SONICWALL

Capture Threat Assessment Report

ROVERMOOT
Feb 04 2023 17:16:31 - Feb 10 2023 17:02:34
Period: 6 Day(s)
Serial Number: 18C241420850
Firewall Type: SonicWALL TZ 270
SonicOS Version: 7.0.1-5095-R3599

Prepared By:
ROVERMOOT

SECURE MORE.
FEAR LESS.

Table of Contents

EXECUTIVE SUMMARY

The Capture Threat Assessment (CTA) Report summarizes the business and security risks facing **ROVERMOOT**. 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.

APPLICATIONS	212
VULNERABLE APPLICATIONS	7
TOTAL THREATS	76,733
EXPLOITS	76,733
MALWARE	0
UNSEEN MALWARE	0

KEY FINDINGS

212 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.

76,733 total threats detected on your network, including exploits, spyware, malware and unseen malware, and botnets.

RECOMMENDATIONS

1 4 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 4 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 0 Botnet Infections

You do not have any Botnet Infections within your network at this point.

4 4 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.

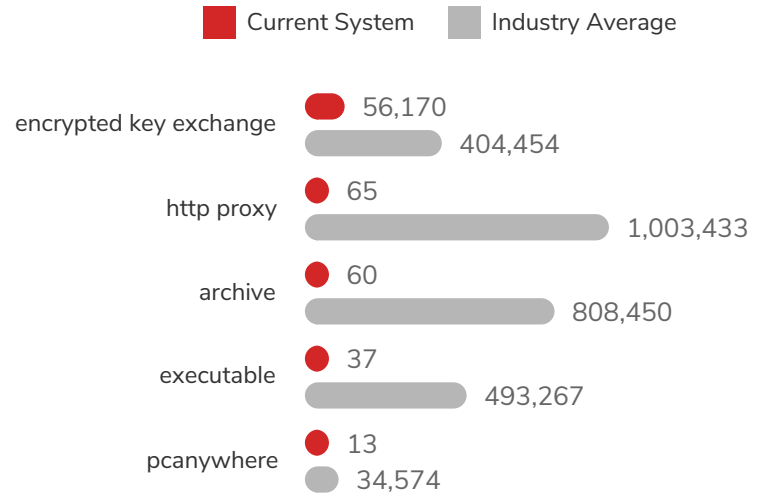
APPLICATION HIGHLIGHTS

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.

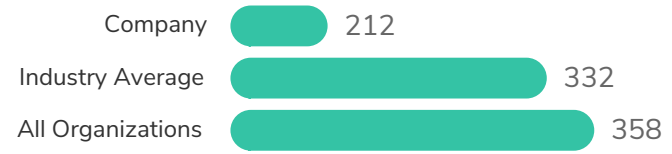
VULNERABLE APPLICATIONS

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.

VULNERABLE APPLICATIONS



NUMBER OF APPLICATIONS ON NETWORK



KEY FINDINGS

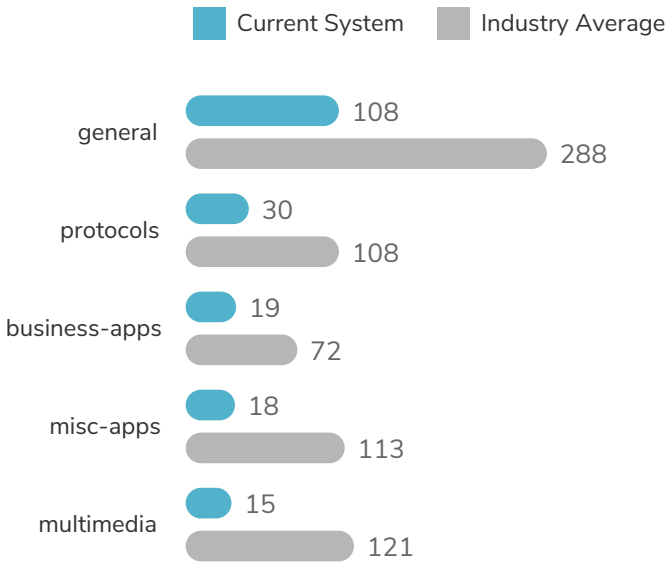
Vulnerable applications such as encrypted key exchange, http proxy, arc were detected on the network, which should be investigated since they can lead to possible exploitation.

212 total applications were observed on your network across **7** sub-categories, whereas an industry average of **332** total applications seen in other organizations.

