Capture Threat Assessment

User Guide

SONICWALL®

Contents

1

Overview

Capture Threat Assessment (also known as CTA) is a SonicWall service that provides network traffic and threat report generation. The service is provided directly from the SonicOS firewall interface. You can navigate to the Capture Threat Assessment page to generate the report. The output is generated in PDF format, and previous reports are saved in the cloud and displayed in a table so you can access them later.

Topics:

- Description
- Changes Since Last Release
- Features
- CTA 1.0 Report Availability

Description

The Capture Threat Assessment service accurately identifies real-time vulnerabilities, exploits, intrusions and other network-based threats. With it, you can see security gaps in the organization and better understand the risks. Components of this service includes:

- A risk assessment and management report with detailed information about your environment
- A simple risk-scoring system that gives an accurate appraisal of your risk profile
- Early detection of threats so you can respond before the threats become security liabilities

The data used for this analysis is gathered by SonicWall during the report time period. It is a snapshot in time of the different threats that have been identified and blocked by your SonicWall firewall. A report run today may show different threats and risks than a report run tomorrow. The report also provides application and user-based data, including application traffic, top users, top URL categories, session counts and top countries to give insight into the traffic on your network.

A big benefit of the CTA report is that you can schedule a complimentary review and interpretation with one of our security experts. You can get an even stronger understanding of the risks and review solutions to combat those risks.

Changes Since Last Release

The new Capture Threat Assessment has been redesigned. Some content has been enhanced to include recommendations, and additional risk parameters have been added. The document template and data presentation has been updated to organize data more effectively and improve usability. You can customize your CTA report by personalizing it with company names and logos, but also by selecting which parameter to include or exclude. That way you can focus on things that are most important to you.

Specific improvements and features for this release include the following:

- Executive information is summarized in a single page and can be customized.
- Details about URL activity and associated threat details is provided.
- File type and application visibility has been added.
- Global and industry level comparisons show how your infrastructure compares to others.
- The organizational risk posture shows where your organization is at risk.
- Recommendations have been expanded to include actionable items.
- Reports now have some customizable features.

Refer to Features for more information.

Features

For this release, several new features have been added or enhanced in the Capture Threat Assessment.

Topics:

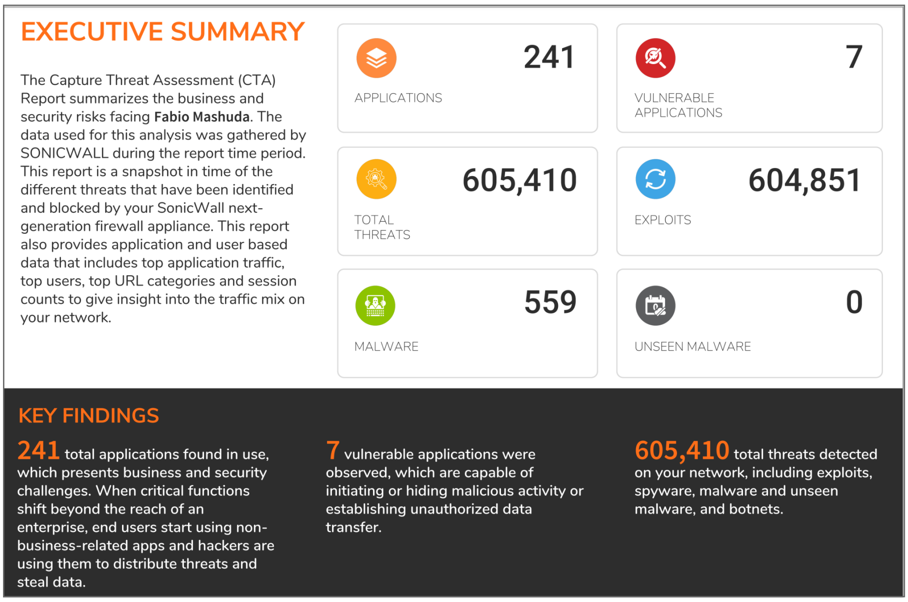
- Executive Summary
- Recommendations
- Application Information
- Shadow IT
- Web Activity
- File Sharing Applications
- Glimpse of the Threats
- Usage Statistics
- Report Configuration
- Capture Cloud Ecosystem

Executive Summary

The Executive Briefing of the prior version transformed into a more informative Executive Summary. Aside from description of the CTA report, you can see a roll-up of certain key elements. They include:

- Applications
- Vulnerable Applications
- Total threats
- Exploits
- Malware
- Zero-day attacks

Further, the Executive Summary takes the top elements from above and summarizes the key findings associated with them.



EXECUTIVE SUMMARY

The Capture Threat Assessment (CTA) Report summarizes the business and security risks facing **Fabio Mashuda**. The data used for this analysis was gathered by SONICWALL during the report time period. This report is a snapshot in time of the different threats that have been identified and blocked by your SonicWall next-generation firewall appliance. This report also provides application and user based data that includes top application traffic, top users, top URL categories and session counts to give insight into the traffic mix on your network.

241 APPLICATIONS	7 VULNERABLE APPLICATIONS
605,410 TOTAL THREATS	604,851 EXPLOITS
559 MALWARE	0 UNSEEN MALWARE

KEY FINDINGS

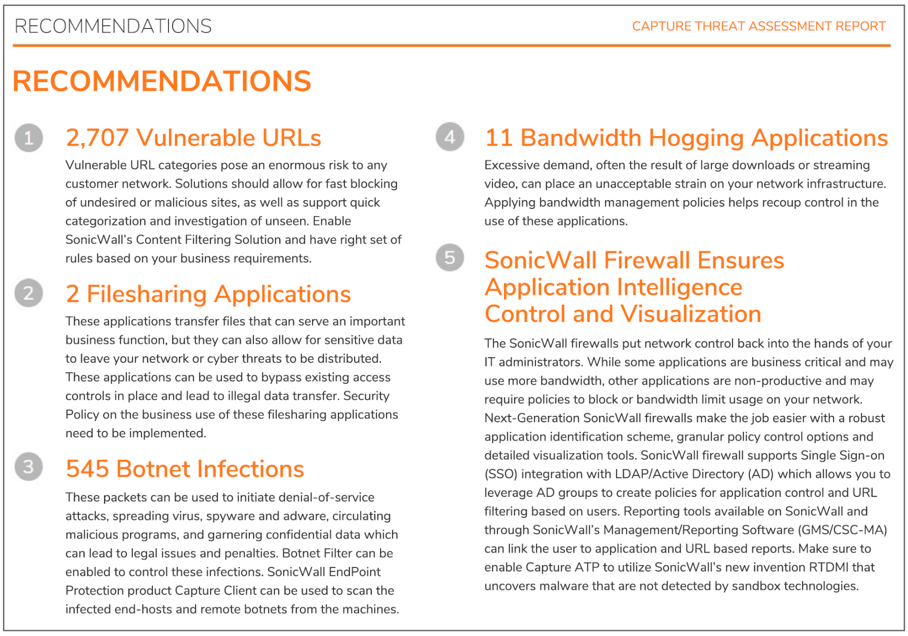
241 total applications found in use, which presents business and security challenges. When critical functions shift beyond the reach of an enterprise, end users start using non-business-related apps and hackers are using them to distribute threats and steal data.

7 vulnerable applications were observed, which are capable of initiating or hiding malicious activity or establishing unauthorized data transfer.

605,410 total threats detected on your network, including exploits, spyware, malware and unseen malware, and botnets.

Recommendations

The Recommendations section follows the Executive Summary in the CTA report.



RECOMMENDATIONS CAPTURE THREAT ASSESSMENT REPORT

RECOMMENDATIONS

1 2,707 Vulnerable URLs

Vulnerable URL categories pose an enormous risk to any customer network. Solutions should allow for fast blocking of undesired or malicious sites, as well as support quick categorization and investigation of unseen. Enable SonicWall's Content Filtering Solution and have right set of rules based on your business requirements.

2 2 Filesharing Applications

These applications transfer files that can serve an important business function, but they can also allow for sensitive data to leave your network or cyber threats to be distributed. These applications can be used to bypass existing access controls in place and lead to illegal data transfer. Security Policy on the business use of these filesharing applications need to be implemented.

3 545 Botnet Infections

These packets can be used to initiate denial-of-service attacks, spreading virus, spyware and adware, circulating malicious programs, and garnering confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections. SonicWall EndPoint Protection product Capture Client can be used to scan the infected end-hosts and remote botnets from the machines.

4 11 Bandwidth Hogging Applications

Excessive demand, often the result of large downloads or streaming video, can place an unacceptable strain on your network infrastructure. Applying bandwidth management policies helps recoup control in the use of these applications.

5 SonicWall Firewall Ensures Application Intelligence Control and Visualization

The SonicWall firewalls put network control back into the hands of your IT administrators. While some applications are business critical and may use more bandwidth, other applications are non-productive and may require policies to block or bandwidth limit usage on your network. Next-Generation SonicWall firewalls make the job easier with a robust application identification scheme, granular policy control options and detailed visualization tools. SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on SonicWall and through SonicWall's Management/Reporting Software (GMS/CSC-MA) can link the user to application and URL based reports. Make sure to enable Capture ATP to utilize SonicWall's new invention RTDMI that uncovers malware that are not detected by sandbox technologies.

Based on what the reporting shows, the top five recommendations are provided. A brief description and the recommended corrective action is provided for each.

Application Information

The Application information has been expanded to show different views of similar data.

Topics:

- Application Highlights
- Vulnerable Applications
- Application Categories
- Risky Applications

Application Highlights

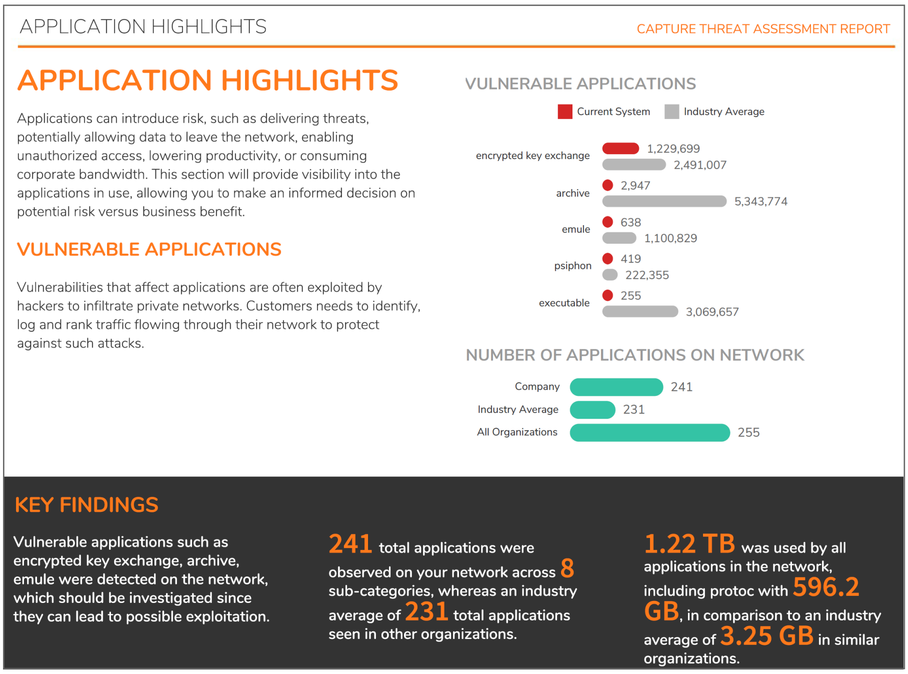
Applications can introduce different kinds of risk. These include:

- Delivering threats
- Potentially allowing data to leave the network
- Enabling unauthorized access
- Lowering productivity
- Consuming corporate bandwidth

The Application section provides visbility into the applications in use so you can compare the risk of their continued use to the business benefit.

