

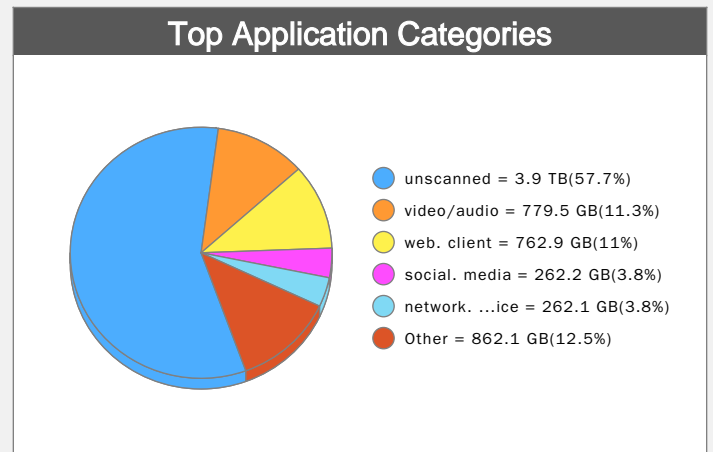
360 Degree Activities Report



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.fortiguard.com/encyclopedia/application>



Most Used High Bandwidth applications

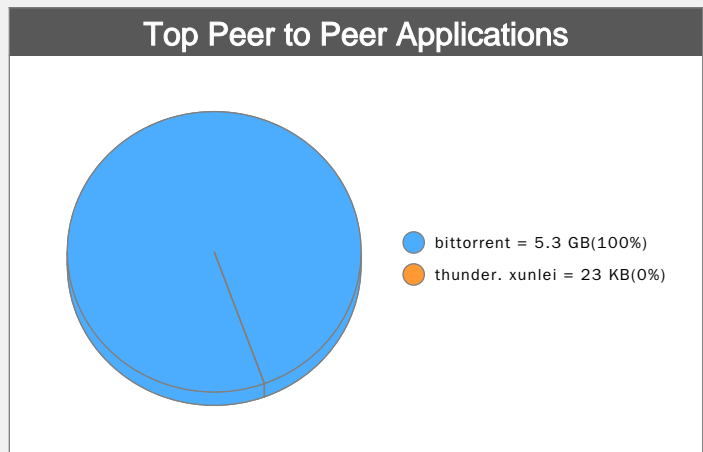
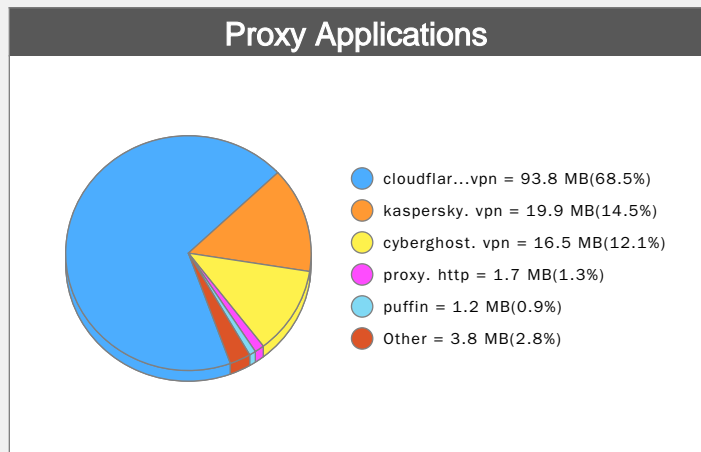
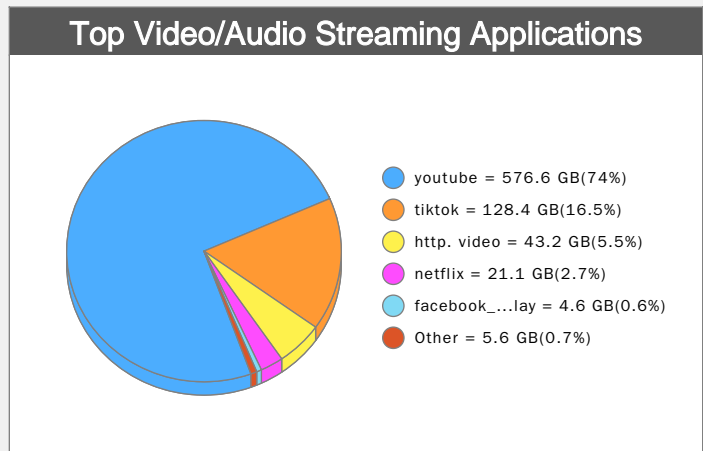
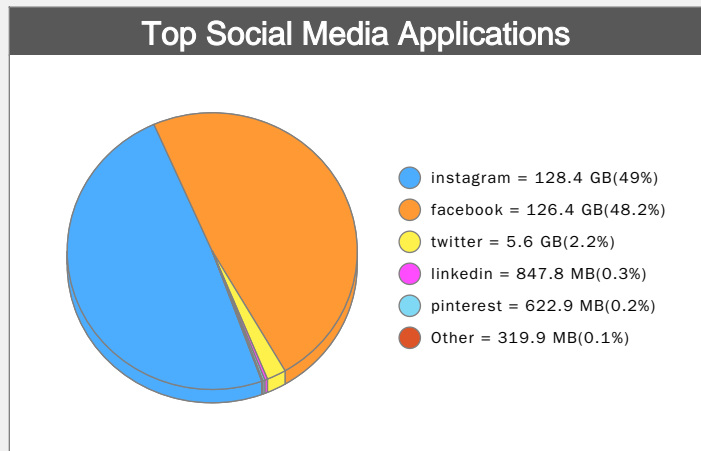
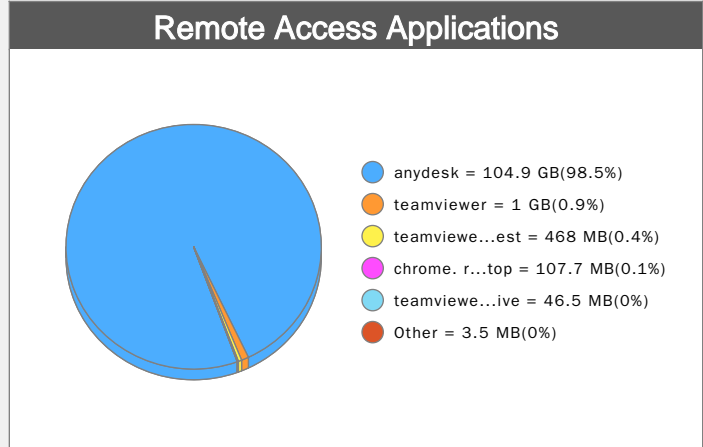
Application	Category	Risk	Traffic(Sent/Received)	%
youtube	video/audio	1	28.8 GB / 547.8 GB	66.6%
tiktok	video/audio	1	4.9 GB / 123.5 GB	14.8%
http.video	video/audio	1	504 MB / 42.7 GB	5.0%
netflix	video/audio	1	348.1 MB / 20.8 GB	2.4%
mediafire	storage.backup	2	82.9 MB / 17.4 GB	2.0%
google.photos	storage.backup	2	16.9 GB / 442.8 MB	2.0%
onedrive	storage.backup	2	1.7 GB / 12.7 GB	1.7%
icloud	storage.backup	2	11.2 GB / 2.6 GB	1.6%
mega	storage.backup	2	184.6 MB / 9.4 GB	1.1%
bittorrent	p2p	3	3 GB / 2.3 GB	0.6%
google.drive	storage.backup	2	2.9 GB / 2.1 GB	0.6%
facebook_video.play	video/audio	1	793.2 MB / 3.8 GB	0.5%
rtmp	video/audio	1	2.1 GB / 57.7 MB	0.2%
spotify	video/audio	2	222.5 MB / 1.5 GB	0.2%
google.cloud.storage	storage.backup	2	1.3 GB / 279.9 MB	0.2%
dailymotion	video/audio	1	48.8 MB / 1.4 GB	0.2%
dropbox	storage.backup	2	393 MB / 920.8 MB	0.1%
wetransfer	storage.backup	2	15 MB / 761 MB	0.1%
samsung.cloud	storage.backup	2	126.1 MB / 41.6 MB	0.0%
amazon.video	video/audio	1	8.8 MB / 143.6 MB	0.0%
Other	Other		28.3 MB / 266.5 MB	0.0%
			Total: 75.5 GB / 790.7 GB	

Legend: Sent (Yellow), Received (Blue)



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.





