



Enterprise Security Lifecycle Review

Quick Start Guide

September 2019

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

[Security Lifecycle Review – Introduction](#)

[Key Elements](#)

[Common Questions](#)

[Data Retention and Storage Questions](#)

[Quick Start Walkthrough](#)

[Data Collection](#)

[Login to Salesforce](#)

[Report Generation From Salesforce](#)

[View Existing Report](#)

[Report Content](#)

[Summary](#)

[Navigation Menu](#)

[In-Line Help](#)

[Applications at a Glance](#)

[Applications that introduce risk](#)

[Applications that introduce risk - Detail](#)

[SaaS Applications](#)

[SaaS Applications By Hosting Risk](#)

[URL Activity](#)

[File Transfer Analysis](#)

[Threats at a Glance](#)

[High Risk and Malicious File Type Analysis](#)

[Application Vulnerabilities](#)

[Known and Unknown Malware](#)

[Command and Control Analysis](#)

[DNS Service Analysis](#)

[Summary](#)

[Traffic Distribution](#)

[Domains and Destination Distribution](#)

[Malicious Traffic Origin Countries and DNS Tunneling Requests](#)

[Known Malware and Families](#)

[Report Summary](#)

Security Lifecycle Review – Introduction

The Security Lifecycle Review summarizes the business and security risks facing an organization, providing an opportunity to review the findings and take joint action on them during an initial evaluation or as part of a regular visibility and security checkup. The review integrates existing Application Visibility data with WildFire™ cloud-based threat analysis service, SaaS-based application visibility and more. Findings are based on data collected by an on-site device or submitted to the WildFire cloud during a specified time period, including: applications, SaaS-based applications, URL traffic, content types, and known and unknown threats traversing the network.

Key Elements

- Visibility into the applications and threats exposing vulnerabilities.
- Analysis of all application traffic on the network, the capacity impact of these applications and the relative security risks observed.
- Comparison data for the customer's organization versus their industry peers.
- High-risk URL categories on the network.
- Known and unknown malware information.
- Key areas to focus on for reducing risk exposure.

Common Questions

1. How can I access the Security Lifecycle Review report?

As a Palo Alto Networks® partner, you can generate an SLR by selecting an opportunity from Partner portal. Please refer to the Quick Start Walkthrough section for details of the SLR generation process.

2. How do I generate the Statsdump file?

You will be able to generate the Statsdump file from your local device through the device management UI or using CLI (tftp export/scp export). Refer to the Quick Start Walkthrough section for instructions on generating the Statsdump file.

3. Which browsers are supported?

The most recent stable versions of Microsoft® Internet Explorer®, Mozilla® Firefox® and Google Chrome™ are supported.

4. What if we don't enable Wildfire, URL Filtering or Threat Prevention?

Rather than publish a blank page with no data, we will dynamically remove those pages from the report. We recommend running all evaluations with WildFire, URL Filtering and Threat Prevention enabled when possible.

5. What are the new malware related updates added to the report?

- **Information on Malware detected at the Endpoint:** Known and Unknown Malware section will include information on Malware detected at the Endpoint to highlight the need for having both endpoint and firewall for prevention.
Note: Information on Malware detected at the Endpoint will be available in the report only for customers who have not purchased Traps and the data depends on the Malware observed in their network
- **Top Tags and matching samples:** Command and Control Analysis section will include Top Tags and matching samples for the following tag classes: malware family, campaign and malicious behavior. Allows customers to take quick action to remediate possible threats.
- **Threats by Destination Countries:** Command and Control Analysis section will include a map of countries that malware sessions targeted. The map highlights the countries that received the most number of malware sessions.

6. What is the goal behind the Malware updates added to the SLR report?

The goal is to leverage the malware information seen by the Firewall and correlate the information with Wildfire data to showcase the value for Cortex XDR, Traps and Autofocus.

7. Are the Malware updates added to the SLR report available for all customers?

- Information on Malware detected at Endpoint is available only for Customers who have not purchased Traps.

- Information on Top Tags and Matching Samples and Threats by destination countries are available for all customers regardless of whether they have purchased Traps or not.

8. I found a bug. What should I do?

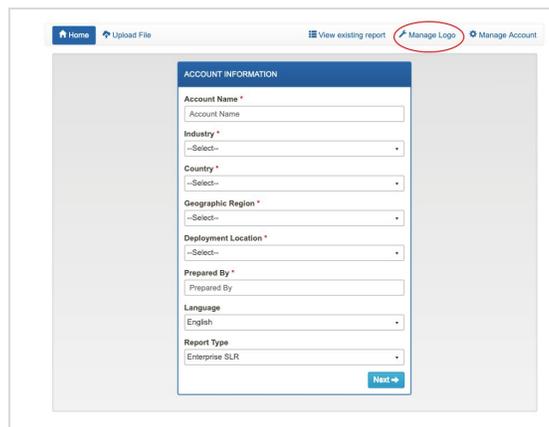
Email slr_support@paloaltonetworks.com, including a detailed description of the bug/issue, screenshots of the error/issue and the Statsdump file used to generate the report.

9. I have a feature request/feedback. What should I do?

Email slr_feedback@paloaltonetworks.com, for any feature request or feedback for SLR.

10. Can partners white-label the new report with their logo and company info?

Yes, partners can click on the “Manage Logo” button located on the top right from the SLR homepage to customize the report with their logo and company information.



11. Will I need to login via Salesforce.com/Partner Portal and begin reports via Opportunities?

Yes, all Palo Alto Networks SEs and partners must begin reports via Opportunities in Salesforce.com or the Partner Portal, respectively.

12. How can I view the previous reports created?

All Palo Alto Networks SEs and partners can view the reports created by them from the Home page of the SLR portal or via Opportunities in Salesforce.com or the Partner Portal, respectively. SLR reports created for a specific opportunity will be available for viewing in the “Tools” section on the right side from the opportunity view.

Data Retention and Storage Questions

1. What type of data/information is used to create the report?

SLR derives information from two sources:

- Statsdump file, which is generated by customers directly from their NGFWs. (Customers can open the Statsdump file to see data present, which are XMLs with summarized results of device logs.)
- Information from the customers WildFire public cloud submissions

The above mentioned data sources are controlled by the customer. Customers can choose to generate the Statsdump file or setup the WildFire submission policy. Please note the SLR only contains summarized statistical information, not original samples, IP addresses, user name, etc.

2. Is this information stored or saved by Palo Alto networks after the report is run?

SLR data is maintained indefinitely on secured Palo Alto Networks servers, meeting industry best-practices for protecting information. Removal requests can be processed 1:1. The data is anonymized and the trending results across the entire set are shared in threat reports on a regular basis.

3. Are actual files used or presented within the report (such as if WildFire is used or files seen by the device)

Actual files are never used or presented within the report.

Resources

- o <https://live.paloaltonetworks.com/t5/Customer-Resources/tkb-p/CustomerResources>
- o In-line help is available for all sections of the report.

Quick Start Walkthrough

You can generate an SLR from Partner portal by following the steps below.

Data Collection

SLR generation requires an export of data from the installed Palo Alto Networks device. The file generated pulls the data from the last seven days and compresses it into a tar.gz file. This generation process can be done via the management GUI or CLI.

From the device management UI:

- Select the Device tab.
- Select Support on the left-hand side.
- Click on the “Generate Statsdump” link in the main section.
- A “Save as” dialog box will appear, allowing you to save the tar.gz file to a specific location.

Using CLI, two options are available:

- tftp export stats-dump to [ip address]
- scp export stats-dump to [username@ipaddress.path]

NOTE:

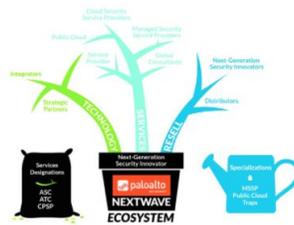
- *Once the tar.gz file has been generated, do not unzip or alter it in any way. The file upload process will fail if the file is altered.*
- *Statsdump period when generated from the GUI is by default always seven days. You can use CLI to extend the time period.*

Logging In to the Partner Portal

1. Generate a Statsdump file for the customer from their local device as per above process
2. Visit the Palo Alto Networks Partner Portal: <https://www.paloaltonetworks.com/partners.html>, and log in to your account. If you do not have an account, click the “Request Access” button below the login field.

[Home](#) > [Partners](#)

NextWave Partner Ecosystem Overview



Right Strategy, Right Philosophy,
Right Platform, and Right Partners.

The NextWave Partner Ecosystem is a community of world-class security experts and leaders who are committed to prevention and making breaches a thing of the past. Together we are providing a new approach to security that is rapidly gaining momentum.

[Learn More](#)

NextWave Partner Portal

Login »

Request Access »

[Follow Us](#) » [Contact Us](#) »

Learn

It takes an ecosystem to address the increasingly complex and long-term issues threatening today's customers. We need partners that deliver, manage, and integrate with, our next-generation security platform to make threat prevention a reality.

To learn more click on the appropriate NextWave Partner Program:

[NextWave Channel Partner Program Summary](#)

[Channel Partner](#)

[Managed Security Service Provider Partner](#)

Become

To succeed in today's market we are focused on providing our partners with a variety of program options to best fit their business needs. Our programs goal is to provide access to innovative and disruptive technology that maximizes differentiation and allows our partners to build a sustainable security practice with Palo Alto Networks.

To get started or to inquire about creating a partnership please click the appropriate program:

[NextWave Channel Partner Program](#)

[NextWave Managed Security Services Provider](#)

Find

More and more customers are looking for a trusted advisor that can provide a security platform that delivers a high degree of threat prevention across every step in an attack lifecycle. The Palo Alto Networks NextWave Partner Ecosystem has a wide range of global partners with different expertise ready to help you.

To find a partner simply click the partner type below based on your need.

[NextWave Channel Partner](#)

[NextWave Managed Security Services Provider](#)

Report Generation From the Partner Portal

1. Click on “Track Deals” to view your open Opportunities.

Home > Partners > NextWave Channel Partner Portal

NextWave Channel Partner Portal

NextWave Channel Partner Portal

NextWave Channel Partner Program

Distributors

Help Me Learn

Help Me Sell

Help Me Market

Regional Content

- Americas
- SLED (Americas Only)
- APAC
- EMEA
- Japan

Contact Us

- Email

TRAINING PARTNER LEARNING CENTER

REGISTER DEALS

TRACK DEALS

TRAPS DEMO SYSTEM

TRACK NEXTWAVE PARTNER STATUS

MANAGE PARTNER LOCATOR

UPDATE PARTNER PORTAL USERS

SECURITY LIFECYCLE REVIEW

MARKETING DEVELOPMENT FUNDS

CAMPAIGNS

EVENTS

SERVICES

Win the battle for your endpoints.

Traps 4.1 Expands Ransomware Protection

Public Cloud Specialization Details

MSSP Specialization Details

PROMOTIONS

GET BEHIND THE WHEEL

Win for Everv Ultimate Test Drive

Secure Up the Endpoint

Connections

- Access NextWave Channel Partner Newsletters
- Subscribe to the NextWave Newsletter
- Follow us on Twitter
- View Partner Blog

2. Select the appropriate opportunity.

palalto NETWORKS
the enterprise security company

CONTENT LOGOUT

HOME LEADS DEALS OPPORTUNITIES MGF ONBOARDING TASKS EVAL REQUESTS EVAL INVENTORY REPORTS

Welcome, Demo PartnerPortal

Demo PartnerPortal
My Company Profile
My Profile

Channel Manager

Partner Actions

- Register A Deal
- Track My Deals
- Service Equipments
- Deals Eligible for Extension
- Manage Partner Locator
- Manage Users
- Tracker

Search

Search All

GO!

