browser-based	179,280,129	3,064
5	bittorrent	general-internet	file-sharing	peer-to-peer	141,849,043	2,919
4	docstoc-base	general-internet	file-sharing	browser-based	107,144,990	1,245
4	live-mesh-base	general-internet	file-sharing	client-server	64,812,019	3,652
4	mediafire	general-internet	file-sharing	browser-based	27,960,135	544
5	xunlei	general-internet	file-sharing	peer-to-peer	9,447,431	237
4	tftp	general-internet	file-sharing	client-server	6,378,966	124
4	leapfile	general-internet	file-sharing	browser-based	1,866,442	60
4	office-live	general-internet	file-sharing	client-server	1,764,052	486
5	fileserve	general-internet	file-sharing	browser-based	1,758,672	121
4	putlocker	general-internet	file-sharing	browser-based	911,649	49
4	divshare	general-internet	file-sharing	browser-based	806,216	34
4	megaupload	general-internet	file-sharing	browser-based	655,720	40
4	file-host	general-internet	file-sharing	browser-based	279,684	12
5	emule	general-internet	file-sharing	peer-to-peer	146,246	12,291
4	qq-download	general-internet	file-sharing	peer-to-peer	139,589	13
4	fs2you	general-internet	file-sharing	browser-based	26,550	146
5	imesh	general-internet	file-sharing	peer-to-peer	20,396	6
5	flashget	general-internet	file-sharing	peer-to-peer	17,496	8
5	ares	general-internet	file-sharing	peer-to-peer	6,456	5
4	sugarsync	general-internet	file-sharing	client-server	2,466	3
5	hotfile	general-internet	file-sharing	browser-based	1,728	2
4	ifolder	general-internet	file-sharing	client-server	860	1
5	filesonic	general-internet	file-sharing	browser-based	290	2
4	web-browsing	general-internet	internet-utility	browser-based	1,022,566,846,826	22,179,799
4	flash	general-internet	internet-utility	browser-based	158,436,800,881	156,867
5	rss	general-internet	internet-utility	client-server	4,848,499,935	48,434
4	web-crawler	general-internet	internet-utility	browser-based	305,837,941	1,446
4	google-desktop	general-internet	internet-utility	client-server	17,393,181	1,744
4	mobile-me	general-internet	internet-utility	browser-based	2,827,976	22
4	zamzar	general-internet	internet-utility	browser-based	1,896,535	87
4	apple-appstore	general-internet	internet-utility	client-server	5,196	1
5	http-audio	media	audio-streaming	browser-based	30,632,503,680	5,861
4	pandora-tv	media	audio-streaming	browser-based	85,676	8
5	youtube-base	media	photo-video	browser-based	794,438,117,672	64,230
4	rtmpt	media	photo-video	browser-based	143,575,265,482	467,568
5	http-video	media	photo-video	browser-based	74,698,881,187	15,479
5	asf-streaming	media	photo-video	browser-based	20,214,822,137	625

4	dailymotion	media	photo-video	browser-based	4,294,514,400	3,018
5	vimeo	media	photo-video	browser-based	4,097,890,325	3,983
4	justin.tv	media	photo-video	browser-based	1,334,745,030	144
5	tudou	media	photo-video	browser-based	898,937,697	479
4	rtmp	media	photo-video	browser-based	726,458,006	716
5	youku	media	photo-video	browser-based	543,126,119	231
4	limelight	media	photo-video	browser-based	286,203,546	1,064
4	rtmpe	media	photo-video	browser-based	283,322,921	323
4	ppstream	media	photo-video	peer-to-peer	140,748,509	4,627
4	youtube-safety-mode	media	photo-video	browser-based	140,135,860	16
4	yahoo-douga	media	photo-video	browser-based	133,573,064	788
4	youtube-uploading	media	photo-video	browser-based	84,975,512	20
4	sky-player	media	photo-video	client-server	66,149,998	44
5	brightcove	media	photo-video	browser-based	33,028,117	275
4	mogulus	media	photo-video	browser-based	23,090,336	198
5	funshion	media	photo-video	client-server	16,255,497	786
4	pplive	media	photo-video	peer-to-peer	3,178,580	250
4	metacafe	media	photo-video	browser-based	1,628,462	128
5	sopcast	media	photo-video	peer-to-peer	16,360	13
4	veetle	media	photo-video	browser-based	10,148	2
4	socialtv	media	photo-video	browser-based	1,643	1
4	ssl	networking	encrypted-tunnel	browser-based	480,191,784,585	13,850,959
4	ssh	networking	encrypted-tunnel	client-server	4,764,041,770	65,330
5	hamachi	networking	encrypted-tunnel	peer-to-peer	603,545,587	28,287
4	tor	networking	encrypted-tunnel	client-server	280,314,014	4,542
4	dns	networking	infrastructure	network-protocol	7,823,820,284	131,889,828
4	icmp	networking	ip-protocol	network-protocol	2,687,618,962	12,414,893
5	http-proxy	networking	proxy	browser-based	203,458,544,016	27,556,042
5	cgiproxy	networking	proxy	browser-based	972,202,458	14,073
5	glype-proxy	networking	proxy	browser-based	142,123,159	2,782
5	kproxy	networking	proxy	browser-based	4,902,156	282
5	phproxy	networking	proxy	browser-based	1,950,120	44
4	labnol-proxy	networking	proxy	browser-based	561,837	16
5	coralcdn-user	networking	proxy	browser-based	316,520	17
5	guardster	networking	proxy	browser-based	4,986	2
4	ms-rdp	networking	remote-access	client-server	854,849,154	353
5	logmein	networking	remote-access	client-server	461,110,419	2,238
5	x11	networking	remote-access	client-server	182,507,954	55
5	vnc-base	networking	remote-access	client-server	165,937,418	18