Vulnerable Applications

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. By logging and ranking traffic through these applications, you can also take steps to protect them. The Vulnerable applications are identified and charted. You can see how you do compared to the average value of companies in your industry and also compared to all organizations.



APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION HIGHLIGHTS

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.

VULNERABLE APPLICATIONS

Vulnerabilities that affect applications are often exploited by hackers to infiltrate private networks. Customers needs to identify, log and rank traffic flowing through their network to protect against such attacks.

KEY FINDINGS

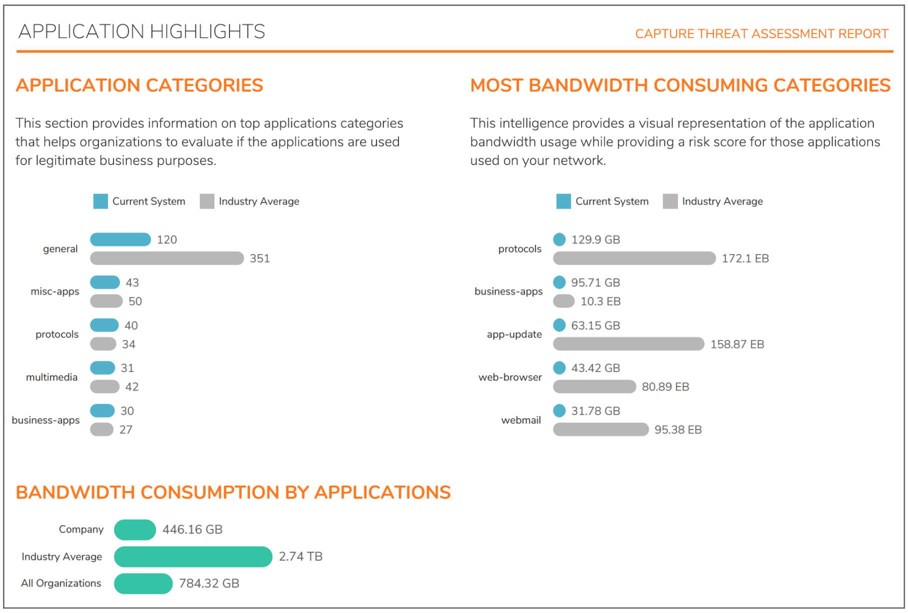
Vulnerable applications such as encrypted key exchange, archive, emule were detected on the network, which should be investigated since they can lead to possible exploitation.

241 total applications were observed on your network across 8 sub-categories, whereas an industry average of 231 total applications seen in other organizations.

1.22 TB was used by all applications in the network, including protoc with 596.2 GB, in comparison to an industry average of 3.25 GB in similar organizations.

Application Categories

You can use Application Categories to organize the applications and determine if they are used for legitimate business purposes. Your numbers are compared to industry averages so you can validate against them. Within this section you can also see what bandwidth is being consumed by certain categories or by specific applications.



APPLICATION HIGHLIGHTS

CAPTURE THREAT ASSESSMENT REPORT

APPLICATION CATEGORIES

This section provides information on top applications categories that helps organizations to evaluate if the applications are used for legitimate business purposes.

	Current System	Industry Average
general	120	351
misc-apps	43	50
protocols	40	34
multimedia	31	42
business-apps	30	27

MOST BANDWIDTH CONSUMING CATEGORIES

This intelligence provides a visual representation of the application bandwidth usage while providing a risk score for those applications used on your network.

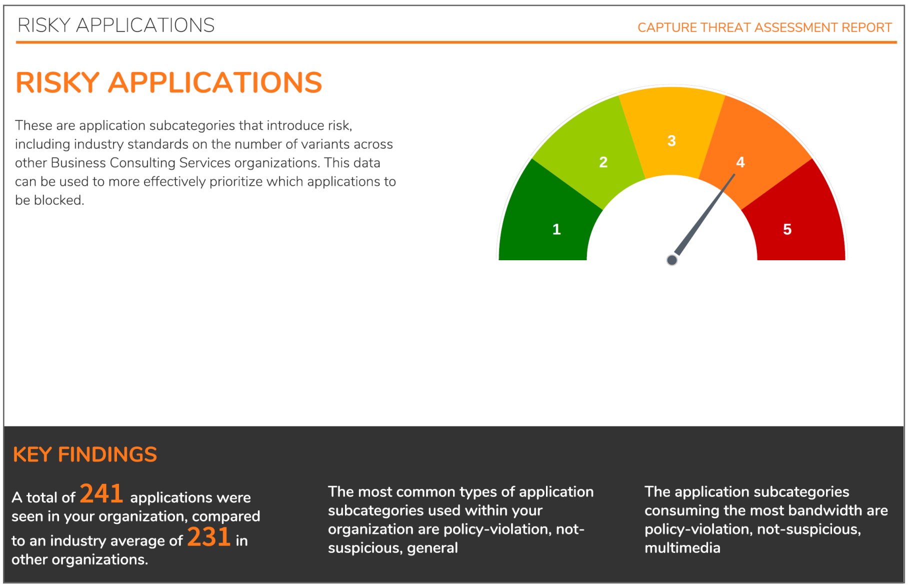
	Current System	Industry Average
protocols	129.9 GB	172.1 EB
business-apps	95.71 GB	10.3 EB
app-update	63.15 GB	158.87 EB
web-browser	43.42 GB	80.89 EB
webmail	31.78 GB	95.38 EB

BANDWIDTH CONSUMPTION BY APPLICATIONS

Company	446.16 GB
Industry Average	2.74 TB
All Organizations	784.32 GB

Risky Applications

The section on Risky Applications has been expanded to include several views of the data. It's an attempt to assess the risk of your applications by first categorizing them into industry-standard categories and then comparing them to the number of variants that exist across other organizations. This data can help you decide what applications need to be blocked. You can immediately see where you fall on a 1 to 5 risk scale to understand your overall risk.



RISKY APPLICATIONS

CAPTURE THREAT ASSESSMENT REPORT

RISKY APPLICATIONS

These are application subcategories that introduce risk, including industry standards on the number of variants across other Business Consulting Services organizations. This data can be used to more effectively prioritize which applications to be blocked.

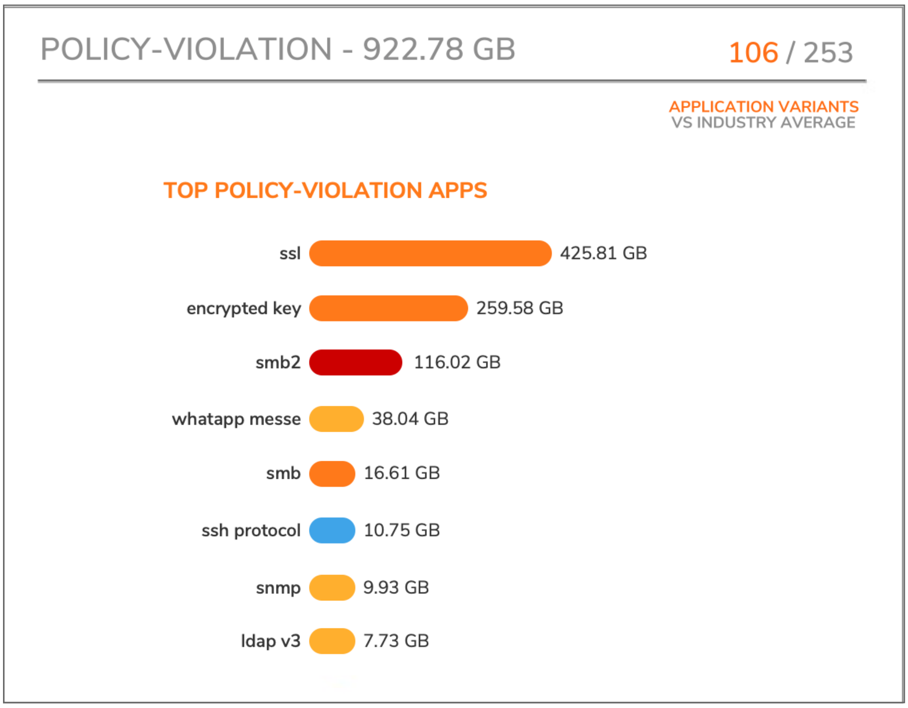
KEY FINDINGS

A total of 241 applications were seen in your organization, compared to an industry average of 231 in other organizations.

The most common types of application subcategories used within your organization are policy-violation, not-suspicious, general

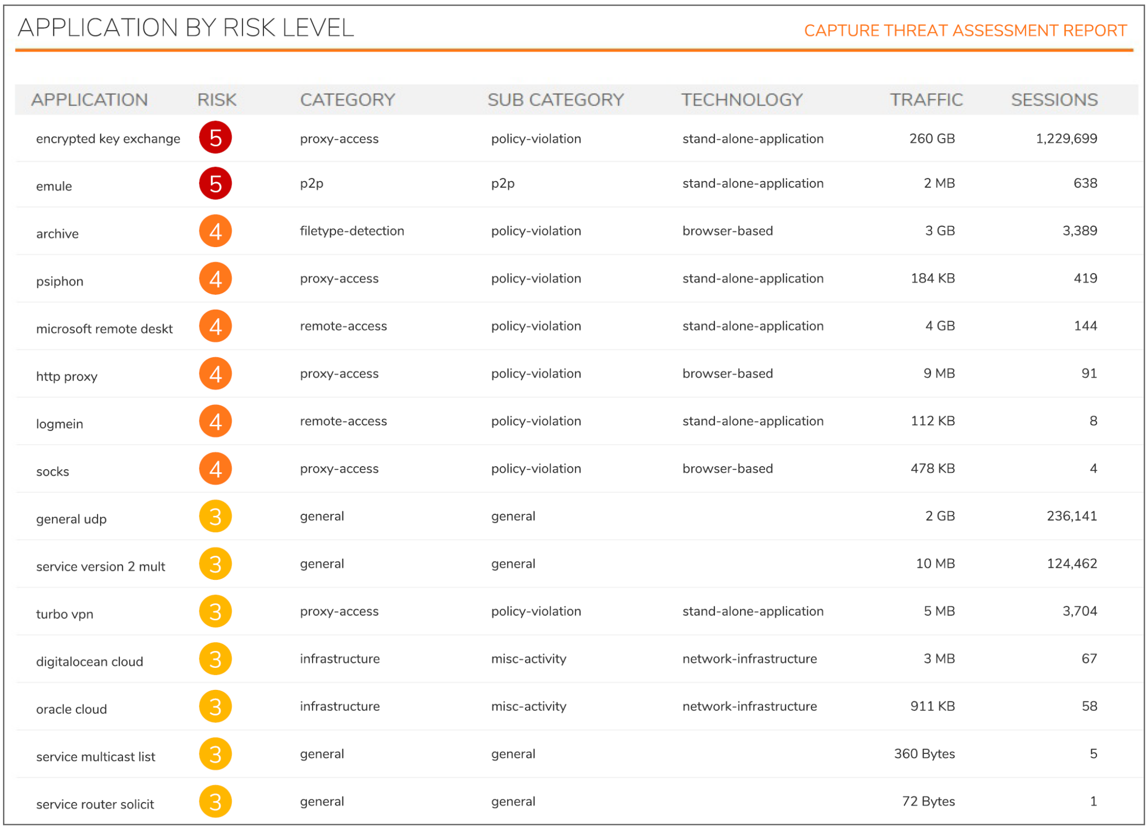
The application subcategories consuming the most bandwidth are policy-violation, not-suspicious, multimedia

The top Risky Applications categories are individually graphed and grouped on a page so you can see the detail associated with them. For example, the graph for the Top Policy Violation Apps is shown below.



