SECURITY LIFECYCLE REVIEW

Acme

PREPARED BY
Palo Alto Networks
Acme
www.paloaltonetworks.com

Report Period: 8 Days
Tue, Jun 20, 2017 - Tue, Jun 27, 2017

COMPANY**NAME**
INSERT YOUR TAGLINE HERE

TABLE OF CONTENTS

EXECUTIVE SUMMARY
FOR Acme

Key Findings:

- **328** total applications are in use, presenting potential business and security challenges. As critical functions move outside of an organization's control, employees use non-work-related applications, or cyberattackers use them to deliver threats and steal data.
- **75** high-risk applications were observed, including those that can introduce or hide malicious activity, transfer files outside the network, or establish unauthorized communication.
- **6,752** total threats were found on your network, including vulnerability exploits, known and unknown malware, and outbound command and control activity.

The Security Lifecycle Review summarizes the business and security risks facing **Acme**. The data used for this analysis was gathered by Palo Alto Networks during the report time period. The report provides actionable intelligence around the applications, URL traffic, types of content, and threats traversing the network, including recommendations that can be employed to reduce the organization's overall risk exposure.

328
APPLICATIONS IN USE

75
HIGH RISK APPLICATIONS

6,752
TOTAL THREATS

3,580
VULNERABILITY EXPLOITS

22
KNOWN MALWARE

84
UNKNOWN MALWARE

Report Period: 8 Days
Start: Tue, Jun 20, 2017
End: Tue, Jun 27, 2017
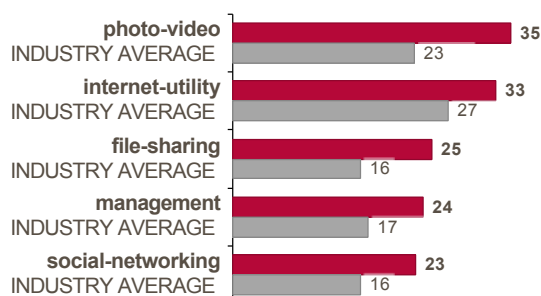
Applications at a Glance

Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision on potential risk versus business benefit.
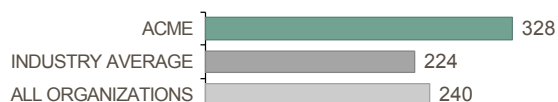
Key Findings:

- High-risk applications such as **photo-video, internet-utility and file-sharing** were observed on the network, which should be investigated due to their potential for abuse.
- **328** total applications were seen on the network across **28** sub-categories, as opposed to an industry average of **224** total applications seen in other **High Technology** organizations.
- **561.42GB** was used by all applications, including **collaboration** with **134.46GB**, compared to an industry average of **624.47GB** in similar organizations.
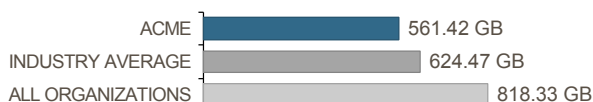
High-Risk Applications

The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.

	Value	Industry Average
photo-video	35	23
internet-utility	33	27
file-sharing	25	16
management	24	17
social-networking	23	16

Number of Applications on Network

ACME	328
INDUSTRY AVERAGE	224
ALL ORGANIZATIONS	240

Bandwidth Consumed by Applications

ACME	561.42 GB
INDUSTRY AVERAGE	624.47 GB
ALL ORGANIZATIONS	818.33 GB

Categories with the Most Applications

The following categories have the most applications variants, and should be reviewed for business relevance.

	Value	Industry Average
business-systems	97	63
collaboration	79	49
general-internet	58	41
media	54	34
networking	40	35

Categories Consuming the Most Bandwidth

Bandwidth consumed by application category shows where application usage is heaviest, and where you could reduce operational resources.

	Value	Industry Average
collaboration	134.46 GB	31.95 GB
networking	123.34 GB	169.63 GB
general-internet	123.26 GB	92.22 GB
media	121.45 GB	32.64 GB
business-systems	58.91 GB	88.94 GB

paloalto NETWORKS®

Applications that Introduce Risk

The top applications (sorted by bandwidth consumed) for application subcategories that introduce risk are displayed below, including industry benchmarks on the number of variants across other **High Technology** organizations. This data can be used to more effectively prioritize your application enablement efforts.

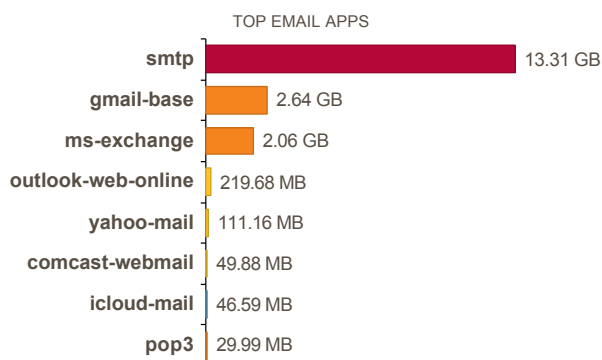**RISK LEVEL**

5 ⎤
4 ⎦ – High
3
2
1

Key Findings:

- A total of **328** applications were seen in your organization, compared to an industry average of **224** in other **High Technology** organizations.
- The most common types of application subcategories are **photo-video, internet-utility and file-sharing**.
- The application subcategories consuming the most bandwidth are **internet-conferencing, encrypted-tunnel and internet-utility**.
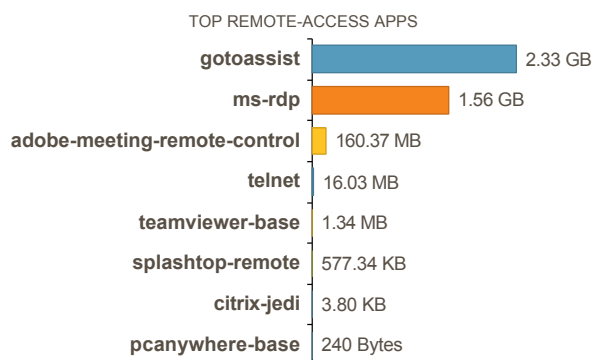
Email – 18.52GB

16 | **9**
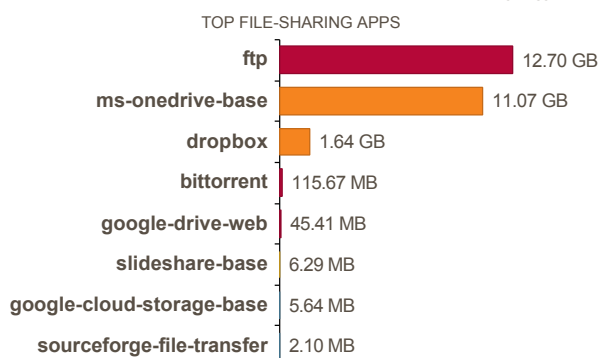APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP EMAIL APPS

