



# Cyber Threat Assessment

Report Date: July 31, 2018 11:16

Data Range: 2018-07-24 00:00 2018-07-30 23:59 CST (FAZ local)

# Table of Contents

Organizational File Usage .....	3
Files Needing Inspection .....	3
Breakdown of File Types .....	3
Results of Executable Sandbox Analysis .....	4
Top Sandbox-identified Malicious EXEs .....	4
Top Sources of Sandbox Discovered Malware .....	4
Recommended Actions .....	5
Security and Threat Prevention .....	6
High Risk Applications .....	6
High Risk Applications .....	6
Application Vulnerability Exploits .....	6
Top Application Vulnerability Exploits Detected .....	7
Malware, Botnets and Spyware/Adware .....	8
Top Malware, Botnets and Spyware/Adware Detected .....	8
At-Risk Devices and Hosts .....	8
Most At-Risk Devices and Hosts .....	8
Encrypted Web Traffic .....	9
HTTPS vs. HTTP Traffic Ratio .....	9
Top Source Countries .....	9
Top Source Countries .....	9
User Productivity .....	10
Application Usage .....	10
App Categories .....	10
Cloud Usage (SaaS) .....	10
Cloud Usage (IaaS) .....	10
Application Category Breakdowns .....	11
Remote Access Applications .....	11
Proxy Applications .....	11
Top Social Media Applications .....	11
Top Video/Audio Streaming Applications .....	11
Top Gaming Applications .....	11
Top Peer to Peer Applications .....	11
Web Usage .....	12
Top Web Categories .....	12
Top Web Applications .....	13
Websites Frequented .....	14
Most Visited Web Domains .....	14
Top Websites by Browsing Time .....	14
Network Utilization .....	16
Bandwidth .....	16
Average Bandwidth by Hour .....	16
Top Bandwidth Consuming Sources/Destinations .....	16
FortiGuard Security and Services .....	17
Appendix A .....	18
Devices .....	18

## Executive Summary



### Security and Threat Prevention

**IPS Attacks Detected:** 118

**Malware/Botnets Detected:** 6

**High-Risk Applications Used:** 4

**Malicious Websites Detected:** 10

Last year, over 2,100 enterprises were breached as a result of poor internal security practices and latent vendor content security. The average cost of a corporate security breach is estimated at \$3.5 million USD and is rising at 15% year over year. Intrusions, malware/botnets and malicious applications collectively comprise a massive risk to your enterprise network. These attack mechanisms can give attackers access to your most sensitive files and database information. FortiGuard Labs mitigates these risks by providing award-winning content security and is consistently rated among industry leaders by objective third parties such as NSS Labs, VB 100 and AV Comparatives.



### User Productivity

**Applications Detected:** 189

**Top Used Application:** HTTPS.BROWSER

**Top Application Category:** Web.Client

**Websites Visited:** 8896

**Top Website:** 7.tlu.dl.delivery.mp.microsoft.com

**Top Web Category:** Information Technology

User application usage and browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate a lack of proper enforcement of corporate usage policies. Most enterprises recognize that personal use of corporate resources is acceptable. But there are many grey areas that businesses must keep a close eye on including: use of proxy avoidance/peer to peer applications, inappropriate web browsing, phishing websites, and potentially illegal activity - all of which expose your company to undue liability and potential damages. With over 5,800 application control rules and 250 million categorized websites, FortiGuard Labs provides telemetry that FortiOS uses to keep your business running effectively.



### Network Utilization

**Total Bandwidth:** 106148673286

**Top Host by Bandwidth:** 192.168.0.151

Performance effectiveness is an often undervalued aspect of security devices, but firewalls must keep up with the line speeds that today's next generation switches operate at. A recent survey by Infonetix indicates that 77% of decision-makers at large organizations feel that they must upgrade their network security performance (100+ Gbps aggregate throughput) in the coming year. FortiGates leverage FortiASICs to accelerate CPU intensive functions such as packet forwarding and pattern matching. This offloading typically results in a 5-10X performance increase when measured against competitive solutions.