High Risk Application

The FortiGuard research team assigns a risk rating of 0 to 4 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 3 or higher.

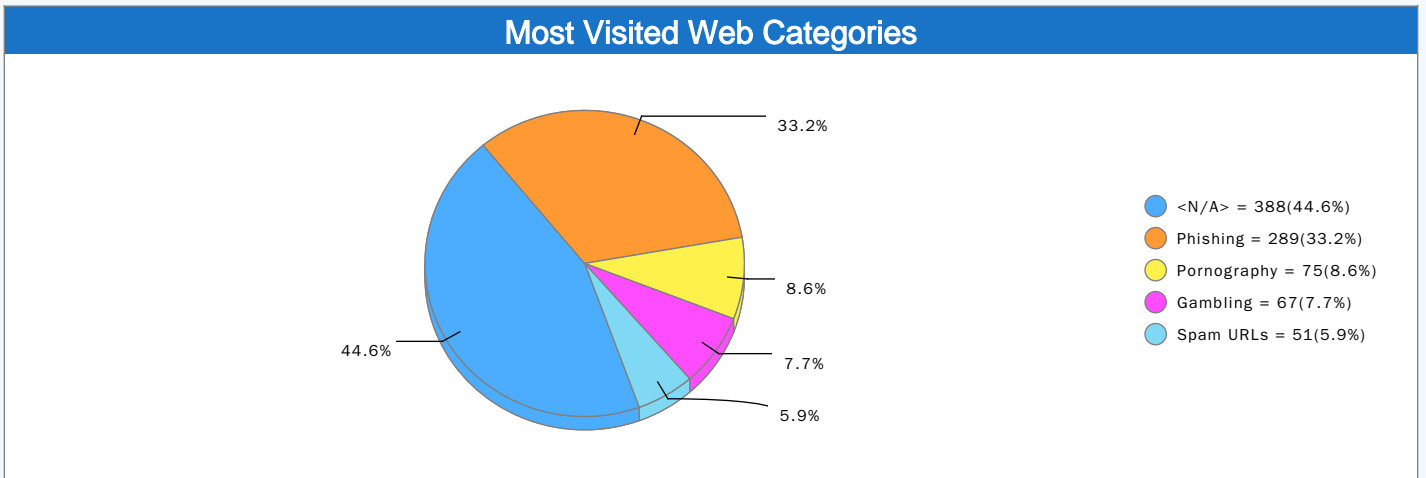
High Risk Application In Use								
Risk	Application	Category	Technology	User	%	Session	%	
4	skyvpn	proxy	Client-Server	1	3.3%	1	0.0%	
4	hotspot.shield	proxy	Client-Server	1	3.3%	63	0.0%	
4	hola.unblocker	proxy	Client-Server	1	3.3%	392	0.0%	
4	psiphon	proxy	Client-Server	1	3.3%	45	0.0%	
4	cyberghost.vpn	proxy	Client-Server	1	3.3%	40846	1.5%	
4	veepn.vpn	proxy	Client-Server	1	3.3%	1	0.0%	
4	zenmate	proxy	Browser-Based	1	3.3%	272	0.0%	
4	thunder.vpn	proxy	Client-Server	1	3.3%	23	0.0%	
4	opera.vpn	proxy	Client-Server	1	3.3%	47	0.0%	
4	x-vpn	proxy	Client-Server	1	3.3%	2	0.0%	
4	cloudflare.1.1.1.1.vpn	proxy	Client-Server	1	3.3%	79064	2.9%	
4	okhttp.library.vpn	proxy	Client-Server	1	3.3%	548	0.0%	
4	tor	proxy	Client-Server	1	3.3%	618	0.0%	
4	proxy.http	proxy	Network-Protocol	1	3.3%	2304	0.1%	
4	kaspersky.vpn	proxy	Client-Server	1	3.3%	9612	0.4%	
4	ultrasurf_9.6+	proxy	Client-Server	1	3.3%	4	0.0%	
4	socks5	proxy	Network-Protocol	1	3.3%	3	0.0%	
4	proxy.websites	proxy	Browser-Based	1	3.3%	4	0.0%	
4	browsec	proxy	Client-Server	1	3.3%	3	0.0%	
4	monero.cryptocurrency.miner	general.interest	Client-Server	1	3.3%	8996	0.3%	
	Other	Other	Other	10	33.3%	2564144	94.7%	
				Total: 30		Total: 2.7 M		



Web Traffic Analysis

Web Activities

Identifying which web categories and websites are accessed by applications provides additional data points for administrators to understand the network traffic usage. Defining appropriate application policies along with web filtering policies will greatly reduce the business risk. Fortinet's proprietary web filtering database is developed by the FortiGuard research team. The database contains more than 47 million rated websites with real-time updates; the websites are categorized into 76 web categories to allow highly-granular web filtering policies.