App	Bandwidth
smtp	13.31 GB
gmail-base	2.64 GB
ms-exchange	2.06 GB
outlook-web-online	219.68 MB
yahoo-mail	111.16 MB
comcast-webmail	49.88 MB
icloud-mail	46.59 MB
pop3	29.99 MB

Remote-Access – 4.06GB

9 | **8**
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP REMOTE-ACCESS APPS

App	Bandwidth
gotoassist	2.33 GB
ms-rdp	1.56 GB
adobe-meeting-remote-control	160.37 MB
telnet	16.03 MB
teamviewer-base	1.34 MB
splashtop-remote	577.34 KB
citrix-jedi	3.80 KB
pcanywhere-base	240 Bytes

File-Sharing – 25.6GB

25 | **16**
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP FILE-SHARING APPS

App	Bandwidth
ftp	12.70 GB
ms-onedrive-base	11.07 GB
dropbox	1.64 GB
bittorrent	115.67 MB
google-drive-web	45.41 MB
slideshare-base	6.29 MB
google-cloud-storage-base	5.64 MB
sourceforge-file-transfer	2.10 MB

Encrypted-Tunnel – 102.92GB

6 | **6**
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP ENCRYPTED-TUNNEL APPS

App	Bandwidth
ssl	83.79 GB
ssh	18.97 GB
ipsec-esp-udp	160.32 MB
freenet	8.03 MB
ike	261.74 KB
dtls	2.75 KB

paloalto NETWORKS

Instant-Messaging – 306.75MB

12 | 10
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP INSTANT-MESSAGING APPS

App	Value
whatsapp-base	156.57 MB
facebook-chat	79.09 MB
ms-lync-base	45.58 MB
kik	15.63 MB
jabber	4.87 MB
snapchat	1.96 MB
boldchat-logmein	1.67 MB
wechat-base	570.78 KB

Social-Networking – 8.34GB

23 | 16
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP SOCIAL-NETWORKING APPS

App	Value
facebook-base	5.88 GB
twitter-base	1.75 GB
google-plus-base	253.34 MB
linkedin-base	207.68 MB
pinterest-base	101.60 MB
hootsuite	85.57 MB
reddit-base	27.80 MB
tumblr-base	19.67 MB

Photo-Video – 85.63GB

35 | 23
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP PHOTO-VIDEO APPS

App	Value
streampix	16.62 GB
youtube-base	16.15 GB
http-video	14.96 GB
rtcp	10.11 GB
facebook-video	7.44 GB
nfl-streaming	5.65 GB
instagram-base	5.42 GB
rtp-base	2.78 GB

Proxy – 72.24KB

2 | 2
APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP PROXY APPS

App	Value
http-proxy	71.63 KB
socks	620 Bytes

paloalto NETWORKS

Applications that Introduce Risk — Detail

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
5	smtp	collaboration	email	client-server	13.31GB	71157
4	gmail-base	collaboration	email	browser-based	2.64GB	10348
4	ms-exchange	collaboration	email	client-server	2.06GB	1703
3	outlook-web-online	collaboration	email	browser-based	219.68MB	9106
3	yahoo-mail	collaboration	email	browser-based	111.16MB	2087
3	comcast-webmail	collaboration	email	browser-based	49.88MB	462
2	icloud-mail	collaboration	email	client-server	46.59MB	1418
4	pop3	collaboration	email	client-server	29.99MB	155
4	ssl	networking	encrypted-tunnel	browser-based	83.79GB	1927883
4	ssh	networking	encrypted-tunnel	client-server	18.97GB	6289
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	160.32MB	251
5	freenet	networking	encrypted-tunnel	peer-to-peer	8.03MB	12852
2	ike	networking	encrypted-tunnel	client-server	261.74KB	296
1	dtls	networking	encrypted-tunnel	client-server	2.75KB	4
5	ftp	general-internet	file-sharing	client-server	12.7GB	914
4	ms-onedrive-base	general-internet	file-sharing	client-server	11.07GB	1345
4	dropbox	general-internet	file-sharing	client-server	1.64GB	4957
5	bittorrent	general-internet	file-sharing	peer-to-peer	115.67MB	38294
5	google-drive-web	general-internet	file-sharing	browser-based	45.41MB	302
3	slideshare-base	general-internet	file-sharing	browser-based	6.29MB	64
2	google-cloud-storage-base	general-internet	file-sharing	browser-based	5.64MB	37
2	sourceforge-file-transfer	general-internet	file-sharing	client-server	2.1MB	5
1	whatsapp-base	collaboration	instant-messaging	client-server	156.57MB	2789
3	facebook-chat	collaboration	instant-messaging	browser-based	79.09MB	1328
2	ms-lync-base	collaboration	instant-messaging	client-server	45.58MB	30

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	kik	collaboration	instant-messaging	client-server	15.63MB	334
5	jabber	collaboration	instant-messaging	client-server	4.87MB	13
2	snapchat	collaboration	instant-messaging	client-server	1.96MB	76
4	boldchat-logmein	collaboration	instant-messaging	browser-based	1.67MB	164
2	wechat-base	collaboration	instant-messaging	client-server	570.78KB	201
1	streampix	media	photo-video	client-server	16.62GB	171
4	youtube-base	media	photo-video	browser-based	16.15GB	5578
5	http-video	media	photo-video	browser-based	14.96GB	967
1	rtcp	media	photo-video	client-server	10.11GB	677
4	facebook-video	media	photo-video	browser-based	7.44GB	3662
2	nfl-streaming	media	photo-video	browser-based	5.65GB	104
2	instagram-base	media	photo-video	client-server	5.42GB	7593
3	rtp-base	media	photo-video	client-server	2.78GB	664
5	http-proxy	networking	proxy	browser-based	71.63KB	90
5	socks	networking	proxy	network-protocol	620Bytes	1
2	gotoassist	networking	remote-access	browser-based	2.33GB	185721
4	ms-rdp	networking	remote-access	client-server	1.56GB	650
3	adobe-meeting-remote-control	networking	remote-access	browser-based	160.37MB	2
2	telnet	networking	remote-access	client-server	16.03MB	8
3	teamviewer-base	networking	remote-access	client-server	1.34MB	22
1	splashtop-remote	networking	remote-access	client-server	577.34KB	133
2	citrix-jedi	networking	remote-access	client-server	3.8KB	14
2	pcanywhere-base	networking	remote-access	client-server	240Bytes	4
4	facebook-base	collaboration	social-networking	browser-based	5.88GB	50900
2	twitter-base	collaboration	social-networking	browser-based	1.75GB	17459

Notes:

Risk	Application	Category	Sub Category ▲	Technology	Bytes	Sessions
2	google-plus-base	collaboration	social-networking	browser-based	253.34MB	5111
3	linkedin-base	collaboration	social-networking	browser-based	207.68MB	7694
2	pinterest-base	collaboration	social-networking	browser-based	101.6MB	1816
3	hootsuite	collaboration	social-networking	browser-based	85.57MB	1028
1	reddit-base	collaboration	social-networking	browser-based	27.8MB	389
2	tumblr-base	collaboration	social-networking	browser-based	19.67MB	236

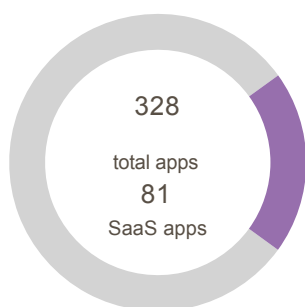**Notes:**

SaaS Applications

SaaS–based application services continue to redefine the network perimeter. Often labeled "shadow IT," most of these services are adopted directly by individual users, business teams, or even entire departments. In order to minimize data security risks you need control over SaaS applications used your network .
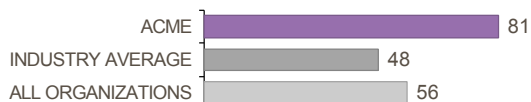
Key Findings

- **File-Sharing** subcategory has the most number of unique SaaS applications.
- In terms of data movement, **vidyo** is the most used SaaS application in your organization.