# Sandbox Analysis

Today's increasingly sophisticated threats can mask their maliciousness and bypass traditional antimalware security. Conventional antimalware engines are, in the time afforded and to the certainty required, often unable to classify certain payloads as either good or bad; in fact, their intent is unknown. Sandboxing helps solve this problem – it entices unknown files to execute in a protected environment, observes its resultant behavior and classifies its risk based on that behavior. With this functionality enabled for your assessment, we have taken a closer look at files traversing your network.

## Organizational File Usage

### Total Files Detected ( 0 )

During the assessment period, we monitored the total number of files that were sent across your network. These files could have been email attachments, files uploaded to file sharing services, downloads from the Internet, etc. This number will give you an idea of the sheer amount of file-based activity either inbound or outbound.

### Subset of Files Which Could be Sent for Sandbox Inspection ( )

While some file types like .png files are extremely low risk in nature, others can be executed or contain macros and other active code that could exhibit malicious behaviors. Common files types such as exe, doc, xls, and zip should be inspected for their potential to deliver threats to your network. Fortinet's sandboxing technologies can inspect more than 50 different file types even while obfuscated within multiple layers of compression.

### Files Needing Inspection

No matching log data for this report
--------------------------------------

### Breakdown of File Types

No matching log data for this report
--------------------------------------

## Results of Executable Sandbox Analysis

### Total EXE Files Analyzed ( 0 )

As a highest risk file type, we started with executables which, after a standard anti-malware check on the FortiGate, were sent to the sandbox for further inspection. The number here represents the subset of executables that were sent to the sandbox for additional scrutiny.

### Total Malicious EXEs Found ( 0 )

Of the Total EXE Files Analyzed, certain files may have tested positive for malicious threat payloads upon further inspection. Often times this subsequent identification is due to later stage downloads or communications that are known to be malicious. This is the number of malicious files that were discovered during our executable analysis.

### Top Sandbox-identified Malicious EXEs

No matching log data for this report

### Top Sources of Sandbox Discovered Malware

No matching log data for this report

# Recommended Actions

## Application Vulnerability Attacks Detected ( 9 )

Application vulnerabilities (also known as IPS attacks) act as entry points used to bypass security infrastructure and allow attackers a foothold into your organization. These vulnerabilities are often exploited due to an overlooked update or lack of patch management process. Identification of any unpatched hosts is the key to protecting against application vulnerability attacks.

## Malware Detected ( 6 )

Malware can take many forms: viruses, trojans, spyware/adware, etc. Any instances of malware detected moving laterally across the network could also indicate a threat vector originating from inside the organization, albeit unwittingly. Through a combination of signature and behavioral analysis, malware can usually be prevented from executing and exposing your network to malicious activity. Augmenting your network with APT/sandboxing technology (e.g. FortiSandbox) can also prevent previously unknown malware (zero-day threats) from propagating within your network.

## Botnet Infections ( 0 )

Bots can be used for launching denial-of-service (DoS) attacks, distributing spam, spyware and adware, propagating malicious code, and harvesting confidential information which can lead to serious financial and legal consequences. Botnet infections need to be taken seriously and immediate action is required. Identify botnet infected computers and clean them up using antivirus software. Fortinet's FortiClient can be used to scan and remove botnets from the infected hosts.

## Malicious Websites Detected ( 10 )

Malicious websites are sites known to host software/malware that is designed to covertly collect information, damage the host computer or otherwise manipulate the target machine without the user's consent. Generally visiting a malicious website is a precursor to infection and represents the initial stages of the kill chain. Blocking malicious sites and/or instructing employees not to visit/install software from unknown websites is the best form of prevention here.

## Phishing Websites Detected ( 3 )

Similar to malicious websites, phishing websites emulate the webpages of legitimate websites in an effort to collect personal or private (logins, passwords, etc.) information from end users. Phishing websites are often linked to within unsolicited emails sent to your employees. A skeptical approach to emails asking for personal information and hovering over links to determine validity can prevent most phishing attacks.

## Proxy Applications Detected ( 1 )

These applications are used (usually intentionally) to bypass in-place security measures. For instance, users may circumvent the firewall by disguising or encrypting external communications. In many cases, this can be considered a willful act and a violation of corporate use policies.

## Remote Access Applications Detected ( 4 )

Remote access applications are often used to access internal hosts remotely, thus bypassing NAT or providing a secondary access path (backdoor) to internal hosts. In the worst case scenario, remote access can be used to facilitate data exfiltration and corporate espionage activity. Many times, the use of remote access is unrestricted and internal corporate use changes should be put into practice.