Advanced Search...

Recent Opportunities

View: Recently Viewed Opportunities

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z I Other All

EXPORT TO EXCEL

Action	Opportunity Name	Account Name	Close Date	Stage	Opportunity Owner Alias
<input type="checkbox"/> Edit	Test Opportunity for Partner Portal	End User Account	5/5/2016	3 - Evaluation Planning	

3. Scroll down and click on the “Create Report” button. You can also view past reports here.

Security Lifecycle Reviews (Opportunity)		CREATE REPORT				
Action	Risk Report Id	Account	Delivery Date	Delivery Status	Report URL	Report Type
Edit Del	RR41539	[REDACTED]			View Report	SLRP
Edit Del	RR41573	[REDACTED]			View Report	SLRP

4. Choose the appropriate report (Security Lifecycle Review is the default selection).

Welcome, Demo PartnerPortal

Demo PartnerPortal
[My Company Profile](#)
[My Profile](#)

Channel Manager

Partner Actions

- Register A Deal
- Track My Deals
- Service Engagements
- Deals Eligible for Extension
- Manage Partner Locator
- Manage Users
- Tracker

Search

Search All

[Advanced Search...](#)

Report Types:

Security Lifecycle Review

Service Provider SLR

Prevention Posture Assessment

Executive SLR

Security Lifecycle Review GENERATE REPORT CANCEL

Report Input Filters: = Required Information

Account

Opportunity

Industry

Country

Geographic Region

Deployment Location

Report Language

5. Fill in the required fields below Report Input Filters, then click on the “Generate Report” button.

Report Types:

Security Lifecycle Review

Service Provider SLR

Prevention Posture Assessment

Executive SLR

Security Lifecycle Review GENERATE REPORT CANCEL

Report Input Filters: = Required Information

Account

Opportunity

Industry

Country

Geographic Region

Deployment Location

Report Language

- You will automatically be logged in to the SLR portal with the information you entered. Fill out the “Prepared By” field (with who will be presenting the report) and click “Next.”

The screenshot shows a web interface for the SLR portal. At the top, there is a navigation bar with 'Home', 'Upload File', 'View existing report', and 'Manage Logo'. The main content area is titled 'ACCOUNT INFORMATION' and contains the following fields:

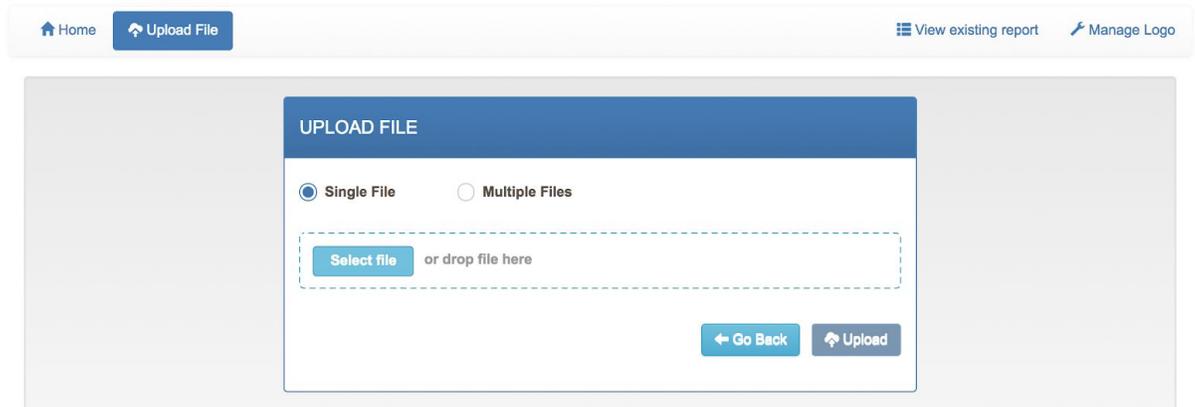
- Account Name ***: Text input field containing 'Palo Alto Networks (TEST ACCT)'
- Industry ***: Dropdown menu with 'High Technology' selected
- Country ***: Dropdown menu with 'United States' selected
- Geographic Region ***: Dropdown menu with 'North America, Latin America, Canada' selected
- Deployment Location ***: Dropdown menu with 'Perimeter/Internet Gateway' selected
- Prepared By ***: Text input field containing 'Palo Alto Networks'
- Language**: Dropdown menu with 'English' selected
- Report Type**: Dropdown menu with 'Enterprise SLR' selected

An orange arrow points to the 'Next' button at the bottom right of the form.

- Upload Files feature offers two ways to upload files to generate the report. To add files, do one of the following:

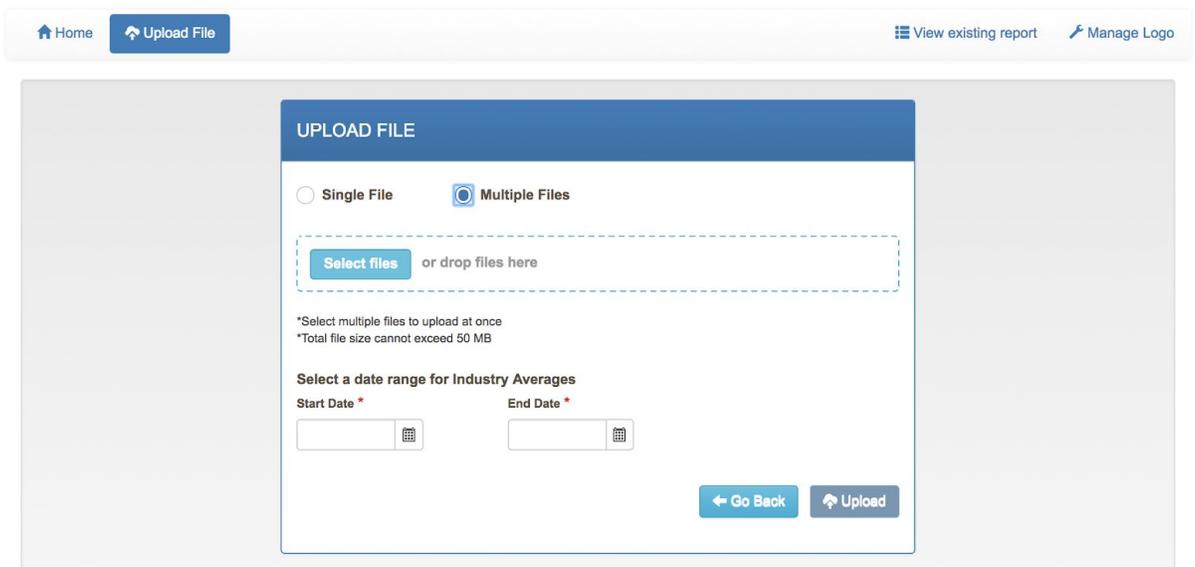
Single File Upload

Select the "Single File" option and Click on the "Select File" button . Select the file that you want to upload in the File Upload dialog box, and then click on the "Upload" button to start uploading the file.



Multiple Files Upload

To upload multiple files, click on the "Multiple Files" option from the "Upload Files" screen and select the files you would like to upload. Once the files have been selected, click on the "Upload" button to start uploading the files.



If you have already uploaded the same Statsdump file, you will see a warning, which allows you to re-upload the file or view the existing report.

View Existing Report

This allows you to view all Security Lifecycle Reviews you have created. Navigate to this from the "Home" page on the portal.

Announcements

- PAN-OS 8.0/8.0.1 is not supported by SLR. Click [here](#) for details.
- SLR works with a wide range of browsers. Click [here](#) to see the list of supported browsers for SLR.

[Home](#)

[Upload File](#)



[View existing report](#)

[Manage Logo](#)

ACCOUNT INFORMATION

Account Name *

Account Name

Industry *

--Select--

Country *

--Select--

Geographic Region *

--Select--

Deployment Location *

--Select--

Prepared By *

Prepared By

Language

English

Report Type

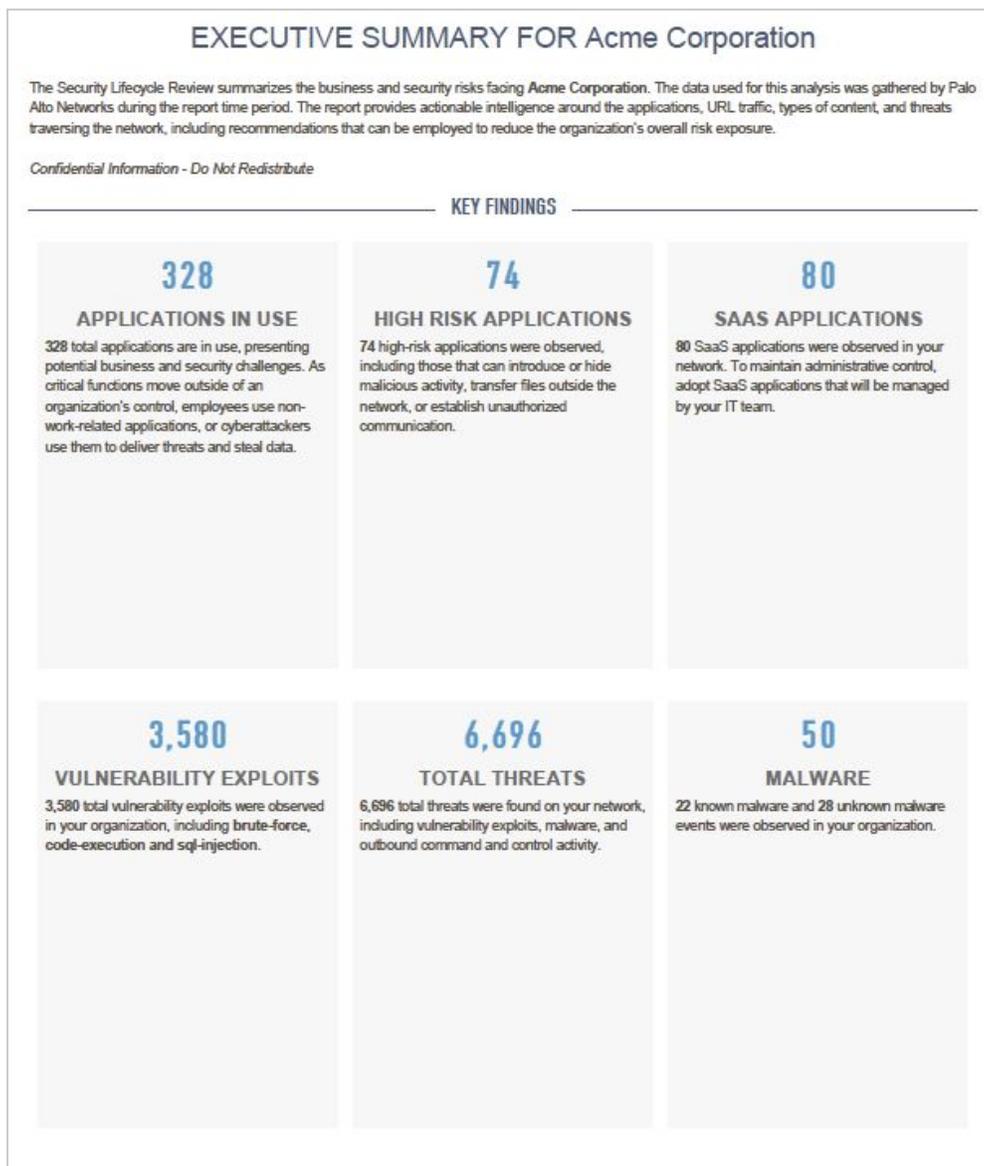
Enterprise SLR

Next →

Report Content

Summary

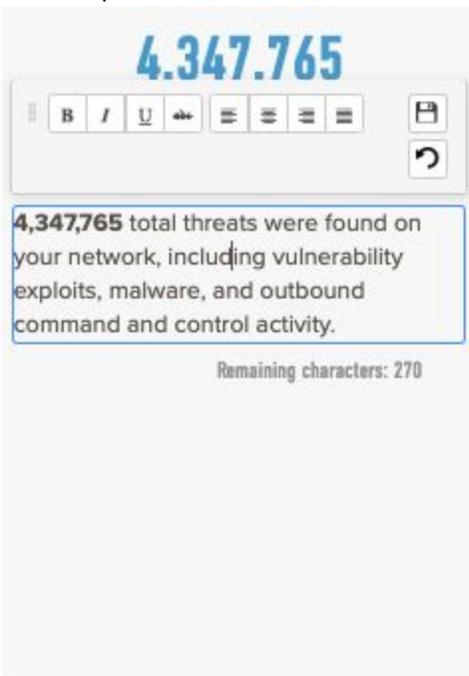
The Summary page provides a high-level summary of the applications and threats observed on the analyzed network.



