SECURITY LIFECYCLE REVIEW

ACME

PREPARED BY:

ACME
Palo Alto Networks
www.acmecorporation.com

The Security Lifecycle Review summarizes the threat exposure and security risks facing **ACME** and the customers connecting to their networks. The data used for this analysis was gathered by Palo Alto Networks during the report period shown below. The report provides actionable intelligence and risk assessment around the applications, URL traffic, and types of content that are traversing the **ACME** network as well as the volume and types of threats and vulnerabilities that are observed. Recommendations are provided that can be employed to reduce the overall risk exposure for both the network operator and their customers.

Report Period: 8 DAYS
Fri, Jun 11, 2021 - Fri, Jun 18, 2021
Confidential Information - Do Not Redistribute

TABLE OF CONTENTS

EXECUTIVE SUMMARY FOR ACME

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.

Confidential Information - Do Not Redistribute

KEY FINDINGS

450

APPLICATIONS IN USE

450 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.

81

HIGH RISK APPLICATIONS

81 high-risk applications were observed, including those that can introduce or hide malicious activity, transfer files outside the network, or establish unauthorized communication.

181

SAAS APPLICATIONS

181 SaaS applications were observed in your network. To maintain administrative control, adopt SaaS applications that will be managed by your IT team.

388,065

VULNERABILITY EXPLOITS

388,065 total vulnerability exploits were observed in your organization, including **overflow, Other, and code-execution**.

388,066

TOTAL THREATS

388,066 total threats were found on your network, including vulnerability exploits, malware, and outbound command and control activity.

Applications at a Glance

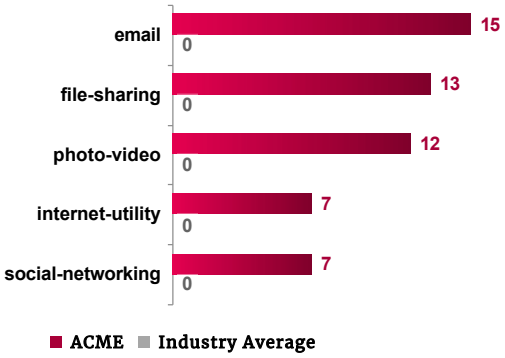
Applications can introduce risk, such as delivering threats, potentially allowing data to leave the network, enabling unauthorized access, lowering productivity, or consuming corporate bandwidth. This section will provide visibility into the applications in use, allowing you to make an informed decision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

KEY FINDINGS

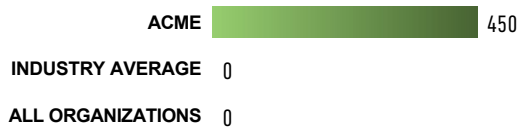
- High-risk applications such as **email, file-sharing, and photo-video** were observed on the network, which should be investigated due to their potential for abuse.
- **450** total applications were seen on the network across **25** sub-categories, as opposed to an industry average of **0** total applications seen in other **High Technology** organizations.
- **7.31 TB** was used by all applications, including **media** with **3.97 TB**, compared to an industry average of **0 Bytes** in similar organizations.

HIGH-RISK APPLICATIONS

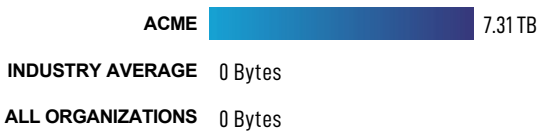
The first step to managing security and business risk is identifying which applications can be abused to cause the most harm. We recommend closely evaluating applications in these categories to ensure they are not introducing unnecessary compliance, operational, or cyber security risk.



NUMBER OF APPLICATIONS ON NETWORK

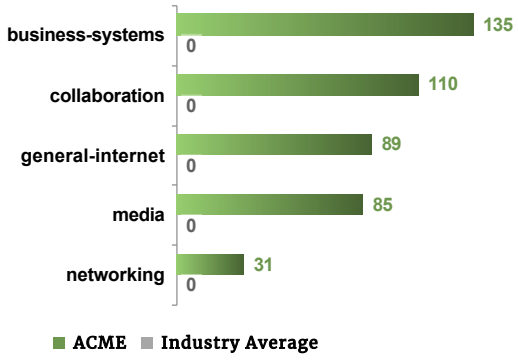


BANDWIDTH CONSUMED BY APPLICATIONS



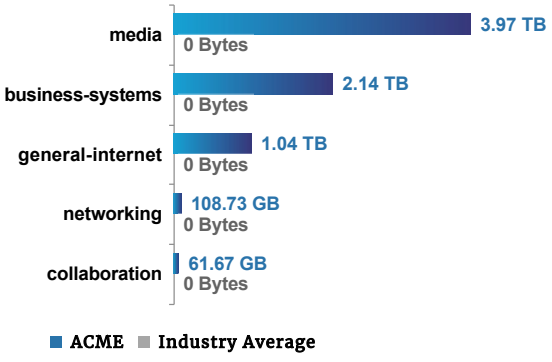
CATEGORIES WITH THE MOST APPLICATIONS

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



CATEGORIES CONSUMING THE MOST BANDWIDTH

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



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
3
2
1
] – High

KEY FINDINGS

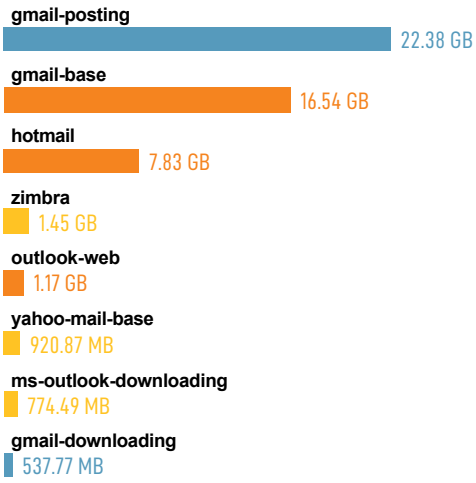
- A total of **450** applications were seen in your organization, compared to an industry average of **0** in other **High Technology** organizations.
- The most common types of application subcategories are **photo-video, file-sharing, and internet-utility**.
- The application subcategories consuming the most bandwidth are **photo-video, software-update, and internet-utility**.