## P2P and Filesharing Applications ( 0 )

These applications can be used to bypass existing content controls and lead to unauthorized data transfer and data policy violations. Policies on appropriate use of these applications need to be implemented.

# Security and Threat Prevention

## High Risk Applications

The FortiGuard research team assigns a risk rating of 1 to 5 to an application based on the application behavioral characteristics. The risk rating can help administrators to identify the high risk applications quickly and make a better decision on the application control policy. Applications listed below were assigned a risk rating of 4 or higher.

### High Risk Applications



















Risk	Application Name	Category	Technology	User	Bandwidth	Session
4	 RDP	 Remote.Access	Client-Server	237	0 B	765
4	 VNC	 Remote.Access	Client-Server	97	0 B	219
4	 AnyDesk	 Remote.Access	Client-Server	7	40.05 MB	115
4	 TeamViewer	 Remote.Access	Client-Server	8	1.63 MB	68
4	 Rsh	 Remote.Access	Client-Server	12	1.06 KB	33
4	 Rexec	 Remote.Access	Client-Server	9	0 B	20
4	 Rlogin	 Remote.Access	Client-Server	5	0 B	8
4	 Citrix.Receiver	 Remote.Access	Client-Server	2	106.38 KB	3
4	 TeamViewer_CallRequest	 Remote.Access	Client-Server	2	1.28 MB	2

Figure 1: Highest risk applications sorted by risk and sessions

## Application Vulnerability Exploits

Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and then develops signatures to detect them. FortiGuard currently leverages a database of more than 5,800 known application threats to detect attacks that evade traditional firewall systems. For more information on application vulnerabilities, please refer to FortiGuard at: <http://www.fortiguard.com/intrusion>.

## Top Application Vulnerability Exploits Detected










Severity	Threat Name	Type	CVE-ID	Victim	Source	Count
5	 D-Link.DSL-2750B.CLI.OS.Command.Injection	OS Command Injection		2	31	35
5	 MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	Buffer Errors	CVE-2017-7269	2	16	18
5	 Dasan.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	2	13	13
5	 Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	Code Injection	CVE-2017-3506,CVE-2017-10271	1	2	2
4	 JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	OS Command Injection		2	37	38
4	 PHP.CGI.Argument.Injection	Code Injection	CVE-2012-1823,CVE-2012-2311	2	1	2
4	 Obfuscated.Rich.Text.Format	Anomaly	CVE-2018-0802	2	1	2
2	 ZmEu.Vulnerability.Scanner	Malware		1	1	6
2	 Masscan.Scanner	Anomaly		2	1	2

Figure 2: Top vulnerabilities identified, sorted by severity and count



## Malware, Botnets and Spyware/Adware

There are numerous channels that cybercriminals use to distribute malware. Most common methods motivate users to open an infected file in an email attachment, download an infected file, or click on a link leading to a malicious site. During the security assessment, Fortinet identified a number of malware and botnet-related events which indicate malicious file downloads or connections to botnet command and control sites.

### Top Malware, Botnets and Spyware/Adware Detected




Malware Name	Type	Application	Victim	Source	Count
Malicious_Behavior.SB	Virus	 SMTP	1	1	21
VBA/TrojanDownloader.JMR!tr	Virus	 SMTP	1	4	6
Malicious_Behavior.SB	Virus	 POP3	1	1	2

Figure 3: Common Malware, Botnets, Spyware and Adware detected

## At-Risk Devices and Hosts

Based on the types of activity exhibited by an individual host, we can approximate the trustworthiness of each individual client. This client reputation is based on key factors such as websites browsed, applications used and inbound/outbound destinations utilized. Ultimately, we can create an overall threat score by looking at the aggregated activity used by each individual host.