49.84 GB was used by all applications in the network, including proxy- with **19.51 GB**, in comparison to an industry average of **2.72 GB** in similar organizations.

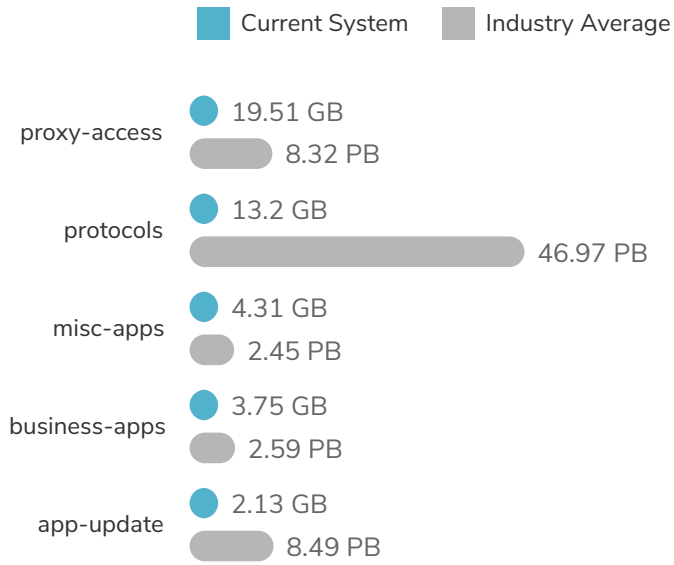
APPLICATION CATEGORIES

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

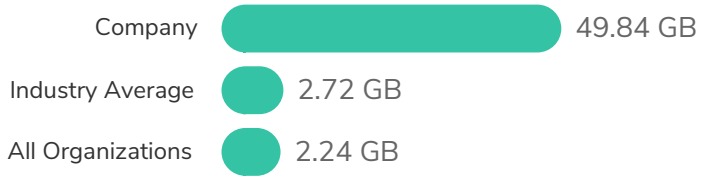


MOST BANDWIDTH CONSUMING CATEGORIES

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



BANDWIDTH CONSUMPTION BY APPLICATIONS



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 **212** applications were seen in your organization, compared to an industry average of **332** in other organizations.

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

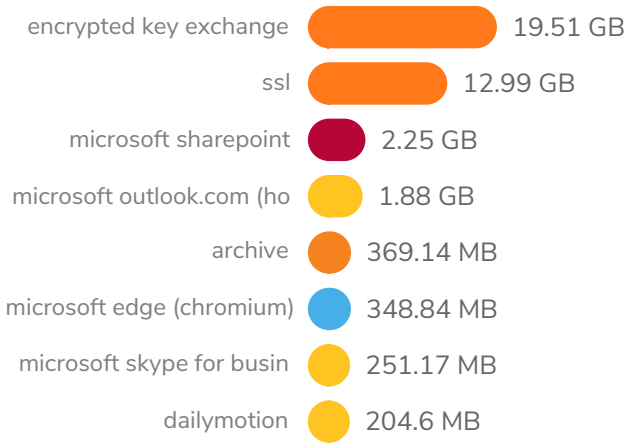
The application subcategories consuming the most bandwidth are policy-violation, not-suspicious, general