Key Elements

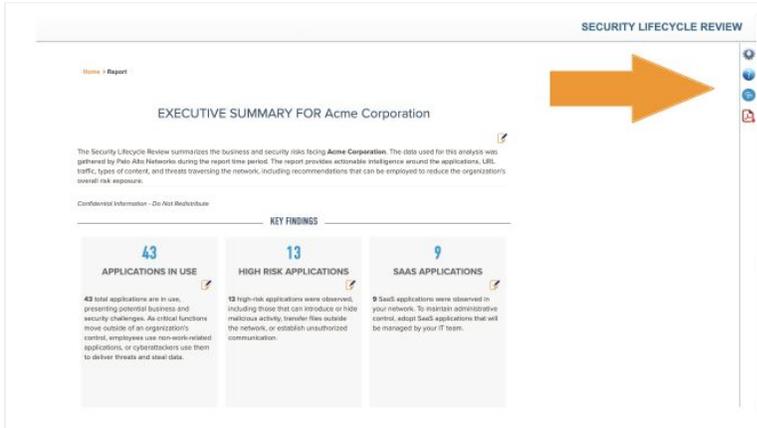
- **Applications in Use:** Total applications observed on the network.
- **High Risk Applications:** Total of risk level 4 and 5 applications observed on the network.
- **Total Threats:** Sum of vulnerability exploits, known (from Statsdump), and unknown threats (from WildFire cloud) observed.
- **Vulnerability Exploits:** Total vulnerability exploits observed.
- **Known Malware:** Known malware seen on the customer's network, which could be prevented by Threat Prevention.

The “notepad” icon denotes sections that allow full text edit.



Navigation Menu

The navigation bar on the right contains some useful menu items to help you understand key features and customization options.



- 


Clicking on the “gear” icon allows you to remove/add pages or page numbers, or skip to specific pages within the report.
- 


Clicking on the “help” icon allows you to access the Security Lifecycle Review resources.
- 


Clicking on the “tour” icon gives you a quick overview of the report’s layout and the options available for customizing it.
- 


Clicking on the “download” icon downloads a PDF version of the report.

In-Line Help

In-line help is available for key sections and charts in the report. Clicking on the  icon opens up a dialog box with a description of the chart/table displayed in the section.

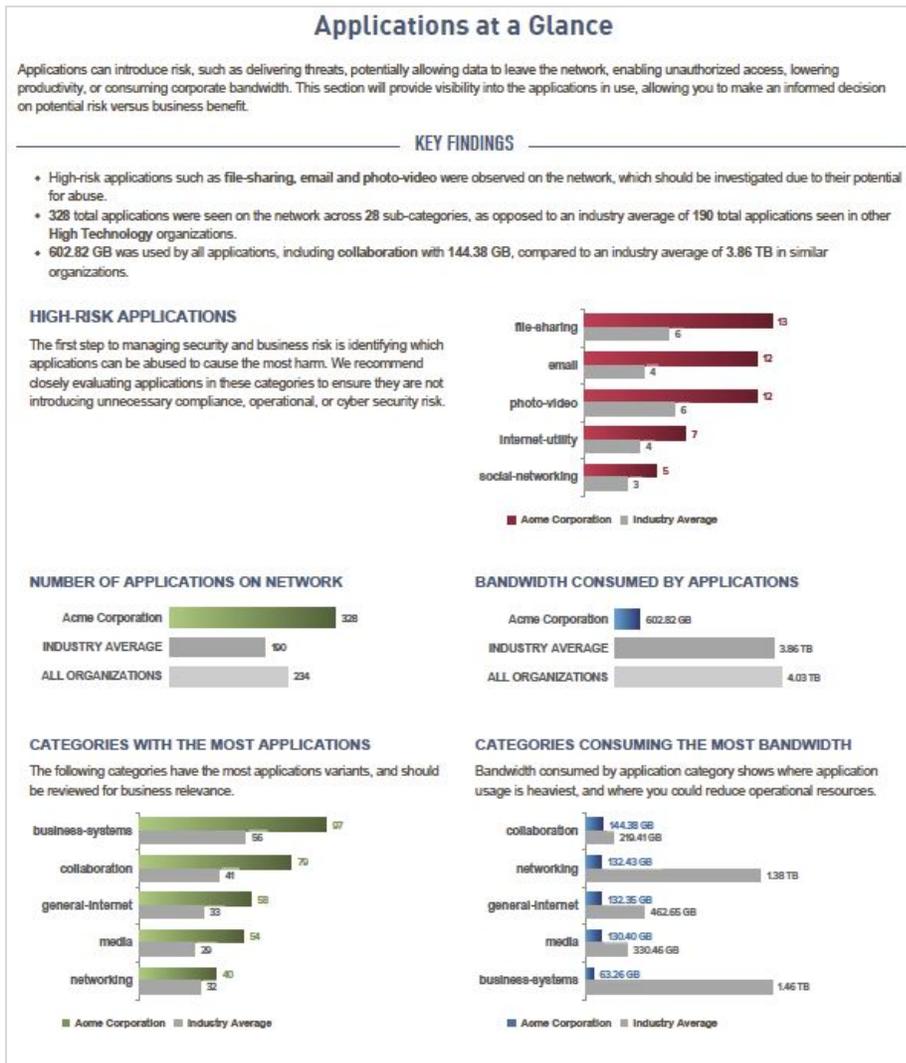
HIGH-RISK APPLICATIONS 

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.

Category	Acme Corporation	Industry Average
file-sharing	13	6
email	12	4
photo-video	12	6
internet-utility	7	4
social-networking	5	3

Applications at a Glance

This section provides a high-level view of the application categories, bandwidth consumed and high-risk applications in use across the network.



Key Highlights

High-Risk Applications

- Count of high-risk (i.e., easily abused) applications per subcategory that are present.
- Default view, composed of social networking, file sharing, email, remote access and encrypted tunnel.
- Displays how many applications per subcategory are seen across all users in your industry for benchmarking.
- View can be customized using the input field.

- Number of Applications on Network:
- Total number of applications on the network.

Number of Applications on Network

- Total number of applications on the network.
- Total applications per top application categories.
- Benchmarks across industry and all organizations.

Bandwidth Consumed by Applications

- Total bandwidth used by applications on the network.
- Total bandwidth used per top application categories.
- Benchmarks across industry and all organizations.

The “High-Risk Applications” section can be customized to better reflect what is important to your organization. The default view is: social networking, file sharing, email, remote access and encrypted tunnel. To customize this section, remove one of the existing subcategories, click on the input field, select a new entry and click “Go.”

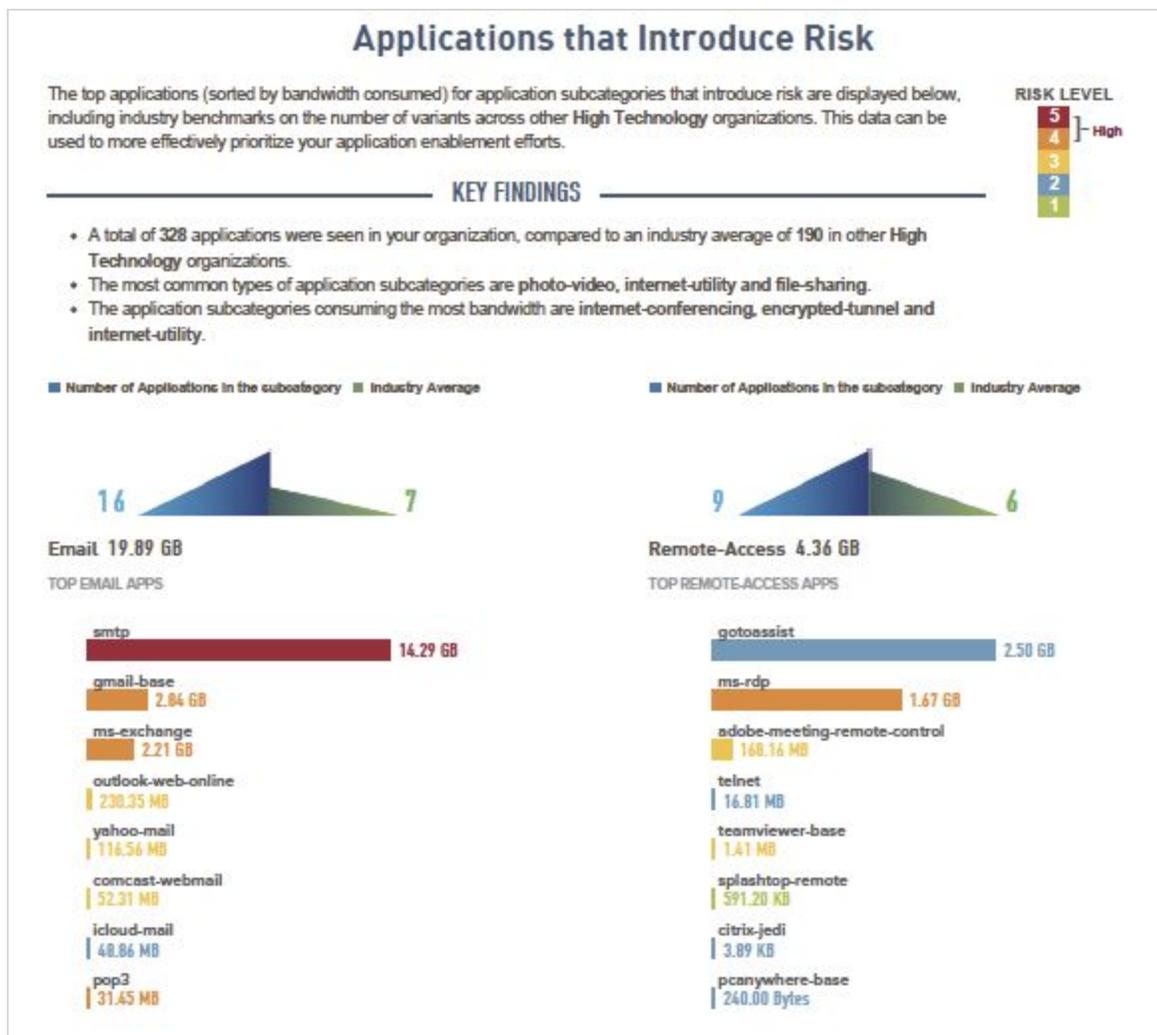


Applications that introduce risk

This section provides information on the top eight application subcategories, sorted in descending order by bandwidth consumed.