Number of Applications in the subcategory **Industry Average**

33 0

Email 52.94 GB

TOP EMAIL APPS

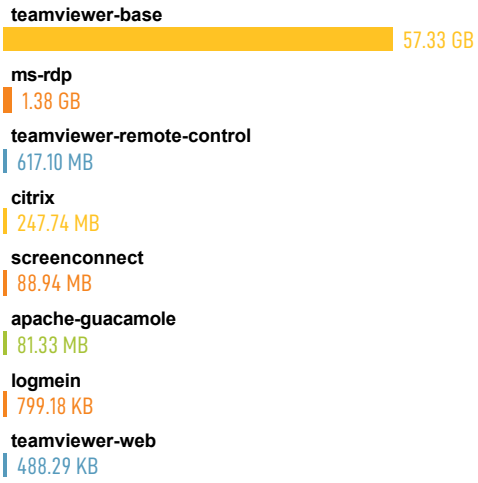


Number of Applications in the subcategory **Industry Average**

11 0

Remote-Access 59.75 GB

TOP REMOTE-ACCESS APPS

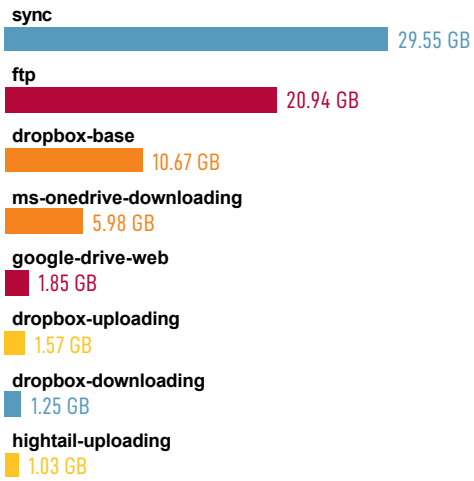


Number of Applications in the subcategory | Industry Average

47 | 0

File-Sharing 75.27 GB

TOP FILE-SHARING APPS

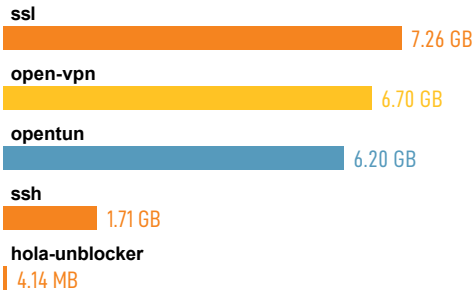


Number of Applications in the subcategory | Industry Average

5 | 0

Encrypted-Tunnel 21.88 GB

TOP ENCRYPTED-TUNNEL APPS

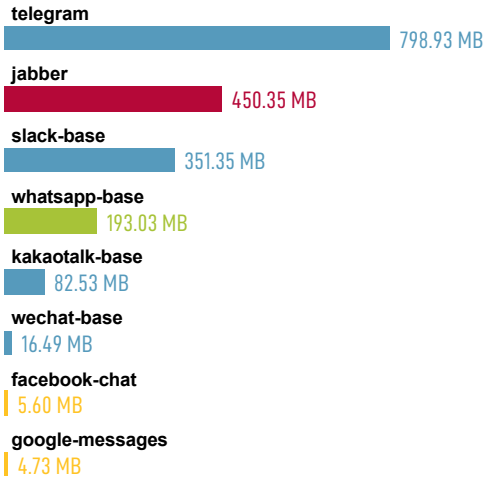


Number of Applications in the subcategory | Industry Average

20 | 0

Instant-Messaging 1.91 GB

TOP INSTANT-MESSAGING APPS

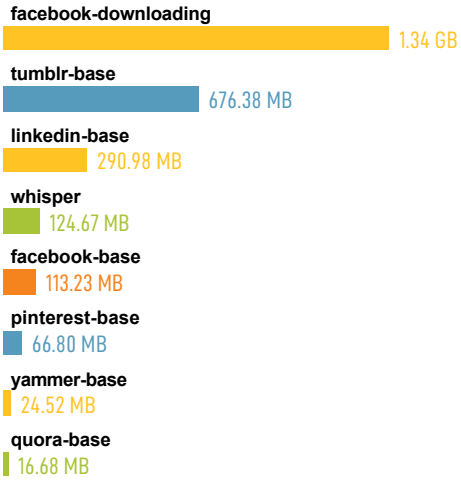


Number of Applications in the subcategory | Industry Average

27 | 0

Social-Networking 2.69 GB

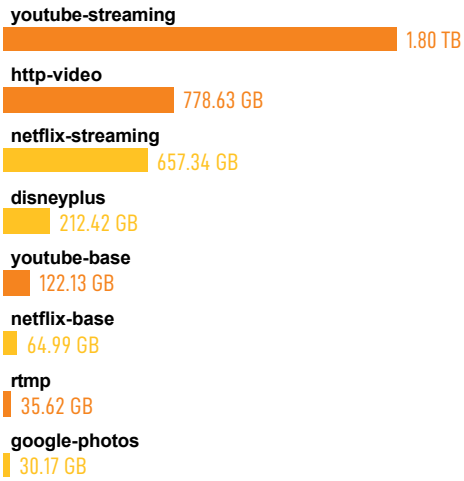
TOP SOCIAL-NETWORKING APPS



Number of Applications in the subcategory | Industry Average

Photo-Video 3.78 TB

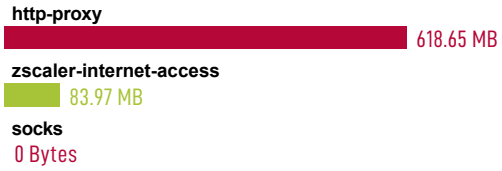
TOP PHOTO-VIDEO APPS



Number of Applications in the subcategory | Industry Average

Proxy 702.62 MB

TOP PROXY APPS



Applications that Introduce Risk — Detail

RISK	APPLICATION	CATEGORY	SUB CATEGORY	TECHNOLOGY	BYTES	SESSIONS
2	gmail-posting	collaboration	email	browser-based	22.38 GB	61305
4	gmail-base	collaboration	email	browser-based	16.54 GB	102661
4	hotmail	collaboration	email	browser-based	7.83 GB	141057
3	zimbra	collaboration	email	browser-based	1.45 GB	13945
4	outlook-web	collaboration	email	browser-based	1.17 GB	11816
3	yahoo-mail-base	collaboration	email	browser-based	920.87 MB	45710
3	ms-outlook-downloading	collaboration	email	browser-based	774.49 MB	255
2	gmail-downloading	collaboration	email	browser-based	537.77 MB	391
4	ssl	networking	encrypted-tunnel	browser-based	7.26 GB	271955
3	open-vpn	networking	encrypted-tunnel	client-server	6.7 GB	199
2	opentun	networking	encrypted-tunnel	client-server	6.2 GB	5
4	ssh	networking	encrypted-tunnel	client-server	1.71 GB	570900
4	hola-unblocker	networking	encrypted-tunnel	client-server	4.14 MB	4900
2	sync	general-internet	file-sharing	browser-based	29.55 GB	24200
5	ftp	general-internet	file-sharing	client-server	20.94 GB	248445
4	dropbox-base	general-internet	file-sharing	client-server	10.67 GB	51628
4	ms-onedrive-downloading	general-internet	file-sharing	client-server	5.98 GB	1343
5	google-drive-web	general-internet	file-sharing	browser-based	1.85 GB	11791
3	dropbox-uploading	general-internet	file-sharing	client-server	1.57 GB	59
2	dropbox-downloading	general-internet	file-sharing	client-server	1.25 GB	2198
3	hightail-uploading	general-internet	file-sharing	browser-based	1.03 GB	30
2	telegram	collaboration	instant-messaging	client-server	798.93 MB	2623
5	jabber	collaboration	instant-messaging	client-server	450.35 MB	61691
2	slack-base	collaboration	instant-messaging	browser-based	351.35 MB	624