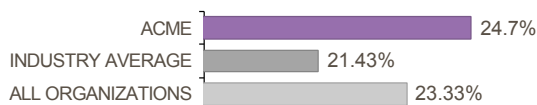**SaaS Applications by Numbers**

Review the applications being used in your organization. To maintain administrative control, adopt SaaS applications that will be managed by your IT team
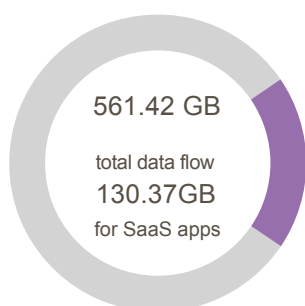

NUMBER OF SAAS APPLICATIONS

ACME	81
INDUSTRY AVERAGE	48
ALL ORGANIZATIONS	56

PERCENTAGE OF ALL APPLICATIONS

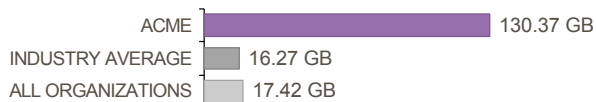|	
ACME	24.7%
INDUSTRY AVERAGE	21.43%
ALL ORGANIZATIONS	23.33%

Donut chart: 328 total apps / 81 SaaS apps

SaaS Application Bandwidth

Monitor the volume of data movement to and from SaaS applications. Understand the nature of the applications and how they are being used

SAAS APPLICATION BANDWIDTH

ACME	130.37 GB
INDUSTRY AVERAGE	16.27 GB
ALL ORGANIZATIONS	17.42 GB

PERCENTAGE OF ALL BANDWIDTH

ACME	23.22%
INDUSTRY AVERAGE	2.6%
ALL ORGANIZATIONS	2.13%

Donut chart: 561.42 GB total data flow / 130.37GB for SaaS apps

paloalto NETWORKS
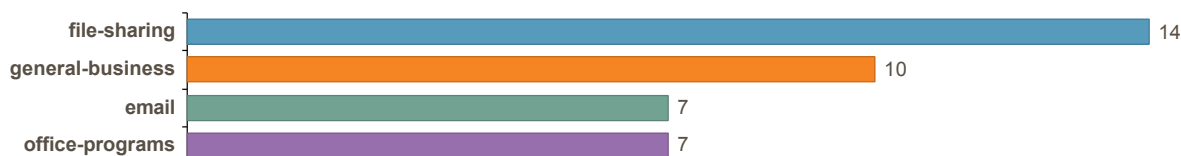
TOP SAAS APPLICATION SUBCATEGORIES

The following displays the number of applications in each application subcategory. This allows you to assess the most used applications organization.

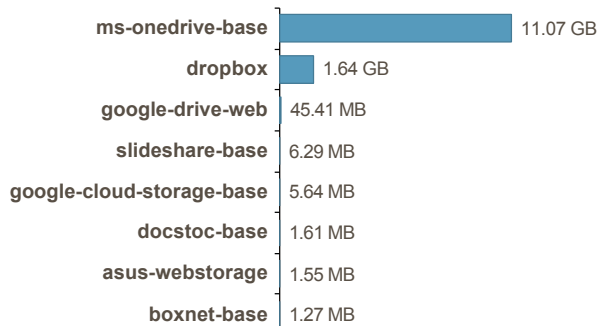**Top SaaS application subcategories by total number of applications**

file-sharing	14
general-business	10
email	7
office-programs	7

The following shows the top used applications by data movement within the subcategories identified above.

File-Sharing – 12.78GB

14 **16**
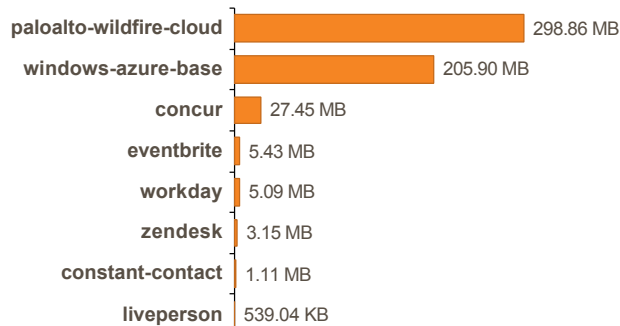APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP FILE-SHARING APPS

ms-onedrive-base	11.07 GB
dropbox	1.64 GB
google-drive-web	45.41 MB
slideshare-base	6.29 MB
google-cloud-storage-base	5.64 MB
docstoc-base	1.61 MB
asus-webstorage	1.55 MB
boxnet-base	1.27 MB

General-Business – 547.6MB

10 **10**
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP GENERAL-BUSINESS APPS

paloalto-wildfire-cloud	298.86 MB
windows-azure-base	205.90 MB
concur	27.45 MB
eventbrite	5.43 MB
workday	5.09 MB
zendesk	3.15 MB
constant-contact	1.11 MB
liveperson	539.04 KB

Email – 3.09GB

7 **9**
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP EMAIL APPS

gmail-base	2.64 GB
outlook-web-online	219.68 MB
yahoo-mail	111.16 MB
comcast-webmail	49.88 MB
icloud-mail	46.59 MB
aim-mail	26.77 MB
gmx-mail	45.02 KB

Office-Programs – 415.74MB

7 **7**
APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP OFFICE-PROGRAMS APPS