At the top of the graph, you can see how much bandwidth is being consumed by this category of Risky Applications. To the right of the bandwidth, the total number of application variants in your own network is compared to the industry average. The bar chart below that shows the relative distribution of the bandwidth between the applications listed. Similar reports are shown for other top categories.

Individual applications are also assessed for risk. A ranked list is provided at the end of the Risky Applications section and shows detail like this:



APPLICATION BY RISK LEVEL

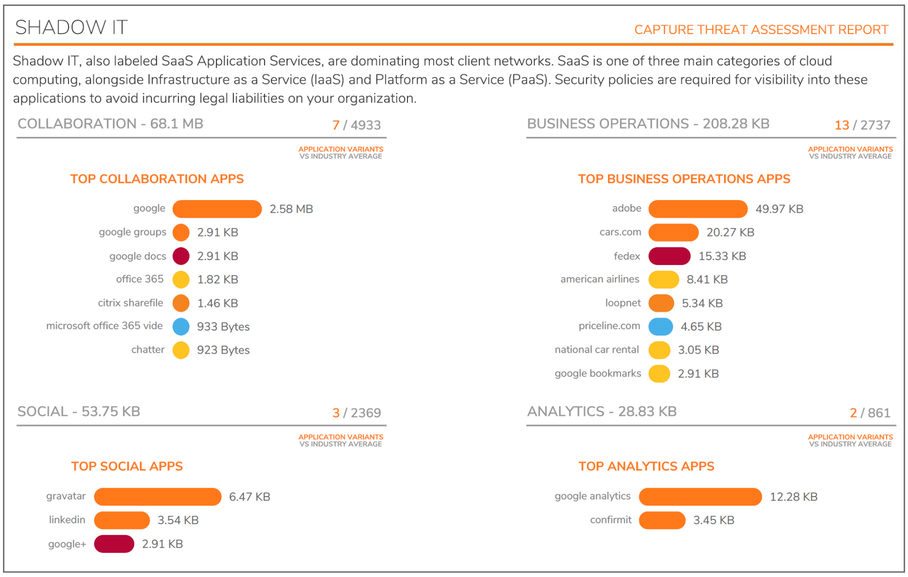
CAPTURE THREAT ASSESSMENT REPORT

APPLICATION	RISK	CATEGORY	SUB CATEGORY	TECHNOLOGY	TRAFFIC	SESSIONS
encrypted key exchange	5	proxy-access	policy-violation	stand-alone-application	260 GB	1,229,699
emule	5	p2p	p2p	stand-alone-application	2 MB	638
archive	4	filetype-detection	policy-violation	browser-based	3 GB	3,389
psiphon	4	proxy-access	policy-violation	stand-alone-application	184 KB	419
microsoft remote deskt	4	remote-access	policy-violation	stand-alone-application	4 GB	144
http proxy	4	proxy-access	policy-violation	browser-based	9 MB	91
logmein	4	remote-access	policy-violation	stand-alone-application	112 KB	8
socks	4	proxy-access	policy-violation	browser-based	478 KB	4
general udp	3	general	general		2 GB	236,141
service version 2 mult	3	general	general		10 MB	124,462
turbo vpn	3	proxy-access	policy-violation	stand-alone-application	5 MB	3,704
digitalocean cloud	3	infrastructure	misc-activity	network-infrastructure	3 MB	67
oracle cloud	3	infrastructure	misc-activity	network-infrastructure	911 KB	58
service multicast list	3	general	general		360 Bytes	5
service router solicit	3	general	general		72 Bytes	1

Shadow IT

Shadow IT, also called SaaS Application Services, are dominating most client networks. SaaS (Software as a Service) is one of three main categories of cloud computing, along with Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Security policies are required for visibility into these applications to avoid incurring legal liabilities on your organization.

ⓘ **NOTE:** In the CTA 2.2 release, the Shadow IT application is only available for firewalls that have been added to CSC-MA (Capture Security Center-Management). Additionally, the Analytics license is required for CSC-MA to get in-depth analysis of Shadow IT applications. Refer to Getting Started with Capture Security Center for information on CSC-MA licensing.



SHADOW IT

CAPTURE THREAT ASSESSMENT REPORT

Shadow IT, also labeled SaaS Application Services, are dominating most client networks. SaaS is one of three main categories of cloud computing, alongside Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). Security policies are required for visibility into these applications to avoid incurring legal liabilities on your organization.

COLLABORATION - 68.1 MB 7 / 4933

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP COLLABORATION APPS

google	2.58 MB
google groups	2.91 KB
google docs	2.91 KB
office 365	1.82 KB
citrix sharefile	1.46 KB
microsoft office 365 vide	933 Bytes
chatter	923 Bytes

BUSINESS OPERATIONS - 208.28 KB 13 / 2737

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP BUSINESS OPERATIONS APPS

adobe	49.97 KB
cars.com	20.27 KB
fedex	15.33 KB
american airlines	8.41 KB
loopnet	5.34 KB
priceline.com	4.65 KB
national car rental	3.05 KB
google bookmarks	2.91 KB

SOCIAL - 53.75 KB 3 / 2369

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP SOCIAL APPS

gravatar	6.47 KB
linkedin	3.54 KB
google+	2.91 KB

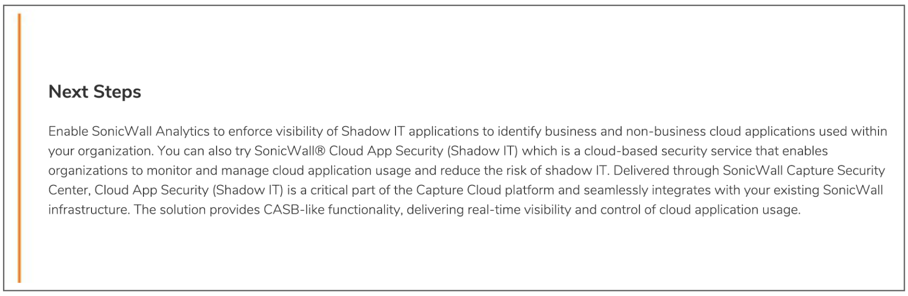
ANALYTICS - 28.83 KB 2 / 861

APPLICATION VARIANTS VS INDUSTRY AVERAGE

TOP ANALYTICS APPS

google analytics	12.28 KB
confirmit	3.45 KB

If no data is available, the page displays a message saying so. You may need to have Analytics licensing enabled to capture the Shadow IT data in this report. Next steps are identified for you to follow as in the following example:

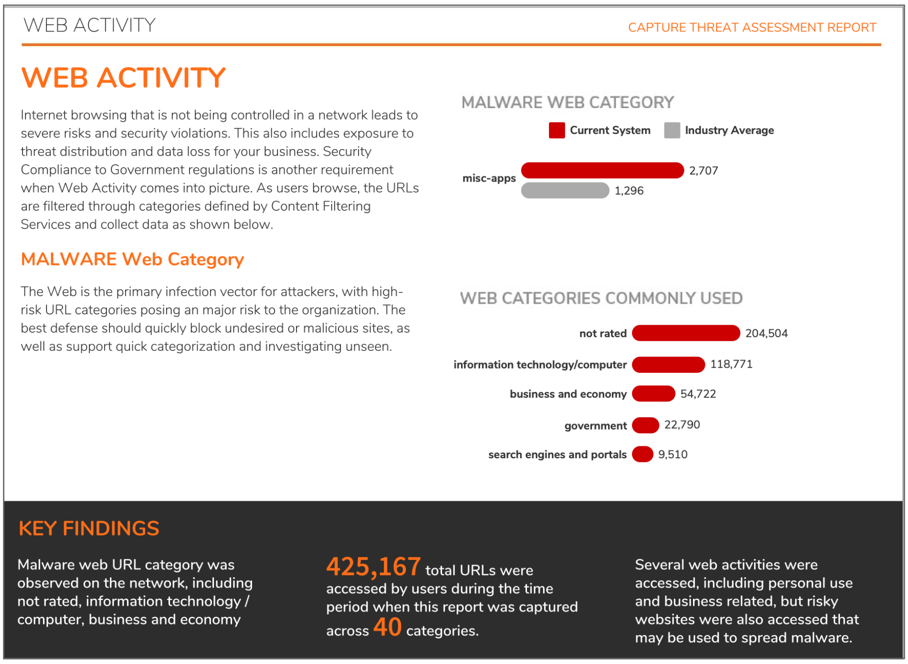


Next Steps

Enable SonicWall Analytics to enforce visibility of Shadow IT applications to identify business and non-business cloud applications used within your organization. You can also try SonicWall® Cloud App Security (Shadow IT) which is a cloud-based security service that enables organizations to monitor and manage cloud application usage and reduce the risk of shadow IT. Delivered through SonicWall Capture Security Center, Cloud App Security (Shadow IT) is a critical part of the Capture Cloud platform and seamlessly integrates with your existing SonicWall infrastructure. The solution provides CASB-like functionality, delivering real-time visibility and control of cloud application usage.

Web Activity

Internet browsing that is not being controlled in a network leads to severe risks and potential security violations, including exposure to threat distribution and data loss for your business. If you are not monitoring web activity, you may also be at risk for not being able to comply with various government security requirements. For the CTA report, URLs are filtered through categories defined by the Content Filtering services. The findings are graphed and summarized in the Key Findings of this section.



WEB ACTIVITY

CAPTURE THREAT ASSESSMENT REPORT

WEB ACTIVITY

Internet browsing that is not being controlled in a network leads to severe risks and security violations. This also includes exposure to threat distribution and data loss for your business. Security Compliance to Government regulations is another requirement when Web Activity comes into picture. As users browse, the URLs are filtered through categories defined by Content Filtering Services and collect data as shown below.

MALWARE Web Category

The Web is the primary infection vector for attackers, with high-risk URL categories posing an major risk to the organization. The best defense should quickly block undesired or malicious sites, as well as support quick categorization and investigating unseen.