POLICY-VIOLATION - 38.32 GB

60 / 482

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP POLICY-VIOLATION APPS

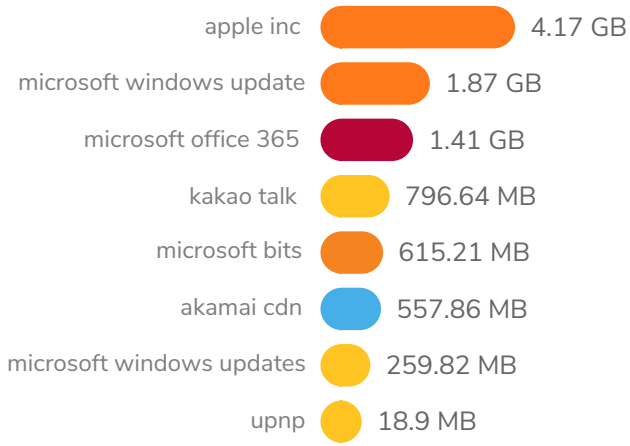


NOT-SUSPICIOUS - 9.69 GB

28 / 240

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP NOT-SUSPICIOUS APPS

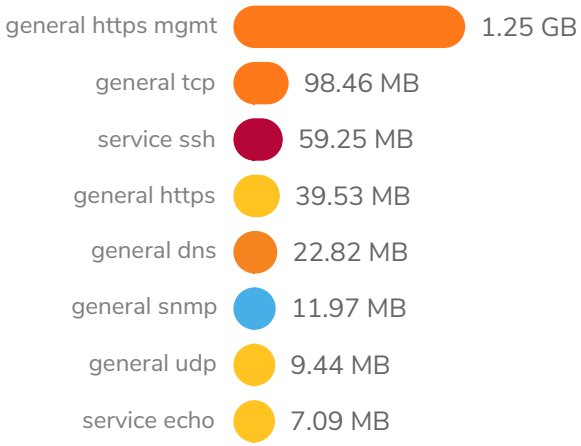


GENERAL - 1.52 GB

105 / 288

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP GENERAL APPS

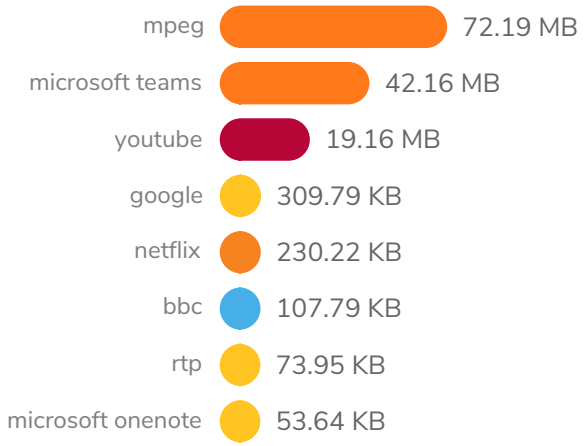


MULTIMEDIA - 134.28 MB

8 / 114

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP MULTIMEDIA APPS

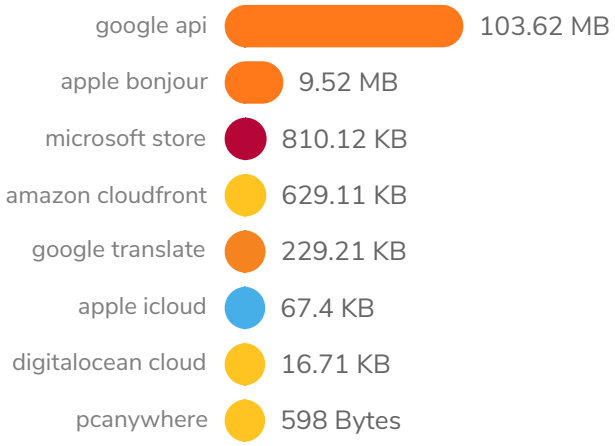


MISC-ACTIVITY - 114.86 MB

10 / 27

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP MISC-ACTIVITY APPS

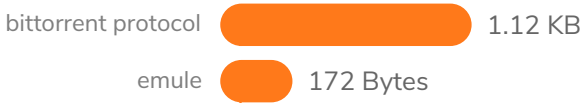


P2P - 1.29 KB

2 / 8

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP P2P APPS

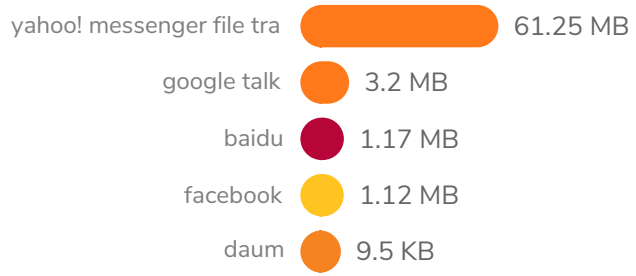


IM - 66.75 MB

5 / 26

APPLICATION VARIANTS
VS INDUSTRY AVERAGE

TOP IM APPS



APPLICATION BY RISK LEVEL

APPLICATION	RISK	CATEGORY	SUB CATEGORY	TECHNOLOGY	TRAFFIC	SESSIONS
encrypted key exchange	5	proxy-access	policy-violation	stand-alone-application	20 GB	56,170
archive	4	filetype-detection	policy-violation	browser-based	370 MB	67
http proxy	4	proxy-access	policy-violation	browser-based	720 KB	65
executable	4	filetype-detection	policy-violation	browser-based	28 MB	37
pcanywhere	4	remote-access	misc-activity	stand-alone-application	598 Bytes	13