1	whatsapp-base	collaboration	instant-messaging	client-server	193.03 MB	37329

Notes:

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
2	kakaotalk-base	collaboration	instant-messaging	client-server	82.53 MB	160
2	wechat-base	collaboration	instant-messaging	client-server	16.49 MB	8268
3	facebook-chat	collaboration	instant-messaging	browser-based	5.6 MB	11
3	google-messages	collaboration	instant-messaging	browser-based	4.73 MB	82
4	youtube-streaming	media	photo-video	browser-based	1.8 TB	198436
4	http-video	media	photo-video	browser-based	778.63 GB	46783
3	netflix-streaming	media	photo-video	browser-based	657.34 GB	94056
3	disneyplus	media	photo-video	browser-based	212.42 GB	23074
4	youtube-base	media	photo-video	browser-based	122.13 GB	411471
3	netflix-base	media	photo-video	browser-based	64.99 GB	86888
4	rtmp	media	photo-video	browser-based	35.62 GB	2
3	google-photos	media	photo-video	browser-based	30.17 GB	1392
5	http-proxy	networking	proxy	browser-based	618.65 MB	40266
1	zscaler-internet-access	networking	proxy	browser-based	83.97 MB	67557
5	socks	networking	proxy	network-protocol	0 Bytes	0
3	teamviewer-base	networking	remote-access	client-server	57.33 GB	780334
4	ms-rdp	networking	remote-access	client-server	1.38 GB	64
2	teamviewer-remote-control	networking	remote-access	client-server	617.1 MB	116
3	citrix	networking	remote-access	client-server	247.74 MB	208951
4	screenconnect	networking	remote-access	client-server	88.94 MB	107
1	apache-guacamole	networking	remote-access	client-server	81.33 MB	5
4	logmein	networking	remote-access	client-server	799.18 KB	97
2	teamviewer-web	networking	remote-access	browser-based	488.29 KB	7
3	facebook-downloading	collaboration	social-networking	browser-based	1.34 GB	906
2	tumblr-base	collaboration	social-networking	browser-based	676.38 MB	651

Notes:

RISK	APPLICATION	CATEGORY	SUB CATEGORY ▲	TECHNOLOGY	BYTES	SESSIONS
3	linkedin-base	collaboration	social-networking	browser-based	290.98 MB	2387
1	whisper	collaboration	social-networking	browser-based	124.67 MB	175
4	facebook-base	collaboration	social-networking	browser-based	113.23 MB	7469
2	pinterest-base	collaboration	social-networking	browser-based	66.8 MB	457
3	yammer-base	collaboration	social-networking	client-server	24.52 MB	365
1	quora-base	collaboration	social-networking	browser-based	16.68 MB	134

Notes:

SaaS Applications

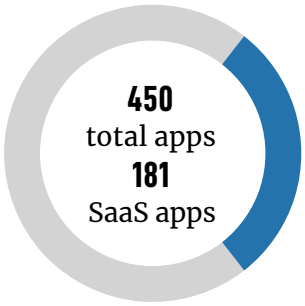
SaaS–based application services continue to redefine the network perimeter. Often labeled "shadow IT," most of these services are adopted directly by individual users, business teams, or even entire departments. To minimize data security risks, you need control over SaaS applications used your network.

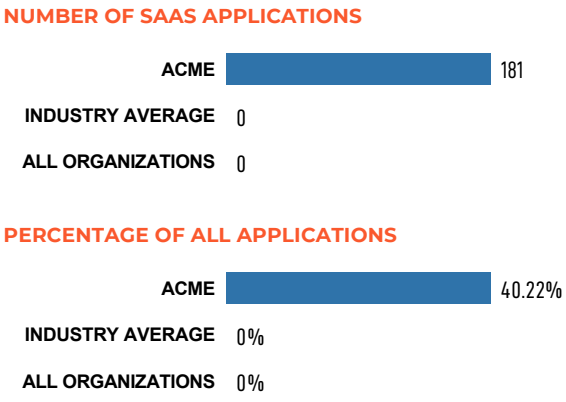
KEY FINDINGS

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

SAAS APPLICATIONS BY NUMBERS

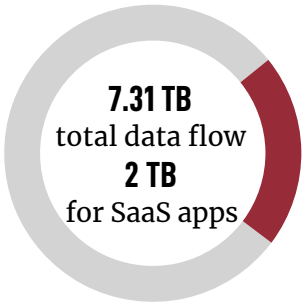
Review the applications being used in your organization. To maintain administrative control, adopt SaaS applications that will be managed by your IT team.