MALWARE WEB CATEGORY

WEB CATEGORIES COMMONLY USED

not rated 204,504
information technology/computer 118,771
business and economy 54,722
government 22,790
search engines and portals 9,510

KEY FINDINGS

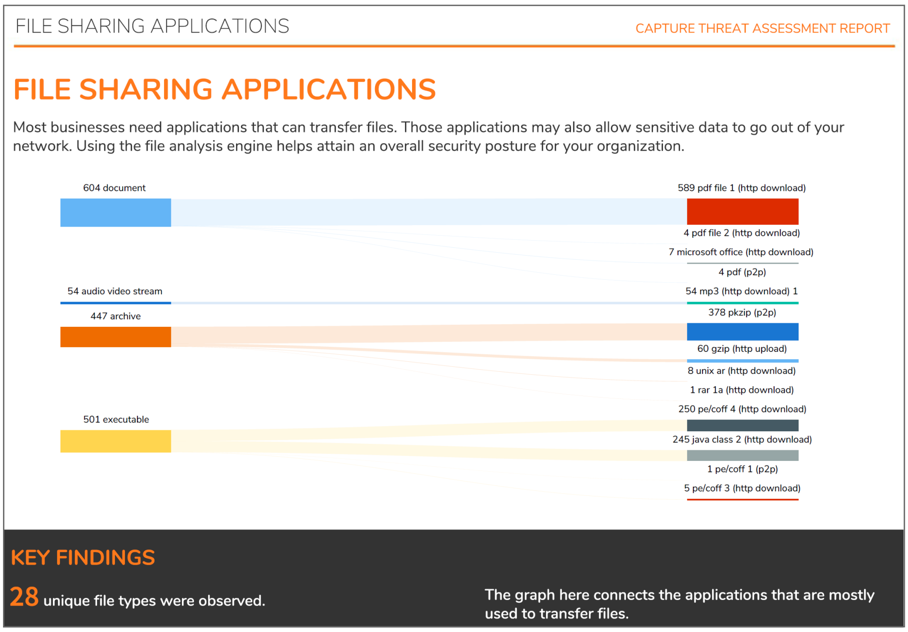
Malware web URL category was observed on the network, including not rated, information technology / computer, business and economy

425,167 total URLs were accessed by users during the time period when this report was captured across 40 categories.

Several web activities were accessed, including personal use and business related, but risky websites were also accessed that may be used to spread malware.

File Sharing Applications

Most businesses need applications that can transfer files. Those applications may also all sentive data to go out of your network. Using the file analysis engine helps attain a secure posture for your organization.



FILE SHARING APPLICATIONS

CAPTURE THREAT ASSESSMENT REPORT

FILE SHARING APPLICATIONS

Most businesses need applications that can transfer files. Those applications may also allow sensitive data to go out of your network. Using the file analysis engine helps attain an overall security posture for your organization.

604 document
54 audio video stream
447 archive
501 executable
589 pdf file 1 (http download)
4 pdf file 2 (http download)
7 microsoft office (http download)
4 pdf (p2p)
54 mp3 (http download) 1
378 pkzip (p2p)
60 gzip (http upload)
8 unix ar (http download)
1 rar 1a (http download)
250 pe/coff 4 (http download)
245 java class 2 (http download)
1 pe/coff 1 (p2p)
5 pe/coff 3 (http download)

KEY FINDINGS

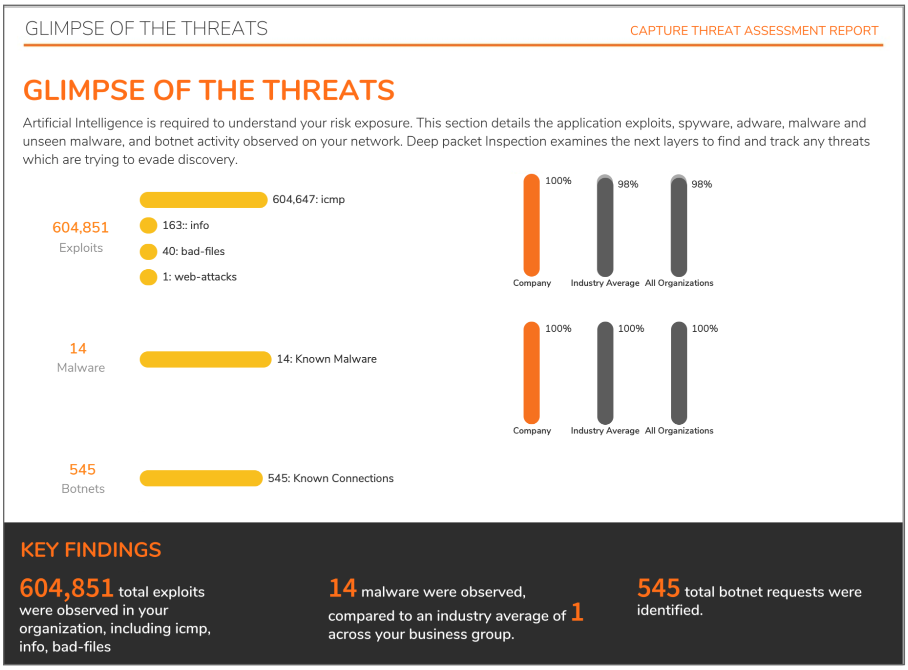
28 unique file types were observed.

The graph here connects the applications that are mostly used to transfer files.

Glimpse of the Threats

Artificial intelligence is required to understand your risk exposure. This sections details the application exploits, spyware, adware, malware and unseen malware and, botnet activity observed on your network. Deep Packet Inspection takes the information collected and examines the next layers to find and track any threats that are actively trying to evade discovery.

In addition to seeing what is found on your network, bar graphs are used to compare your environment to the industry average and the average is for all organizations.



GLIMPSE OF THE THREATS

CAPTURE THREAT ASSESSMENT REPORT

GLIMPSE OF THE THREATS

Artificial Intelligence is required to understand your risk exposure. This section details the application exploits, spyware, adware, malware and unseen malware, and botnet activity observed on your network. Deep packet Inspection examines the next layers to find and track any threats which are trying to evade discovery.

KEY FINDINGS

604,851 total exploits were observed in your organization, including icmp, info, bad-files

14 malware were observed, compared to an industry average of 1 across your business group.

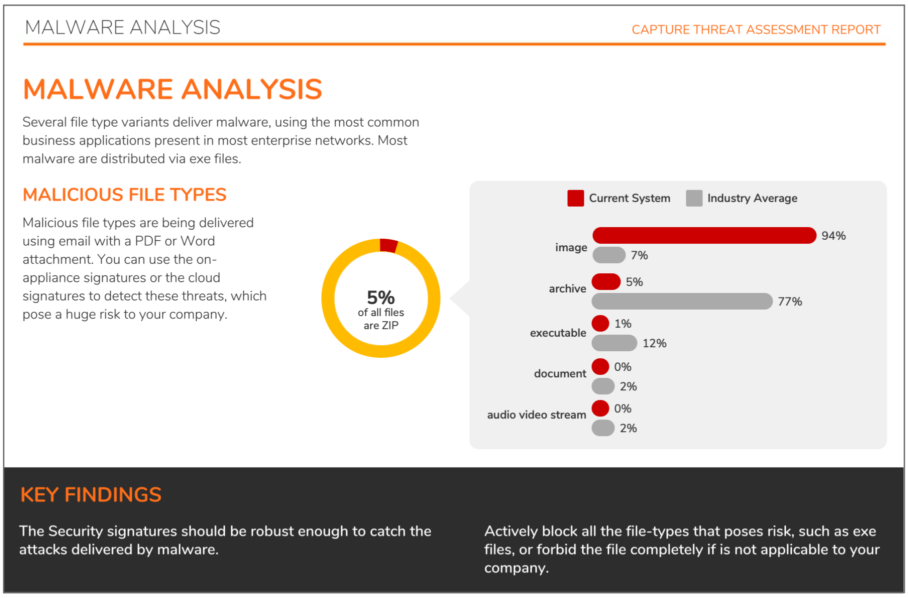
545 total botnet requests were identified.

Topics:

- Malware Analysis
- Unseen Malware
- Exploits
- Botnet Analysis

Malware Analysis

Several file type variances deliver malware, using the most common business applications found in most enterprise networks. While most malware are distributed via `.exe` files, some malicious file types are being delivered using email with a PDF or Word attachment. You can use the on-appliance signatures or the cloud signatures to detect these threats, which pose a huge risk to your company.



MALWARE ANALYSIS

CAPTURE THREAT ASSESSMENT REPORT

MALWARE ANALYSIS

Several file type variants deliver malware, using the most common business applications present in most enterprise networks. Most malware are distributed via exe files.

MALICIOUS FILE TYPES

Malicious file types are being delivered using email with a PDF or Word attachment. You can use the on-appliance signatures or the cloud signatures to detect these threats, which pose a huge risk to your company.

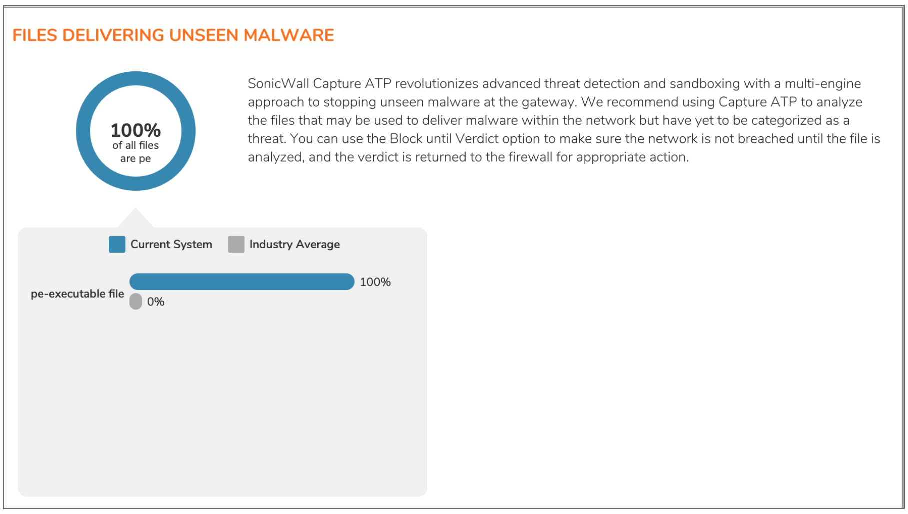
KEY FINDINGS

The Security signatures should be robust enough to catch the attacks delivered by malware.

Actively block all the file-types that poses risk, such as exe files, or forbid the file completely if is not applicable to your company.

Unseen Malware

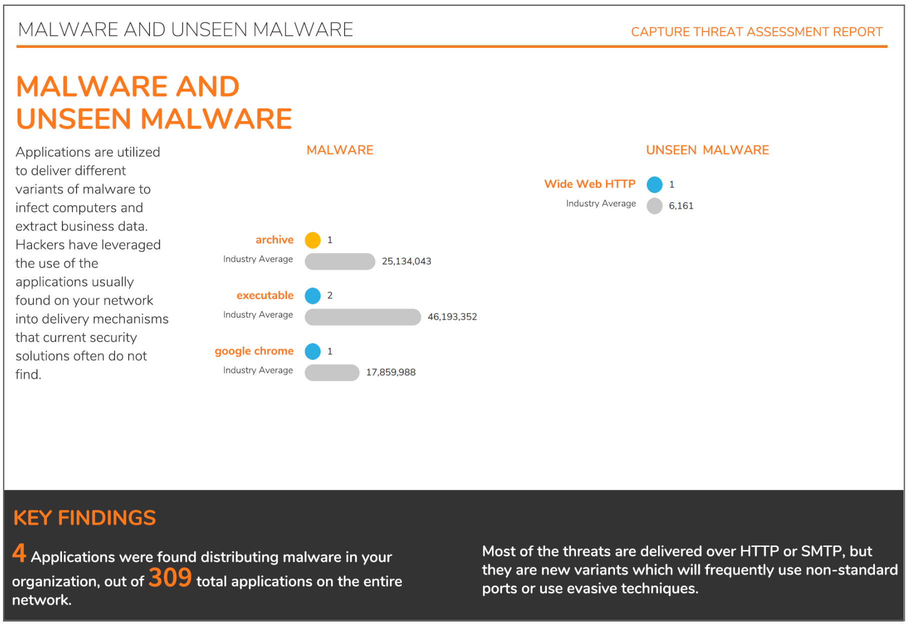
SonicWall Capture Advanced Threat Protection (Capture ATP) revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. Capture ATP can be used to analyze the files that may be used to deliver malware within the network but hasn't yet been categorized as a threat. You can use the **Block until Verdict** option to make sure the network is not breached while the file is being analyzed. Once the verdict is returned to the firewall, appropriate action can be taken.



