



# Cyber Threat Assessment

Report Date: October 16, 2020 13:08

Data Range: 2020-09-16 00:00:00 2020-10-15 23:59:59EST (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 Country/Region .....	9
Top Source Country/Region .....	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 .....	12
Websites Frequented .....	13
Most Visited Web Domains .....	13
Top Websites by Browsing Time .....	13
Network Utilization .....	15
Bandwidth .....	15
Average Bandwidth by Hour .....	15
Top Bandwidth Consuming Sources/Destinations .....	15
FortiGuard Security and Services .....	16
Appendix A .....	17
Devices (1) .....	17

## Executive Summary



### Security and Threat Prevention

**IPS Attacks Detected:** 195

**High-Risk Applications Used:** 28

**Malware/Botnets Detected:** 3

**Malicious Websites Detected:** 104

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:** 422

**Top Application Category:** Collaboration

**Top Website:** contentsync.onenote.com

**Top Used Application:** HTTPS.BROWSER

**Websites Visited:** 67656

**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:** 3748277127863

**Top Host by Bandwidth**

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 Infonetics 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 ( )

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 ( )

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 ( )

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 ( 24 )

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 ( 0 )

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 ( 3 )

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 ( 104 )

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 ( 21 )

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 ( 18 )

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 ( 4 )

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
5	 Hola.Unblocker	 Proxy	Client-Server	23	40.64 MB	3,245
5	 FastLemon.VPN	 Proxy	Client-Server	3	2.19 MB	2,855
5	 Psiphon	 Proxy	Client-Server	14	141.53 MB	2,482
5	 Proxy.HTTP	 Proxy	Network-Protocol	17	467.49 MB	1,015
5	 Monero.Cryptocurrency.Miner	 General.Interest	Client-Server	1	1.10 MB	370
5	 Opera.VPN	 Proxy	Client-Server	3	1.23 MB	207
5	 Cloudflare.1.1.1.1.VPN	 Proxy	Client-Server	6	2.03 MB	177
5	 SurfEasy.VPN	 Proxy	Client-Server	10	1.15 MB	115
5	 Hotspot.Shield	 Proxy	Client-Server	1	7.99 KB	22
5	 Hoxx.VPN	 Proxy	Client-Server	1	36.70 KB	4
5	 DroidVPN	 Proxy	Client-Server	1	4.60 KB	3
5	 Proxy.Websites	 Proxy	Browser-Based	1	720.67 KB	2
5	 ZenMate	 Proxy	Browser-Based	1	9.63 KB	2
5	 Touch.VPN	 Proxy	Client-Server	1	10.54 KB	2
5	 Hamachi	 Proxy	Client-Server	1	1.35 KB	1
5	 SOCKS4	 Proxy	Network-Protocol	1	509 B	1
5	 SOCKS5	 Proxy	Network-Protocol	1	628 B	1
4	 RDP	 Remote.Access	Client-Server	485	66.91 MB	107,654
4	 BitTorrent	 P2P	Peer-to-Peer	10	21.71 MB	89,752
4	 TeamViewer	 Remote.Access	Client-Server	18	108.18 MB	12,536