Figure 2: High risk applications (rating of 4 or 5) that are traversing the network.

Application Characteristics That Determine Risk

The Palo Alto Networks research team uses the application behavioral characteristics to determine a risk rating of 1 through 5. The characteristics are an integral piece of the application visibility that administrators can use to learn more about a new application that they may find on the network and in turn, make a more informed decision about how to treat the application.

Application Behavioral Characteristic Definitions

Prone to misuse used for malicious purposes or is easily configured to expose more than intended. Examples include external proxy, remote access, and P2P filesharing applications.

Tunnels other applications able to transport other applications. Examples include SSH and SSL as well as UltraSurf, TOR and RTSP, RTMPT.

Has known vulnerabilities the application has had known vulnerability exploits.

Transfers files able to transfer files from one network to another. Examples include filesharing and file transfer applications of all types, as well as IM and email.

Used by malware has been used to propagate malware, initiate an attack or steal data. Applications that are used by malware include collaboration (email, IM, etc) and general Internet categories (filesharing, Internet utilities).

Consumes bandwidth application consumes 1 Mbps or more regularly through normal use. Examples include P2P, streaming media, as well as software updates and other business applications.

Evasive uses a port or protocol for something other than its intended purpose with intent to ease deployment or hide from existing security infrastructure.

With the knowledge of which applications are traversing the network, their individual characteristics and which employees are using them, Customer ABC is enabled to more effectively decide how to treat the applications traffic through associated security policies. Note that many applications carry multiple behavioral characteristics.

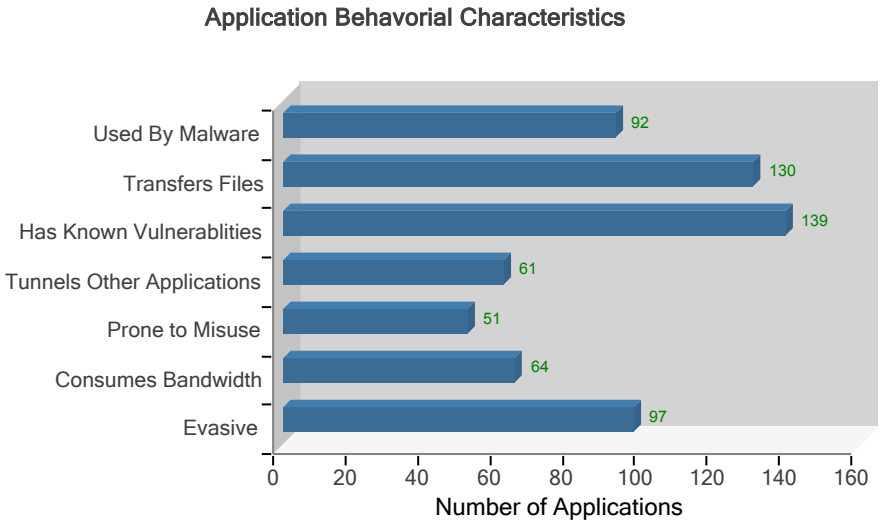


Figure 3: Behavioral characteristics of the high risk applications detected

Top Applications Traversing the Network

The top 35 applications (based on bandwidth consumption), sorted by category and subcategory are shown below. The ability to view the application category, subcategory and technology is complemented by the behavioral characteristics (previous page), resulting in a more complete picture of the business benefit an application may provide.