FILES DELIVERING UNSEEN MALWARE

SonicWall Capture ATP revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. We recommend using Capture ATP to analyze the files that may be used to deliver malware within the network but have yet to be categorized as a threat. You can use the Block until Verdict option to make sure the network is not breached until the file is analyzed, and the verdict is returned to the firewall for appropriate action.

Applications are also used to deliver different variants of malware to infect computers and extract data. Hackers have turned these applications into delivery mechanisms that current solutions often don't see. The CTA report identifies the key findings and charts them for your review.



MALWARE AND UNSEEN MALWARE

CAPTURE THREAT ASSESSMENT REPORT

MALWARE AND UNSEEN MALWARE

Applications are utilized to deliver different variants of malware to infect computers and extract business data. Hackers have leveraged the use of the applications usually found on your network into delivery mechanisms that current security solutions often do not find.

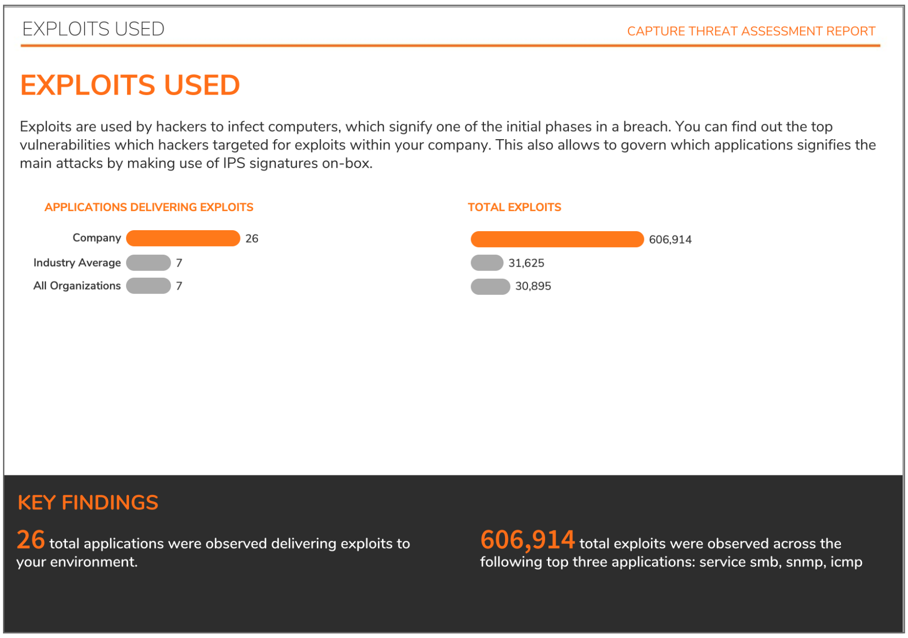
KEY FINDINGS

4 Applications were found distributing malware in your organization, out of 309 total applications on the entire network.

Most of the threats are delivered over HTTP or SMTP, but they are new variants which will frequently use non-standard ports or use evasive techniques.

Exploits

Exploits are used by hackers to infect computers and signify one of the initial phases of a breach. Capture Threat Assessment can help you detect the exploitable vulnerabilities within your company that hackers target . It shows you how many applications are delivering exploits in your company and provides the average for your industry and for all organizations so you can compare.



EXPLOITS USED

CAPTURE THREAT ASSESSMENT REPORT

EXPLOITS USED

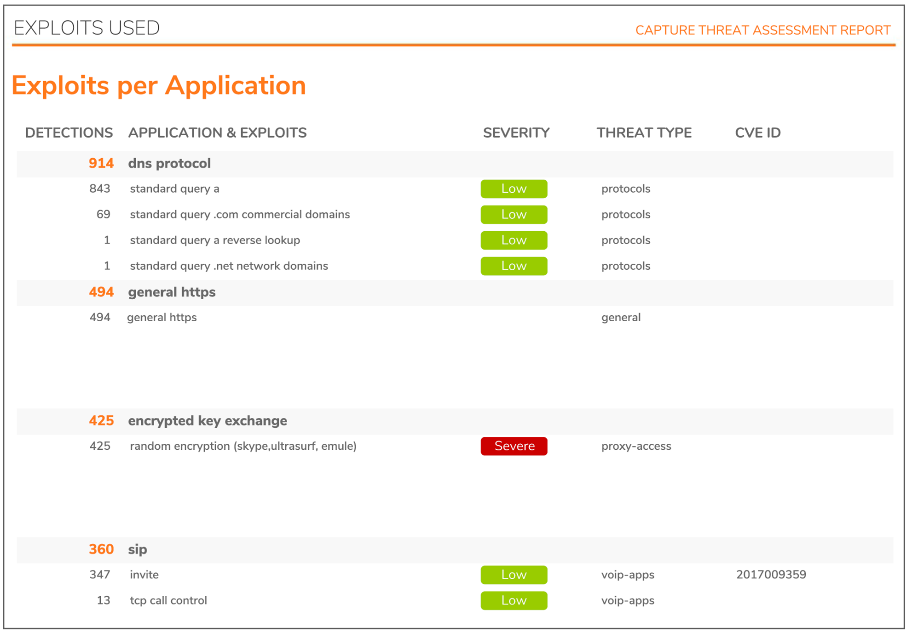
Exploits are used by hackers to infect computers, which signify one of the initial phases in a breach. You can find out the top vulnerabilities which hackers targeted for exploits within your company. This also allows to govern which applications signifies the main attacks by making use of IPS signatures on-box.

KEY FINDINGS

26 total applications were observed delivering exploits to your environment.

606,914 total exploits were observed across the following top three applications: service smb, snmp, icmp

You can also see the top exploits presented in list form.



EXPLOITS USED

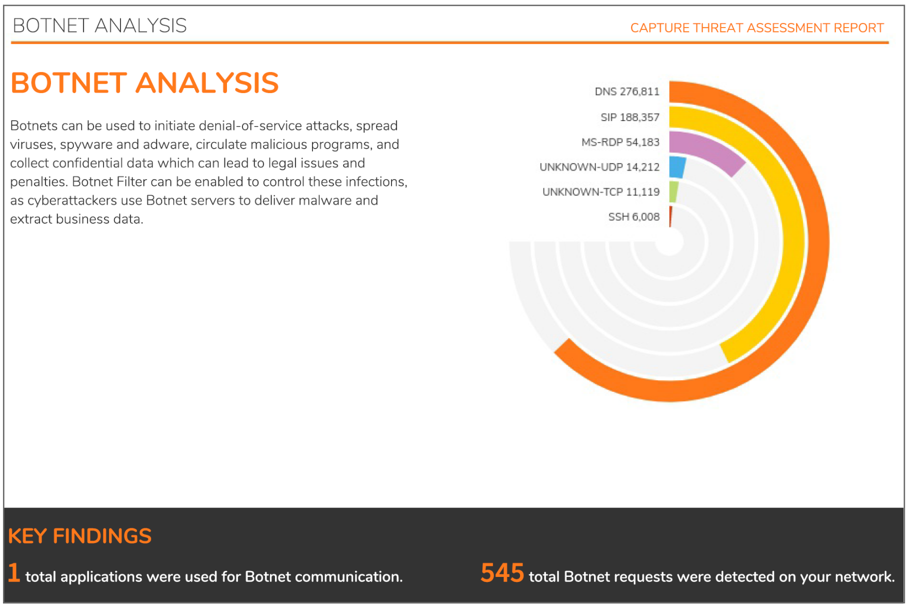
CAPTURE THREAT ASSESSMENT REPORT

Exploits per Application

DETECTIONS	APPLICATION & EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
914	**dns protocol**			
843	standard query a	Low	protocols	
69	standard query .com commercial domains	Low	protocols	
1	standard query a reverse lookup	Low	protocols	
1	standard query .net network domains	Low	protocols	
494	**general https**			
494	general https		general	
425	**encrypted key exchange**			
425	random encryption (skype,ultrasurf, emule)	Severe	proxy-access	
360	**sip**			
347	invite	Low	voip-apps	2017009359
13	tcp call control	Low	voip-apps	

Botnet Analysis

Botnets can be used to initiate denial-of-service attacks; spread viruses, spyware, and adware; circulate malicious programs; and collect confidential data. These types of issues can potentially lead to legal issues and penalties for not protecting data. The Botnet Filter can be enabled to control these infections as cyber attackers use Botnet servers to deliver malware and extract business data. The CTA report highlights the botnet requests detected on your network.



BOTNET ANALYSIS

CAPTURE THREAT ASSESSMENT REPORT

BOTNET ANALYSIS

Botnets can be used to initiate denial-of-service attacks, spread viruses, spyware and adware, circulate malicious programs, and collect confidential data which can lead to legal issues and penalties. Botnet Filter can be enabled to control these infections, as cyberattackers use Botnet servers to deliver malware and extract business data.

KEY FINDINGS

1 total applications were used for Botnet communication.

545 total Botnet requests were detected on your network.

Usage Statistics

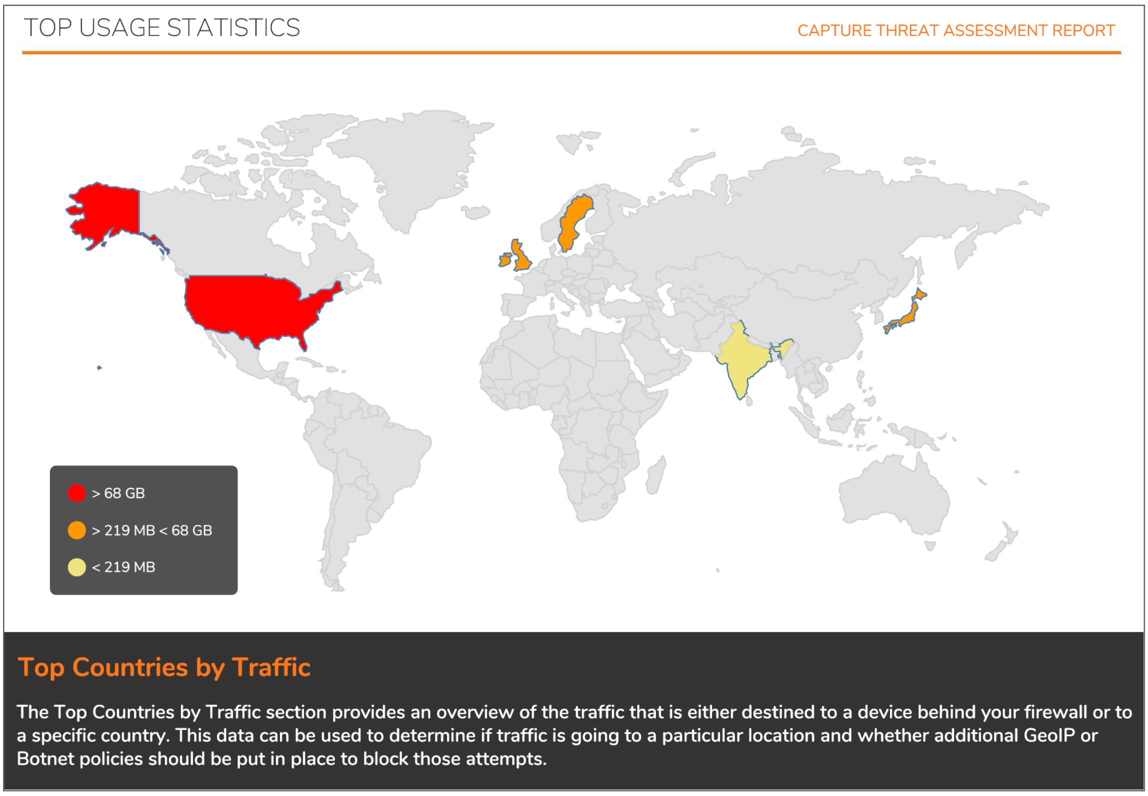
The CTA report pulls together a number of usage statistics so you can see how and where your network is being most used.