microsoft remote deskt	4	remote-access	policy-violation	stand-alone-application	5 KB	11
socks	4	proxy-access	policy-violation	browser-based	71 KB	1
general udp	3	general	general		10 MB	32,546
general llmnr	3	general	general		423 KB	5,952
service version 2 mult	3	general	general		304 KB	913
faceapp	3	mobile-apps	policy-violation	stand-alone-application	46 MB	575
service apple bonjour	3	general	general		254 KB	119
service multicast list	3	general	general		1008 Bytes	5
bacnet protocol	3	scada-apps	misc-activity	network-infrastructure	65 Bytes	1
digitalocean cloud	3	infrastructure	misc-activity	network-infrastructure	17 KB	1

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.

NO Data available. Make Sure to have Analytics licensing enabled to capture Shadow IT data in this report.

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.

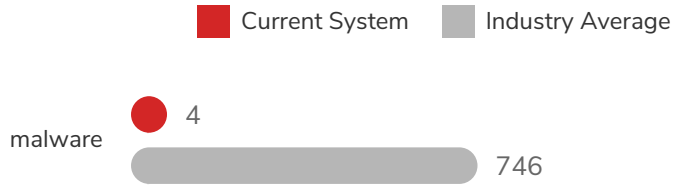
WEB ACTIVITY

Internet browsing that is not being controlled in a network leads to severe risks and 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.

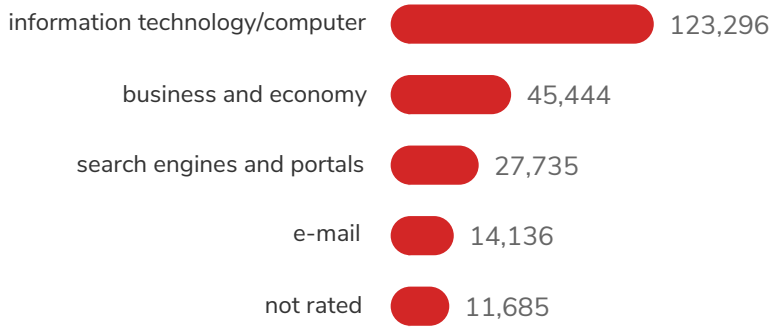
MALWARE Web Category

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



KEY FINDINGS

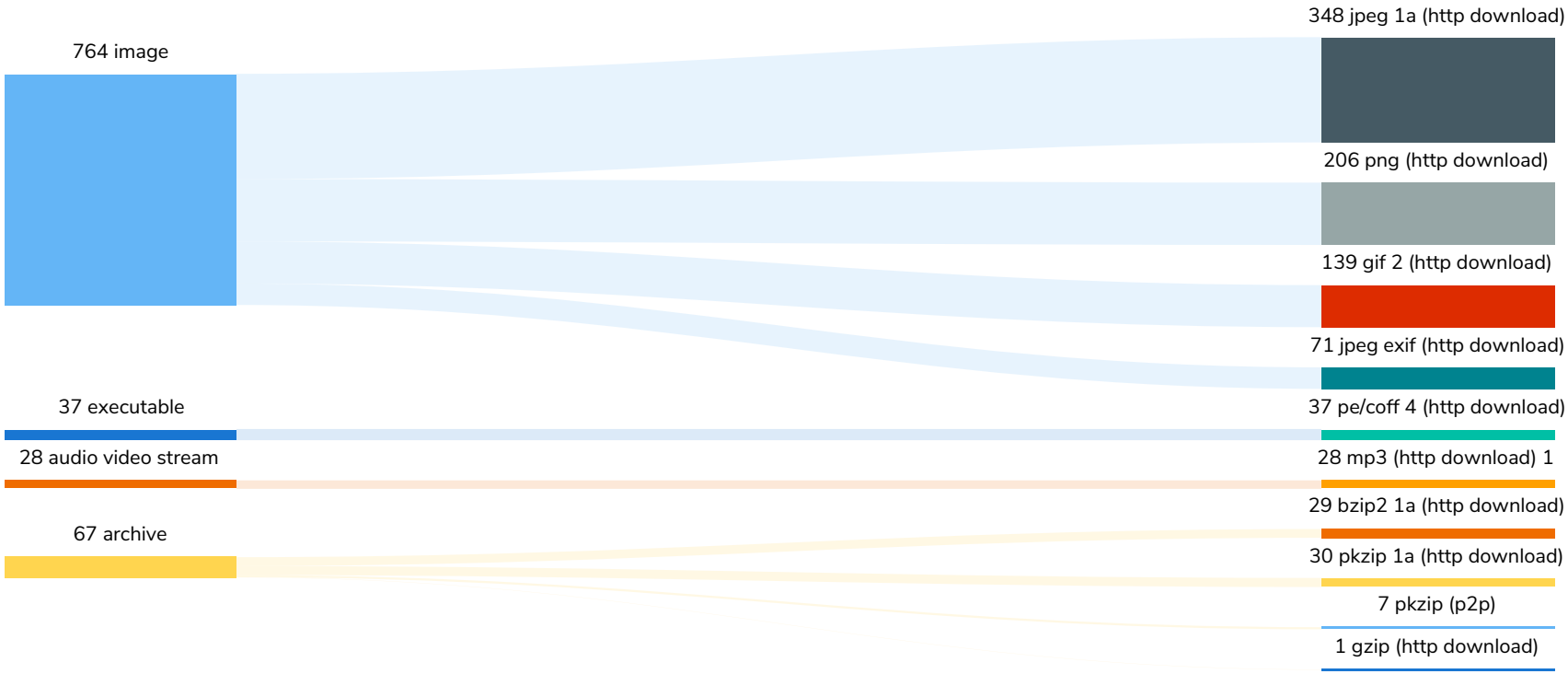
Malware web URL category was observed on the network, including information technology / computer, business and economy, search engines and portals