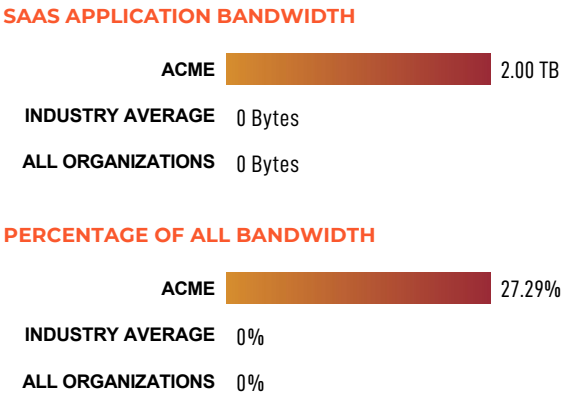




SAAS APPLICATION BANDWIDTH

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

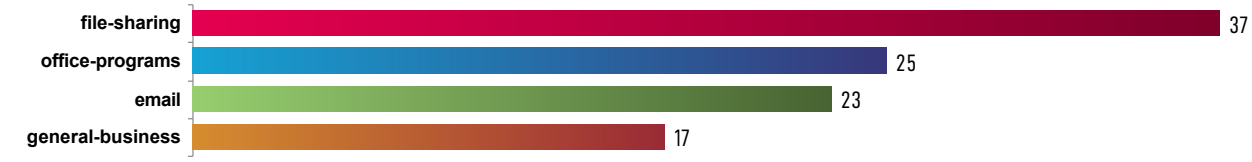




TOP SAAS APPLICATION SUBCATEGORIES

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

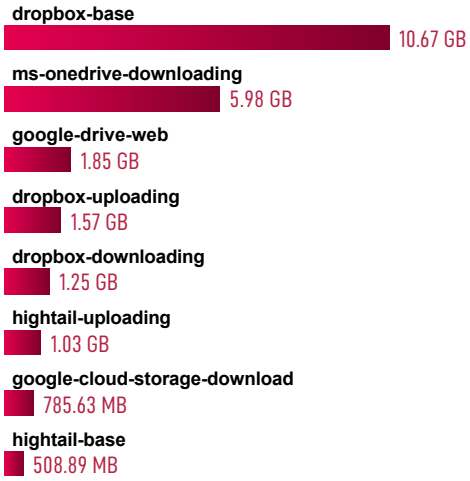
TOP SAAS APPLICATION SUBCATEGORIES BY TOTAL NUMBER OF APPLICATIONS



Number of Applications in the subcategory Industry Average

File-Sharing 24.75 GB

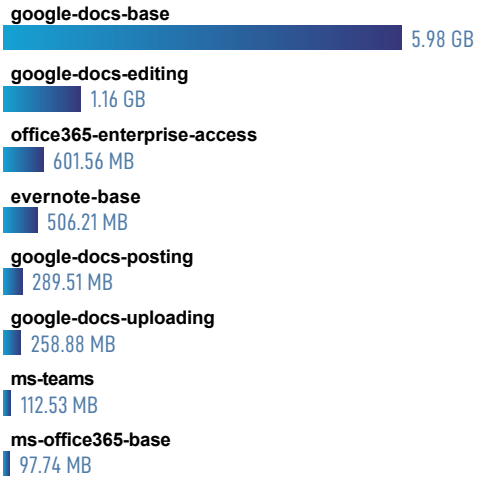
TOP FILE-SHARING APPS



Number of Applications in the subcategory Industry Average

Office-Programs 9.17 GB

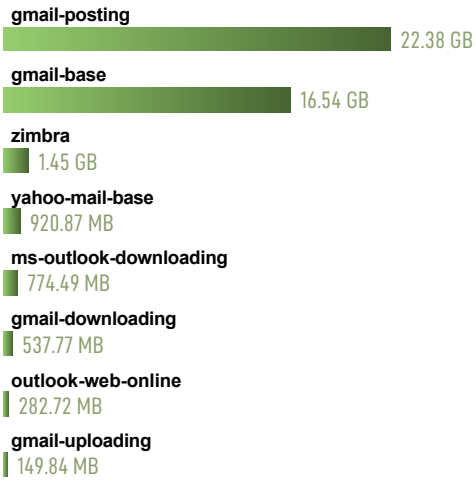
TOP OFFICE-PROGRAMS APPS



Number of Applications in the subcategory | Industry Average

Email 43.45 GB

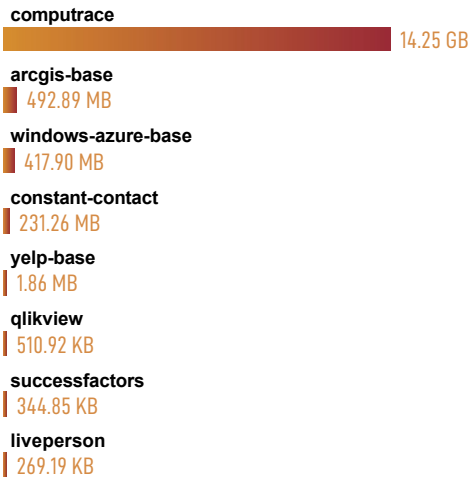
TOP EMAIL APPS



Number of Applications in the subcategory | Industry Average

General-Business 15.39 GB

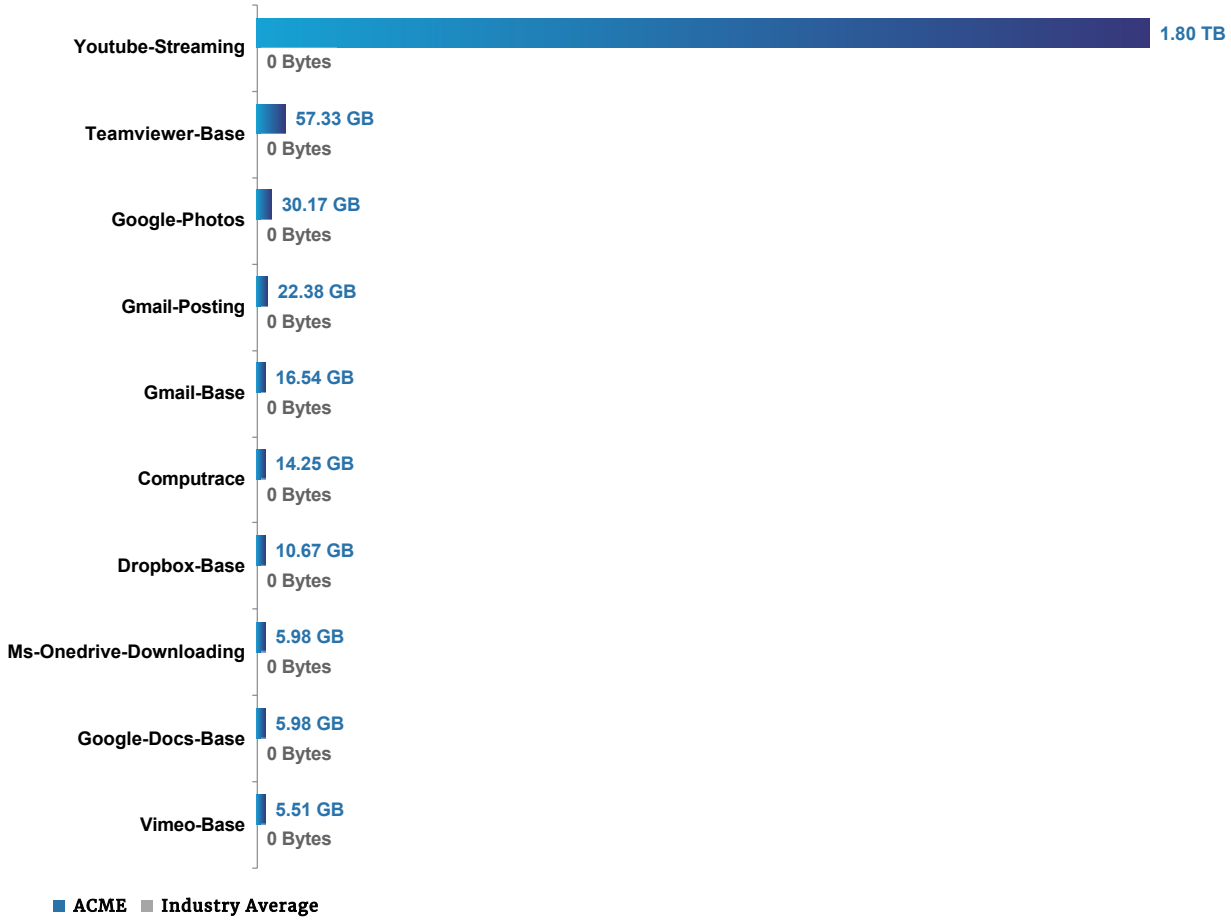
TOP GENERAL-BUSINESS APPS



TOP SAAS APPLICATIONS

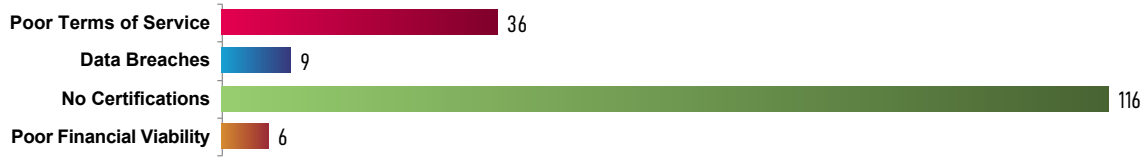
The following displays the top 10 SaaS applications used in your organization and the application usage compared against your industry peers and all other Palo Alto Networks customers.

TOP SAAS APPLICATIONS BY DATA MOVEMENT



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.



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

60.75 GB
Apps with Poor Terms of Service

- teamviewer-base — 57.33 GB
- yahoo-mail-base — 920.87 MB
- teamviewer-remote-control — 617.10 MB
- new-relic — 602.75 MB
- backblaze-backup — 463.49 MB
- mailchimp — 285.95 MB
- constant-contact — 231.26 MB
- yahoo-mail-downloading — 125.69 MB

1.34 GB
Apps with Data Breaches

- yahoo-mail-base — 920.87 MB
- mailchimp — 285.95 MB
- yahoo-mail-downloading — 125.69 MB
- yahoo-mail-uploading — 2.15 MB
- mega-base — 1.17 MB