Topics:

- Top Countries
- Top Session Usage by IP
- Top Traffic Usage by IP
- Top User Sessions
- Top User Traffic

Top Countries

The Top Countries by Traffic section of the CTA report shows an overview of the traffic displayed on a world map.



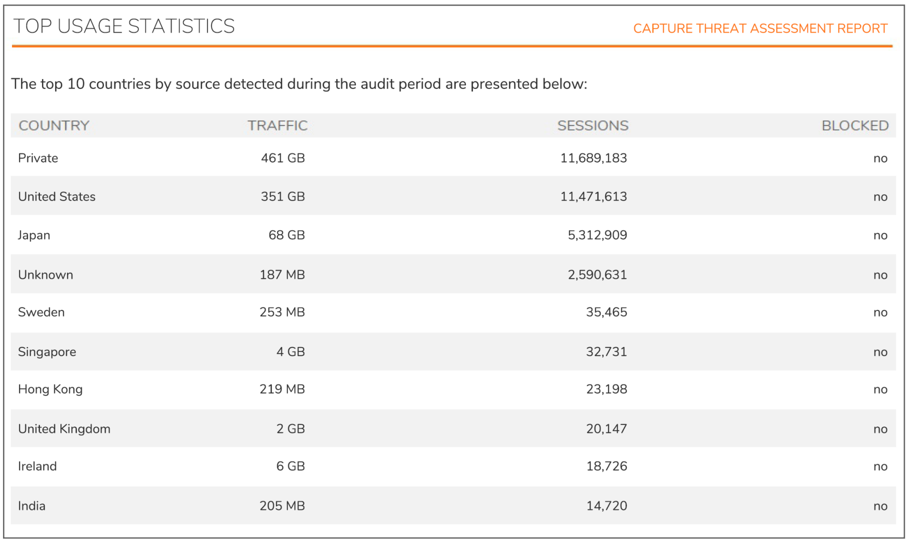
TOP USAGE STATISTICS

CAPTURE THREAT ASSESSMENT REPORT

Top Countries by Traffic

The Top Countries by Traffic section provides an overview of the traffic that is either destined to a device behind your firewall or to a specific country. This data can be used to determine if traffic is going to a particular location and whether additional GeoIP or Botnet policies should be put in place to block those attempts.

The top 10 countries detected are presented with more detail in the table. You can see how much traffic and how many sessions were detected and whether they were blocked.



TOP USAGE STATISTICS

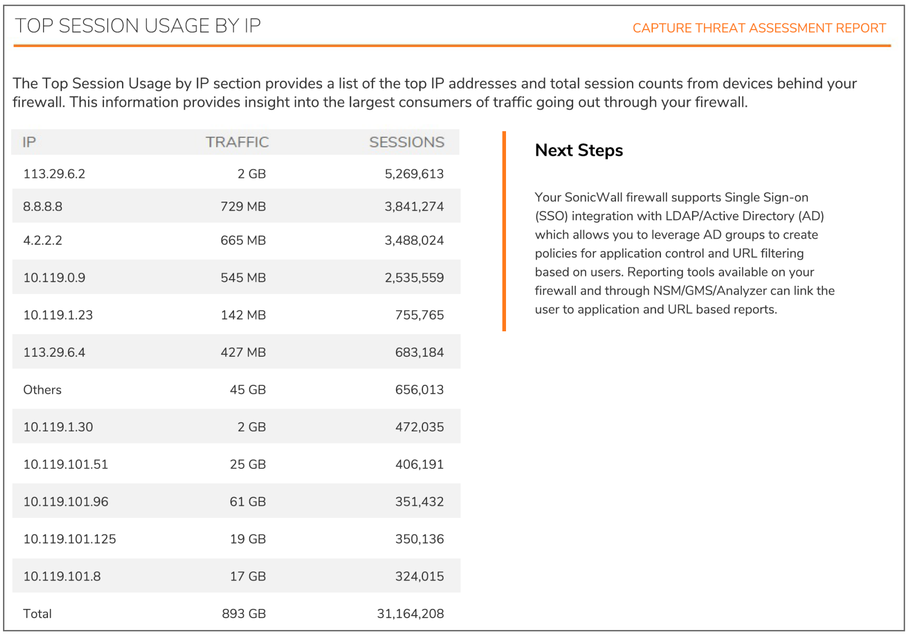
CAPTURE THREAT ASSESSMENT REPORT

The top 10 countries by source detected during the audit period are presented below:

COUNTRY	TRAFFIC	SESSIONS	BLOCKED
Private	461 GB	11,689,183	no
United States	351 GB	11,471,613	no
Japan	68 GB	5,312,909	no
Unknown	187 MB	2,590,631	no
Sweden	253 MB	35,465	no
Singapore	4 GB	32,731	no
Hong Kong	219 MB	23,198	no
United Kingdom	2 GB	20,147	no
Ireland	6 GB	18,726	no
India	205 MB	14,720	no

Top Session Usage by IP

The Top Session Usage by IP section provides a list of the top IP addresses and total session counts from devices behind your firewall. This shows you the largest consumers of traffic going out through your firewall.



TOP SESSION USAGE BY IP

CAPTURE THREAT ASSESSMENT REPORT

The Top Session Usage by IP section provides a list of the top IP addresses and total session counts from devices behind your firewall. This information provides insight into the largest consumers of traffic going out through your firewall.

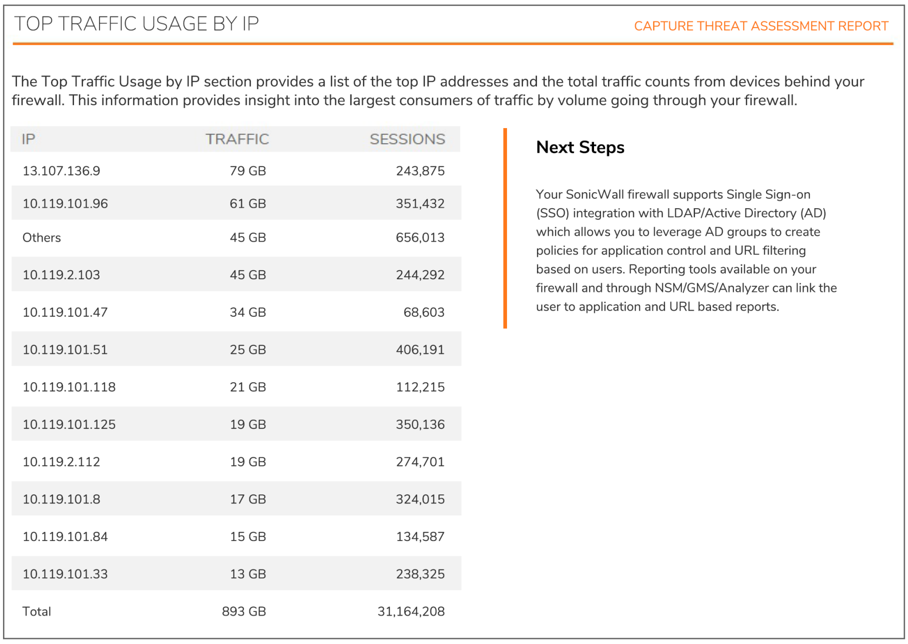
IP	TRAFFIC	SESSIONS
113.29.6.2	2 GB	5,269,613
8.8.8.8	729 MB	3,841,274
4.2.2.2	665 MB	3,488,024
10.119.0.9	545 MB	2,535,559
10.119.1.23	142 MB	755,765
113.29.6.4	427 MB	683,184
Others	45 GB	656,013
10.119.1.30	2 GB	472,035
10.119.101.51	25 GB	406,191
10.119.101.96	61 GB	351,432
10.119.101.125	19 GB	350,136
10.119.101.8	17 GB	324,015
Total	893 GB	31,164,208

Next Steps

Your SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through NSM/GMS/Analyzer can link the user to application and URL based reports.

Top Traffic Usage by IP

The Top Traffic Usage by IP section provides a list of the top IP addresses and total traffic counts from devices behind your firewall. This shows you the largest consumers of traffic by volume going through your firewall.



TOP TRAFFIC USAGE BY IP

CAPTURE THREAT ASSESSMENT REPORT

The Top Traffic Usage by IP section provides a list of the top IP addresses and the total traffic counts from devices behind your firewall. This information provides insight into the largest consumers of traffic by volume going through your firewall.

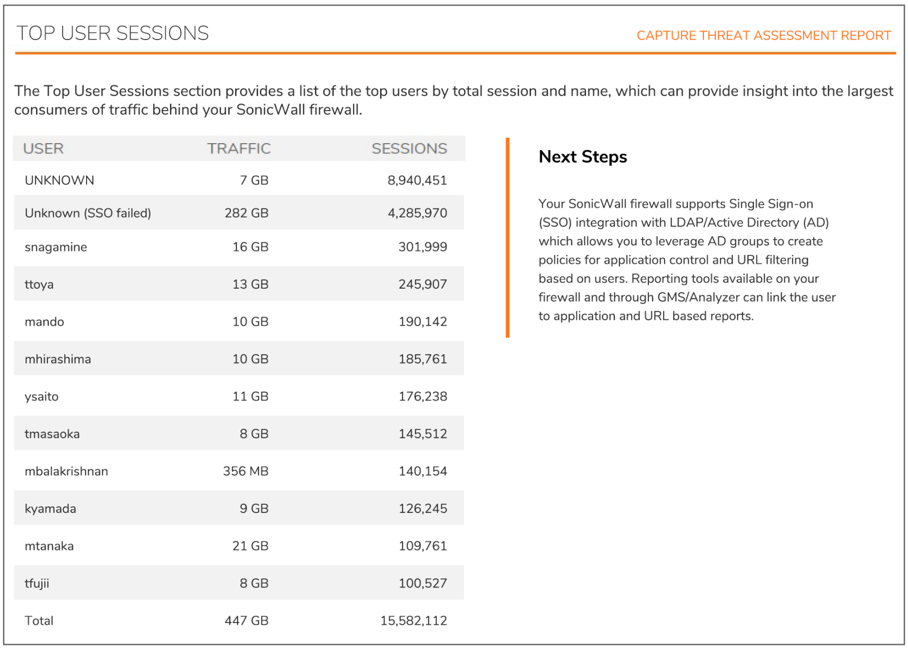
IP	TRAFFIC	SESSIONS
13.107.136.9	79 GB	243,875
10.119.101.96	61 GB	351,432
Others	45 GB	656,013
10.119.2.103	45 GB	244,292
10.119.101.47	34 GB	68,603
10.119.101.51	25 GB	406,191
10.119.101.118	21 GB	112,215
10.119.101.125	19 GB	350,136
10.119.2.112	19 GB	274,701
10.119.101.8	17 GB	324,015
10.119.101.84	15 GB	134,587
10.119.101.33	13 GB	238,325
Total	893 GB	31,164,208

Next Steps

Your SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through NSM/GMS/Analyzer can link the user to application and URL based reports.