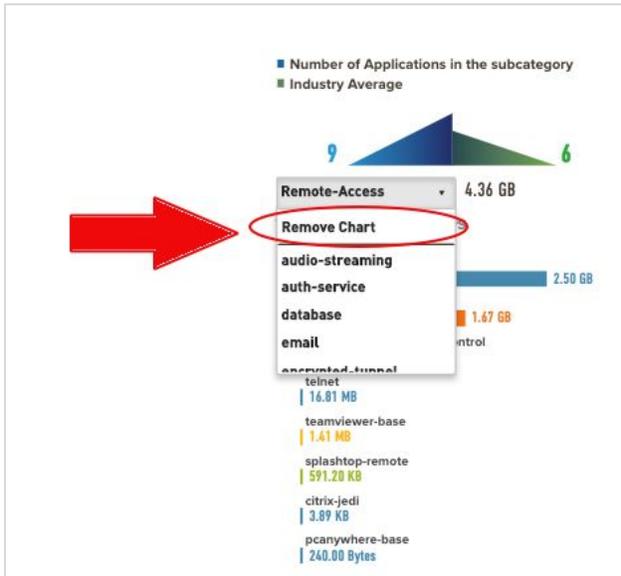
Key Elements

- Each application subcategory contains the top eight applications per subcategory, sorted by bandwidth consumed.
- The number in each header (e.g., 18.52GB for email), shows the total bandwidth consumed by each subcategory, not just the top eight applications. The bar charts in the upper right of each header (e.g., 16/9 for email), show the total number of applications per subcategory versus industry benchmarks.
- The default view shows email, remote access, file sharing, encrypted tunnel, instant messaging, social media, photo-video and proxy. This view can be customized.

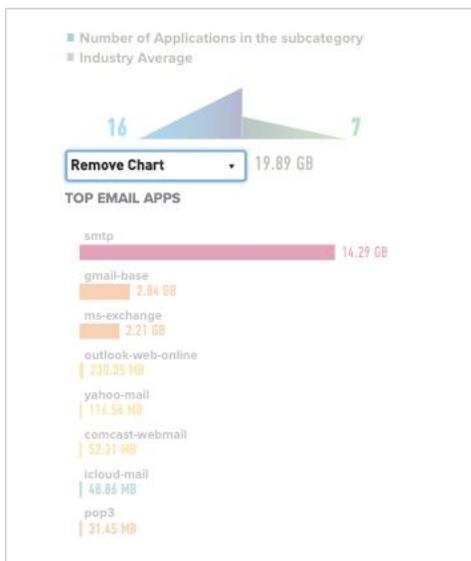


Applications in the view can be customized by selecting any application subcategory from the drop-down

list. This selection will reflect in the application detail table in the next section, which provides further detail on the top applications per subcategory.



The “Remove Chart” option from the dropdown list can be used to remove charts and customize the view. When the “Remove chart option is selected from the drop-down list, the chart grays out allowing the user to select a different application category to replace the chart or delete the chart without replacement. Once the customization is complete, the pdf version of the report will have the applications view with the updated charts.



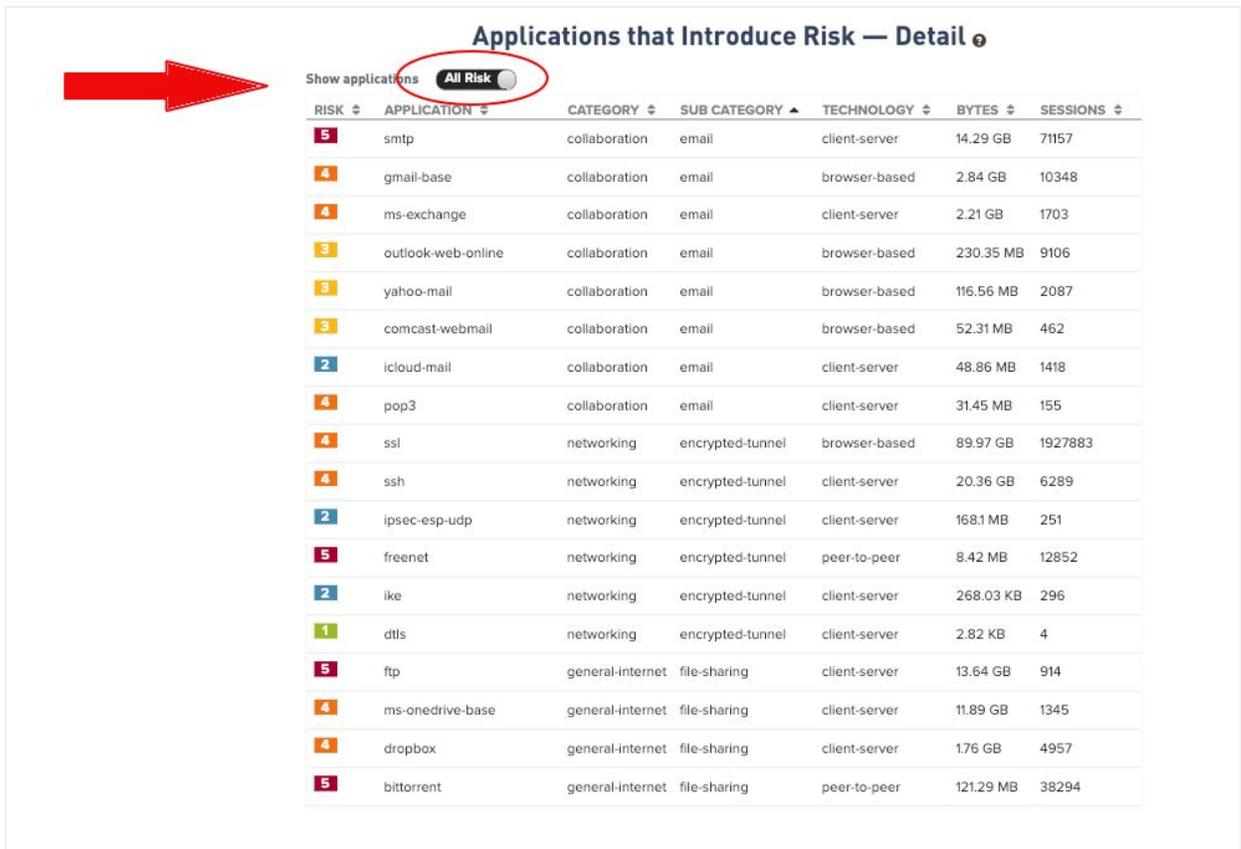
Note: The Palo Alto Networks research team uses the application behavioral characteristics to determine a risk rating of 1 through 5, with 5 being the highest.

Applications that introduce risk - Detail

This section provides details on the application subcategories that introduce risk selected previously, with sortable information on risk level, application, category, subcategory, technology, bytes and sessions displayed.

Key Elements

- Default sort order is by the subcategories selected on the previous page, descending by bytes.
- The data in the application detail view table can be sorted by selecting any column heading.
- The risk toggle button lets you select applications by risk level by switching the toggle to “All Risk” or “High Risk” .



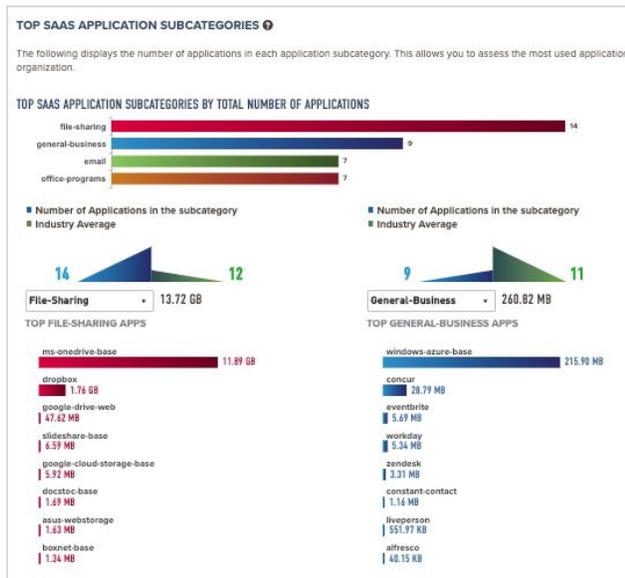
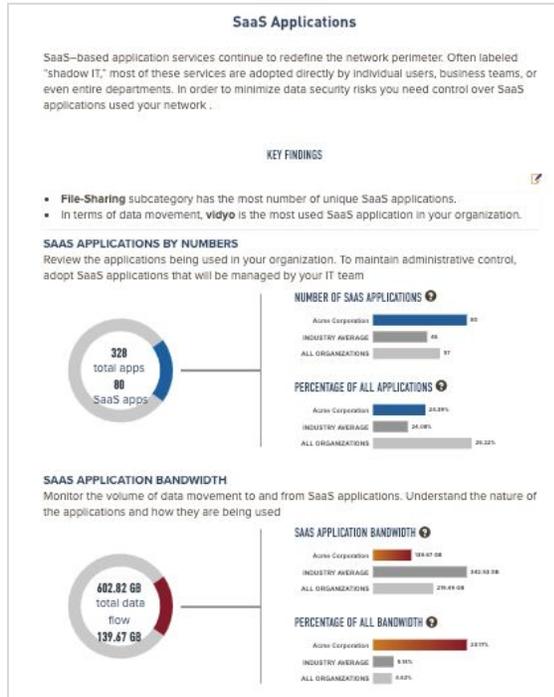
Applications that Introduce Risk — Detail

Show applications **All Risk**

RISK	APPLICATION	CATEGORY	SUB CATEGORY	TECHNOLOGY	BYTES	SESSIONS
5	smtp	collaboration	email	client-server	14.29 GB	71157
4	gmail-base	collaboration	email	browser-based	2.84 GB	10348
4	ms-exchange	collaboration	email	client-server	2.21 GB	1703
3	outlook-web-online	collaboration	email	browser-based	230.35 MB	9106
3	yahoo-mail	collaboration	email	browser-based	116.56 MB	2087
3	comcast-webmail	collaboration	email	browser-based	52.31 MB	462
2	icloud-mail	collaboration	email	client-server	48.86 MB	1418
4	pop3	collaboration	email	client-server	31.45 MB	155
4	ssl	networking	encrypted-tunnel	browser-based	89.97 GB	1927883
4	ssh	networking	encrypted-tunnel	client-server	20.36 GB	6289
2	ipsec-esp-udp	networking	encrypted-tunnel	client-server	168.1 MB	251
5	freenet	networking	encrypted-tunnel	peer-to-peer	8.42 MB	12852
2	ike	networking	encrypted-tunnel	client-server	268.03 KB	296
1	dtls	networking	encrypted-tunnel	client-server	2.82 KB	4
5	ftp	general-internet	file-sharing	client-server	13.64 GB	914
4	ms-onedrive-base	general-internet	file-sharing	client-server	11.89 GB	1345
4	dropbox	general-internet	file-sharing	client-server	1.76 GB	4957
5	bittorrent	general-internet	file-sharing	peer-to-peer	121.29 MB	38294