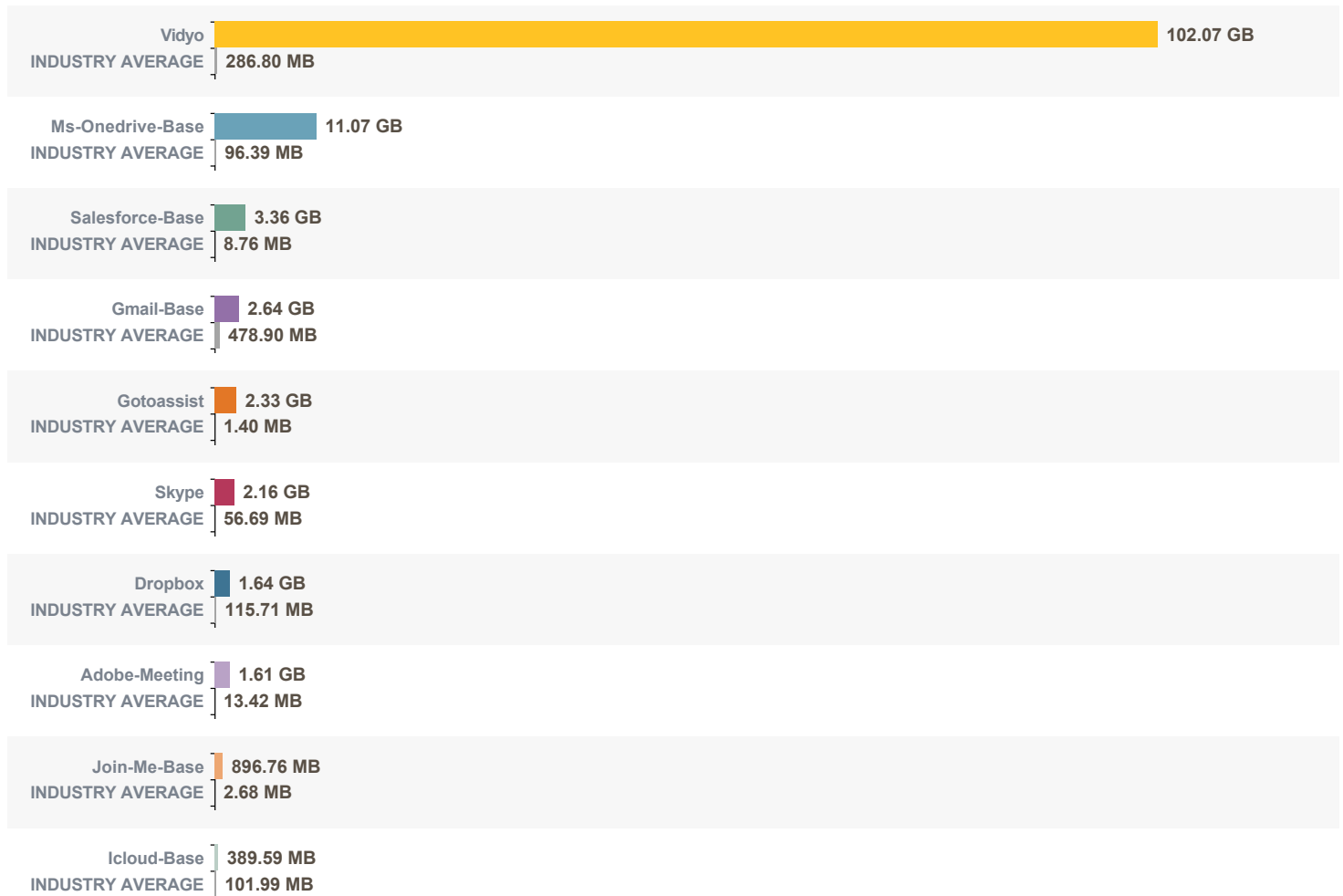|	
google-docs-base	262.75 MB
ms-office365-base	91.35 MB
docusign	45.73 MB
evernote-base	12.10 MB
yahoo-calendar	2.81 MB
office-on-demand	933.08 KB
google-calendar-base	93.05 KB

TOP SAAS APPLICATIONS

The following displays the top 10 SaaS applications used in your organization and the application usage comparison against your industry peers and all other Palo Alto Networks customers.

Top SaaS Applications by Data Movement

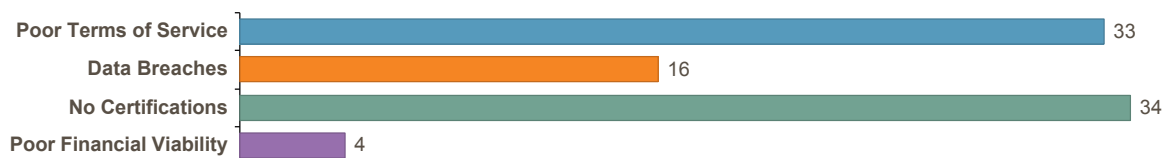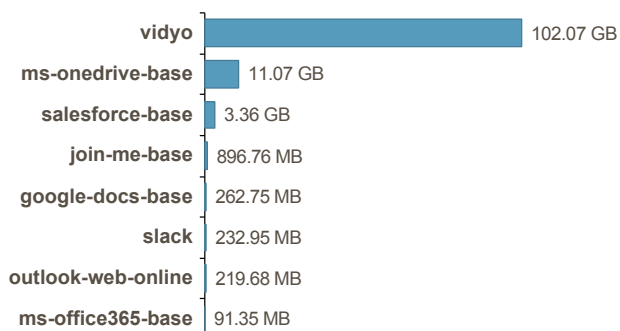|	
Vidyo	102.07 GB
INDUSTRY AVERAGE	286.80 MB
Ms-Onedrive-Base	11.07 GB
INDUSTRY AVERAGE	96.39 MB
Salesforce-Base	3.36 GB
INDUSTRY AVERAGE	8.76 MB
Gmail-Base	2.64 GB
INDUSTRY AVERAGE	478.90 MB
Gotoassist	2.33 GB
INDUSTRY AVERAGE	1.40 MB
Skype	2.16 GB
INDUSTRY AVERAGE	56.69 MB
Dropbox	1.64 GB
INDUSTRY AVERAGE	115.71 MB
Adobe-Meeting	1.61 GB
INDUSTRY AVERAGE	13.42 MB
Join-Me-Base	896.76 MB
INDUSTRY AVERAGE	2.68 MB
Icloud-Base	389.59 MB
INDUSTRY AVERAGE	101.99 MB

SaaS Applications by Hosting Risk

Based on your SaaS usage, it is imperative to regularly review SaaS applications being accessed, who is accessing them, and how they are being used.
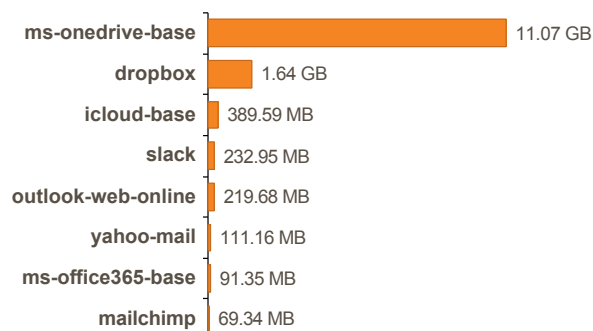The following chart displays the number of applications by each hosting risk characteristic.

Poor Terms of Service	33
Data Breaches	16
No Certifications	34
Poor Financial Viability	4

The following charts display the top applications by bandwidth for each hosting risk characteristic.