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.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	CVE-2015-2051,CVE-2019-10891	1	12	12
5	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	Code Injection	CVE-2009-0545,CVE-2019-12725	1	2	11
5	Bladabindi.Botnet			1	4	9
5	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection		1	9	9
5	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Code Injection	CVE-2019-16759	1	1	7
5	Dasan.GPON.Remote.Code.Execution	OS Command Injection	CVE-2018-10561,CVE-2018-10562	1	6	6
5	Gh0st.Rat.Botnet			1	4	5
5	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Code Injection	CVE-2020-7373,CVE-2020-17496	1	1	4
5	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	CVE-2019-9082,CVE-2018-20062	1	3	4
5	DrayTek.Vigor.Router.Web.Management.Page.Command.Injection	OS Command Injection	CVE-2020-8515	1	1	1
5	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	OS Command Injection	CVE-2018-7600	1	1	1
5	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	CVE-2015-8562	1	1	1
4	Mirai.Botnet			1	11	11
4	PHP.CGI.Argument.Injection	Code Injection	CVE-2012-1823,CVE-2012-2311	1	2	5
4	PhpStudy.Web.Server.Remote.Code.Execution	Code Injection		1	1	3
4	ThinkPHP.HTTP.VARS.S.Remote.Code.Injection	Code Injection		1	2	2
4	ThinkPHP.Request.Method.Remote.Code.Execution	Code Injection		1	2	2
4	MS.Edge.Scripting.Engine.DataView.Memory.Corruption	Buffer Errors	CVE-2016-0024	1	1	1
4	Netlink.GPON.Router.formPing.Remote.Command.Injection	OS Command Injection		1	1	1
4	Tongda.Office.Anywhere.Unauthorized.File.Upload	Improper Authentication		1	1	1
3	PHP.Diescan	Anomaly		1	2	95
3	SSL.RSA.Temporary.Key.Security.Bypass	Information Disclosure	CVE-2015-0204,CVE-2015-1067,CVE-2015-1637	2	2	2
3	HTTP.Referer.Header.SQL.Injection	SQL Injection	CVE-2007-1061	1	1	1
3	Phpweb.CMS.appcode.Information.Disclosure	Information Disclosure		1	1	1

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
Mirai.Botnet	Virus	HTTP	1	11	11
Bladabindi.Botnet	Virus	HTTP	1	4	6
Gh0st.Rat.Botnet	Virus	HTTP	1	4	4

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

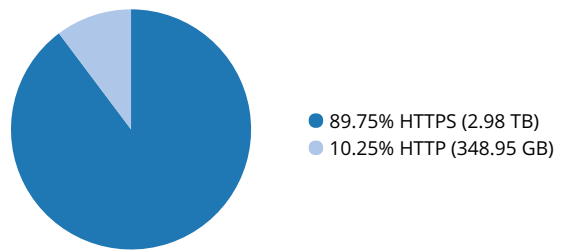
Device	Scores
10.1.211.42	229,290
10.1.242.140	201,760
10.1.240.17	65,370
10.1.241.146	62,650
10.1.248.56	37,305
10.1.241.34	23,400
10.1.240.222	23,290
10.1.241.84	22,645
10.1.248.7	17,570

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 Country/Region

By looking at IP source traffic, we can determine the originating country/region 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 Country/Region

Country/Region	Bandwidth
Australia	23.37 GB
United States	351.09 MB
Japan	39.12 MB
China	36.12 MB
Hong Kong	19.15 MB
Singapore	14.46 MB
Korea, Republic of	13.65 MB
Sweden	11.04 MB
Netherlands	8.54 MB
Germany	7.43 MB

Figure 5: Activity originating from these country/region 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.

### App Categories

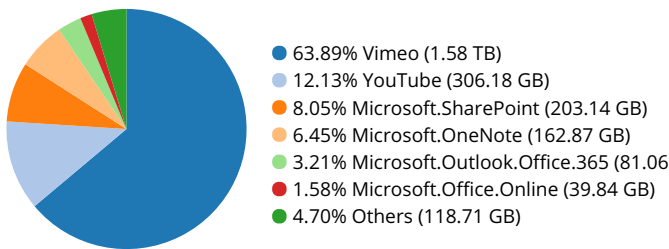
Video/Audio	57.74%
Collaboration	16.61%
Update	8.82%
Web.Client	5.84%
General.Interest	3.72%
Email	2.84%
Network.Service	1.65%
Storage.Backup	1.23%
Cloud.IT	0.74%
Social.Media	0.57%
Others	0.23%



For application category details, see: <http://www.fortiguard.com/encyclopedia/application>

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).

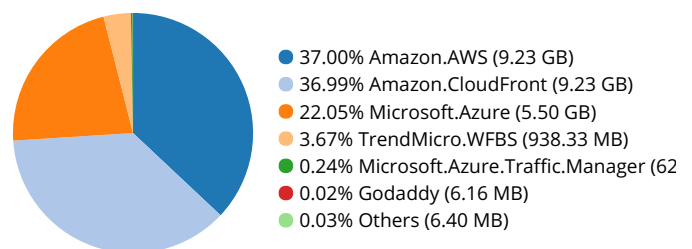
### Cloud Usage (SaaS)



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.