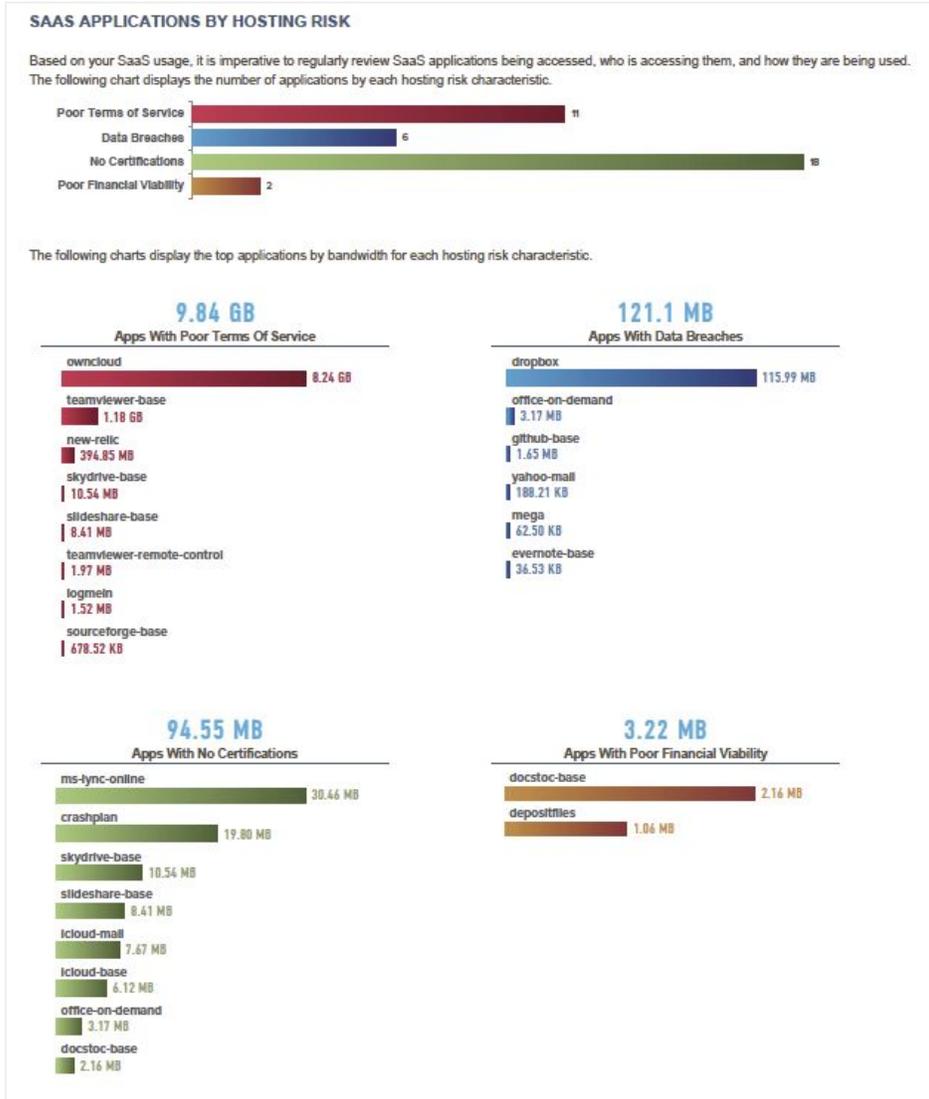
SaaS Applications

The SaaS Applications section provides visibility into the SaaS-based applications observed on the network, sorted by application subcategory.



SaaS Applications By Hosting Risk

The SaaS applications by hosting risk section provides an overview into SaaS Applications with unfavorable risk characteristics such as “Data Breaches”, “Poor Terms of Service”, “No Certifications” etc.can compromise enterprise data and security.



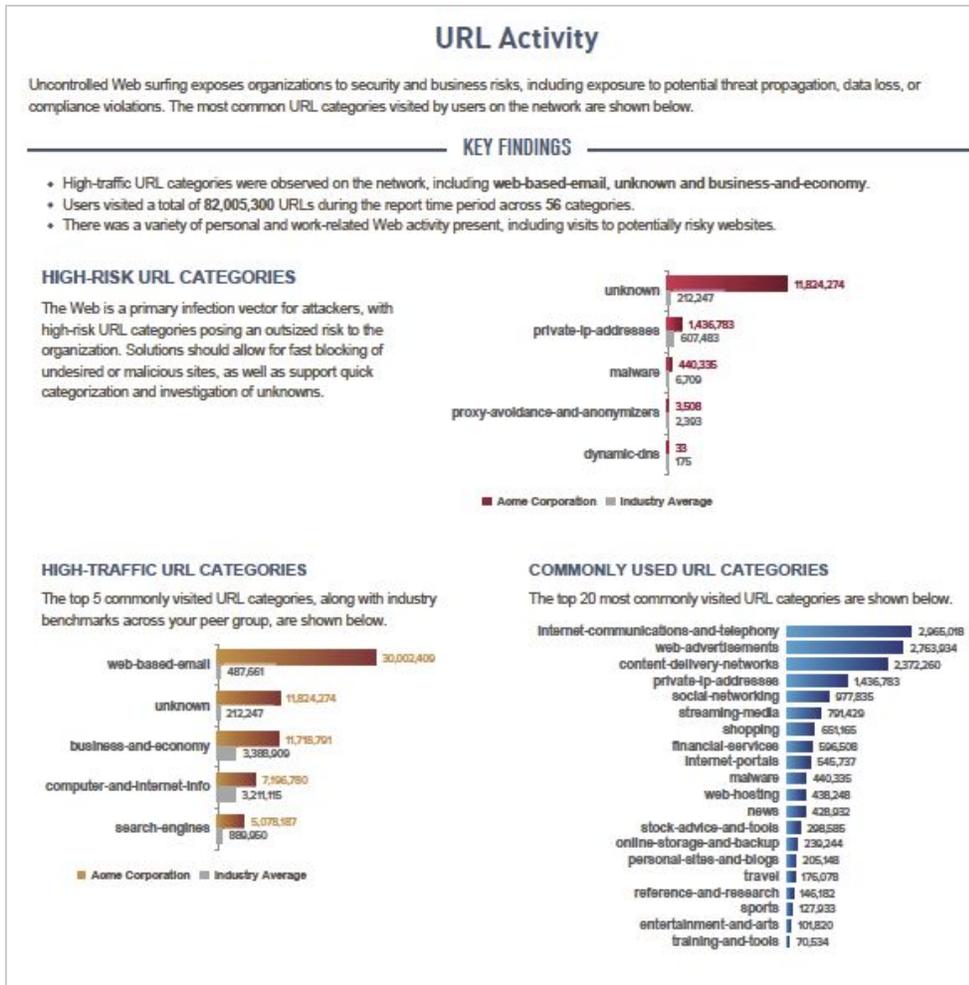
- Displays number of applications for each of the risk characteristics: poor terms of service, data breaches, no certifications and poor financial viability.
- Displays the top 8 applications by bandwidth for each risk hosting characteristics.

SaaS Application Characteristic	Description
Data Breaches	Applications that may have released secure information to an untrusted source within the past three years.
Poor Terms of Service	Applications with unfavorable terms of service that can compromise enterprise data.
No Certifications	Applications lacking current compliance to industry programs or certifications such as SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA, or FEDRAMP.
Poor Financial Viability	Applications with the potential to be out of business within the next 18 to 24 months.
IP Based Restrictions	Applications without IP-based restrictions for user access. Note: The data for the IP Based Restrictions characteristic is available to view in the Network Activity graphs and to generate a custom report.

For a more detailed view of a specific application or characteristic, apply the local filters in the ACC network activity graphs to narrow the scope of the data so that you can isolate specific attributes and analyze information you want to view/present in greater detail.

URL Activity

The URL Activity section displays activity on the URL categories being visited by users on the network.



Key Elements

High-Risk URL Categories

- Pre-defined list of categories that present the most risk to the business, which can be customized via the input field.
- Default view is: unknown, private IP addresses, malware sites, proxy avoidance and dynamic DNS.
- Industry benchmarks are also displayed.

High-Traffic URL Categories

- The top five URL categories being visited, in descending order by hits, including industry benchmarks.
- Commonly used URL categories: the top 20 URL categories, in descending order by hits.

The “High-Risk URL Categories” section can be customized to better reflect what is important to you. To customize this section, remove one of the existing subcategories, click on the input field, select a new entry, and click “Go.”

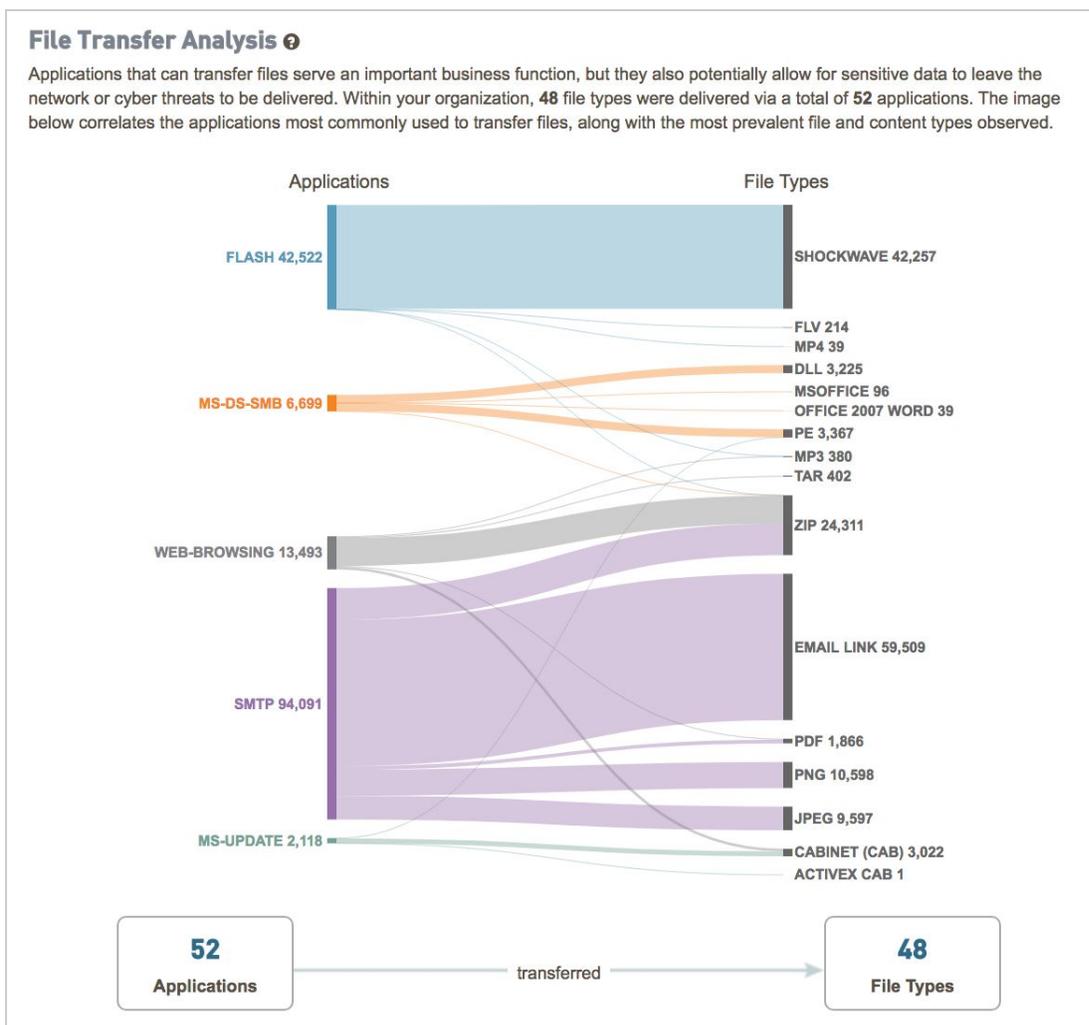


File Transfer Analysis

This page displays the top five applications and the most common content types they are transferring.