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
2	ldap	business-systems	auth-service	client-server	18,911,214,404	4,629,859
2	mssql-db	business-systems	database	client-server	26,556,867,539	115,329
3	hp-jetdirect	business-systems	management	client-server	20,233,231,770	143,910
5	google-docs-base	business-systems	office-programs	browser-based	41,633,763,580	14,895
4	ms-update	business-systems	software-update	client-server	24,395,025,867	85,182
3	symantec-av-update	business-systems	software-update	client-server	17,971,076,742	180,476
3	ms-ds-smb	business-systems	storage-backup	client-server	113,310,728,947	2,158,072
3	nfs	business-systems	storage-backup	client-server	10,565,321,342	4
4	ms-exchange	collaboration	email	client-server	90,489,681,905	838,610
5	smtp	collaboration	email	client-server	52,324,415,049	229,232
4	gmail-base	collaboration	email	browser-based	19,770,419,222	266,309
3	yahoo-mail	collaboration	email	browser-based	13,463,765,796	526,681
3	gotomeeting	collaboration	internet-conferencing	client-server	22,024,086,711	2,774
3	webex-base	collaboration	internet-conferencing	client-server	8,157,947,397	34,883
3	sharepoint-base	collaboration	social-business	browser-based	14,007,827,774	61,172
4	facebook-base	collaboration	social-networking	browser-based	13,506,875,716	959,886
2	twitter-base	collaboration	social-networking	browser-based	8,968,282,256	744,608
4	dropbox	general-internet	file-sharing	client-server	71,306,108,068	49,057
4	sharefile	general-internet	file-sharing	browser-based	28,965,723,195	329
4	skydrive-base	general-internet	file-sharing	browser-based	12,051,827,913	42,611
4	web-browsing	general-internet	internet-utility	browser-based	1,022,566,846,826	22,179,799
4	flash	general-internet	internet-utility	browser-based	158,436,800,881	156,867
3	grooveshark	media	audio-streaming	browser-based	47,864,197,745	82,467
5	http-audio	media	audio-streaming	browser-based	30,632,503,680	5,861
1	shoutcast	media	audio-streaming	client-server	12,657,703,648	288
5	youtube-base	media	photo-video	browser-based	794,438,117,672	64,230
4	rtmpt	media	photo-video	browser-based	143,575,265,482	467,568
5	http-video	media	photo-video	browser-based	74,698,881,187	15,479
5	asf-streaming	media	photo-video	browser-based	20,214,822,137	625
4	ssl	networking	encrypted-tunnel	browser-based	480,191,784,585	13,850,959
2	netbios-ns	networking	infrastructure	network-protocol	34,010,505,778	8,273,281
2	snmp-base	networking	infrastructure	client-server	30,583,933,520	56,569,462
2	msrpc	networking	infrastructure	network-protocol	15,624,336,434	3,124,147
1	ipv6	networking	ip-protocol	network-protocol	10,469,696,734	286,249
5	http-proxy	networking	proxy	browser-based	203,458,544,016	27,556,042

Figure 4: Top applications that are consuming the most bandwidth, sorted by category, subcategory and technology

Key observations on top 35 (out of 464) applications in use:

The most common types of applications are photo-video and email.

Application Subcategories

The subcategory breakdown of all the applications found, sorted by bandwidth consumption provides an excellent summary of where the application usage is heaviest. These data points can help IT organizations more effectively prioritize their application enablement efforts.

Sub-Category	Number of Applications	Bytes Consumed	Sessions Consumed
internet-utility	32	1,214,020,285,176	50,783,569
photo-video	55	1,064,866,249,610	818,925
encrypted-tunnel	8	485,985,389,405	13,956,761
proxy	8	204,580,605,252	27,573,258
email	33	197,573,744,831	2,306,786
file-sharing	45	128,550,470,645	1,063,902
storage-backup	5	123,907,863,739	2,158,567
infrastructure	31	102,264,936,924	211,047,826
audio-streaming	17	101,939,088,942	126,605
software-update	16	55,866,996,572	410,090
office-programs	10	41,945,426,587	31,522
social-networking	46	41,494,440,221	2,292,090
management	22	37,477,819,872	1,377,680
internet-conferencing	10	33,503,329,599	60,988
database	7	30,945,587,431	257,733
auth-service	7	27,243,155,418	8,383,479
remote-access	20	15,382,254,514	74,363
social-business	4	14,187,963,286	64,630
ip-protocol	4	13,157,321,440	12,701,148
general-business	17	10,713,525,925	218,821
erp-crm	4	5,331,079,488	32,679
instant-messaging	27	4,777,865,450	432,037
voip-video	14	3,650,853,188	108,526
web-posting	9	1,587,988,567	5,558
gaming	9	222,273,053	5,243
routing	4	7,350,363	7,772
Grand Total	**464**	**3,961,183,865,498**	**336,300,558**

Figure 5: Subcategory breakdown of all the applications found, sorted by bytes consumed.

Key observations on application subcategories:

The application subcategories that are consuming the highest amount of bandwidth are: internet-utility, photo-video, encrypted-tunnel.

Applications That Use HTTP

The top 25 applications (based on bandwidth consumed) that use HTTP in some way, shape or form (but may not use port 80) are shown below. Many applications use HTTP to speed deployment and simplify access while non-business applications may use it to bypass security. Knowing exactly which applications use HTTP is a critical datapoint when assembling an application enablement policy.