Apps with Poor Terms of Service - 118.53GB
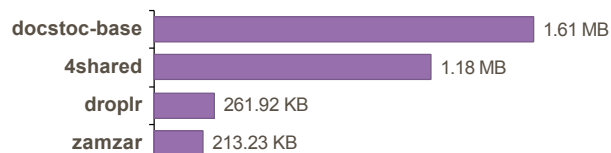
vidyo	102.07 GB
ms-onedrive-base	11.07 GB
salesforce-base	3.36 GB
join-me-base	896.76 MB
google-docs-base	262.75 MB
slack	232.95 MB
outlook-web-online	219.68 MB
ms-office365-base	91.35 MB

Apps with Data Breaches - 13.88GB

ms-onedrive-base	11.07 GB
dropbox	1.64 GB
icloud-base	389.59 MB
slack	232.95 MB
outlook-web-online	219.68 MB
yahoo-mail	111.16 MB
ms-office365-base	91.35 MB
mailchimp	69.34 MB

Apps with No Certifications - 3.35GB

gotoassist	2.33 GB
icloud-base	389.59 MB
paloalto-wildfire-cloud	298.86 MB
yahoo-mail	111.16 MB
comcast-webmail	49.88 MB
icloud-mail	46.59 MB
crashplan	31.98 MB
concur	27.45 MB

Apps with Poor Financial Viability - 3.25MB

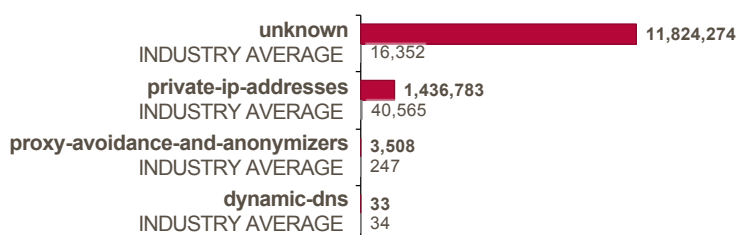|	
docstoc-base	1.61 MB
4shared	1.18 MB
droplr	261.92 KB
zamzar	213.23 KB

URL Activity

Uncontrolled Web surfing exposes organizations to security and business risks, including exposure to potential threat propagation, data loss, or compliance violations. The most common URL categories visited by users on the network are shown below.

Key Findings:

- High-traffic URL categories were observed on the network, including **web-based-email, unknown and business-and-economy**.
- Users visited a total of **82,005,300** URLs during the report time period across **56** categories.
- There was a variety of personal and work-related Web activity present, including visits to potentially risky websites.
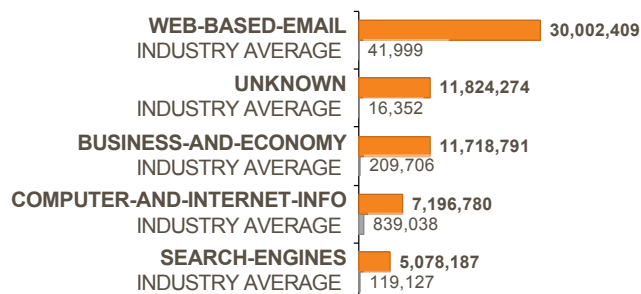
High-Risk URL Categories

The Web is a primary infection vector for attackers, with high-risk URL categories posing an outsized risk to the organization. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unknowns.
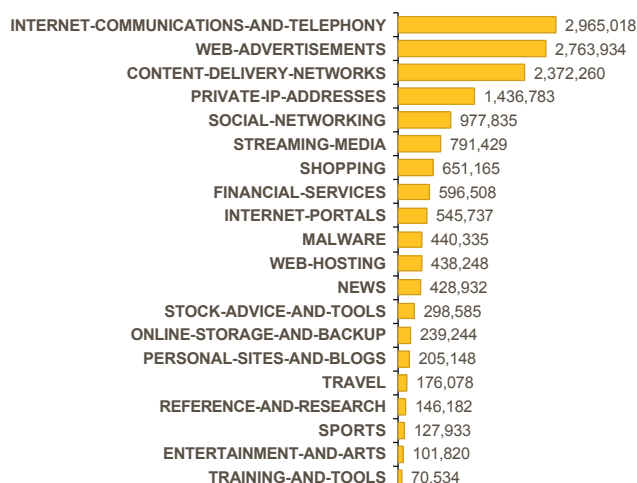
Category	Value
unknown	11,824,274
INDUSTRY AVERAGE	16,352
private-ip-addresses	1,436,783
INDUSTRY AVERAGE	40,565
proxy-avoidance-and-anonymizers	3,508
INDUSTRY AVERAGE	247
dynamic-dns	33
INDUSTRY AVERAGE	34

High-Traffic URL Categories

The top 5 commonly visited URL categories, along with industry benchmarks across your peer group, are shown below.

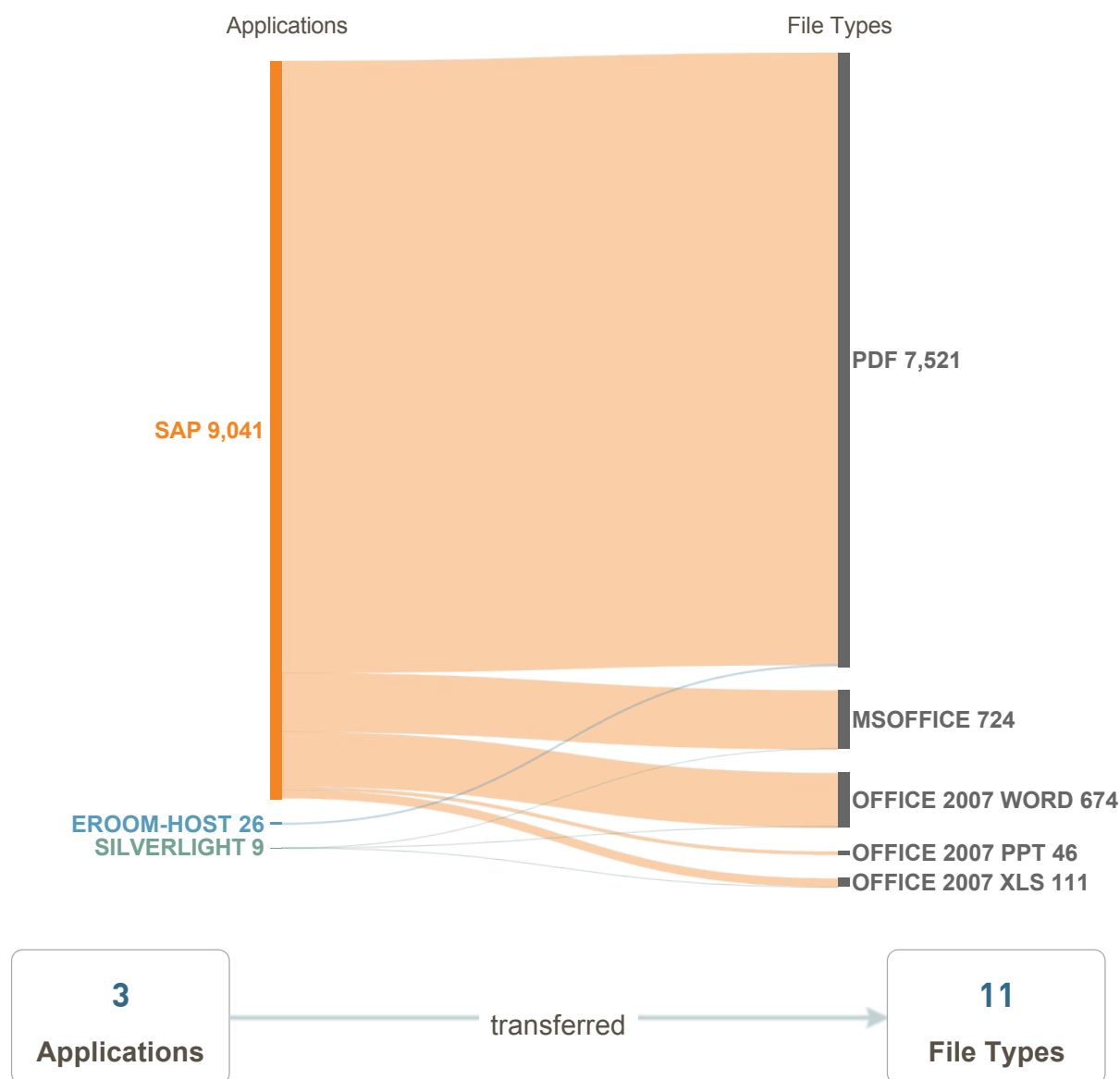| Category	Value
WEB-BASED-EMAIL	30,002,409
INDUSTRY AVERAGE	41,999
UNKNOWN	11,824,274
INDUSTRY AVERAGE	16,352
BUSINESS-AND-ECONOMY	11,718,791
INDUSTRY AVERAGE	209,706
COMPUTER-AND-INTERNET-INFO	7,196,780
INDUSTRY AVERAGE	839,038
SEARCH-ENGINES	5,078,187
INDUSTRY AVERAGE	119,127