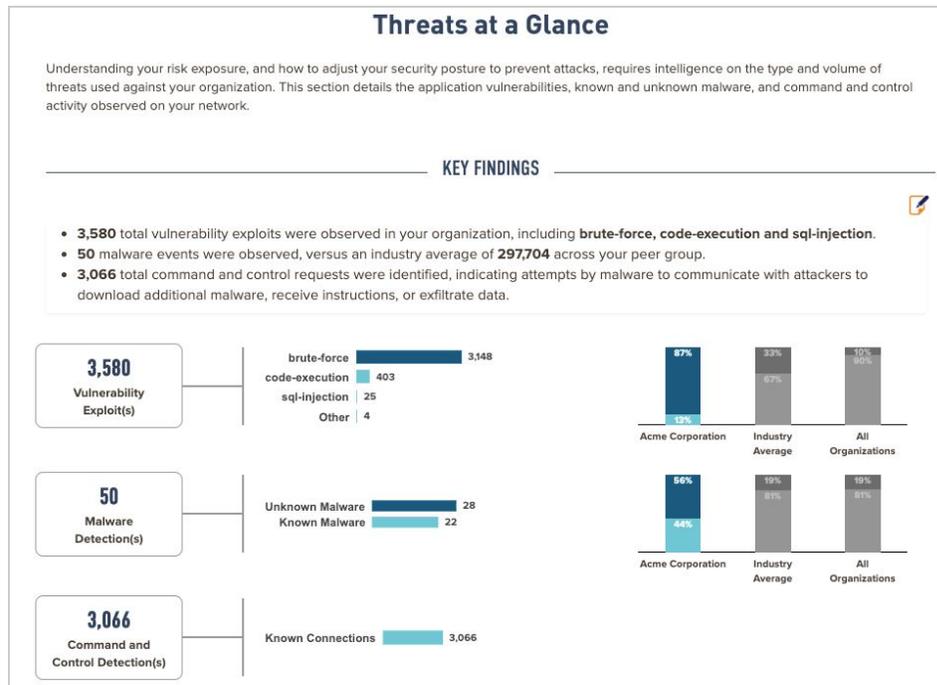
Key Elements

- The left side lists the top five applications delivering the most file types, and the right side indicates up to five of the file types being delivered.
- Correlates which file types are being delivered by which applications.
- The bottom section shares the total number of applications delivering unique file types (and how many types).



Threats at a Glance

This page displays highlights from the vulnerability exploits, malware, and command-and-control activity observed on the network.



Key Elements

Vulnerability Detections

- Total vulnerability exploits observed
- Breakout chart shows the top four categories of vulnerability exploits.
- Industry benchmarks show the percentage of vulnerability exploits in the organization, versus industry peers and all organizations, for the top vulnerability category (for instance, "Botnet") versus all other categories.

Malware Detections

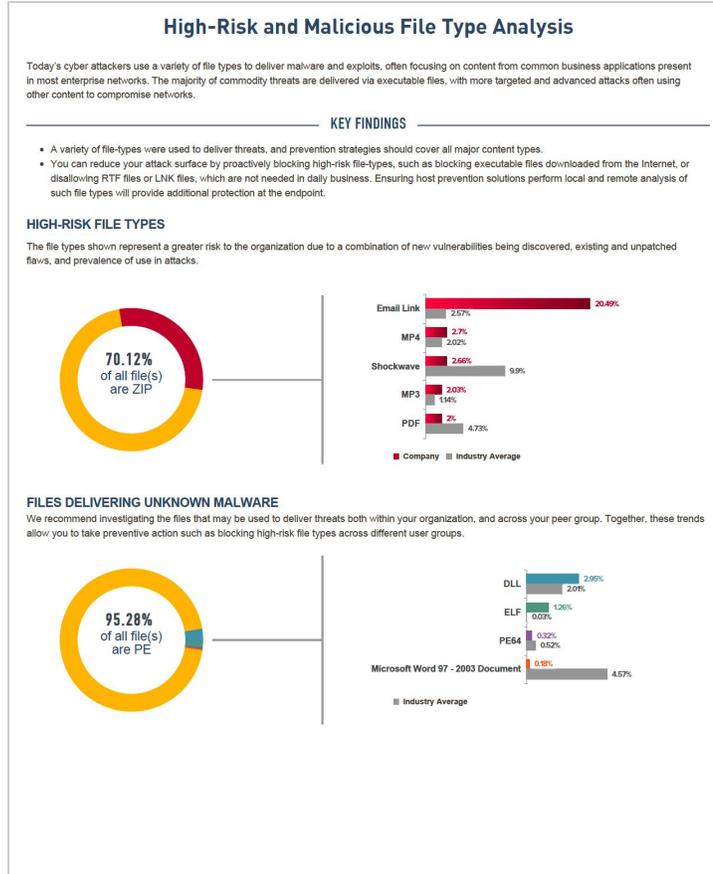
- Sum of known (Threat Prevention) and unknown (WildFire) malware observed.
- Industry benchmarks show the percentages of known and unknown malware seen in the organization versus industry peers and all organizations.

Command and Control Detections

- Sum of known (Threat Prevention) and unknown (WildFire) outbound command-and-control connections.
- Note: “Known” refers to malicious connections from inside the network, whereas “unknown” refers to potential activity observed from malicious samples being executed in the WildFire cloud, not necessarily your local network.
- Industry benchmarks show the percentages of known and unknown command-and-control traffic seen in the organization versus industry peers and all organizations.
- Files Potentially Leaving the Network: Total files leaving the network delivered by the count of applications delivering them.

High Risk and Malicious File Type Analysis

The High-Risk and Malicious File Type Analysis page displays the details of the high risk-file types present on the network as well as those delivering unknown threats detected via WildFire.



Application Vulnerabilities

The Application Vulnerabilities page provides a view of the top five applications experiencing the greatest volume of vulnerability exploits.

Key Elements

- **Applications Delivering Exploits:** Total applications being used to deliver vulnerability exploits, with industry and all organization benchmarks.
- **Vulnerability Detections:** Total count of vulnerability exploit detections, with industry and all organization benchmarks.
- **Unique Vulnerability Exploits:** Total unique vulnerability exploits (the same exploit used repeatedly will only be counted once), with industry and all organization benchmarks.
- **Vulnerabilities per Application:** Top 10 applications listed in descending order by severity level, then count. Includes count of vulnerability exploits, threat name, severity, threat type and CVE, when available.
- **Severity Filter:** The filter icon next to the “Severity” header provides the option to filter the vulnerability exploits by the severity levels: Critical, High, Info, Medium, Low .

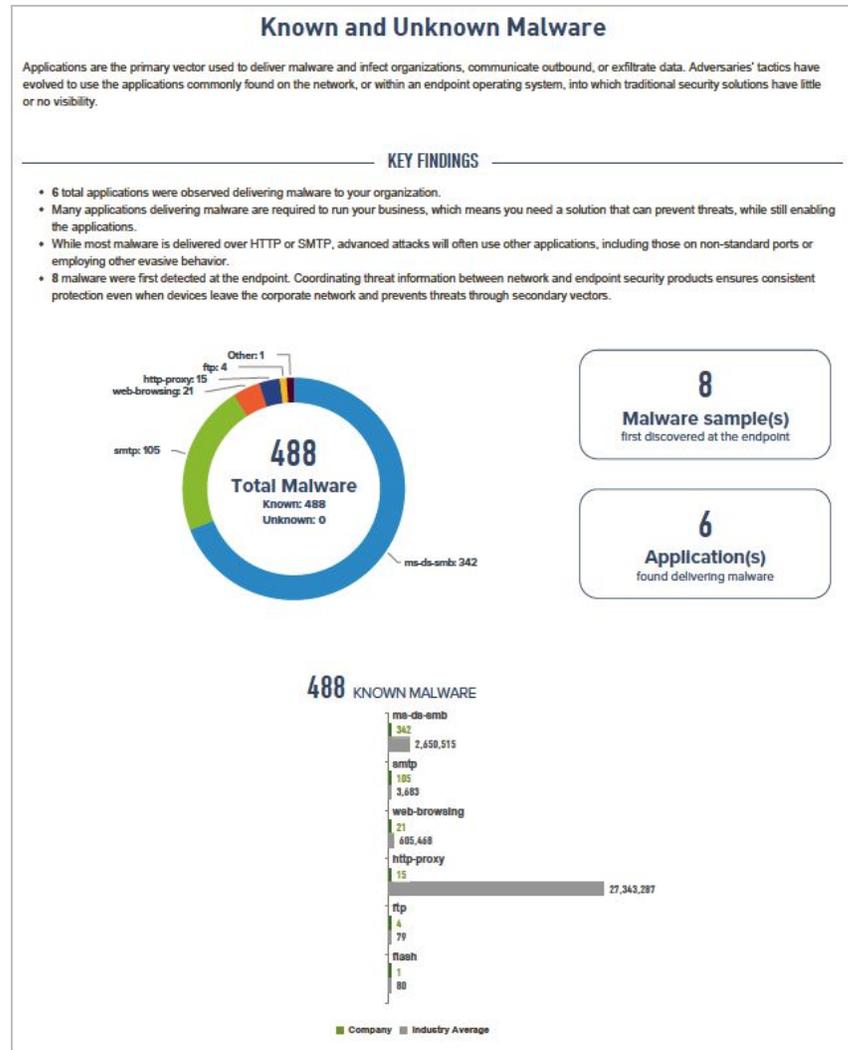
Vulnerability Exploits per Application (top 5 applications with most detections) ?

DETECTIONS	APPLICATION & VULNERABILITY EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
653,523	ssl			
1	OpenSSL SSLv2 Malformed Client Key Parsing Buffer Overflow Vulnerability	Critical		CVE-2002-0656
1	Microsoft IIS Server SChannel Denial of Service Vulnerability	High		CVE-2010-3229
1	Mozilla Network Security Services SSLv2 Server Stack Overflow	High		CVE-2007-0009
633,867	Use of insecure SSLv3.0 Found in Server Response	Info		CVE-2014-3566
19,448	POODLE Bites Vulnerability	Info		CVE-2014-8730
197	OpenSSL TLS Heartbeat Found	Info		CVE-2016-0800;
8	SSL Version 2 Weak RSA Cipher Detected	Info		CVE-2016-0703
82,383	ms-ds-smb			
9	Microsoft SMB Client Response Parsing Vulnerability	Critical	code-execution	CVE-2016-3385
36	SMB: User Password Brute-force Attempt	High	brute-force	
326	Microsoft Windows SMB NTLM Authentication Lack of Entropy Vulnerability	Medium	brute-force	CVE-2010-0231
6	Microsoft Windows Registry Read Attempt	Low	info-leak	
2	Microsoft Windows WinReg Access Attempt	Low	code-execution	
1	Microsoft Windows RPC Encrypted Data Detected	Low	code-execution	
77,441	Microsoft Windows SMB Negotiate Request	Info	brute-force	
3,825	Service Enum Through SMB ServiceEnum2	Info	info-leak	
559	NetBIOS null session	Info	info-leak	
141	Windows SMB Login Attempt	Info	brute-force	

Known and Unknown Malware

This section shows the top 10 applications delivering known (Threat Prevention) and unknown (WildFire) malware and the number of malware detected at Endpoint.

Note: Availability of information on Malware detected at the Endpoint is based on the products deployed and the malware found in the network.