Top User Sessions

The CTA report provides a list of top users in the section called Top User Sessions. The table shows the number of sessions and the amount of traffic for the top users identified.



TOP USER SESSIONS

CAPTURE THREAT ASSESSMENT REPORT

The Top User Sessions section provides a list of the top users by total session and name, which can provide insight into the largest consumers of traffic behind your SonicWall firewall.

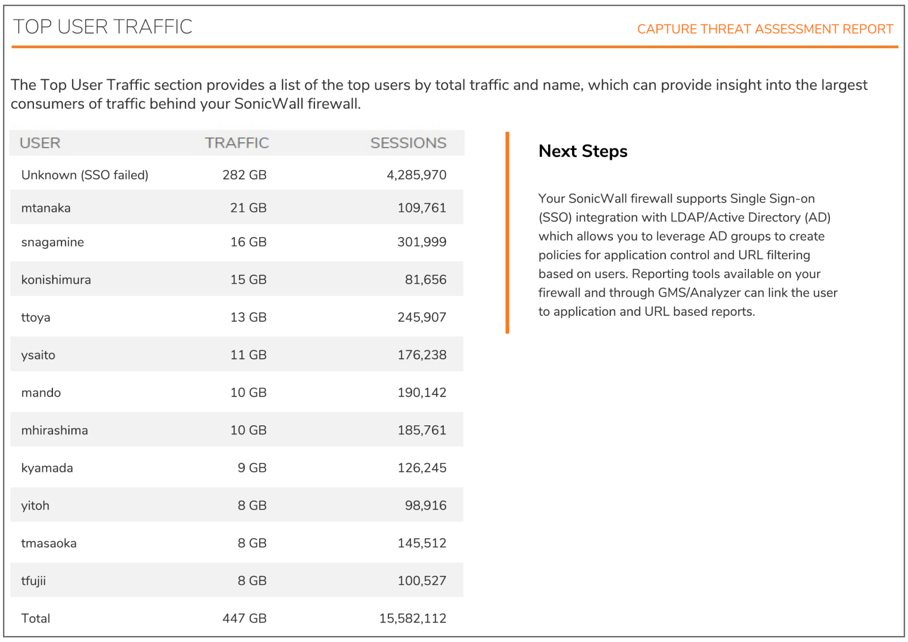
USER	TRAFFIC	SESSIONS
UNKNOWN	7 GB	8,940,451
Unknown (SSO failed)	282 GB	4,285,970
snagamine	16 GB	301,999
ttoya	13 GB	245,907
mando	10 GB	190,142
mhirashima	10 GB	185,761
ysaito	11 GB	176,238
tmasaoka	8 GB	145,512
mbalakrishnan	356 MB	140,154
kyamada	9 GB	126,245
mtanaka	21 GB	109,761
tfujii	8 GB	100,527
Total	447 GB	15,582,112

Next Steps

Your SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

Top User Traffic

The Top User Traffic section provides a list of the top users, based on total traffic per user. The table provides insight into the largest consumers of traffic behind your SonicWall firewall. You can also review the next steps you can take to decrease your overall risk.



TOP USER TRAFFIC

CAPTURE THREAT ASSESSMENT REPORT

The Top User Traffic section provides a list of the top users by total traffic and name, which can provide insight into the largest consumers of traffic behind your SonicWall firewall.

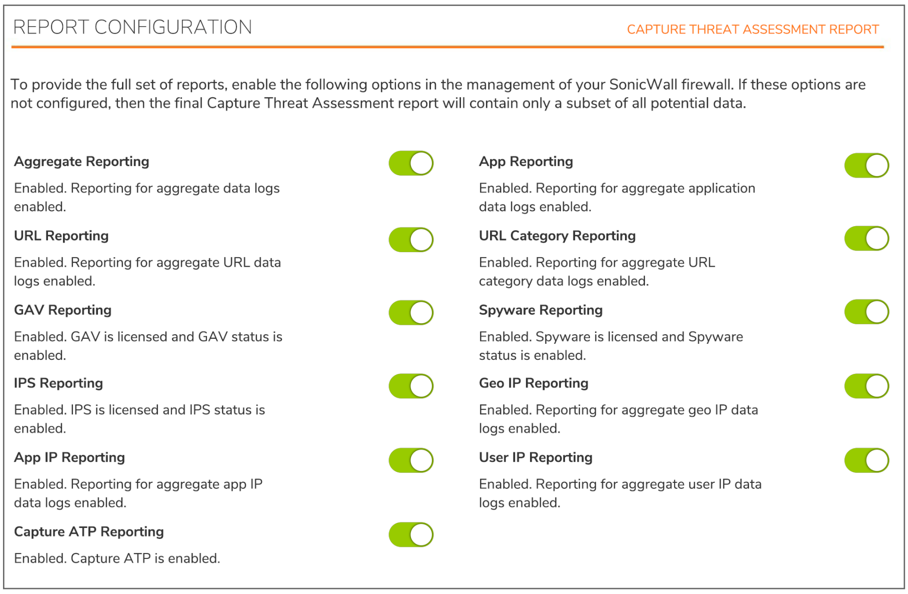
USER	TRAFFIC	SESSIONS
Unknown (SSO failed)	282 GB	4,285,970
mtanaka	21 GB	109,761
snagamine	16 GB	301,999
konishimura	15 GB	81,656
ttoya	13 GB	245,907
ysaito	11 GB	176,238
mando	10 GB	190,142
mhirashima	10 GB	185,761
kyamada	9 GB	126,245
yitoh	8 GB	98,916
tmasaoka	8 GB	145,512
tfujii	8 GB	100,527
Total	447 GB	15,582,112

Next Steps

Your SonicWall firewall supports Single Sign-on (SSO) integration with LDAP/Active Directory (AD) which allows you to leverage AD groups to create policies for application control and URL filtering based on users. Reporting tools available on your firewall and through GMS/Analyzer can link the user to application and URL based reports.

Report Configuration

To provide all the data to generate a complete Capture Threat Assessment several options need to be enabled within the management of your SonicWall firewall. If all options are not enabled, only a subset of the possible data is included in the report.



REPORT CONFIGURATION

CAPTURE THREAT ASSESSMENT REPORT

To provide the full set of reports, enable the following options in the management of your SonicWall firewall. If these options are not configured, then the final Capture Threat Assessment report will contain only a subset of all potential data.

Aggregate Reporting

Enabled. Reporting for aggregate data logs enabled.

URL Reporting

Enabled. Reporting for aggregate URL data logs enabled.

GAV Reporting

Enabled. GAV is licensed and GAV status is enabled.

IPS Reporting

Enabled. IPS is licensed and IPS status is enabled.

App IP Reporting

Enabled. Reporting for aggregate app IP data logs enabled.

Capture ATP Reporting

Enabled. Capture ATP is enabled.

App Reporting

Enabled. Reporting for aggregate application data logs enabled.

URL Category Reporting

Enabled. Reporting for aggregate URL category data logs enabled.

Spyware Reporting

Enabled. Spyware is licensed and Spyware status is enabled.

Geo IP Reporting

Enabled. Reporting for aggregate geo IP data logs enabled.

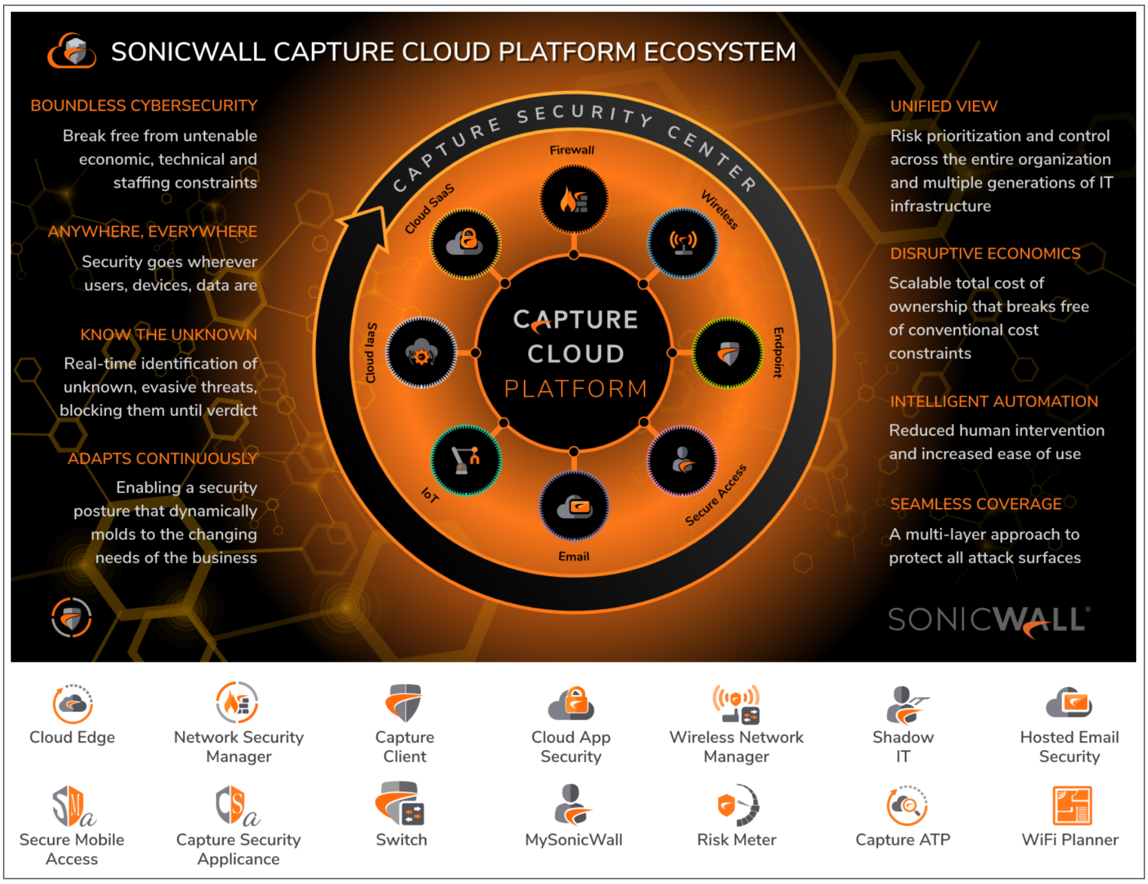
User IP Reporting

Enabled. Reporting for aggregate user IP data logs enabled.

If a feature report is not enabled, refer to the appropriate *SonicOS* or *SonicOSX Administration Guide* for the details.