Commonly Used URL Categories

The top 20 most commonly visited URL categories are shown below.

Category	Value
INTERNET-COMMUNICATIONS-AND-TELEPHONY	2,965,018
WEB-ADVERTISEMENTS	2,763,934
CONTENT-DELIVERY-NETWORKS	2,372,260
PRIVATE-IP-ADDRESSES	1,436,783
SOCIAL-NETWORKING	977,835
STREAMING-MEDIA	791,429
SHOPPING	651,165
FINANCIAL-SERVICES	596,508
INTERNET-PORTALS	545,737
MALWARE	440,335
WEB-HOSTING	438,248
NEWS	428,932
STOCK-ADVICE-AND-TOOLS	298,585
ONLINE-STORAGE-AND-BACKUP	239,244
PERSONAL-SITES-AND-BLOGS	205,148
TRAVEL	176,078
REFERENCE-AND-RESEARCH	146,182
SPORTS	127,933
ENTERTAINMENT-AND-ARTS	101,820
TRAINING-AND-TOOLS	70,534

File Transfer Analysis

Applications that can transfer files serve an important business function, but they also potentially allow for sensitive data to leave the network or cyber threats to be delivered. Within your organization, **11** file types were delivered via a total of **3** applications. The image below correlates the applications most commonly used to transfer files, along with the most prevalent file and content types observed.

Applications	File Types

SAP 9,041

PDF 7,521

MSOFFICE 724

OFFICE 2007 WORD 674

EROOM-HOST 26
SILVERLIGHT 9

OFFICE 2007 PPT 46
OFFICE 2007 XLS 111

3
Applications

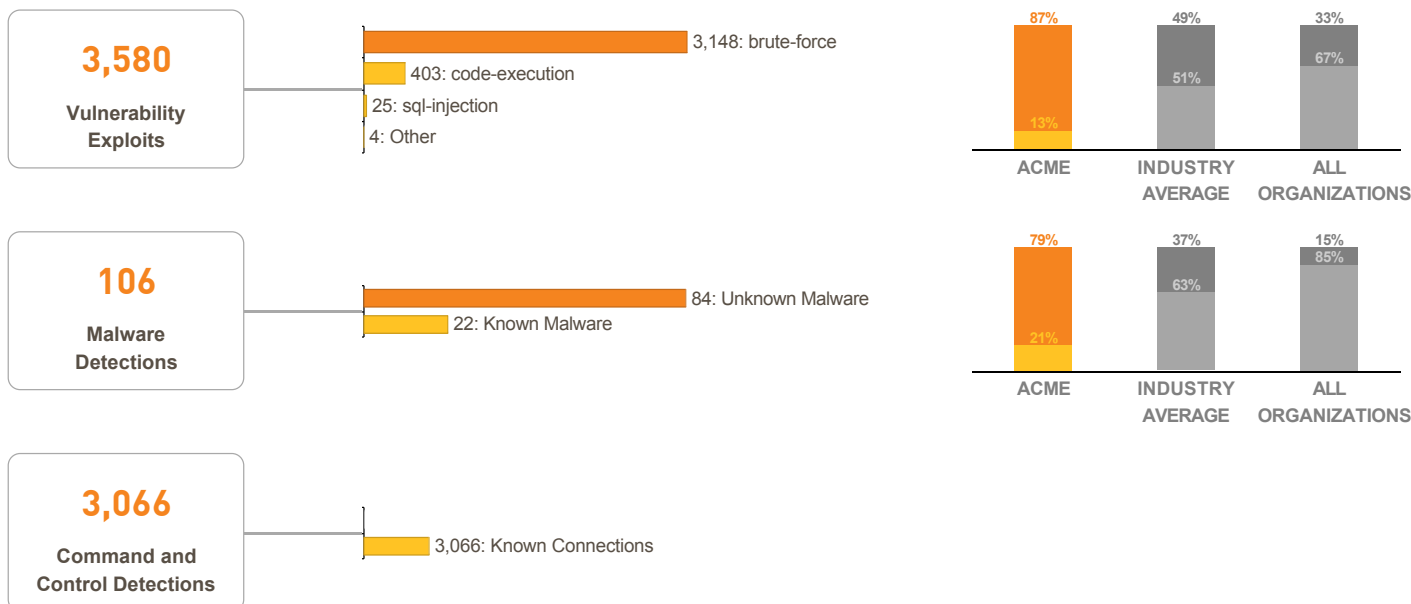transferred →

11
File Types

Threats at a Glance

Understanding your risk exposure, and how to adjust your security posture to prevent attacks, requires intelligence on the type and volume of threats used against your organization. This section details the application vulnerabilities, known and unknown malware, and command and control activity observed on your network.
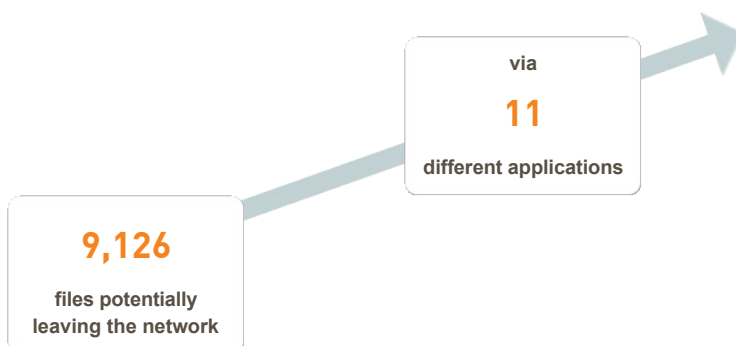
Key Findings:

- **3,580** total vulnerability exploits were observed in your organization, including **brute-force, code-execution and sql-injection**.
- **106** malware events were observed, versus an industry average of **1,346** across your peer group.
- **3,066** total command and control requests were identified, indicating attempts by malware to communicate with attackers to download additional malware, receive instructions, or exfiltrate data.