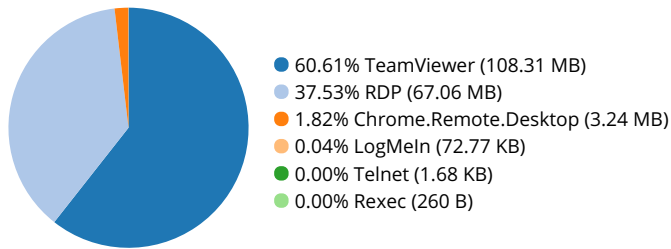
### Cloud Usage (IaaS)



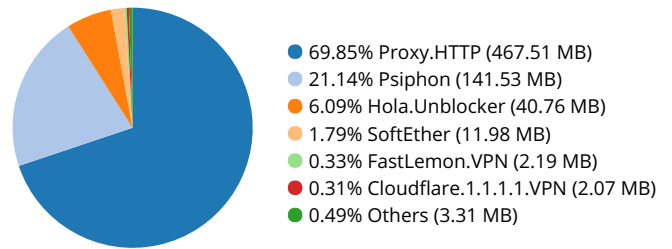
# Application Category Breakdowns

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.

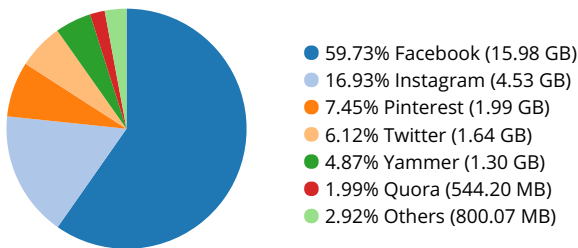
## Remote Access Applications



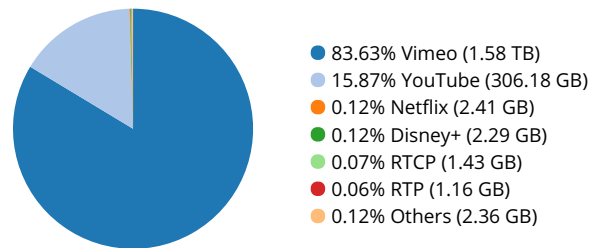
## Proxy Applications



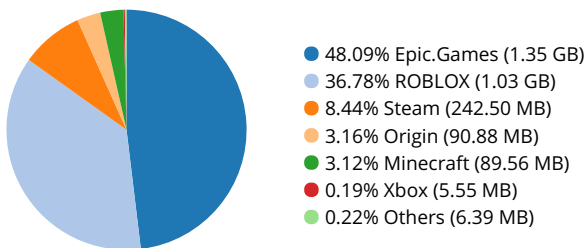
## Top Social Media Applications



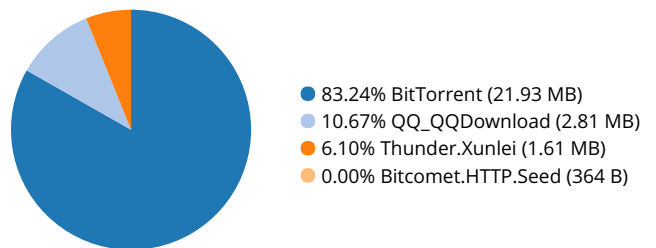
## Top Video/Audio Streaming Applications



## Top Gaming Applications



## Top Peer to Peer Applications



## 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	2,010	11,618,102	881.67 GB
Search Engines and Portals	1,881	1,027,816	45.42 GB
Reference	7,508	876,969	21.92 GB
Web-based Email	1,515	608,237	75.03 GB
Education	1,609	485,262	27.29 GB
Web-based Applications	1,584	440,125	14.46 GB
Advertising	1,600	405,455	7.03 GB
Content Servers	1,698	329,280	92.78 GB
File Sharing and Storage	1,742	269,006	29.92 GB
Streaming Media and Download	1,687	252,032	1.87 TB