### Most At-Risk Devices and Hosts


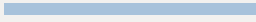

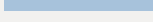
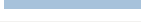

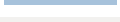
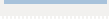
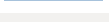

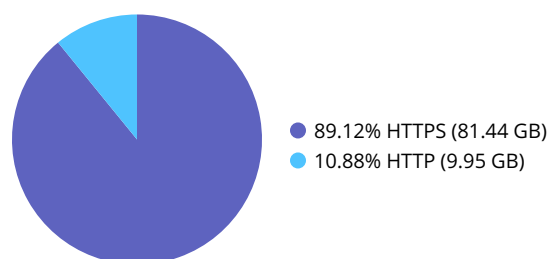
Device	Scores
190.143.136.42	 373,970
192.168.26.63	 149,705
192.168.0.156	 136,605
192.168.26.66	 87,555
192.168.26.60	 80,245
192.168.26.61	 78,760
192.168.26.80	 66,625
192.168.26.95	 60,200
192.168.0.151	 57,490
69.64.45.125	 53,955

Figure 4: These devices should be audited for malware and intrusion susceptibility

## Encrypted Web Traffic

From a security perspective, it's important to visualize how much of your web-based traffic is encrypted. Encrypted traffic poses very real challenges for enterprises who want to ensure that those same applications are not being used for malicious purposes, including data exfiltration. Ideally, your firewall can inspect encrypted traffic at high speeds - this is why performance and hardware/ASIC offloading are key when evaluating a firewall.

HTTPS vs. HTTP Traffic Ratio



## Top Source Countries

By looking at IP source traffic, we can determine the originating country of any particular request. Certain botnets, command and control functions, and even remote access can be session heavy and indicative of targeted attacks or persistent threats from nation-states. This chart is representative of country-based traffic - activity from specific originating nations may be anomalous and warrant further investigation.

### Top Source Countries

Country	Bandwidth
United States	1.87 GB
Guatemala	253.51 MB
El Salvador	13.77 MB
Netherlands	10.98 MB
Canada	8.58 MB
United Kingdom	6.89 MB
Turkey	6.58 MB
Italy	5.59 MB
Germany	4.37 MB
France	3.66 MB

Figure 5: Activity originating from these countries should be audited for expected traffic sources

# User Productivity

## Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application control. FortiGuard maintains thousands of application sensors and can even perform deep application inspection. For example, IT managers can get unprecedented visibility into filenames sent to the cloud or the titles of videos being streamed.

For application category details, see:

<http://www.fortiguards.com/encyclopedia/application>

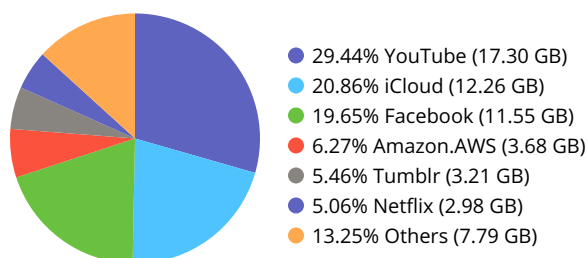
### App Categories

Video/Audio	22.16%
Web.Client	17.46%
Social.Media	16.19%
Storage.Backup	14.22%
General.Interest	11.23%
Collaboration	7.09%
Update	4.04%
Cloud.IT	3.98%
Network.Service	2.92%
Email	0.50%
Others	0.20%



With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. Unfortunately for enterprises, this means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

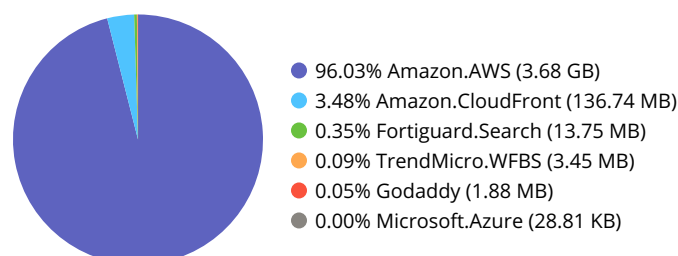
### Cloud Usage (SaaS)



IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.