Risk	HTTP Application	Technology	Bytes	Sessions
4	web-browsing	browser-based	1,022,566,846,826	22,179,799
5	youtube-base	browser-based	794,438,117,672	64,230
5	http-proxy	browser-based	203,458,544,016	27,556,042
4	flash	browser-based	158,436,800,881	156,867
4	rtmpt	browser-based	143,575,265,482	467,568
4	ms-exchange	client-server	90,489,681,905	838,610
5	http-video	browser-based	74,698,881,187	15,479
4	dropbox	client-server	71,306,108,068	49,057
3	grooveshark	browser-based	47,864,197,745	82,467
5	google-docs-base	browser-based	41,633,763,580	14,895
5	http-audio	browser-based	30,632,503,680	5,861
4	sharefile	browser-based	28,965,723,195	329
4	ms-update	client-server	24,395,025,867	85,182
3	gotomeeting	client-server	22,024,086,711	2,774
5	asf-streaming	browser-based	20,214,822,137	625
4	gmail-base	browser-based	19,770,419,222	266,309
3	symantec-av-update	client-server	17,971,076,742	180,476
2	msrpc	network-protocol	15,624,336,434	3,124,147
3	sharepoint-base	browser-based	14,007,827,774	61,172
4	facebook-base	browser-based	13,506,875,716	959,886
3	yahoo-mail	browser-based	13,463,765,796	526,681
1	shoutcast	client-server	12,657,703,648	288
4	skydrive-base	browser-based	12,051,827,913	42,611
2	twitter-base	browser-based	8,968,282,256	744,608
3	webex-base	client-server	8,157,947,397	34,883

Figure 6: Top HTTP applications identified ranked in terms of bytes consumed.

Key observations on top 25 (out of 349) HTTP applications in use:

There is a mix of both work and non-work related applications traversing the network that can use HTTP in some way or another.

Top URL Categories in Use

Identifying and controlling both the applications traversing the network and the web sites a user is allowed to visit is an ideal approach to safely enabling applications. As a result, organizations are protected from a full spectrum of legal, regulatory, productivity and resource utilization risks. The most commonly visited URL categories are shown in the table below.

URL Category	Count
business-and-economy	12,324,042
search-engines	4,176,341
content-delivery-networks	3,347,768
unknown	3,288,567
web-advertisements	3,036,954
news-and-media	3,034,400
computer-and-internet-info	3,011,787
private-ip-addresses	1,944,833
shopping	1,888,818
streaming-media	1,626,144
internet-portals	1,549,721
social-networking	1,207,404
web-based-email	962,672
financial-services	703,414
sports	699,224
travel	571,212
society	562,097
auctions	493,282
shareware-and-freeware	430,405
reference-and-research	379,204
entertainment-and-arts	353,828
personal-sites-and-blogs	341,728
motor-vehicles	251,791
dynamically-generated-content	233,509
computer-and-internet-security	206,833

Figure 7: Top URL categories visited

Key observations on the top 25 most frequently visited URLs visited:

The URL category report shows a mix of work and non-work related web activity.

Application Vulnerabilities Discovered

The increased visibility into the applications on the network, regardless of port hopping, tunneling or other evasive tactics that may be used, extends into vulnerability exploit protection to ensure that the threat is detected and blocked. The application vulnerabilities discovered on the network, ranked by severity and count are shown in the table below.

Threat Name	Application	Category	Severity	Count
Microsoft SQL Server Stack Overflow Vulnerability	mssql-mon	code-execution	Critical	964
Microsoft ASP.Net Information Leak brute force Attempt	web-browsing	brute-force	Critical	781
Microsoft ASP.Net Information Leak brute force Attempt	flash	brute-force	Critical	25
Microsoft IIS ASP.NET NULL Byte Injection Information Disclosure Vulnerability	hotmail	info-leak	Critical	10
Microsoft ASP.Net Information Leak brute force Attempt	silverlight	brute-force	Critical	9
Microsoft Windows Print Spooler Service Format String Vulnerability	netbios-dg	code-execution	Critical	5
Oracle Java SE Remote Java Runtime Environment Remote Code Execution Vulnerability	web-browsing	code-execution	Critical	4
OpenSSL SSLv2 Malformed Client Key Parsing Buffer Overflow Vulnerability	ssl	code-execution	Critical	2
Blackhole Exploit Kit	web-browsing	code-execution	Critical	2
Microsoft Internet Information Server ISAPI Extension Buffer Overflow Vulnerability	http-proxy	code-execution	Critical	1
SIP Max-Forwards Header Field Overflow	sip	overflow	High	93,177
HTTP NTLM Authentication Brute Force Attack	http-proxy	brute-force	High	83,858
MIT Kerberos kadmind RPC Library Unix Authentication Stack Overflow Vulnerability	rpc	code-execution	High	7,309
HTTP NTLM Authentication Brute Force Attack	apple-update	brute-force	High	3,627
HTTP Forbidden Brute Force Attack	http-proxy	brute-force	High	1,696
Fragroute Evasion Attack For Unknown-tcp Traffic	unknown-tcp	code-execution	High	1,043
HTTP: User Authentication Brute-force Attempt	sharepoint-base	brute-force	High	743
HTTP Forbidden Brute Force Attack	sharepoint-base	brute-force	High	742
HTTP Forbidden Brute Force Attack	web-browsing	brute-force	High	636
HTTP NTLM Authentication Brute Force Attack	facebook-base	brute-force	High	556
FTP: login brute force attempt	ftp	brute-force	High	520
HTTP NTLM Authentication Brute Force Attack	twitter-base	brute-force	High	501
HTTP NTLM Authentication Brute Force Attack	hotmail	brute-force	High	359
HTTP NTLM Authentication Brute Force Attack	rtmpt	brute-force	High	341
HTTP: User Authentication Brute-force Attempt	sharepoint-documents	brute-force	High	304

Figure 8: Top vulnerabilities identified, sorted by severity and count.