258,289 total URLs were accessed by users during the time period when this report was captured across **38** 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 allow sensitive data to go out of your network. Using the file analysis engine helps attain an overall security posture for your organization.



KEY FINDINGS

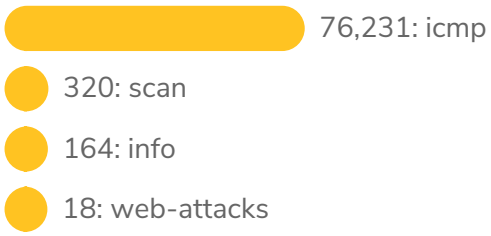
11 unique file types were observed.

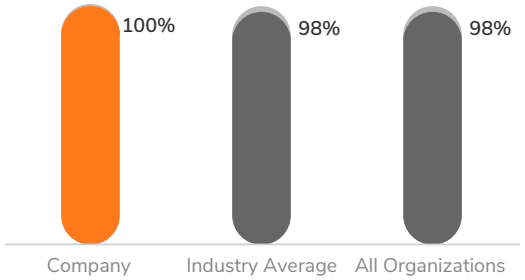
The graph here connects the applications that are mostly used to transfer files.

GLIMPSE OF THE THREATS

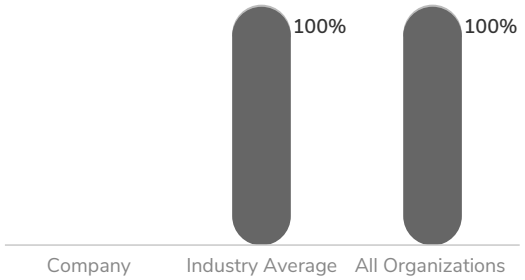
Artificial Intelligence is required to understand your risk exposure. This section details the application exploits, spyware, adware, malware and unseen malware, and botnet activity observed on your network. Deep packet Inspection examines the next layers to find and track any threats which are trying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

76,733
Exploits





0
Malware



0
Botnets

KEY FINDINGS

76,733 total exploits were observed in your organization, including icmp, scan, info

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

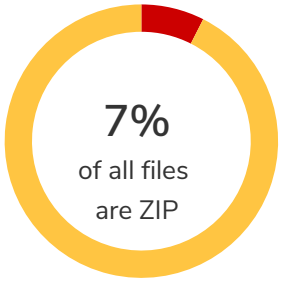
0 total botnet requests were identified.