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
Vimeo	36,758	1.58 TB
YouTube	221,732	306.18 GB
MS.Windows.Update	247,264	247.19 GB
Microsoft.SharePoint	379,839	203.13 GB
HTTPS.BROWSER	4,508,183	187.82 GB
Microsoft.OneNote	2,901,762	162.86 GB
Microsoft.Outlook.Office.365	582,855	81.06 GB
HTTPS	9,332,713	69.08 GB
Microsoft.Portal	1,973,131	67.23 GB
Microsoft.Office.Online	498,772	39.84 GB
Google.Services	1,020,324	39.22 GB
Adobe.Web	213,568	37.90 GB
SSL	752,389	32.27 GB
OneDrive	44,202	28.68 GB
Microsoft.Office.Update	34,373	27.50 GB
HTTP	2,328,768	22.67 GB
Microsoft.Office.365.Portal	370,614	20.33 GB
Microsoft.Authentication	829,297	16.51 GB
Facebook	82,200	15.93 GB
Microsoft.Teams	475,529	12.01 GB
Apple.Store	38,295	11.78 GB
Google.Services	70,563	11.41 GB
Google.Accounts	45,431	10.62 GB
HTTP.Segmented.Download	481	10.61 GB
Amazon.AWS	28,650	9.23 GB

## 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
contentsync.onenote.com	Information Technology	2,221,986
api.vivi.io	Information Technology	965,858
mail2013.hillcrest.qld.edu.au	Reference	613,555
outlook.office365.com	Web-based Email	430,540
login.microsoftonline.com	Information Technology	375,526
www.google.com	Search Engines and Portals	331,761
device-gateway.capenetworks.io	Information Technology	261,193
mobile.pipe.aria.microsoft.com	Information Technology	235,347
2.tlu.dl.delivery.mp.microsoft.com	Information Technology	189,938
hillcrestqldedu.sharepoint.com	Information Technology	189,844

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)
presence.teams.microsoft.com	Information Technology	181:07:01
4.sophosxl.net	Information Technology	180:36:16
safebrowsing.googleapis.com	Information Technology	178:26:39
outlook.office365.com	Web-based Email	177:46:12
outlook.office.com	Web-based Email	158:57:47
config.teams.microsoft.com	Information Technology	155:36:54
ctldl.windowsupdate.com	Information Technology	155:36:40
tass.hillcrest.qld.edu.au	Reference	154:25:15
teams.events.data.microsoft.com	Information Technology	147:18:58
hccfed.hillcrest.qld.edu.au	Reference	145:47:38
hillcrestqldedu-my.sharepoint.com	Information Technology	145:44:42
www.google.com	Business, Search Engines and Portals	144:16:23
hillcrestqldedu.sharepoint.com	Information Technology	142:47:48
self.events.data.microsoft.com	Information Technology	142:08:41
clientservices.googleapis.com	Information Technology	141:21:26
api.vivi.io	Information Technology	139:50:53
client.wns.windows.com	Information Technology	137:37:37
teams.microsoft.com	Information Technology	130:27:21
mobile.pipe.aria.microsoft.com	Information Technology	119:42:51
api.bugfender.com	Information Technology	117:46:46
device-gateway.capenetworks.io	Information Technology	116:54:58
array612.prod.do.dsp.mp.microsoft.com	Information Technology	112:43:43
auc-excel.officeapps.live.com	Web-based Applications	104:02:44