- yahoo-mail-posting — 647.01 KB
- yandex-disk — 74.68 KB
- microsoft-dynamics-crm — 74.65 KB

1.87 TB
Apps with No Certifications

- youtube-streaming — 1.80 TB
- gmail-posting — 22.38 GB
- computrace — 14.25 GB
- ms-onedrive-downloading — 5.98 GB
- vimeo-base — 5.51 GB
- google-analytics — 4.18 GB
- youtube-uploading — 1.94 GB
- google-drive-web — 1.85 GB

465.1 MB
Apps with Poor Financial Viability

- backblaze-backup — 463.49 MB
- gmx-mail — 1.04 MB
- onehub-base — 469.70 KB
- classin — 95.67 KB
- rezgo — 10.73 KB
- daum-mail — 2.05 KB

Advanced URL Filtering Analysis

Fri, Jun 11, 2021 - Fri, Jun 18, 2021

As applications move to the cloud and people work from anywhere, it's becoming more important—and more difficult—to secure web traffic. Web-based attacks like phishing, command-and-control and other fileless attacks are coming at higher volume, greater speed, and increased sophistication. The Palo Alto Networks Advanced URL Filtering service gives you deep insight into your web traffic, empowers you to control web access through granular policies and enables you to prevent web-based threats in real-time.

1,014,052
TOTAL URL REQUESTS

Advanced URL Filtering has analyzed **1,014,052** URL requests in your network. The Web has become one of the most commonly used attack surfaces and malicious web-pages can be used for malware delivery, command-and-control (C2), or data exfiltration.

12,444
MALICIOUS REQUESTS

Advanced URL Filtering has identified **12,444** malicious requests. These malicious requests include malware, phishing, command and control and grayware.

402
MALICIOUS IP ADDRESSES

Advanced URL Filtering has identified **402** malicious IP addresses behind these malicious URLs/domains. These IP addresses can be used as C2 infrastructure to exfiltrate data, deliver malware or send remote commands to a system in your network.