<table>
<tr><td>

3,580

Vulnerability Exploits

</td><td>

3,148: brute-force
403: code-execution
25: sql-injection
4: Other

</td><td>

87% / 13% — ACME
49% / 51% — INDUSTRY AVERAGE
33% / 67% — ALL ORGANIZATIONS

</td></tr>
<tr><td>

106

Malware Detections

</td><td>

84: Unknown Malware
22: Known Malware

</td><td>

79% / 21% — ACME
37% / 63% — INDUSTRY AVERAGE
15% / 85% — ALL ORGANIZATIONS

</td></tr>
<tr><td>

3,066

Command and Control Detections

</td><td>

3,066: Known Connections

</td><td></td></tr>
</table>

Files Leaving the Network

Transferring files is a required and common part of doing business, but you must maintain visibility into what content is leaving the network via which applications, in order to limit your organization's exposure to data loss.

9,126

files potentially leaving the network

via

11

different applications
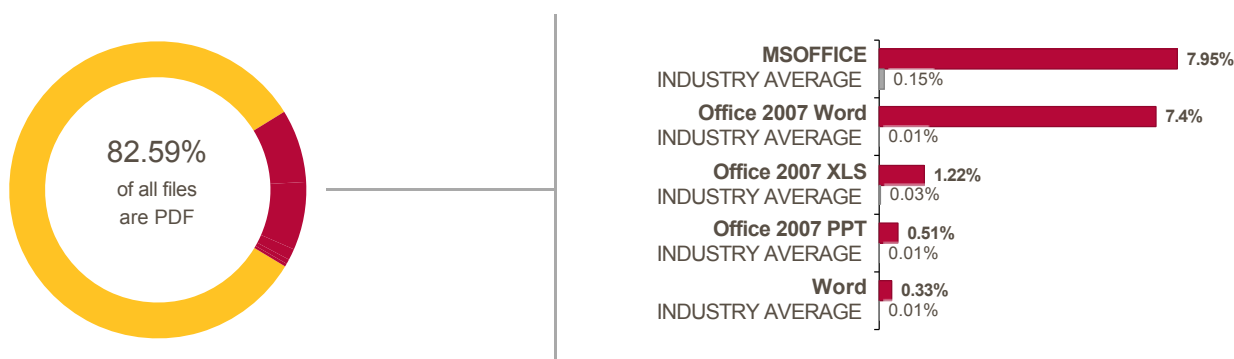
High-Risk and Malicious File Type Analysis

Today's cyber attackers use a variety of file types to deliver malware and exploits, often focusing on content from common business applications present in most enterprise networks. The majority of commodity threats are delivered via executable files, with more targeted and advanced attacks often using other content to compromise networks.

Key Findings:

- A variety of file-types were used to deliver threats, and prevention strategies should cover all major content types.
- You can reduce your attack surface by proactively blocking high-risk file-types, such as blocking executable files downloaded from the Internet, or disallowing RTF files or LNK files, which are not needed in daily business.
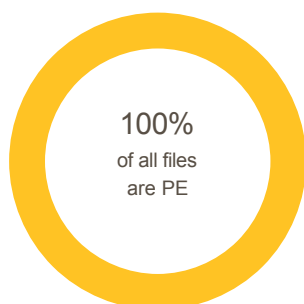
High-Risk File Types

The file types shown represent a greater risk to the organization due to a combination of new vulnerabilities being discovered, existing and unpatched flaws, and prevalence of use in attacks.

82.59%
of all files
are PDF

MSOFFICE	7.95%
INDUSTRY AVERAGE	0.15%
Office 2007 Word	7.4%
INDUSTRY AVERAGE	0.01%
Office 2007 XLS	1.22%
INDUSTRY AVERAGE	0.03%
Office 2007 PPT	0.51%
INDUSTRY AVERAGE	0.01%
Word	0.33%
INDUSTRY AVERAGE	0.01%

Files Delivering Unknown Malware

We recommend investigating the files that may be used to deliver threats both within your organization, and across your peer group. Together, these trends allow you to take preventive action such as blocking high-risk file types across different user groups.
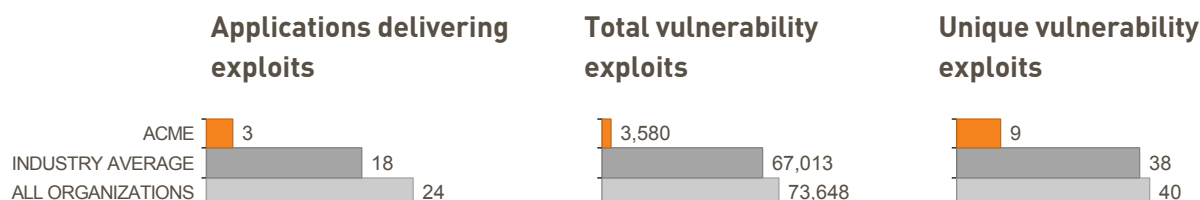

100%
of all files
are PE

Application Vulnerabilities

Application vulnerabilities allow attackers to exploit vulnerable, often unpatched, applications to infect systems, which often represent one of the first steps in a breach. This page details the top five application vulnerabilities attackers attempted to exploit within your organization, allowing you to determine which applications represent the largest attack surface.

Key Findings:

- **3** total applications were observed delivering exploits to your environment.
- **3,580** total vulnerability exploits were observed across the following top three applications: **web-browsing, web-browsing and web-browsing**.
- **9** unique vulnerability exploits were found, meaning attackers continued to attempt to exploit the same vulnerability multiple times.