Key observations on the 25 most commonly detected (out of 537) exploits:

The Palo Alto Networks next-generation firewall is providing visibility into vulnerability exploits traversing the network regardless of port or protocol.

Of the 537 vulnerabilities found, 4% are critical, 25% are high and 4% are medium severity. The remainder are low severity or informational.

Spyware and Viruses Discovered on the Network

The increased visibility into the applications on the network, regardless of port hopping, tunneling or other evasive tactics that may be used, helps ensure that spyware, the associated command and control traffic and viruses are detected and blocked. Examples of spyware and viruses discovered on the network are shown in figures 9 and 10 below.

Threat Name	Application	Type	Severity	Count
ZeroAccess.Gen Command and Control Traffic	unknown-udp	spyware phone home	Critical	3,051,614
Bot: Mariposa Command and Control	unknown-udp	spyware phone home	Critical	105,675
TDL4 DNS Request Traffic	dns	spyware phone home	Critical	465
Alueron Command and Control Traffic	http-proxy	spyware phone home	Critical	292
Win32.Conficker.C p2p	unknown-udp	spyware phone home	Critical	190
ZeroAccess.Gen Command and Control Traffic	bittorrent	spyware phone home	Critical	14
Conficker DNS Request	dns	spyware download	High	200,277
Trojan.agent:orgnet.pl	dns	Suspicious DNS	Medium	33,348
Trojan.inject:comee.pl	dns	Suspicious DNS	Medium	1,974
generic:8jc3b0a2a97ftbll0cza.com	dns	Suspicious DNS	Medium	1,477
Suspicious user-agent strings	web-browsing	spyware phone home	Medium	1,304
Backdoor.bredolab:bhostdb.webtelmex.net.mx	dns	Suspicious DNS	Medium	1,066
Suspicious user-agent strings	http-proxy	spyware phone home	Medium	819
generic:spacingtheinsi.su	dns	Suspicious DNS	Medium	705
generic:logging.vitruvian.biz	dns	Suspicious DNS	Medium	544
generic:a.adtpix.com	dns	Suspicious DNS	Medium	543
generic:xxx.p54c9e.com	dns	Suspicious DNS	Medium	373
Virus.sality:s-188-64-85-58.atmcdn.pl	dns	Suspicious DNS	Medium	202
generic:woohoowoo.com	dns	Suspicious DNS	Medium	183
generic:rankey.nefficient.co.kr	dns	Suspicious DNS	Medium	174
Rogue DNS Servers Request	dns	spyware phone home	Medium	167
Trojan.vbkrypt:peasjv.com	dns	Suspicious DNS	Medium	164
Trojan.vbkrypt:gokrxn.com	dns	Suspicious DNS	Medium	151
generic:ws.smartiengine.com	dns	Suspicious DNS	Medium	105
Trojan.jorik:d0m78c.com	dns	Suspicious DNS	Medium	102

Figure 9: Most common spyware found, sorted by severity and count.

Most Common Viruses Discovered

Threat Name	Application	Count
Virus/Win32.WGeneric.dghz	web-browsing	6
HTML/Trojan.redir.ej	web-browsing	2
Virus/Win32.WGeneric.digl	flash	2

Figure 10: Most common viruses found, sorted by count.

Key observations on the most commonly detected (out of 78) spyware and viruses

The Palo Alto Networks next-generation firewall is providing visibility into the viruses and spyware traversing the network, regardless of port or protocol.

The most common type of malware found is spyware phone home.

Modern Malware Discovered on the Network

A summary of the 30 files analyzed by WildFire during the seven days prior to 03 December 2012 shows that there were 2 pieces of malware found.

Modern Malware Antivirus Vendor Coverage Summary

A summary of the antivirus (AV) vendors who had coverage for the malware found by WildFire, based on VirusTotal (VT) statistics, is shown below.