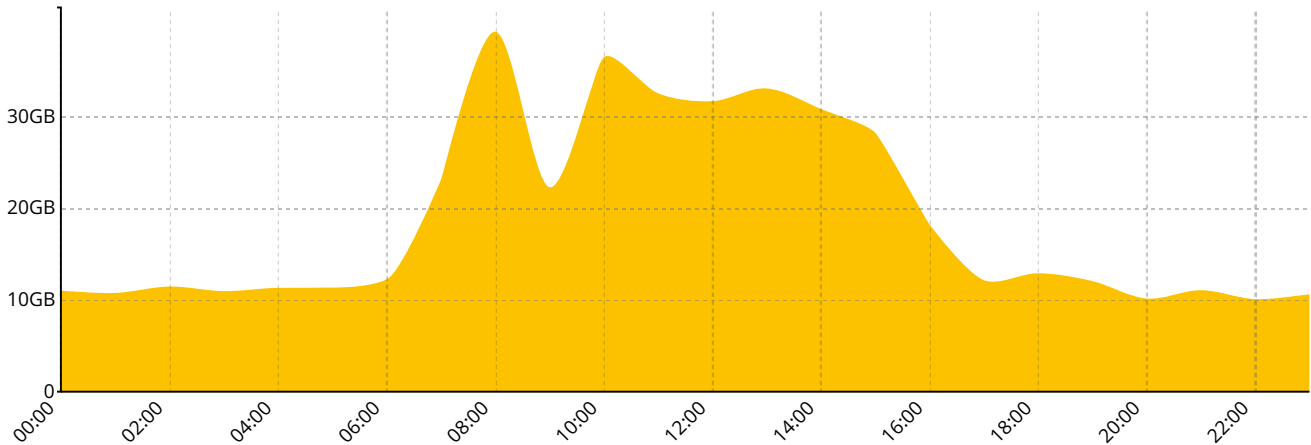
Sites	Category	Browsing Time(hh:mm:ss)
mail2013.hillcrest.qld.edu.au	 Reference	101:37:55
fef.msua02.manage.microsoft.com	 Information Technology	100:41:34
settings-win.data.microsoft.com	 Information Technology	99:07:42
browser.pipe.aria.microsoft.com	 Information Technology	99:07:18
mtalk.google.com	 Instant Messaging	97:55:22
http.00.a.sophosxl.net	 Information Technology	95:53:54
api.sine.co	 Information Technology	94:49:59
login.microsoftonline.com	 Information Technology	94:27:05
substrate.office.com	 Information Technology	93:56:04
cl3.apple.com	 Information Technology	91:56:27
ssl.gstatic.com	 Information Technology	91:51:05
nexusrules.officeapps.live.com	 Web-based Applications	91:28:09
update.googleapis.com	 Information Technology	90:06:25
clients4.google.com	 Search Engines and Portals	89:19:55
cdn.syndication.twimg.com	 Social Networking	85:00:42
www.pinterest.com.au	 Social Networking	84:17:49
v10.vortex-win.data.microsoft.com	 Information Technology	81:10:32
polka.typekit.com	 Information Technology	80:42:28
auc-onenote.officeapps.live.com	 Web-based Applications	80:40:54
login.live.com	 Search Engines and Portals	80:12:07
www.bing.com	 Search Engines and Portals	79:05:42
ecs.office.com	 Information Technology	77:46:51
auc-word-edit.officeapps.live.com	 Web-based Applications	77:00:22
gsp-ssl.ls.apple.com	 Information Technology	75:10:16
tile-service.weather.microsoft.com	 Information Technology	75:06:08
disc601.prod.do.dsp.mp.microsoft.com	 Information Technology	74:21:10
login.windows.net	 Information Technology	73:17:27

# 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
skyfire.vimeocdn.com	1.57 TB
contentsync.onenote.com	135.49 GB
hillcrestqldedu.sharepoint.com	106.71 GB
2.tlu.dl.delivery.mp.microsoft.com	92.56 GB
11.tlu.dl.delivery.mp.microsoft.com	80.09 GB
hillcrestqldedu-my.sharepoint.com	79.71 GB
r1---sn-n02xgavv250-ntqe.googlevideo.com	63.93 GB
outlook.office365.com	62.39 GB
r3---sn-n02xgavv250-ntqe.googlevideo.com	56.27 GB
r2---sn-n02xgavv250-ntqe.googlevideo.com	52.22 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 (1)

CTAP-FortiGate-60E