Applications delivering exploits		Total vulnerability exploits		Unique vulnerability exploits	
ACME	3		3,580		9
INDUSTRY AVERAGE	18		67,013		38
ALL ORGANIZATIONS	24		73,648		40

Vulnerability Exploits per Application (top 5 applications with most detections)

DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY ▼	THREAT TYPE	CVE ID
3,576	**web-browsing**			
9	Microsoft IE GIF Parsing Double Free Vulnerability	Critical	code-execution	CVE-2003-1048
1,573	HTTP Unauthorized Brute Force Attack	High	brute-force	
1,573	HTTP: User Authentication Brute Force Attempt	High	brute-force	
394	Apache Tomcat Windows Installer Default Account Access Vulnerability	High	code-execution	CVE-2011-1889
25	HTTP SQL Injection Attempt	Medium	sql-injection	
1	Microsoft ASP.NET Path Validation Security Bypass Vulnerability	Medium	info-leak	CVE-2004-0847
1	WordPress Cuckootap Theme Arbitrary File Download Vulnerability	Medium	info-leak	
2	**smtp**			
2	QK SMTP Remote Buffer Overflow Vulnerability	Medium	overflow	CVE-2006-5551
2	**ftp**			
2	FTP: login Brute Force attempt	High	brute-force	

Known and Unknown Malware

Applications are the primary vectors used to deliver malware and infect organizations, communicate outbound, or exfiltrate data. Adversaries' tactics have evolved to use the applications commonly found on the network into which traditional security solutions have little or no visibility.

Key Findings:

- **3** total applications were observed delivering malware to your organization, out of **328** total applications on the network.
- Many applications delivering malware are required to run your business, which means you need a solution that can prevent threats, while still enabling the applications.
- While most malware is delivered over HTTP or SMTP, advanced attacks will often use other applications, including those on non-standard ports or employing other evasive behavior.

KNOWN MALWARE		UNKNOWN MALWARE
2	**SMTP** INDUSTRY AVERAGE	68
19		32
16	**WEB-BROWSING** INDUSTRY AVERAGE	**16**
16		16

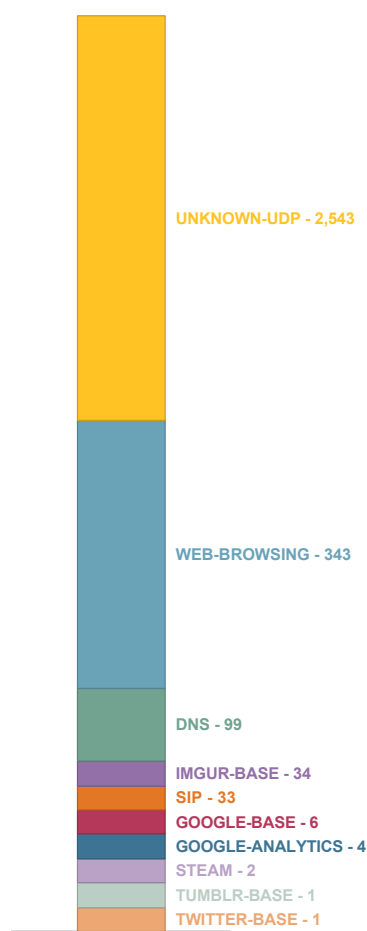| KNOWN MALWARE		UNKNOWN MALWARE
4	**MEDIAFIRE** INDUSTRY AVERAGE	
2		8

3

applications found
delivering malware

Command and Control Analysis

Command-and-control (CnC) activity could indicates a host in the network has been infected by malware, and may be attempting to connect outside of the network to malicious actors, reconnaissance attempts from outside, or other command-and-control traffic. Understanding and preventing this activity is critical, as attackers use CnC to deliver additional malware, provide instruction, or exfiltrate data.
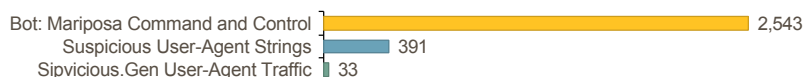
Key Findings:

- **10** total applications were used for command-and-control communication.
- **3,066** total command-and-control requests were seen on your network.
- **99** total suspicious DNS queries were observed.
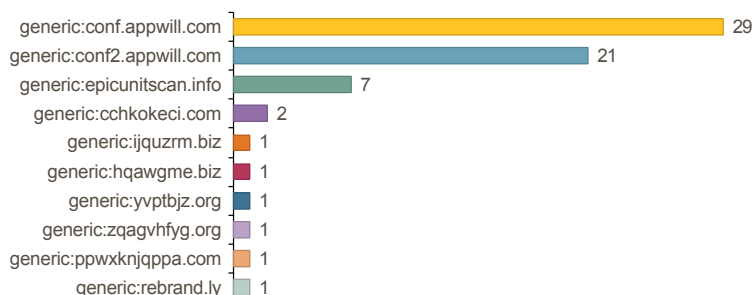
COMMAND AND CONTROL ACTIVITY BY APPLICATION

UNKNOWN-UDP - 2,543

WEB-BROWSING - 343

DNS - 99

IMGUR-BASE - 34

SIP - 33

GOOGLE-BASE - 6

GOOGLE-ANALYTICS - 4

STEAM - 2

TUMBLR-BASE - 1

TWITTER-BASE - 1

Spyware Phone Home: 2,967

This image below represents compromised hosts attempting to connect to external malicious CnC servers.

Bot: Mariposa Command and Control	2,543
Suspicious User-Agent Strings	391
Sipvicious.Gen User-Agent Traffic	33

Suspicious DNS Queries: 99

While DNS is a common and necessary application, it is also commonly used to hide outbound CnC communication, as shown in the chart below.

generic:conf.appwill.com	29
generic:conf2.appwill.com	21
generic:epicunitscan.info	7
generic:cchkokeci.com	2
generic:ijquzrm.biz	1
generic:hqawgme.biz	1
generic:yvptbjz.org	1
generic:zqagvhfyg.org	1
generic:ppwxknjqppa.com	1
generic:rebrand.ly	1

Summary: Acme

The analysis determined that a wide range of applications and cyber attacks were present on the network. This activity represents potential business and security risks to **Acme**, but also an ideal opportunity to implement safe application enablement policies that, not only allow business to continue growing, but reduce the overall risk exposure of the organization.

Highlights Include:

- High-risk applications such as **photo-video, internet-utility and file-sharing** were observed on the network, which should be investigated due to their potential for abuse.
- **328** total applications were seen on the network across **28** sub-categories, as opposed to an industry average of **224** total applications seen in other **High Technology** organizations.
- **3,580** total vulnerability exploits were observed across the following top three applications: **web-browsing, web-browsing and web-browsing**.
- **106** malware events were observed, versus an industry average of **1,346** across your peer group.
- **10** total applications were used for command and control communication.

328
APPLICATIONS IN USE

75
HIGH RISK APPLICATIONS

6,752
TOTAL THREATS

3,580
VULNERABILITY EXPLOITS

22
KNOWN MALWARE

84
UNKNOWN MALWARE

Recommendations:

- Implement safe application enablement polices, by only allowing the applications needed for business, and applying granular control to all others.
- Address high-risk applications with the potential for abuse, such as remote access, file sharing, or encrypted tunnels.
- Deploy a security solution that can detect and prevent threats, both known and unknown, to mitigate risk from attackers.
- Use a solution that can automatically re-program itself, creating new protections for emerging threats, sourced from a global community of other enterprise users.