Most Visited Websites

Web Site	Visits	%	Estimated Browsing Time	%
ssp. swe.xyz	259	29.8%	00h 00m 00s	N/A
ncc. avast.com	143	16.4%	00h 00m 00s	N/A
adx. lsosad.com	49	5.6%	00h 00m 00s	N/A
xml-eu-v4. gipostart-1.co	42	4.8%	00h 00m 00s	N/A
app-api. charityengine.services	37	4.3%	00h 00m 00s	N/A
jb73i0. fsdgled.com	33	3.8%	00h 00m 00s	N/A
cloud. 360safe.com	25	2.9%	00h 00m 00s	N/A
221.181.72.250	21	2.4%	00h 00m 00s	N/A
3ot8y. xikuj.com	16	1.8%	00h 00m 00s	N/A
adserver. juicyads.com	15	1.7%	00h 00m 00s	N/A
excretekings. com	14	1.6%	00h 00m 00s	N/A
ctldl. windowsupdate.com	14	1.6%	00h 00m 00s	N/A
ff. avast.com	9	1.0%	00h 00m 00s	N/A
sanxiao. iibingo.com	8	0.9%	00h 00m 00s	N/A
jp_cloud. cmcm.com	7	0.8%	00h 00m 00s	N/A
feignthat. com	7	0.8%	00h 00m 00s	N/A
wonporn. com	6	0.7%	00h 00m 00s	N/A
platform. hicloud.com	5	0.6%	00h 00m 00s	N/A
connectivitycheck. gstatic.com	5	0.6%	00h 00m 00s	N/A
www. google.com	5	0.6%	00h 00m 00s	N/A
Other	150	17.2%	00h 00m 00s	N/A
Total: 870			Total: 00h 00m 00s	



Web Activities

Most Visited Web Categories and Web Sites					
Category	%	Web Site	%	Visits	Estimated Browsing Time
<N/A>	44.6%		100%	388	00h 00m 00s
Phishing	33.2%	ssp. swe.xyz	89.6%	259	00h 00m 00s
		excretekings. com	4.8%	14	00h 00m 00s
		cdrvrs. com	1.0%	3	00h 00m 00s
		www. aversus.site	0.7%	2	00h 00m 00s
		www. liveupdt.com	0.7%	2	00h 00m 00s
		Other	3.1%	9	00h 00m 00s
Pornography	8.6%	jb73i0. fsdgled.com	44.0%	33	00h 00m 00s
		adserver. juicyads.com	20.0%	15	00h 00m 00s
		wonporn. com	8.0%	6	00h 00m 00s
		xnxx. com	5.3%	4	00h 00m 00s
		a4442. com	5.3%	4	00h 00m 00s
		Other	17.3%	13	00h 00m 00s
Gambling	7.7%	app-api. charityengine.services	55.2%	37	00h 00m 00s
		3ot8y. xikuj.com	23.9%	16	00h 00m 00s
		sanxiao. iibingo.com	11.9%	8	00h 00m 00s
		www. dafabet.com	4.5%	3	00h 00m 00s
		match3games1. iibingo.com	3.0%	2	00h 00m 00s
		Other	1.5%	1	00h 00m 00s
Spam URLs	5.9%	xml-eu-v4. gipostart-1.co	82.4%	42	00h 00m 00s
		feignthat. com	13.7%	7	00h 00m 00s
		mipyjtj35. top	3.9%	2	00h 00m 00s
Total: 870					

Visits



30 percent of data breaches involve organization insiders acting negligently or maliciously. Insiders pose a unique threat to organizations because they have access to proprietary systems and often are able to bypass security measures creating a security blind spot to the risk and security teams. User Behavior Analytics protects organizations from insider threats by continuously monitoring users and endpoints.