Key Elements

- **Total Malware:**The donut chart on the left shows the total Malware detected with a break down of known and unknown malware
- **Malware detected at the Endpoint:**The first callout on the right, next to the donut chart shows shows

the count of Malware detected at the Endpoint (*Availability of information on Malware detected at the endpoint is dependent on the products deployed and the malware observed in the network*)

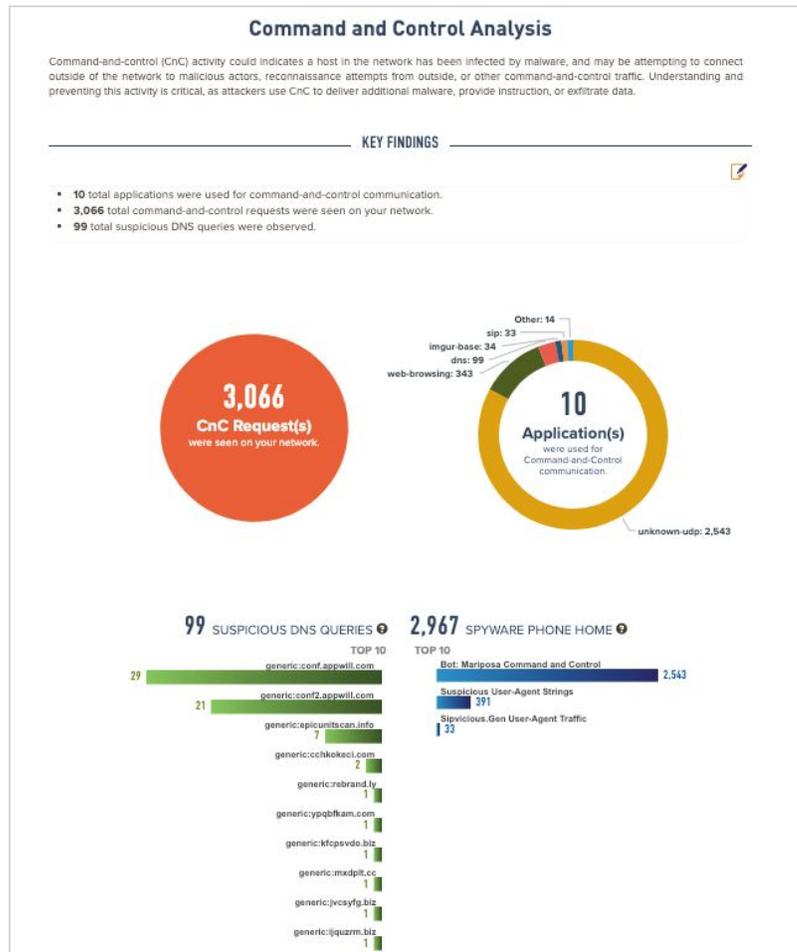
- **Applications delivering malware:** The second callout on the right, next to the donut chart shows shows the number of Applications found delivering malware in the network.
- The bar chart on the right displays the count of known malware being delivered per application for the top 3 applications delivering malware observed in the network.
- The bar chart on the left shows the count of unknown malware being delivered per application , derived via Wildfire for the top 3 applications delivering malware observed.

Command and Control Analysis

This page displays outbound malicious communication from infected hosts on the network from a known threat perspective.

Key Elements

- **Command and Control Activity by Application:** Volume of outbound malicious queries for the top five applications, by count of instances of command-and-control activity.
- **Spyware Phone Home:** Total of all “spyware” category command-and-control activity, and the top threats observed.
- **Suspicious DNS Queries:** Total of all “suspicious DNS” category command-and-control activity, and the top threats observed.
- **Top Malicious Behavior Tags:** List of top tags associated with the malware found in the network
- **Threats by Destination Countries:** A map of countries that malware sessions targeted. The map highlights the country that received the most number of malware sessions.



Top Malware Family Tags	
Tag	Count
VirLock	1,204
ELFinist	311
Galgylt	254
Satori	133
Gogys	115
Upatre	78
il_fm_Urnuy_key	77
Urnuy	76
GandCrab	71
gsr_migam_peculi arGalgylt	61

Top Campaign Tags	
Tag	Count
gsr_lisa_Pecunia	7
SilverTerror	2
BlackVine	1
gsr_mscot_misc_ Tekide	1
OperationComando	1

Top Malicious Behavior Tags	
Tag	Count
il_bar_enum_proc esses	2,350
gsr_lisa_MaintainPe nistence	1,601
gsr_molim_Win_S ervice_Created	1,437
HttpNoUserAgent	1,345
il_fm_use_winnr net	1,326
gsr_ysamuel_MSV B/M80	1,237
DisableJAC	1,192
gsr_molim_onum_l threads	803
ProcessInjection	715
gsr_mscot_Super HiddenFiles	471

- Linked to threats that belong to a certain Malware Family
- Part of a larger Campaign of attacks
- A type of Malicious Behavior that indicates that your system has been compromised
- Public tags are tags shared with the AutoFocus community by your organization and other AutoFocus users. They are visible to all AutoFocus users.
- Private tags are visible only to your organization. Allows you to tag a sample hash or a set of search conditions that might be specific or especially significant to your environment.
- Unit 42 (alerting) tags are created by Unit 42 (the Palo Alto Networks) threat intelligence and research team) for threats and campaigns that pose a direct security risk.
- Unit 42 creates alerting tags for threats discovered by individuals or organizations outside of Unit 42. These tags have a pointed and marked top right corner.



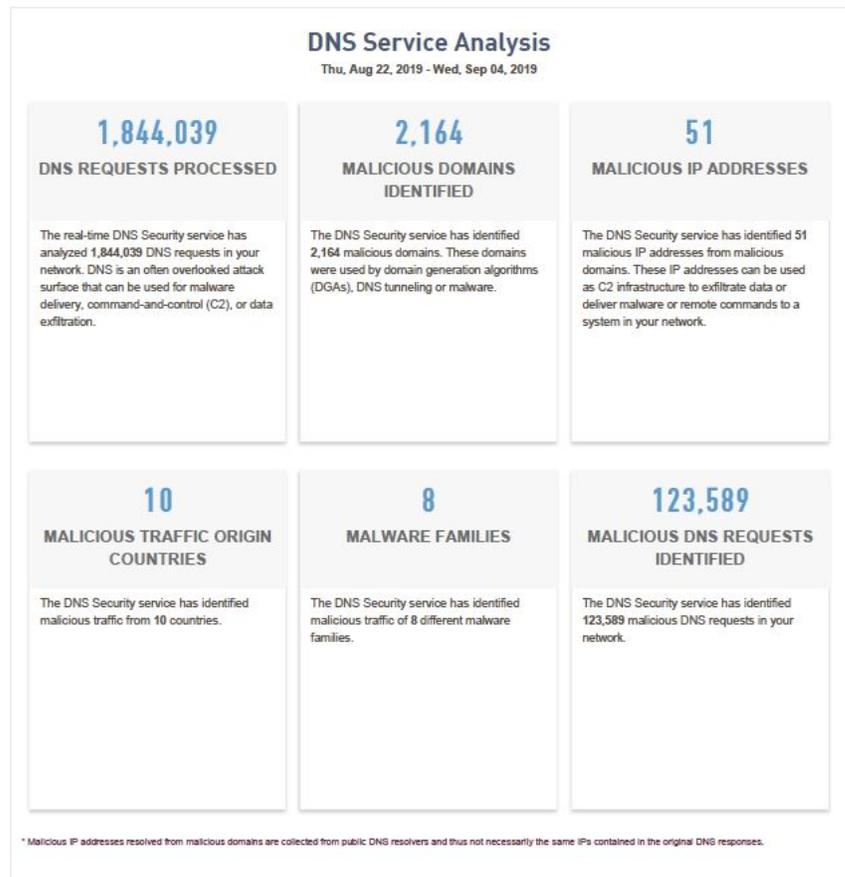
DNS Service Analysis

Note: DNS Service Analysis data findings are available in the SLR for customers with DNS Service Subscription

Summary

This section displays a summary of the findings from the DNS Security service, a cloud-based analytics platform. Findings include :

- DNS Requests processed
- Malicious Domains Identified
- Malicious IPs identified
- Malicious Traffic Origin Countries
- Malware Families
- Malicious Requests identified

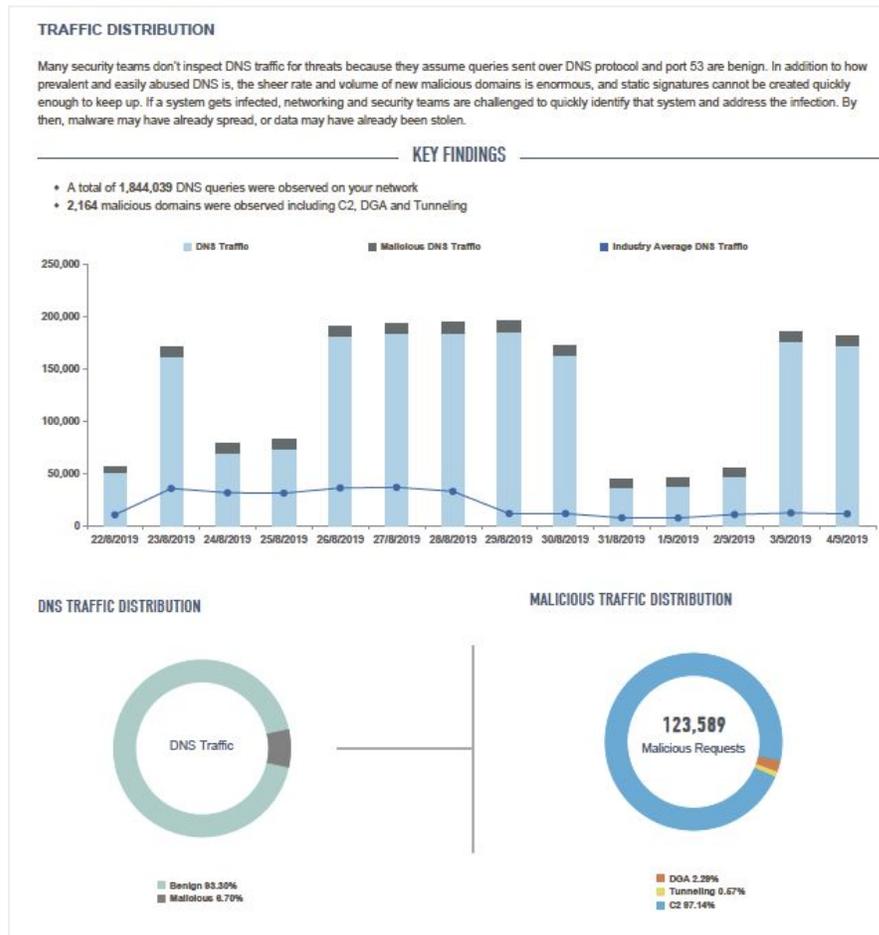


Traffic Distribution

Displays percentage of DNS traffic, Malicious traffic and the distribution of malicious traffic (C2, DGA and Tunneling)

Key Elements

- Bar chart displaying DNS traffic, malicious traffic and the industry benchmarks for DNS traffic
- Donut chart on the left displays the percentage of DNS and Malicious traffic
- Donut chart on the right displays the percentage of C2, DGA and Tunneling queries