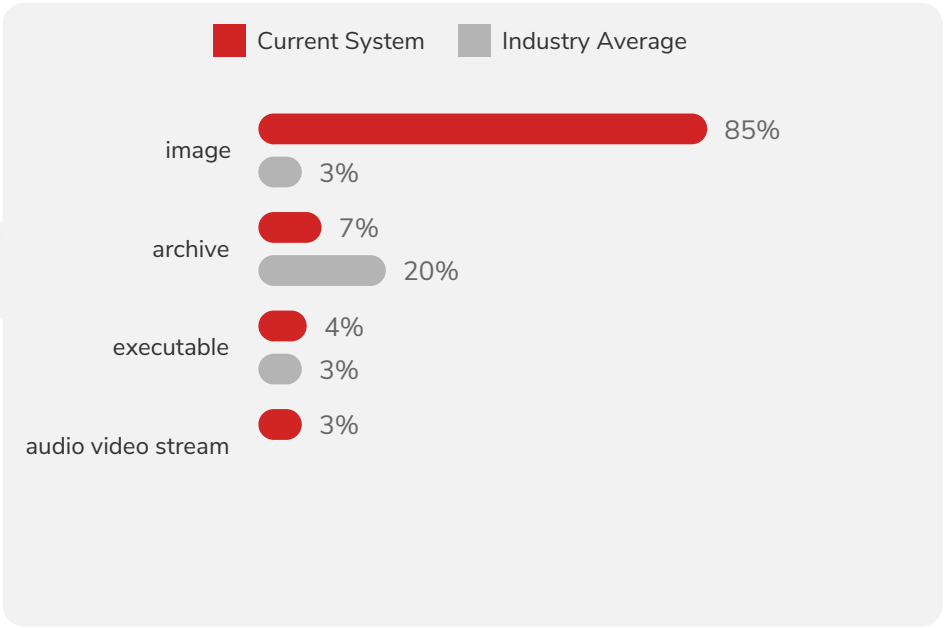
MALWARE ANALYSIS

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.

FILES DELIVERING UNSEEN MALWARE

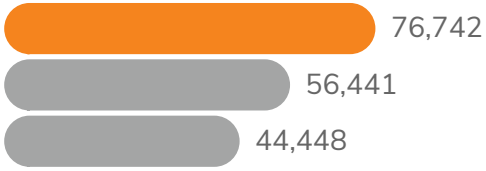
SonicWall Capture ATP revolutionizes advanced threat detection and sandboxing with a multi-engine approach to stopping unseen malware at the gateway. We recommend using Capture ATP to analyze the files that may be used to deliver malware within the network but have yet to be categorized as a threat. 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.

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.

APPLICATIONS DELIVERING EXPLOITS

TOTAL EXPLOITS



KEY FINDINGS

14 total applications were observed delivering exploits to your environment.

76,742 total exploits were observed across the following top three applications: icmp, general sip control, general udp