706,300
URL ANALYZED IN REAL-TIME

706,300 URL requests have been analyzed in real-time. Analyzing URLs in real-time protects users within milliseconds from brand new or never seen before malicious attacks.

45
MALICIOUS URLS REQUEST DETECTED IN REAL-TIME

Advanced URL Filtering has identified **45** malicious URL requests in real-time. These malicious requests include malware, phishing, command and control and grayware.

10
MALICIOUS IP ADDRESSES DETECTED IN REAL-TIME

Advanced URL Filtering has identified **10** malicious IP addresses behind these malicious URLs/domains in real-time. These IP addresses can be used as C2 infrastructure to exfiltrate data, deliver malware or send remote commands to a system in your network.

TRAFFIC DISTRIBUTION

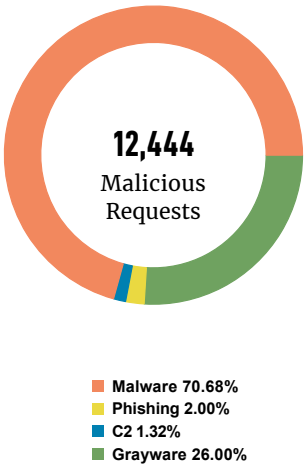
Uncontrolled Web surfing exposes organizations to security and business risks, including exposure to potential cyber-threats, data loss, credential theft or compliance violations. This section will provide visibility into the URL requests in your network, allowing you to make informed decisions regarding potential risk versus business benefit. Malicious URLs and domains in your network should be reviewed to understand who is accessing them, and the potential risk associated with them.

KEY FINDINGS

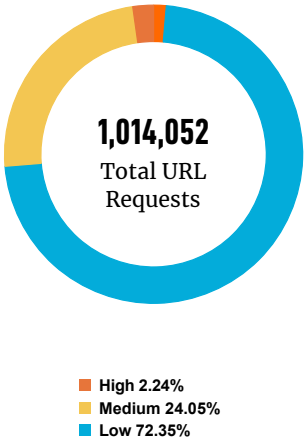
- Users visited a total of **1,014,052** URLs during the report time period across **63** categories.
- **12,444** requests out of that total were to known malicious websites.
- **22,667** high risk and **243,847** medium risk sites were visited.
- **45** malicious requests were analyzed in real-time.

URL REQUEST DISTRIBUTION

MALICIOUS URL REQUEST CATEGORIES



RISK-LEVELS OF URL REQUESTS



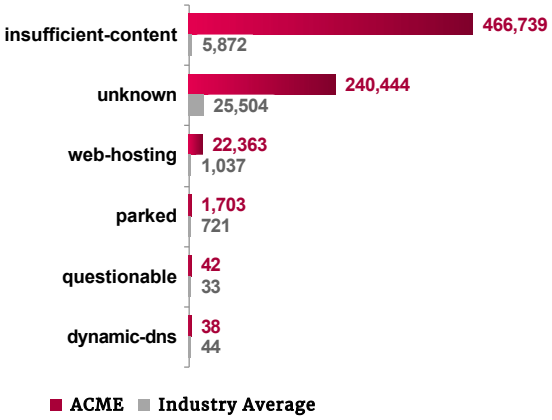
MALICIOUS URL REQUESTS DETECTED IN REAL-TIME

TOP CATEGORIES AND DOMAINS DISTRIBUTION

The following charts list the top visited categories and domains.

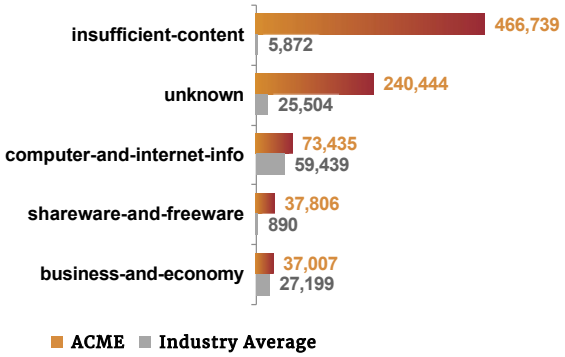
CATEGORIES INTRODUCING POTENTIAL RISK

The Web is a primary attack channel for malicious actors. High risk categories like unknown, insufficient-content, questionable, high-risk, parked, dynamic-dns, web hosting & newly-registered-domain should either be blocked or set for SSL decryption with strict threat control policies to have better visibility and control.



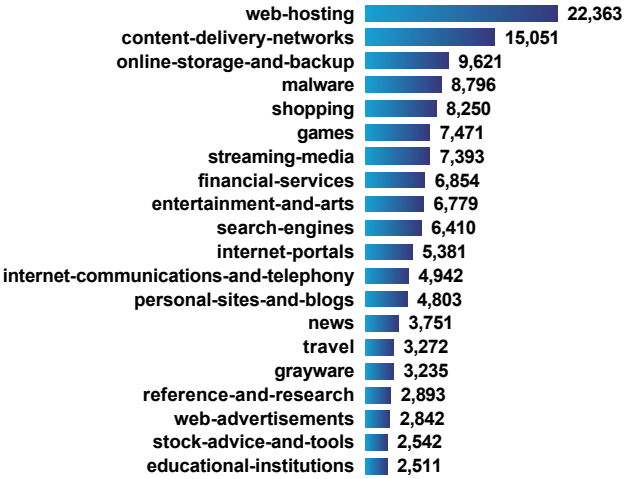
TOP 5 VISITED CATEGORIES

The top 5 most visited URL categories, along with industry benchmarks across your peer group, are shown below. Understanding your web traffic mix over time will help you identify anomalies that may indicate malicious activity.