The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

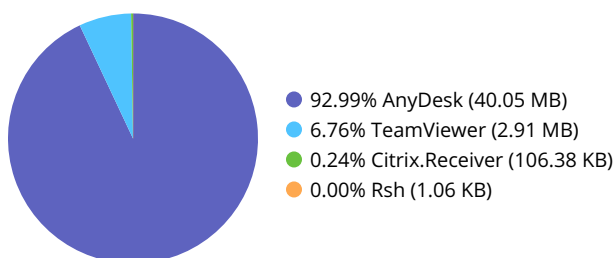
### Cloud Usage (IaaS)



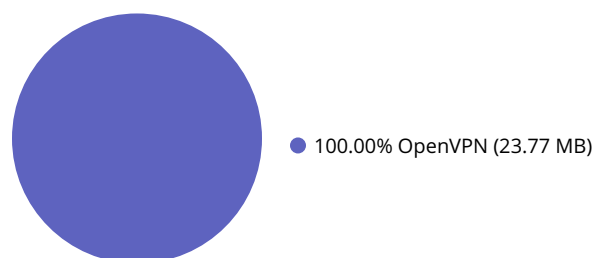
## Application Category Breakdowns

Understanding application subcategories can give invaluable insights into how efficiently your corporate network is operating. Certain application types (such as P2P or gaming applications) are not necessarily conducive to corporate environments and can be blocked or limited in their scope. Other applications may have dual purpose uses (such as video/audio streaming or social media apps) and can be managed accordingly. These charts illustrate application categories sorted by the amount of bandwidth they used during the discovery period.

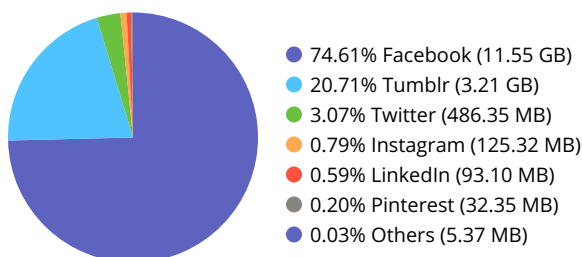
### Remote Access Applications



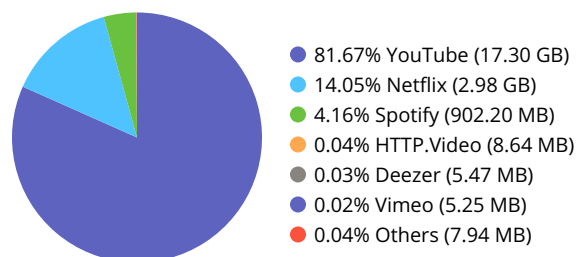
### Proxy Applications



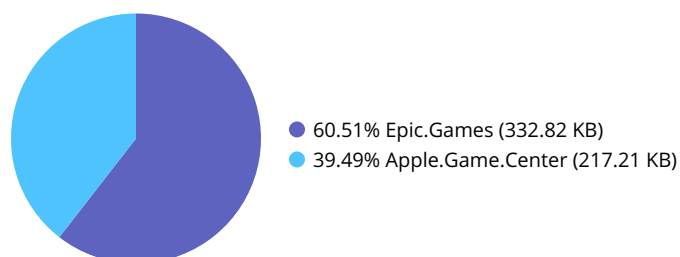
### Top Social Media Applications



### Top Video/Audio Streaming Applications



### Top Gaming Applications













### Top Peer to Peer Applications

No matching log data for this report

## Web Usage

Web browsing habits can not only be indicative of inefficient use of corporate resources, but can also indicate an inefficient optimization of web filtering policies. It can also give some insight into the general web browsing habits of corporate users and assist in defining corporate compliance guidelines.

### Top Web Categories

URL Category	User	Count	Bandwidth
 Information Technology	54	102,125	15.16 GB
 Search Engines and Portals	51	31,395	3.01 GB
 Advertising	49	25,679	774.73 MB
 Content Servers	50	15,717	3.17 GB
 Social Networking	47	15,286	8.26 GB
 Internet Telephony	40	13,461	321.33 MB
 Business	41	11,844	455.04 MB
 Freeware and Software Downloads	35	11,607	77.26 MB
 Internet Radio and TV	31	11,197	412.18 MB
 File Sharing and Storage	42	8,595	495.85 MB

In today's network environments, many applications leverage HTTP for communications – even some you wouldn't normally expect. The primary benefit of HTTP is that communication is ubiquitous, universally accepted and (generally) open on most firewalls. For most business-related and whitelisted applications this typically augments communication, but some non-business applications also use HTTP in either unproductive or potentially nefarious ways.