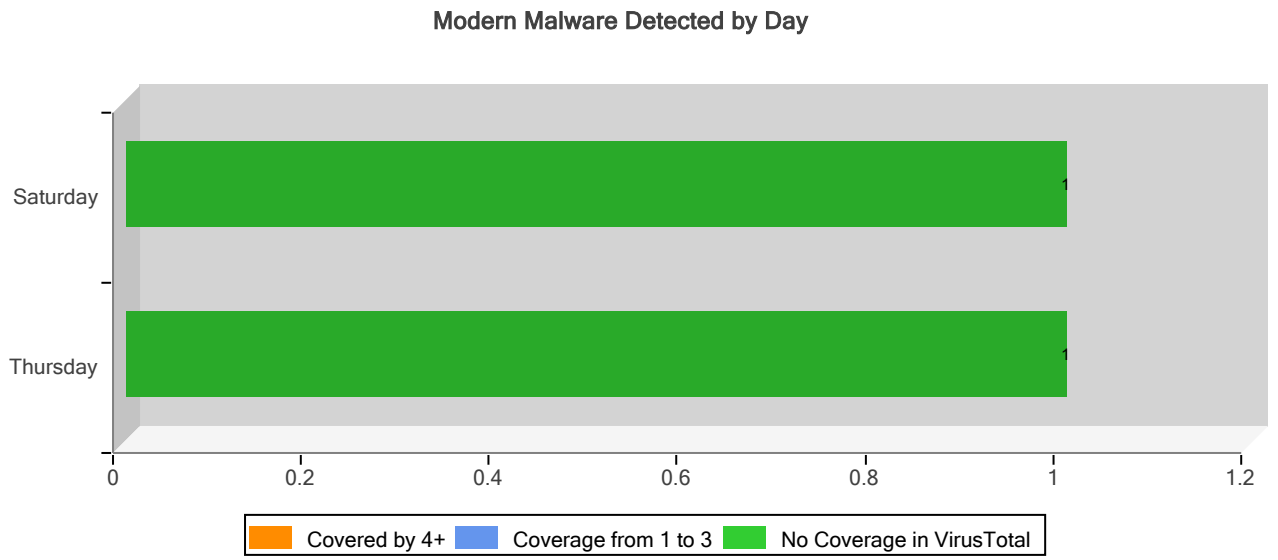


Figure 11: Antivirus vendor coverage for malware detected by WildFire based on VirusTotal statistics.

Sample Malware Detected by WildFire

The list below provides some examples of the malicious files detected by WildFire along with the VirusTotal vendor coverage. The first 30 characters of the filename are shown along with the MD5 checksum which can be used to investigate sample in more detail using the WildFire console.

Filename	MD5	Application	AV Vendor Coverage
about.exe	252cb0f4587c3bb60c9a5b2b50459f07	web-browsing	Unknown to VT
Launcher.exe.deploy	1b185788f9fbb9fe41e56c9e473e867e	web-browsing	Unknown to VT

Figure 12: Examples of malicious files detected by WildFire.

Key observations on the modern malware discovered by WildFire:

The data above shows the presence of 2 malicious files traversing the network that would not have been detected without WildFire analysis. These modern threats are often the leading edge of a sophisticated attack, making detection and remediation a key component of any layered defense strategy.

Files and File Types Traversing the Network

Applications that transfer files have are an integral part of today's business environment. Knowing which types of files and content are traversing the network can help organizations mitigate a range of business and security threats. The table below shows the most common file and content types along with the associated application.

File/Content Name	Data or File	Transfer Direction	Application Used	Count
ZIP	file	Download	web-browsing	22,538
ZIP	file	Download	google-earth	16,839
ZIP	file	Download	symantec-av-update	6,343
ZIP	file	Download	itunes-base	5,087
Microsoft Cabinet (CAB)	file	Download	ms-update	4,344
ZIP	file	Download	sharepoint-base	3,490
FLV File	file	Download	youtube-base	3,287
MP3 File	file	Upload	http-proxy	2,574
ZIP	file	Download	flash	2,414
MP3 File	file	Upload	web-browsing	2,360
Adobe Portable Document Format (PDF)	file	Download	web-browsing	2,329
FLV File	file	Download	flash	2,256
Microsoft PE File	file	Download	web-browsing	2,108
Microsoft PE File	file	Upload	ms-ds-smb	2,043
Quicktime MOV File	file	Download	http-video	1,896
ZIP	file	Upload	sharepoint-documents	1,851
Adobe Portable Document Format (PDF)	file	Upload	smtp	1,771
Windows Executable (EXE)	file	Download	web-browsing	1,459
Java Class File	file	Download	web-browsing	1,420
ZIP	file	Download	sharepoint-documents	1,389
Windows Dynamic Link Library (DLL)	file	Upload	ms-ds-smb	1,386
ZIP	file	Download	silverlight	1,276
MP4 Detected	file	Download	http-video	1,271
ZIP	file	Upload	web-browsing	1,239
ZIP	file	Download	http-proxy	1,174
MP3 File	file	Download	grooveshark	1,082
Windows Dynamic Link Library (DLL)	file	Download	silverlight	998
Microsoft PE File	file	Download	silverlight	998
Microsoft PE File	file	Download	ms-ds-smb	803
Windows Executable (EXE)	file	Download	ms-ds-smb	766

Figure 13: File and content types traversing the network, sorted by type, then by count.

Key observations on the files and content traversing the network:

Files based on type (as opposed to looking only at the file extension) and confidential data patterns (credit card and social security numbers) were detected during the evaluation.

Application Usage by Underlying Technology and Category

The resources consumed (sessions and bytes) based on underlying technology and application subcategory complement the granular application and threat data to provide a more complete summary of the network activity. The charts below show the sessions consumed, based on the underlying application technology and the bytes consumed, based on the application subcategory.