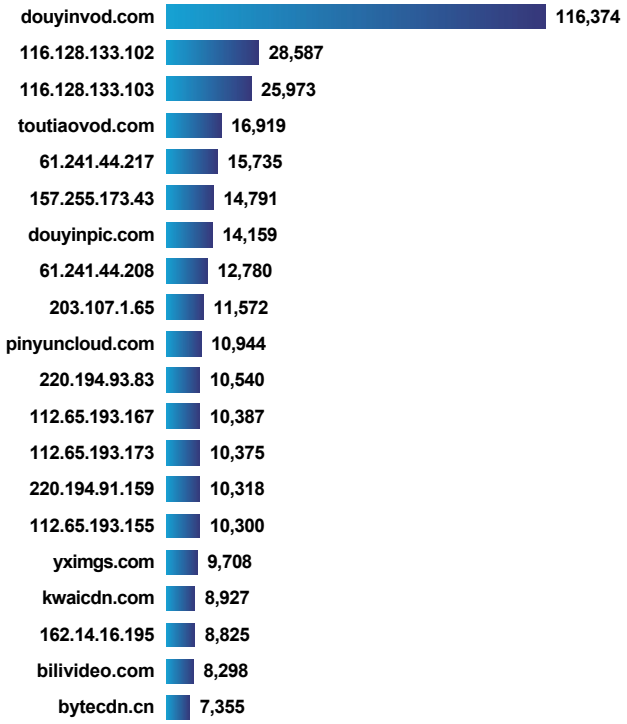
NEXT MOST HIGHLY VISITED CATEGORIES

The next top 20 most visited URL categories are shown below. Understanding your web traffic mix over time will help you identify anomalies that may indicate malicious activity.



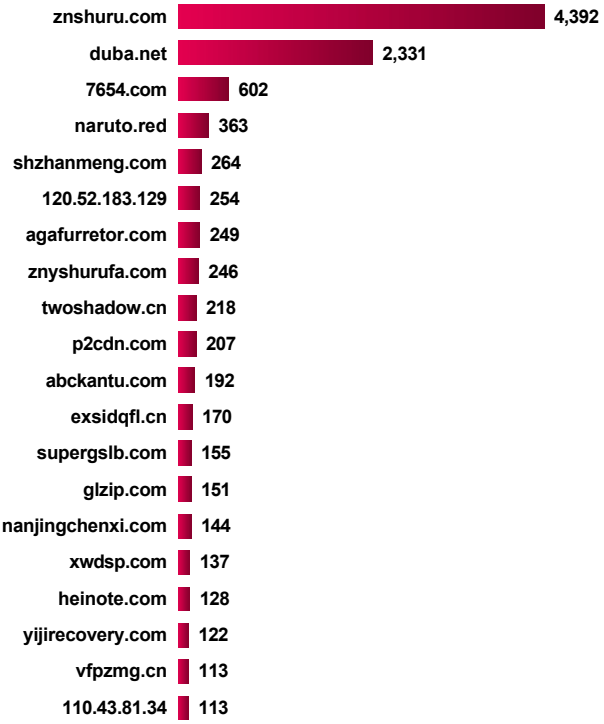
TOP VISITED DOMAINS

The following displays the top 20 visited domains in your network. It is important to regularly view the top visited domains in your network. Understanding your web traffic usage over time will help you identify anomalies that may indicate malicious activity.



TOP VISITED MALICIOUS DOMAINS

The following displays the top 20 malicious domains visited in your network. Malicious domains should be reviewed to understand the volume of the domain requests, who is accessing those domains, and what malware families are associated with those domains. Frequent visits to malicious domains from the same machine may indicate an infected endpoint.



TOP VISITED MALICIOUS URLS IN REAL-TIME

The following displays the top 10 malicious URLs detected in real-time. These URLs were flagged for real-time analysis because they were deemed high risk and had never been seen before. These types of URLs may be the result of either a broad attack campaign or very targeted attack in nature to a specific industry or organization.

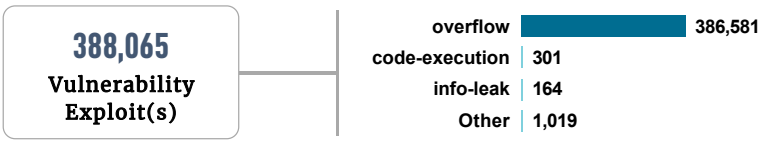
HOSTNAME/IP	URL HITS	EXAMPLE URL
epoint.com.cn	26	yyfw.epoint.com.cn/FrontVoice/JavaScript/Voice.js?%5f=1623868800401
znshuru.com	9	down.znshuru.com/pdf/js/12a18bb2dd3ac973db8156d30a37f37c.bbe
kkdownload.com	4	dl.kkdownload.com/2c8400d5e8e9ba74cc288c5d32c3b7ea.data
kpzip.com	1	i.kpzip.com/n/logo/v1.0.0.2/uc2.gif.md5
1wscqi.cn	1	m.1wscqi.cn/52256785797555359672382659432293494726357241 59.jsp
mi-img.com	1	f2.market.mi-img.com
nearme.com.cn	1	storedl1.nearme.com.cn
wapx.cn	1	app.wapx.cn
91speed.com.cn	1	downza.91speed.com.cn/2021/05/06/iTunes64.rar?ssig=d73b886151a16a5c0f878eeb5ac238296b0ec736%26time%5fstamp=1623724804%26fn=16461a32ac2d18825c6686295d340813

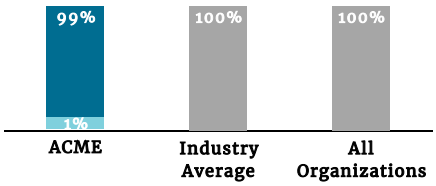
Threats at a Glance

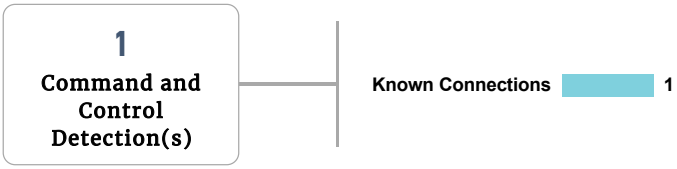
Understanding your risk exposure, and how to adjust your security posture to prevent attacks, requires intelligence on the type and volume of threats used against your organization. This section details the application vulnerabilities, known and unknown malware, and command and control activity observed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

KEY FINDINGS

- **388,065** total vulnerability exploits were observed in your organization, including **overflow, Other, and code-execution**.
- **0** malware events were observed, versus an industry average of **0** across your peer group.
- **1** total command and control requests were identified, indicating attempts by malware to communicate with attackers to download additional malware, receive instructions, or exfiltrate data.