Capture Cloud Ecosystem

A new page has been added to the Capture Threat Assessment: the SonicWall Capture Cloud Platform Ecosystem.



SONICWALL CAPTURE CLOUD PLATFORM ECOSYSTEM

BOUNDLESS CYBERSECURITY

Break free from untenable economic, technical and staffing constraints

ANYWHERE, EVERYWHERE

Security goes wherever users, devices, data are

KNOW THE UNKNOWN

Real-time identification of unknown, evasive threats, blocking them until verdict

ADAPTS CONTINUOUSLY

Enabling a security posture that dynamically molds to the changing needs of the business

UNIFIED VIEW

Risk prioritization and control across the entire organization and multiple generations of IT infrastructure

DISRUPTIVE ECONOMICS

Scalable total cost of ownership that breaks free of conventional cost constraints

INTELLIGENT AUTOMATION

Reduced human intervention and increased ease of use

SEAMLESS COVERAGE

A multi-layer approach to protect all attack surfaces

You can see at a glance how SonicWall visualizes the Capture Cloud Platform and the applications that can be used to effectively manage and protect your infrastructure.

CTA 1.0 Report Availability

The prior version of the Capture Threat Assessment is still available if you would rather work with the version 1.0 format. That process is documented in the knowledge base article Generating Capture Threat Assessment Report(CTA) V 1.0.

2

Generating CTA Reports

You can generate CTA reports directly from your SonicWall firewall. This report generation is only supported on firewalls running SonicOS firmware versions 6.5.4.6-79n and later. Firewalls running older versions of SonicOS only support version 1.0 CTA.

- For firewalls running versions 7.x, navigate to **MONITOR | AppFlow > CTA Report** to access the reports.
- For firewalls running versions 6.5.x, navigate to **INVESTIGATE | Reports > Capture Threat Assessment** to access the reports.

Topics:

Creating a CTA Report

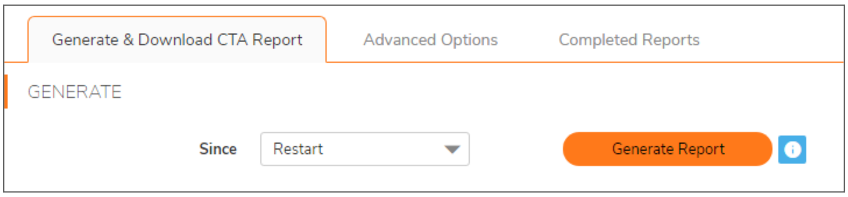
Even though the CTA Report is the same on SonicOS 7.x and SonicOS 6.5.x , the user interface is different so the instructions to generate the report is slightly different. Refer to the following procedures for details:

- Downloading on Version 7.x
- Downloading on Version 6.5.x

Downloading on Version 7.x

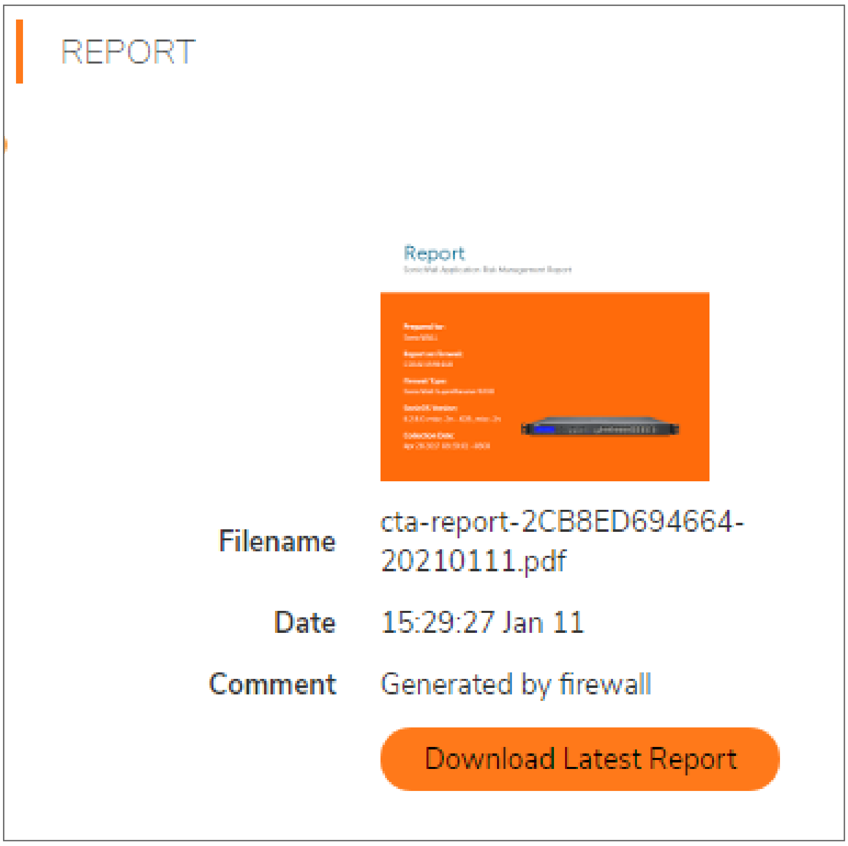
To download a CTA report in SonicOS version 7.x:

1. Navigate to your firewall and log in with your administrator credentials.
2. Select the **MONITOR** option at the top of the page.
3. Navigate to **AppFlow > CTA Report**. The default view is the **Generate & Download CTA Report** tab.



Since: Restart

4. Click on **Generate Report** to post the SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.



Filename: cta-report-2CB8ED694664-20210111.pdf

Date: 15:29:27 Jan 11

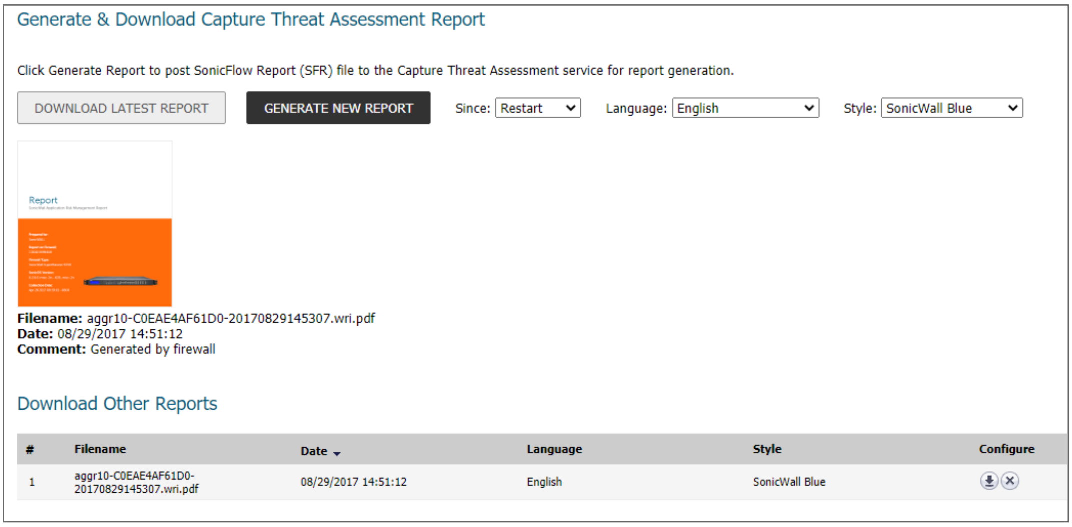
Comment: Generated by firewall

5. When the report completes, click **Download Latest Report**.
6. Double-click on the report to open it in another tab.

Downloading on Version 6.5.x

To create a CTA report in SonicOS version 6.5.x:

1. Navigate to your firewall and log in with your administrator credentials.
2. Select the **INVESTIGATION** view at the top of the page.
3. Navigate to **Reports > Capture Threat Assessment**.



Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Since: Restart Language: English Style: SonicWall Blue

Filename: aggr10-C0EAE4AF61D0-20170829145307.wri.pdf
Date: 08/29/2017 14:51:12
Comment: Generated by firewall

Download Other Reports

#	Filename	Date	Language	Style	Configure
1	aggr10-C0EAE4AF61D0-20170829145307.wri.pdf	08/29/2017 14:51:12	English	SonicWall Blue	⬇ ⊗

4. Set the report parameters:
    - **Since**: select **Restart** or **Last Reset**.
    - **Language**: select the language for the report.
    - **Style**: select the color theme for the report.
5. Click on **Generate New Report** to post the SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.
6. When the report completes, click **Download Latest Report**.
7. Double-click on the report to open it in another tab.

Advanced Options

The **Advanced Options** tab provides the means to customize the CTA Report.

ⓘ **IMPORTANT:** The values in this tab are not saved in the firewall. Customized data is lost once you logout or clear your browser cache.

Topics:

- Text Options
- Report Type
- Select Sections
- Custom Logo

Text Options

The CTA reports can be customized to some degree. Navigate to **MONITOR | AppFlow > CTA Report**, and select **Advanced Options**. In the **Text Options** section, you can add text that customizes your report.

Text Option	Definition
Report Title	Customize the report title by entering the title in this field.
About Text	Provide a brief description about the company the report is for. This appears on the second to the last page of the completed report.
Company Name	Add the name of the company to this field. This is used on the front page and in the back.
Contact Phone	Add the phone number of the contact for this report. The number appears how you type it. If you want dashes, spaces, or parentheses, be sure to include them.
Preparer Name	Put the preparer's name in this field. It appears on the title page of the report.
Contact Email	Add the perparer's email in this field. It appears at the back of the report.

Report Type

You can set the type of report to generate. Navigate to **MONITOR | AppFlow > CTA Report**, and select **Advanced Options**. In the **Report Type** section, check the box for **Executive Summary Only** if you want a smaller report with content summarized for the executive. If you leave that option unselected, a full report is generated.

Select Sections

The content of the CTA Report can be customized by topic. Navigate to **MONITOR | AppFlow > CTA Report**, and select **Advanced Options**. In the **Select Sections** segment, check the topics you want included. Unchecked topics are not added. The topics to chose from include:

- Application Highlights
- Risky Applications
- Web Activity
- File Transfer Investigation
- Glipse of Threats
- Malware Analysis
- Exploits Used
- Known and Unknown Threats
- Botnet Analysis
- Top Countries by Traffic
- Top IPs by Session

- Top IPs by Traffic
- Top Users by Session
- Top Users by Traffic
- Report Configuration

Custom Logo

A custom logo can be added to the CTA Report. It needs to be a PNG in Base 64 format. Navigate to **MONITOR | AppFlow > CTA Report**, and select **Advanced Options**.

Completed Reports

CTA Reports that have been previously run are saved in the cloud and displayed for access later.

To access CTA Reports on firewalls with version 7.x:

1. Navigate to **MONITOR | AppFlow > CTA Report**.
2. Select **Completed Reports**. The table lists the reports that have been run.
3. Select a report and click the **Download** icon to download the report.
4. Click the **Delete** icon to remove it from the table.
5. Use the commands above the table to **Search** the list or **Refresh** it.

To access the CTA Report on firewalls running version 6.5.x:

1. Navigate to **INVESTIGATION | Reports > Capture Threat Assessment**.
2. Scroll to the bottom of the page.
3. Click the **Download** icon (in the **Configure** column) to download the report.
4. Click the **Delete** icon (in the **Configure** column) to remove it from the table.

3

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

Capture Threat Assessment User Guide
Updated - May 2021
232-005607-00 Rev A

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035