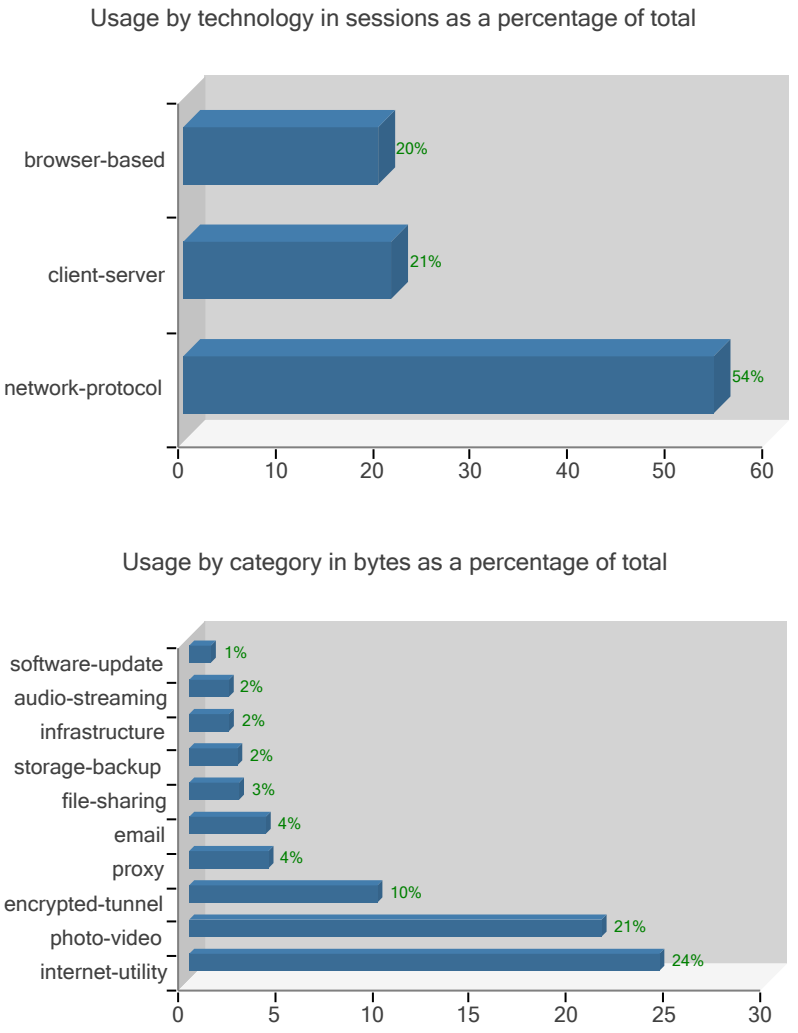


Figure 13: Application usage by category and by technology.

Key observations on application usage by category and technology:

During the evaluation, network-protocol applications consumed 54% of the sessions.

In terms of application usage by category, internet-utility applications consumed 24% of the overall bandwidth.

Findings:

During the planning phase for the Palo Alto Networks analysis, the Customer ABC team explained that their environment is relatively open but the inability to see which applications were traversing the network introduces a wide range of business and security risks. The analysis uncovered the following items.

Activity concealment applications were found. Applications that allowed IT savvy users to conceal their activity and bypass security were found on the network.

P2P and browser-based filesharing application usage. P2P and browser-based file sharing applications were found, exposing Customer ABC to security, data loss and copyright infringement risks.

Streaming media and social networking application usage. Applications that are used for entertainment and socializing (media, audio, social networking) were found on the network. These applications represent secure enablement challenges to IT – how to balance morale, recruitment/retention and end-user satisfaction with productivity, threat exposure, compliance, and data loss risks.

Use of Webmail, IM and VoIP. Examples of these personal use applications were found on the network. Many of these applications can easily bypass firewalls and act as threat vectors as well as being an avenue for data leakage.

Recommendations:

Implement safe application enablement policies.
Like most organizations, Customer ABC lacks fine-grained policy governing application use - because it hasn't historically been necessary or enforceable. With the growth in user-controlled applications, their tendency to carry evasive characteristics to simplify access, and the threats that take advantage of them, we recommend implementing safe application enablement policies that allow, in a controlled manner, the application use.

Address high risk areas such as P2P and browser-based filesharing.
The security and compliance risks associated with these applications may present problems for Customer ABC as employees use these applications to bypass existing traditional controls. Without understanding, categorizing, and mitigating risk in these areas, Customer ABC exposes itself possible unauthorized data transfer, compliance violations and the associated application level threats.

Implement policies dictating use of activity concealment applications.
Proxy, remote access and encrypted tunnel applications are sometimes used by employees who want to conceal their activity. This represents both business and security risks to Customer ABC. Policies dictating the use of these applications should be implemented.

Regain control over streaming media applications.
Customer ABC should look at applying policies to rein in the use of these applications without offending the user community. Possible options would be a time-based schedule, or QoS marking to limit consumption.