## Top Web Applications

Application	Sessions	Bandwidth
YouTube	11,355	17.30 GB
HTTPS.BROWSER	151,949	14.50 GB
iCloud	20,140	12.26 GB
Facebook	21,657	11.55 GB
Amazon.AWS	4,610	3.68 GB
WhatsApp	6,721	3.50 GB
MS.Windows.Update	3,767	3.47 GB
Tumblr	393	3.20 GB
Google.Services	34,087	3.10 GB
Netflix	419	2.98 GB
HTTP.BROWSER	21,715	2.18 GB
Apple.Store	94	1.72 GB
HTTP.Segmented.Download	276	1.61 GB
Amazon.Services	4,073	1.42 GB
Microsoft.CDN	6,181	1.25 GB
Apple.iCloud.Storage	136	1.15 GB
Google.Accounts	12,226	718.28 MB
Microsoft.Portal	22,456	506.75 MB
Twitter	3,906	486.35 MB
Spotify	454	431.05 MB
WebEx	1,215	408.43 MB
Gmail	3,701	326.56 MB
Google.Ads	10,080	297.27 MB
Skype	7,037	234.84 MB
Apple.Services	2,770	218.32 MB

## Websites Frequented




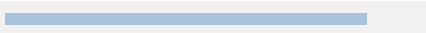



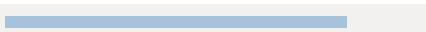

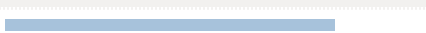







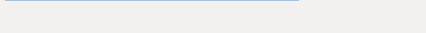







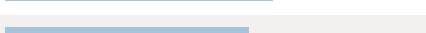



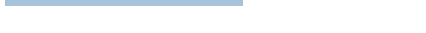





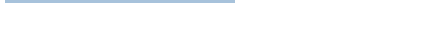
Websites browsed are strong indicators of how employees utilizing corporate resources and how applications communicate with specific websites. Analyzing domains accessed can lead to changes in corporate infrastructure such as website blocking, deep application inspection of cloud-based apps and implementation of web traffic acceleration technologies.

































### Most Visited Web Domains

Domain	Category	Visits
7.tlu.dl.delivery.mp.microsoft.com	 Information Technology	18,212
citrix.sisteco.biz	 Information Technology	12,228
play.google.com	 Freeware and Software Downloads	11,620
store.intcomex.com	 Information Technology	8,873
spclient.wg.spotify.com	 Internet Radio and TV	5,850
static.asm.skype.com	 Internet Telephony	4,937
static-asm.secure.skypeassets.com	 Content Servers	4,660
cdn-ssl.vidible.tv	 Internet Radio and TV	3,518
signal.pod1.avatar.ext.hp.com	 Information Technology	3,474
ocsp.digicert.com	 Information Technology	3,251

Estimated browsing times for individual websites can be useful when trying to get an accurate picture of popular websites. Typically, these represent internal web resources such as intranets, but they can occasionally be indicative of excessive behavior. Browse times can be employed to justify the implementation of web caching technologies or help shape organizational corporate use policies.

### Top Websites by Browsing Time

Sites	Category	Browsing Time(hh:mm:ss)
safebrowsing.googleapis.com	 Information Technology	 51:26:16
clients4.google.com	 Search Engines and Portals	 44:03:12
browser.pipe.aria.microsoft.com	 Information Technology	 43:35:19
www.google.com	 Business, Search Engines and Portals	 41:41:07
store.intcomex.com	 Information Technology	 40:18:23
ssl.gstatic.com	 Information Technology	 37:24:35
mail.google.com	 Web-based Email	 37:18:02
www.google.com.gt	 Global Religion, Search Engines and Portals	 35:51:20
mobile.pipe.aria.microsoft.com	 Information Technology	 35:04:25
www.facebook.com	 Social Networking	 33:50:26
notifications.google.com	 Search Engines and Portals	 32:41:04
clients6.google.com	 Search Engines and Portals	 29:54:51
www.google-analytics.com	 Information Technology, Search Engines and Portals	 29:00:59
www.googleapis.com	 Information Technology	 28:19:45
clientservices.googleapis.com	 Information Technology, Search Engines and Portals	 28:05:23
scontent.fgua4-1.fna.fbcnd.net	 Social Networking	 26:44:44
www.gstatic.com	 Search Engines and Portals	 25:02:19
adservice.google.com	 Search Engines and Portals	 23:13:52