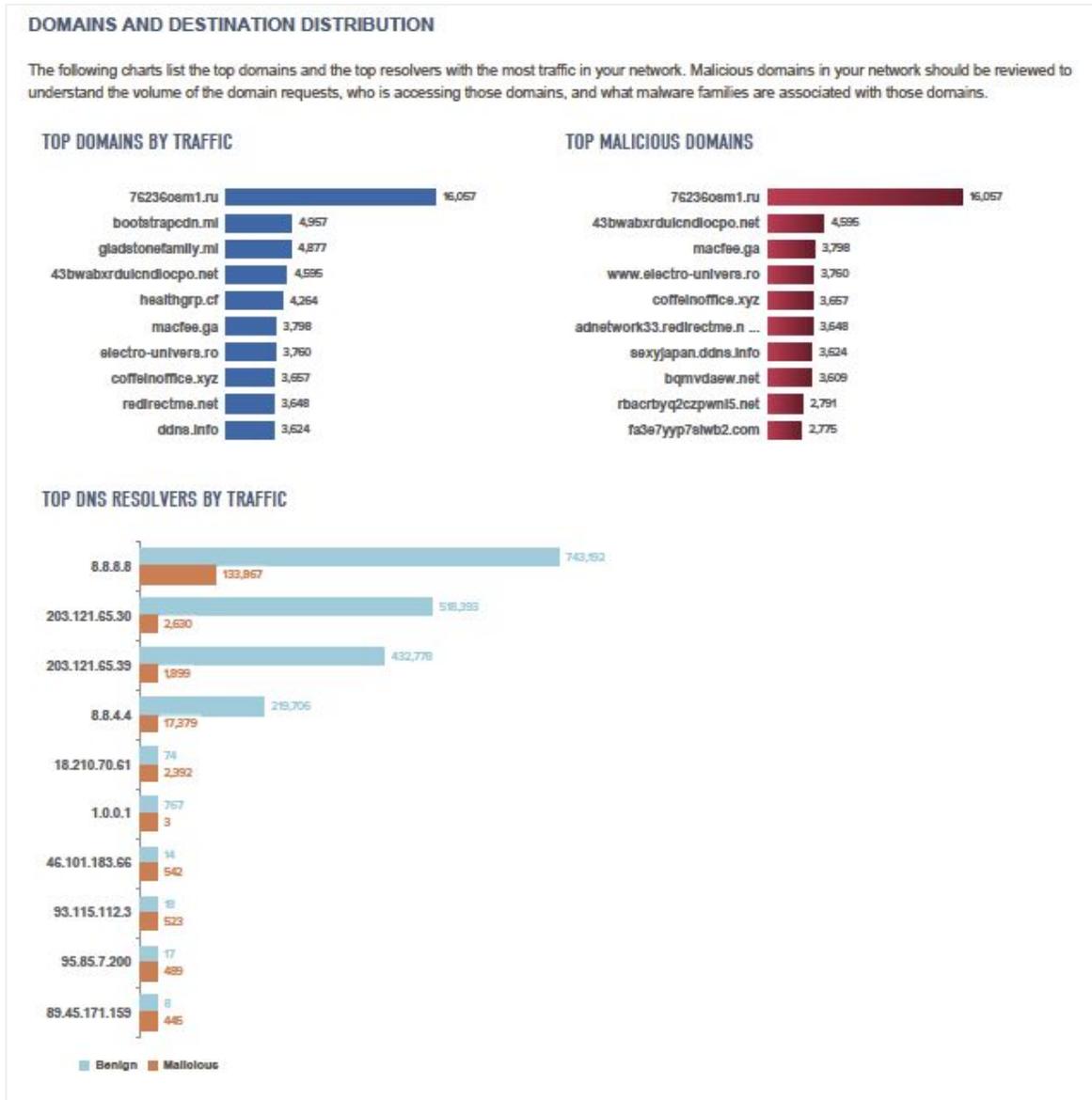


Domains and Destination Distribution

Displays top domains and top destination IPs with the most traffic in your network

Key Elements

- Bar chart on the top left displays top domains by traffic
- Bar chart on the top right displays top malicious domains IPs by traffic
- Bar chart on the bottom left displays top DNS resolvers by traffic observed in your network

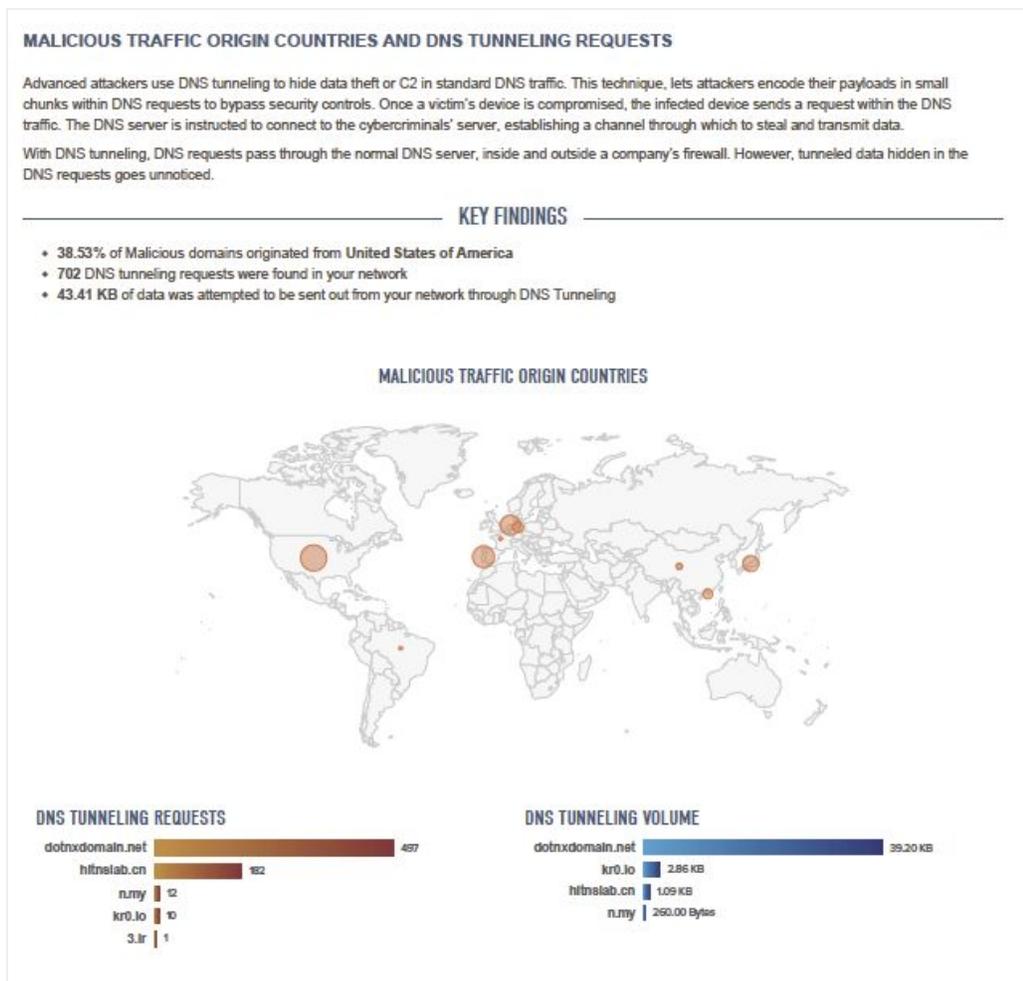


Malicious Traffic Origin Countries and DNS Tunneling Requests

Displays countries identified as sources for Malicious domains, findings on DNS tunneling requests and DNS tunneling volume.

Key Elements

- A map of countries from which malicious traffic originated. The orange circles in the map highlight the countries from which most of the malicious traffic originated.
- Bar chart on the bottom right displays top malicious domains by DNS tunneling volume
- Bar chart on the bottom left displays top malicious domains by number of tunneling requests observed in your network



Known Malware and Families

Displays information on malware families associated with the malicious domains along with information on the tags observed in the network.

Malware Family	Domain Count	Top Domains	Description
corebot	170	<ul style="list-style-type: none"> u8zpkguu.186f9a0e1buu1au55w.com apypk91yy.h0ovx2l2920mk3wu8im.com etzdrc4soz.11ban2mp48m4m1kh3ok26zk.com dusb7c40d.k4ergp68o181qy1n5bn.com u1qp0y9wbcry9eedcuhz1e.0ru1c58hthlyg5epbhazk7m.com 8n2l12uqgc67k3bq4vhsq.07zlnrto2hpgwtju59q.com 2opnom-hr.sqzwy2503f1qrkeliou.com km41ve5gvvy.ppon1x0mvpbf5v2xqz.com eau7oezj-c4vaydaok1bq.26u72l5lg5h0pb9f0p5o.com tylhae-ayj.bx547p7x70e3yo2q63vw.com 	CoreBot's most interesting facility is its plugin system, enabling it to be modular and easily supplemented with new theft capabilities. CoreBot downloads plugins from its command-and-control (C&C) server right after setting its persistence mechanism on the endpoint. It then loads the plugins using the pluginint export function in the plugin's DLL. At present, the main plugin is called 0stealer. CoreBot steals passwords, but it is currently incapable of intercepting real-time data from Web browsers. Instead, it steals saved passwords stored in the endpoint's browsers, scanning for passwords on all the most popular browsers. CoreBot further searches an extensive list of FTP clients, mail clients, webmail accounts, cryptocurrency wallets, private certificates and personal data from a list of various desktop applications.
madmax	27	<ul style="list-style-type: none"> ezbv0ka5-clblepusu8haemvz.dsuno89lo.com x88dxyjjuuf2chp.aklntks09i.com gf7uvwnod2cb17jpdhx.ftjzsz5y6.com aua82hazamoq.qj96bnmuk.com pfesh4330cqy.z5ib8pda1a.com gfhfuyucpp6g6o9b.h9f2nsdb4.com www.8s32e590un.com zyzefan-3.3ib1smwm.com s5.mkkicdnv6.com s4.mkkicdnv4.com 	A targeted malware family which uses a DGA as a backup communications mechanism. Uses extensive obfuscation techniques to defeat static analysis attempts.
rovlrx	14	<ul style="list-style-type: none"> bluasmeel.uioicsm0lp7g1ejb7.com 8xqfo5mdekaxxy.98elmz90c6a22ew6.com mstju5i1gnxj.50wz3g977p9vza91y.com nbub-ggg11hg1vutu.7q13bkq0elguey7v1.com xvwue022.snzzro78881pihq6v.com je8ad6cq2vgge5r3.705qatzogqjhcopo.com z225v244v-mcpcdxu-gzaw.gueygfvrqx118r6lts.com tgj-ol774t1nuw.ja8wegerwq2pazstea.com 29haxhov7kub42vn7k6n-9.prux2k250za0dfeg8.com or-w4el5bz7aw95cwlz1z.pvgtd60q0svhno3v0.com 	Rovlrx writes malicious rootkit drivers to an unpartitioned space of the NTFS drive. This effectively hides the driver since this unpartitioned space cannot be seen by the operating system and security products.

Report Summary

The summary page provides a complete view of all report data, followed by an editable page.

Key Elements

- Summary of the key statistics from the Executive Summary page and various “Key Findings” throughout the report.
- Business-level recommendations.

Summary: Acme Corporation

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 Corporation**, 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 **file-sharing, email and photo-video** 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 **195** total applications seen in other **High Technology** organizations.
- **3,580** total vulnerability exploits were observed across the following top three applications: **web-browsing, smtp and ftp**.
- **50** malware events were observed, versus an industry average of **297,629** across your peer group.
- **10** total applications were used for command and control communication.

KEY FINDINGS

328 APPLICATIONS IN USE	74 HIGH RISK APPLICATIONS	80 SAAS APPLICATIONS
3,580 VULNERABILITY EXPLOITS	6,696 TOTAL THREATS	50 MALWARE DETECTED Known: 22 Unknown: 28

RECOMMENDATIONS

- Implement safe application enablement policies, 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.