Seek Application Visibility and Control
The only way to mitigate the application-level risk is first to know which applications are being used what their business and security risks are, and finally to create and enforce an appropriate firewall policy . There are a few technologies that offer some of the visibility required for certain types of applications, but only next-generation firewalls enable organizations to gain visibility across all application traffic and offer the understanding, control, and scalability to suit enterprises. Accordingly, our recommendation involves deploying a Palo Alto Networks firewall in Customer ABC network and creating safe application enablement policies to ensure that the network is being used according to the organization’s priorities.

Appendix A: Business Risk Definitions

When developing the business risk analysis presented on page 3, the potential impact the application could have on the enterprise and the processes within were taken into account. The resultant risks to the business are defined below.

Productivity

Risk to productivity stems from misuse that can take one of two forms:

- employees are using non-work-related applications instead of doing their job (e.g. social media, personal email, video streaming)
- non-work applications consume so much bandwidth that legitimate applications function poorly (e.g., P2P filesharing, video streaming,)

Compliance

Most organizations must comply with an array of government and business regulations – in the US, this includes GLBA, HIPAA, FD, SOX, FISMA, and PCI. Most of these focus on safeguarding an organization's operational, financial, customer, or employee data. Many of the personal-use applications represent compliance risks to that information either from a data loss perspective or a threat delivery perspective.

Operational Costs

Risks to operational costs come in two flavors – one, having applications and infrastructure that is used inappropriately to such an extent that more must be bought (e.g., WAN circuits upgraded due to streaming video) to ensure that business processes work, and two, incidents and exploits resulting in IT expense (e.g., rebuilding servers or networks following a security incident involving an exploit or virus).

Business Continuity

Business continuity risks refer to applications (or the threats they carry) that can bring down or otherwise make unavailable critical components of certain business processes. Examples include email, transaction processing applications, or public-facing applications harmed by threats or effectively denied service via excessive consumption of resources by non-business applications.

Data Loss

The risk of data loss is the traditional information security set of risks – those associated with the theft, leakage, or destruction of data. Examples include many public thefts of customer data, theft or inadvertent leak of intellectual property, or destruction of data due to a security threat/breach. A variety of threats play a role, including exploits borne by applications (e.g., social media, P2P filesharing, IM, webmail), and non-business-related applications running on enterprise resources (e.g., P2P filesharing, instant messaging, personal webmail).

Appendix B: Key Palo Alto Networks Technologies and Services

Palo Alto Networks next-generation firewalls safely enable applications, users and content across the entire organization using a combination of technologies and services delivered in either a purpose-built hardware platform or in a virtualized form factor.

App-ID: Using multiple traffic classification mechanisms, App-ID accurately identifies the application as soon as the firewall sees it, regardless of which port the application is using or other evasive technique employed. The application identity becomes the basis for all security policy decisions. Unknown applications are categorized for analysis and systematic management.

User-ID: Allows organizations to extend user-based application enablement polices to any user, regardless of which platform they are using. User-ID seamlessly integrates with a wide range of enterprise directories (Microsoft Active Directory, eDirectory, and Open LDAP) and terminal services offerings (Citrix and Microsoft Terminal Services). Integration with Microsoft Exchange, a Captive Portal, and an XML API enable organizations to extend policy to Apple Mac OS X, Apple iOS, and UNIX users that typically reside outside of the domain.

GlobalProtect: Delivers the same safe application enablement policies that are used at the headquarters site, to all users, regardless of location or device. Remote users are automatically and securely connected to the nearest gateway using strong authentication and ss long they are online, they are connected to the corporate network and protected as if they never left the corporate campus. The result is a consistent set of policies, an improved security posture and a reduction in operational costs.

Content-ID: Prevents vulnerability exploits, malware and the related malware generated command-and-control traffic using a uniform signature format and a single pass scanning engine that reduces latency. Threat prevention is applied in full application and protocol context to ensure threats are detected and blocked regardless of evasion techniques used. URL filtering enables policy control over web browsing activity, while file and data filtering help control unauthorized data transfer.

WildFire: Identifies custom malware that is not controlled through traditional signatures by directly executing the files in a cloud-based, virtualized sandbox environment. WildFire observes and monitors more than 100 malicious behaviors and the result is delivered to the administrator. If the file is malicious, a signature is automatically developed and delivered to the user community.

Panorama: Enables organizations to manage a network of Palo Alto Networks firewalls from a central location, balancing the need for global, centralized control with local policy flexibility using features such as templates, and shared policy. With Panorama, all functions of the devices and/or virtual systems under management can be controlled centrally.

Purpose-built hardware or virtualized platform: The entire set of safe application enablement features is available on a family of purpose-built hardware platforms that range from the PA-200, designed for enterprise branch offices, to the PA-5060, which is a high-speed datacenter firewall. The platform architecture is based on a single pass software engine and uses function specific processing for networking, security, threat prevention and management to deliver predictable performance. The exact same firewall functionality that is available in the hardware platforms is also available in the VM-Series virtual firewall, allowing organizations to secure virtualized and cloud-based computing environments.

Appendix C: Additional Information

[Insert additional info]