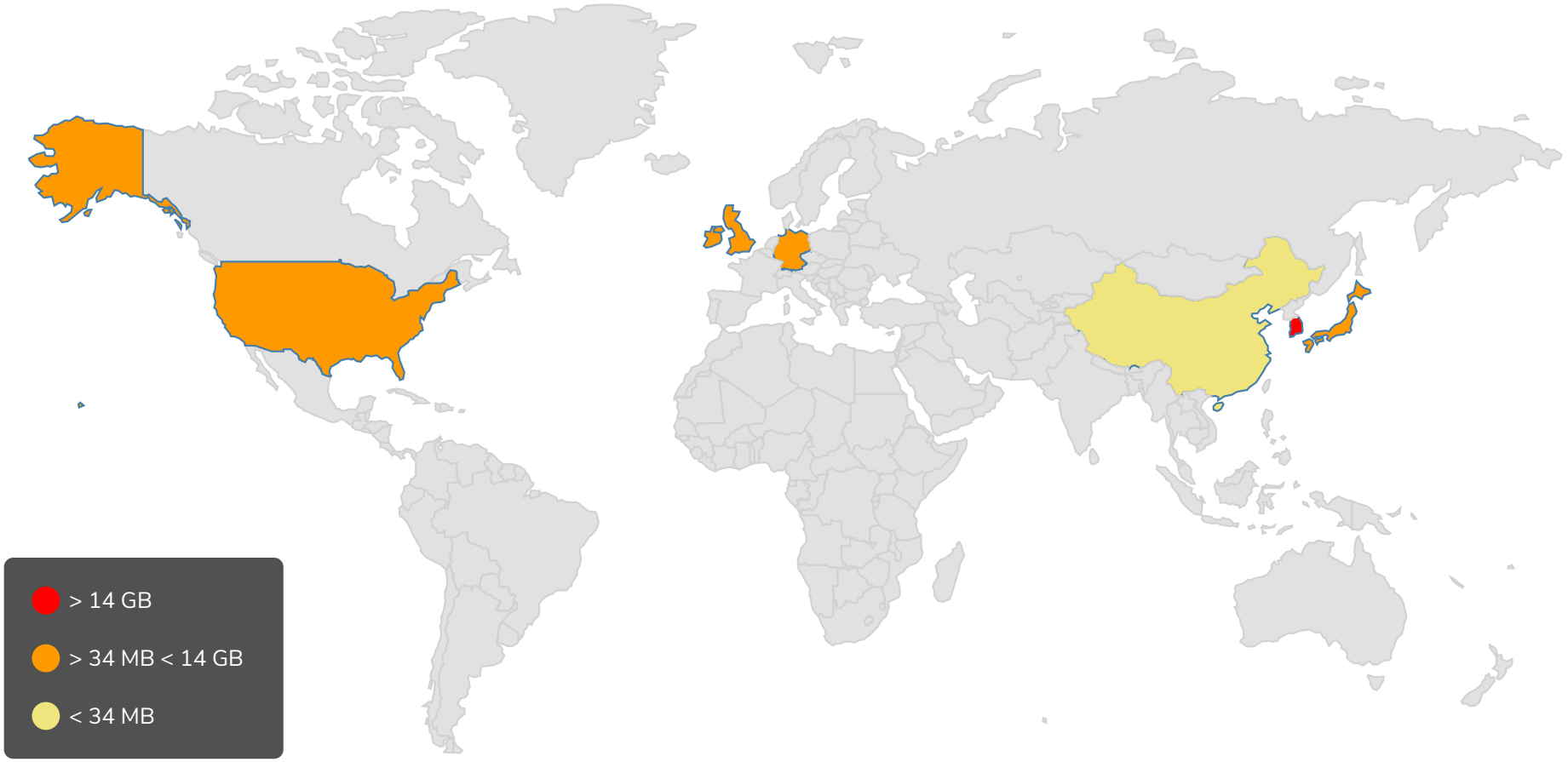
Exploits per Application

You can find out the top exploits and number of detections within your organization

DETECTIONS	APPLICATION & EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
76,228	**icmp**			
75,618	echo reply (0)	Low	protocols	
606	echo (8)	Low	protocols	
4	redirect (5)	Low	protocols	
214	**general sip control**			
214	general sip control		general	
82	**general udp**			
82	general udp		general	
67	**sip**			
41	invite	Low	voip-apps	2017009359
26	register	Low	voip-apps	2011001147

Exploits per Application

DETECTIONS	APPLICATION & EXPLOITS	SEVERITY	THREAT TYPE	CVE ID
52	**service ntp**			
52	service ntp		general	
35	**encrypted key exchange**			
32	random encryption (skype,ultrasurf, emule)	Severe	proxy-access	
3	udp random encryption (ultrasurf)	Severe	proxy-access	2011001852
22	**dns protocol**			
22	standard query a	Low	protocols	
18	**general http**			
18	general http		general	



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 by source detected during the audit period are presented below:

COUNTRY	TRAFFIC	SESSIONS	BLOCKED
Private	51 GB	949,312	0
Korea	25 GB	439,791	0
Unknown	64 MB	324,973	0
United States	14 GB	223,143	0
Japan	9 GB	51,121	0
China	19 MB	25,889	0
Germany	141 MB	20,234	0
United Kingdom	34 MB	18,573	0
Singapore	657 MB	17,857	0
Ireland	34 MB	15,623	0

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 information provides insight into the largest consumers of traffic going out through your firewall.

IP	TRAFFIC	SESSIONS
172.16.1.245	2 GB	233,924
Others	18 GB	215,037
1.209.147.165	232 MB	170,254
1.209.147.162	141 MB	148,379
172.16.0.7	13 MB	77,638
172.16.1.111	4 GB	75,194
1.209.147.163	8 MB	73,669
172.16.1.136	3 GB	64,521
172.16.1.1	4 MB	59,482
172.16.1.66	2 GB	35,216
172.16.1.52	7 GB	33,566
172.16.1.64	5 GB	31,361
Total	100 GB	2,177,846

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.

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
Others	18 GB	215,037
172.16.1.48	9 GB	14,720
172.16.1.139	8 GB	18,470
172.16.1.52	7 GB	33,566
172.16.1.62	6 GB	16,652
172.16.1.64	5 GB	31,361
172.16.1.111	4 GB	75,194
172.16.1.136	3 GB	64,521
172.16.1.53	3 GB	23,746
172.16.1.66	2 GB	35,216
172.16.1.245	2 GB	233,924
172.16.1.20	874 MB	31,109
Total	100 GB	2,177,846

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.