Sites	Category	Browsing Time(hh:mm:ss)
adservice.google.com.gt	 Search Engines and Portals	22:52:44
citrix.sisteco.biz	 Information Technology	22:41:20
fonts.googleapis.com	 Information Technology	20:41:05
www.googletagmanager.com	 Information Technology	20:19:06
static.xx.fbcdn.net	 Social Networking	20:10:20
scontent.xx.fbcdn.net	 Social Networking	18:57:05
fonts.gstatic.com	 Information Technology	17:40:32
ogs.google.com	 Search Engines and Portals	17:38:23
accounts.google.com	 Search Engines and Portals	17:33:08
fls-na.amazon.com	 Shopping	16:51:56
apis.google.com	 Search Engines and Portals	16:47:40
beacons.gcp.gvt2.com	 Search Engines and Portals	16:24:10
android.clients.google.com	 Search Engines and Portals	16:21:55
clients1.google.com	 Search Engines and Portals	16:06:38
ocsp.digicert.com	 Information Technology	16:06:18
eusbn1-client-s.gateway.messenger.live.com	 Instant Messaging	16:01:29
nexus.officeapps.live.com	 Information Technology	16:01:00
video.fgua4-1.fna.fbcdn.net	 Social Networking	15:57:03
docs.google.com	 Web-based Applications	15:29:33
graph.facebook.com	 Social Networking	15:18:24
array506-prod.do.dsp.mp.microsoft.com	 Information Technology	15:15:00
cdn.content.prod.cms.msn.com	 Search Engines and Portals	14:32:40
web.whatsapp.com	 Web Chat	14:27:57
www.googletagservices.com	 Information Technology	14:16:39
csi.gstatic.com	 Search Engines and Portals	13:59:03
ajax.aspnetcdn.com	 Information Technology	13:26:38
www.bing.com	 Search Engines and Portals	13:17:02
edge-mqtt.facebook.com	 Social Networking	13:15:04
contacts.google.com	 Search Engines and Portals	12:48:25
www.amazon.com	 Shopping	12:20:45
people-pa.clients6.google.com	 Search Engines and Portals	12:12:49
cdn.onenote.net	 Information Technology	12:12:44

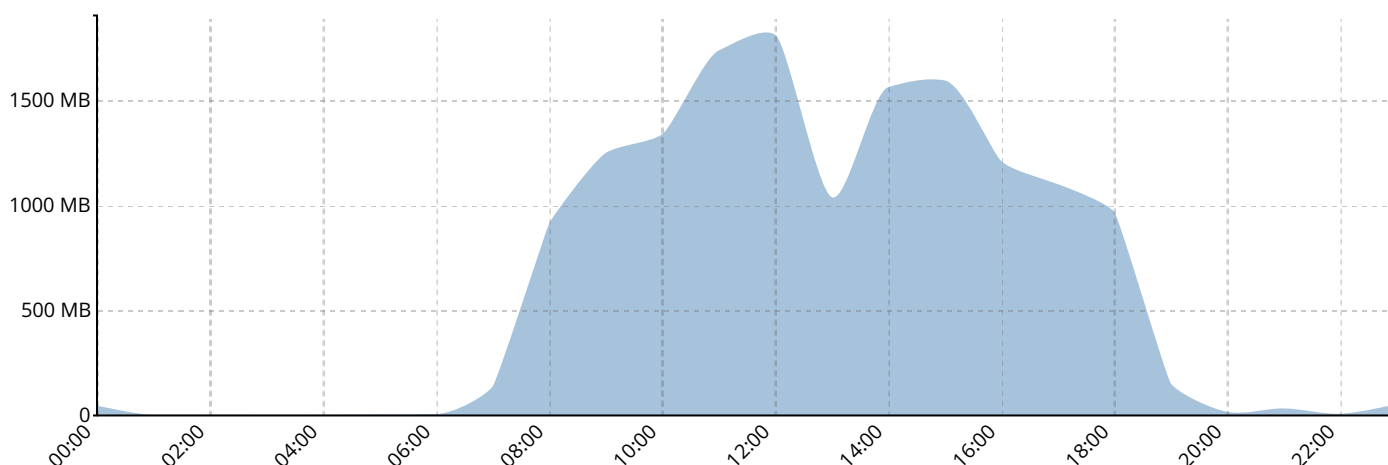


# Network Utilization

## Bandwidth

By looking at bandwidth usage when distributed over an average day, administrators can better understand their organizational ISP connection and interface speed requirements. Bandwidth can also be optimized on an application basis (using throttling), specific users can be prioritized during peak traffic times, and updates can be rescheduled outside of working hours.