Active Users



Most Active Application Users		
User (UnauthUser)	Session	%
N/A(N/A)	560110691	100.0%
	Total: 560.1 M	

Most Active Web Users				
User (UnauthUser)	Visits	%	Estimated Browsing Time	%
N/A(N/A)	870	100.0%	00h 00m 00s	N/A
	Total: 870		Total: 00h 00m 00s	



Applications by Active Users

Most Applications by Most Active Users				
User(UnauthUser)	%	Application	%	Traffic
N/A(N/A)	100%	https	28.5%	68.7 GB/1.9 TB
		tcp	18.3%	967 GB/299.1 GB
		udp	10.7%	202.4 GB/535.8 GB
		https.browser	9.4%	300.1 GB/348.8 GB
		youtube	8.3%	28.8 GB/547.8 GB
		Other	24.8%	234.4 GB/1.4 TB
				Total: 1.8 TB/5 TB

 Sent  Received



Websites by Active Web Users

Most Visited Web Sites by Most Active Users					
User(UnauthUser)	%	Web Site	%	Visits	Estimated Browsing Time
N/A(N/A)	100%	ssp. swe.xyz	29.8%	259	00h 00m 00s
		ncc. avast.com	16.4%	143	00h 00m 00s
		adx. lsosad.com	5.6%	49	00h 00m 00s
		xml-eu-v4. gipostart-1.co	4.8%	42	00h 00m 00s
		app-api. charityengine.services	4.3%	37	00h 00m 00s
		Other	39.1%	340	00h 00m 00s
					Total: 870

Visits









Active Users of Most Applications

Most Active Users of Most Applications					
Application	%	User (UnauthUser)	%	Traffic	
https	28.5%	N/A(N/A)	100%		68.7 GB/1.9 TB
tcp	18.3%	N/A(N/A)	100%		967 GB/299.1 GB
udp	10.7%	N/A(N/A)	100%		202.4 GB/535.8 GB
https.browser	9.4%	N/A(N/A)	100%		300.1 GB/348.8 GB
youtube	8.3%	N/A(N/A)	100%		28.8 GB/547.8 GB
Other	24.8%				234.4 GB/1.4 TB
					Total: 1.8 TB/5 TB

Sent Received



Active Users of Most Visited Web Sites

Most Active Users of Most Visited Web Sites						
Web Site	%	User (UnauthUser)	%	Visits	Estimated Browsing Time	
ssp. swe.xyz	29.8%	N/A(N/A)	100%	 259	00h 00m 00s	
ncc. avast.com	16.4%	N/A(N/A)	100%	 143	00h 00m 00s	
adx. lsoad.com	5.6%	N/A(N/A)	100%	 49	00h 00m 00s	
xml-eu-v4. gipostart-1.co	4.8%	N/A(N/A)	100%	 42	00h 00m 00s	
app-api. charityengine.services	4.3%	N/A(N/A)	100%	 37	00h 00m 00s	
Other	39.1%			 340	00h 00m 00s	
					Total: 870	

 Visits



The rise of modern malware has reshaped the threat landscape. These modern threats bypass traditional antimalware strategies and establish a foothold within the enterprise. They are used by criminals and nation-states to steal sensitive information and attack assets. Fortinet next-generation firewall provides multi-level protection to combat these advanced persistent threat - the reliable visibility and control of all traffic on the network regardless of evasive tactics. The FortiGuard AntiVirus Service employs advanced virus, spyware, and heuristic detection engines to enable FortiGate systems to detect and prevent both new and evolving threats. For AntiVirus see: <http://www.fortiguard.com/antivirus/> .

Threat Detection and Prevention

Top Threats				
Threat	Category	Level	Score	%
Failed Connection Attempt	Firewall Control	Low	4075055	81.8%
MySQL.Login.Brute.Force	Attack	High	3030240	10.3%
cloudflare.1.1.1.1.vpn	Application Control	Medium	815980	2.8%
Backdoor.DoublePulsar	Attack	Critical	621350	2.1%
cyberghost.vpn	Application Control	Medium	214860	0.7%
tcp_port_scan	Anomaly	Critical	199050	0.7%
Andromeda.Botnet	Attack	Critical	178700	0.6%
kaspersky.vpn	Application Control	Medium	96350	0.3%
Ramnit.Botnet	Attack	Critical	47700	0.2%
FSA/RISK_HIGH	Malware	High	39660	0.1%
SSLv3.POODLE.Information.Disclosure	Attack	Medium	34090	0.1%
proxy.http	Application Control	Medium	23630	0.1%
Riskware/Miner	Malware	Critical	10650	0.0%
MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	Attack	Medium	8000	0.0%
ssp. swe.xyz	Web Sites	High	7770	0.0%
tor	Application Control	Medium	6540	0.0%
W32/Agent.OJQ!tr	Malware	Critical	6050	0.0%
okhttp.library.vpn	Application Control	Medium	5380	0.0%
icmp_flood	Anomaly	Critical	4150	0.0%
hola.unblocker	Application Control	Medium	3910	0.0%
			Total: 29.4 M	