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	49 GB	979,771
admin	2 GB	109,152
Total	50 GB	1,088,923

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.

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	49 GB	979,771
admin	2 GB	109,152
Total	50 GB	1,088,923

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.

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.

About SonicWall

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small and medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear. For more information, visit sales@sonicwall.com.

Contact Us

+1.888.557.6642

sales@sonicwall.com

SONICWALL

SECURE MORE.
FEAR LESS.

SONICWALL CAPTURE CLOUD PLATFORM

BOUNDLESS CYBERSECURITY

Break free from untenable economic, technical and staffing constraints

ANYWHERE, EVERYWHERE

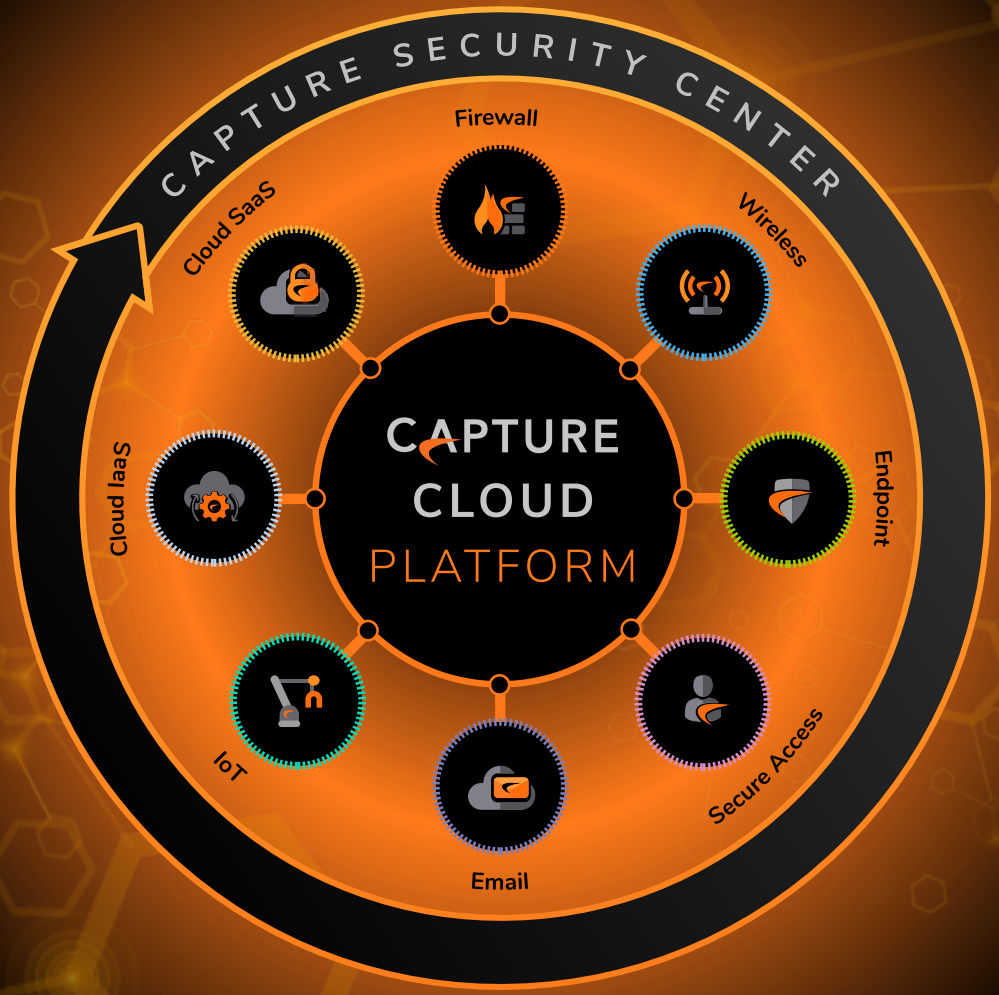
Security goes wherever users, devices, data are

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

SONICWALL®

Cloud Edge

Network Security Manager

Capture Client

Cloud App Security

Wireless Network Manager

Shadow IT

Hosted Email Security

Secure Mobile Access

Capture Security Applicance

Switch

MySonicWall

Risk Meter

Capture ATP

WiFi Planner