### Average Bandwidth by Hour



One of the most telling ways to analyze bandwidth is by looking at destinations and sources generating the most traffic. Common destination sites (e.g. external websites), such as those for OS/firmware updates, can be throttled to allow prioritized, business critical traffic. Internally, high traffic hosts can be optimized through traffic shaping or corporate use policies.

### Top Bandwidth Consuming Sources/Destinations

Host Name	Bandwidth
video.fgua4-1.fna.fbcn.net	3.28 GB
7.tlu.dl.delivery.mp.microsoft.com	2.47 GB
photos.googleapis.com	1.98 GB
78.media.tumblr.com	1.92 GB
scontent.fgua4-1.fna.fbcn.net	1.74 GB
usmia-edge-092.icloud-content.com	1.61 GB
iosapps.itunes.apple.com	1.53 GB
ipv4-c002-gua001-ufinet-gt-isp.1.oa.nflxvideo.net	1.34 GB
mmg-fna.whatsapp.net	1.32 GB
endpoint920510.azureedge.net	1.08 GB

## FortiGuard Security and Services

Knowledge of the threat landscape combined with the ability to respond quickly at multiple levels is the foundation for providing effective security. Hundreds of researchers at FortiGuard Labs scour the cyber landscape every day to discover emerging threats and develop effective countermeasures to protect organizations around the world. They are the reason FortiGuard is credited with over 250 zero-day and vulnerability discoveries and why Fortinet security solutions score so high in real-world security effectiveness tests at NSS Labs, Virus Bulletin, AV Comparatives, and more.



### Next Generation Application Control & IPS

Application control and intrusion prevention (IPS) are foundational security technologies in a next generation firewall like the FortiGate. Organizations worldwide use FortiGuard application control and IPS in the FortiGate platform to manage their applications and block network intrusions (every minute of every day FortiGuard blocks ~470,000 intrusion attempts). FortiGates running application control and IPS are tested for effectiveness in industry comparison tests by NSS Labs and consistently receive Recommended ratings.



### Web Filtering

Every minute of every day FortiGuard Labs processes approximately 43M URL categorization requests and blocks 160k malicious websites. The Web Filtering service rates over 250M websites and delivers nearly 1.5M new URL ratings every week. FortiGuard is the only VBWeb certified web filtering solution - blocking 97.7% of direct malware downloads in 2016 tests.



### AntiVirus and Mobile Security

Every minute of every day FortiGuard Labs neutralizes approximately 95,000 malware programs targeting traditional, mobile and IoT platforms. Patented technologies enable FortiGuard antivirus to identify thousands of current and future malware variants with a single signature – optimizing both security effectiveness and performance. Fortinet consistently receives superior effectiveness results in industry testing with Virus Bulletin and AV Comparatives



### AntiSpam

Every minute of every day FortiGuard Labs blocks approximately 21,000 spam emails and each week the Labs deliver approximately 46M new and updated spam rules. Email is the #1 vector for the start of an advanced attack on an organization so highly effective antispam is a key part of a security strategy.



### Advanced Threat Protection (FortiSandbox)

Thousands of organizations around the world leverage FortiSandbox to identify advanced threats. FortiSandbox consistently receives a Recommended rating for breach detection systems from NSS Labs in industry tests and in 2015 NSS Labs tests achieved a 97%+ breach detection rating.



### IP Reputation

Every minute of every day FortiGuard Labs blocks approximately 32,000 botnet command & control communication attempts. A key part of the attack kill chain on an organization is when the threat communicates with a command & control server – either to download additional threats or to exfiltrate stolen data. IP and Domain address reputation blocks this communication, neutralizing threats.

## Appendix A

### Devices

Teco