Top Viruses		
Virus	Incidents	%
FSA/RISK_HIGH-http	1322	76.1%
Riskware/Miner-http	213	12.3%
W32/Agent.OJQ!tr-http	121	7.0%
JS/ProxyChanger.GB!tr-http	39	2.2%
Android/HiddenApp.KN!tr-http	21	1.2%
JS/Redirector.0C36!tr-http	11	0.6%
FSA/RISK_MALICIOUS-http	4	0.2%
f244bfe57d2cbc83e4113b155c6b8f02676cb80e-http	2	0.1%
Adware/Pirrit!OSX-http	2	0.1%
Adware/DotSetup!o-http	1	0.1%
W64/Agent.FP!tr-http	1	0.1%
W32/Kryptik.HSDC!tr-http	1	0.1%

Total: 1738

Top Virus Victims

Victim	Incidents	%
192.168.30.74	1040	59.8%
192.168.30.153	457	26.3%
192.168.20.127	159	9.1%
192.168.24.82	39	2.2%
192.168.22.183	21	1.2%
192.168.30.113	5	0.3%
192.168.30.229	4	0.2%
192.168.24.70	3	0.2%
192.168.22.68	2	0.1%
192.168.30.144	2	0.1%
192.168.20.115	1	0.1%
192.168.30.117	1	0.1%
192.168.25.124	1	0.1%
192.168.30.64	1	0.1%
192.168.22.236	1	0.1%
192.168.22.184	1	0.1%
Total: 1738		
























Top Attacks		
Attack ID	Incidents	%
MySQL.Login.Brute.Force	101008	82.5%
Backdoor.DoublePulsar	12427	10.2%
Andromeda.Botnet	3574	2.9%
SSLv3.PODLE.Information.Disclosure	3409	2.8%
Ramnit.Botnet	954	0.8%
MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	800	0.7%
TCP.Split.Handshake	117	0.1%
Conficker.Botnet	60	0.0%
Amadey.Botnet	42	0.0%
DCRat.Botnet	8	0.0%
Raccoon.Botnet	5	0.0%
MS.SMB.Server.SMB1.MID.FID.Parsing.Remote.Code....ution	2	0.0%
Oracle.MySQL.For.Windows.MOF.Execution	1	0.0%
Total: 122407		

Top Attack Victims		
Victim	Incidents	%
114.119.187.114	3388	13.8%
192.168.30.27	2183	8.9%
192.168.30.245	1107	4.5%
103.190.95.171	1080	4.4%
103.190.62.243	725	3.0%
103.190.6.139	695	2.8%
103.190.95.155	622	2.5%
103.190.95.230	610	2.5%
222.124.214.14	554	2.3%
222.124.13.206	542	2.2%
222.124.139.169	410	1.7%
222.124.218.210	313	1.3%
222.124.215.229	312	1.3%
222.124.185.83	309	1.3%
222.124.215.228	302	1.2%
222.124.139.234	292	1.2%
222.124.166.131	285	1.2%
192.168.30.108	284	1.2%
222.124.139.233	281	1.1%
103.190.16.160	275	1.1%
Other	9946	40.6%
Total: 24515		

Top Spam by Source IP		
Source	Incidents	%

Device: FortiGate100F-RRI-Pusat(root)