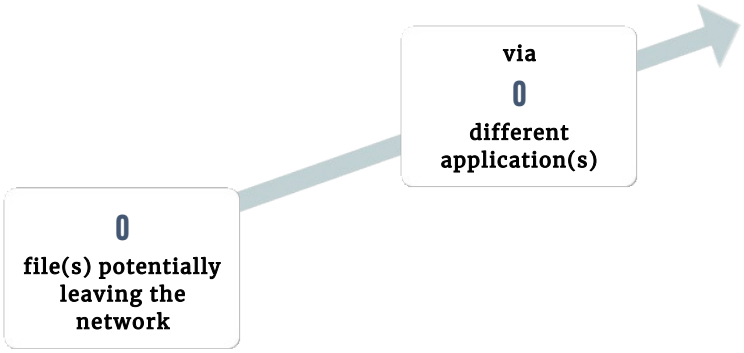






FILES LEAVING THE NETWORK

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.

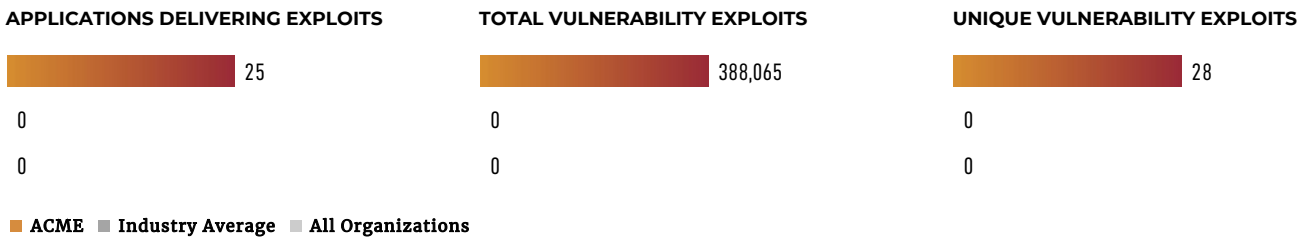


Application Vulnerabilities

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

- **25** total applications were observed delivering exploits to your environment.
- **388,065** total vulnerability exploits were observed across the following top three applications: **unknown-tcp, web-browsing, and ms-update**.
- **28** unique vulnerability exploits were found, meaning attackers continued to attempt to exploit the same vulnerability multiple times.



VULNERABILITY EXPLOITS PER APPLICATION

(TOP 5 APPLICATIONS WITH MOST DETECTIONS)

DETECTIONS	EXPLOIT ID	SEVERITY	THREAT TYPE	CVE ID
385,515	**Unknown-Tcp**			
2	HTTP Abnormal URI Path And Host Field in Header	HIGH		
385,379	HTTP GET Requests Long URI Anomaly	LOW	overflow	CVE-2006-5850, CVE-2007-0774, CVE-2002-1310, CVE-2006-5850
58	IBM WebSphere Faultactor Cross-Site Scripting Vulnerability	LOW	info-leak	CVE-2006-2431
2	FTP Protocol Evasion Application Detection	LOW		
2	Application Identification Evasion Attempt Through Malformed FTP Traffic	LOW		
66	HTTP Non RFC-Compliant Response Found	INFO	info-leak	CVE-2010-2561
6	HTTP Non-RFC Compliant Request	INFO		
1,572	**Web-Browsing**			
323	Microsoft MSXML Memory Corruption Vulnerability	HIGH		
24	Squid HTTP Header Parsing Assertion Failure Denial of Service Vulnerability	HIGH		
7	HTTP: IIS Denial Of Service Attempt	HIGH		
3	HTTP POST Request URI Path Too Long	HIGH	dos	CVE-2006-3546;CVE-2008-3257;CVE-2017-17099
17	HTTP SQL Injection Attempt	MEDIUM		
6	HTTP Directory Traversal Request Attempt	MEDIUM	info-leak	CVE-2018-18990;CVE-2016-8016;CVE-2019-8903;CVE-2021-3019

DETECTIONS	EXPLOIT ID	SEVERITY	THREAT TYPE	CVE ID
1,121	HTTP GET Requests Long URI Anomaly	LOW	overflow	CVE-2006-5850, CVE-2007-0774, CVE-2002-1310, CVE-2006-5850
53	PNG File Chunk Length Abnormal	LOW	code-execution	
9	Suspicious HTTP Evasion Found	LOW	protocol-anomaly	
2	HTTP Response Content Length Too Long	LOW	code-execution	CVE-2004-0492
399	**Ms-Update**			
190	HTTP Response Content Length Too Long	LOW	code-execution	CVE-2004-0492
11	PNG File Chunk Length Abnormal	LOW	code-execution	
198	Microsoft Office File with Macros Detected	INFO		
75	**Disneyplus**			
75	Suspicious Abnormal HTTP Response Found	LOW		
72	**Spotify**			
72	HTTP Unauthorized Brute Force Attack	HIGH		

Command and Control Analysis

Command-and-control (CnC) activity often 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. Detection and response products may provide detail on the malicious network and host activity that has occurred as a result of the identified malware.

KEY FINDINGS

- **1** total applications were used for command-and-control communication.
- **1** total command-and-control requests were seen on your network.
- **0** total suspicious DNS queries were observed.

0 SUSPICIOUS DNS QUERIES

1 SPYWARE PHONE HOME

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**. This is 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

- High-risk applications such as **email, file-sharing, and photo-video** were observed on the network, which should be investigated due to their potential for abuse.
- **450** applications were seen on the network across **25** sub-categories, as opposed to an industry average of **0** applications seen in other **High Technology** organizations.
- **388,065** vulnerability exploits were observed across the following top three applications: **unknown-tcp, web-browsing, and ms-update**.
- **0** malware events were observed, versus an industry average of **0** across your peer group.
- **1** applications were used for command and control communication.

KEY FINDINGS

450
APPLICATIONS IN USE

81
HIGH RISK APPLICATIONS

181
SAAS APPLICATIONS

388,065
VULNERABILITY EXPLOITS

388,066
TOTAL THREATS

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, and encrypted tunnels.
- Investigate command-and-control communication by examining the network or host source. Detection and response or logging solutions may provide an indication of what occurred.
- Deploy a security solution that can detect and prevent threats, both known and unknown, to mitigate the risk of attack.
- Use a solution that can automatically re-program itself and other security products, creating and coordinating new protections for emerging threats, sourced from a global community of other enterprise users.