2023-01-22 00:00 - 2023-01-29 00:00 Asia/Kolkata

193.56.29.178		271	18.6%
103.45.157.171		245	16.8%
23.146.243.12		236	16.2%
45.128.234.165		198	13.6%
5.105.106.107		84	5.8%
193.42.33.79		70	4.8%
180.214.239.18		68	4.7%
139.162.99.243		47	3.2%
5.236.93.123		32	2.2%
194.87.200.194		15	1.0%
193.42.33.76		14	1.0%
193.42.33.7		10	0.7%
94.102.61.22		9	0.6%
106.75.215.239		6	0.4%
154.89.5.213		6	0.4%
154.89.5.217		6	0.4%
194.87.200.151		6	0.4%
118.193.40.46		5	0.3%
193.239.164.115		5	0.3%
80.94.95.204		5	0.3%
Other		117	8.0%
		Total: 1455	

Queried Botnet C-and-C Domains

No Data



Applications that have the ability to transfer files can pose a significant risk of data loss: company's customer data, intellectual property and confidential business trade secrets can be sent out of the organization via these applications. Knowing which types of files and content are transferred crossing the network can help administrators to mitigate the risk by setting up appropriate application policies along with data leak prevention rules on the Fortinet next-generation firewall system.

Data Exfiltration Detection and Prevention

Top Data Leak by Rules

No Data

Top Data Leak by Source

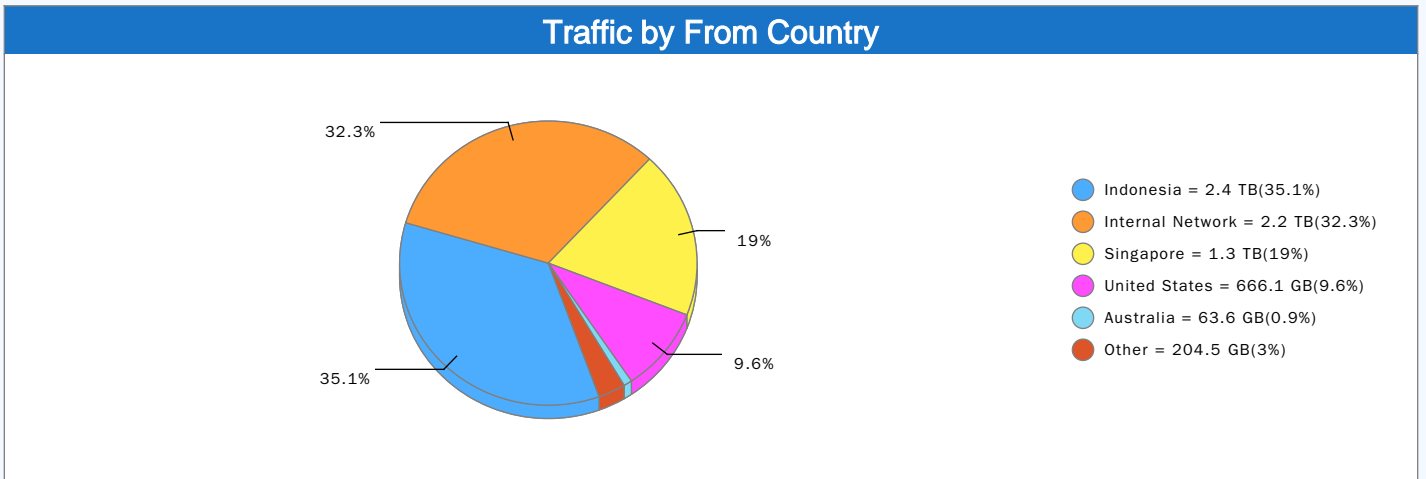
No Data



FortiClient protects your endpoints with an extra layer of security; it's engineered to defeat the latest and most dangerous malware and provides real-time protection on the company's desktops and mobile devices. FortiClient together with Fortinet next generation Firewall delivers fully managed and layered security defences.

Endpoint Detection and Prevention

Most At-Risk Devices and Hosts			
Source	Score		%
192.168.20.127		7567605	26.9%
192.168.30.74		3739725	13.3%
192.168.30.132		3034345	10.8%
10.30.5.6		2167740	7.7%
192.168.30.113		2165680	7.7%
192.168.30.146		1744025	6.2%
192.168.20.6		1159105	4.1%
192.168.30.46		541095	1.9%
192.92.92.93		427220	1.5%
192.168.30.233		409030	1.5%
Other		5180715	18.4%
		Total: 28.1 M	



Device: FortiGate100F-RRI-Pusat(root)

2023-01-22 00:00 - 2023-01-29 00:00 Asia/Kolkata

Appendix: Devices

Report is generated from following devices:

FG100FTK22000969(root)