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.

High Risk Applications Crossing the Network

#	Risk	Application Name	Category	Technology	User	Bandwidth	Session
1	4	RDP	Remote.Access	Client-Server	80	23.53 MB	5,830
2	4	Meraki.Cloud.Controller	Cloud.IT	Client-Server	641	10.12 MB	2,501
3	4	Rlogin	Remote.Access	Client-Server	4	2.52 KB	99
4	4	VNC	Remote.Access	Client-Server	1	798 B	25
5	4	Synergy	Remote.Access	Client-Server	1	4.05 KB	25
6	4	Dameware.Remote	Remote.Access	Client-Server	1	7.07 KB	1

Figure 1: Highest risk applicaitons sorted by risk and sessions

Application Vulnerability Exploits

An application vulnerability could be exploited to compromise the security of the network. The FortiGuard research team analyses application traffic patterns and application vulnerabilities and then develops signatures to prevent the vulnerability exploits. The FortiGuard Intrusion Prevention Service (IPS) provides Fortinet customers with the latest defenses against stealthy network-level threats. It uses a customizable database of more than 5,800 known threats to stop attacks that evade traditional firewall systems. For Application Vulnerability and IPS see: http://www.fortiguard.com/static/intrusionprevention.html.

Top Application Vulnerability Exploits Detected

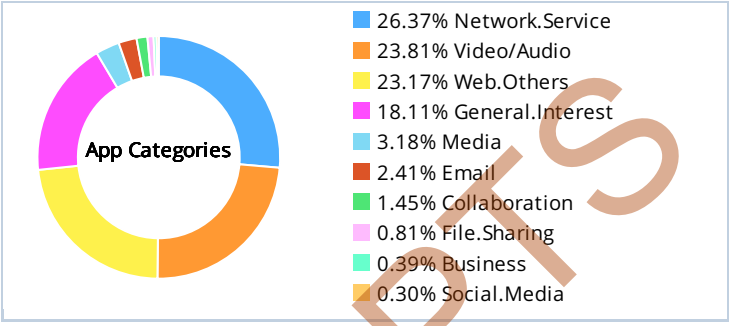
#	Severity	Threat Name	Type	Victim	Source	Count
1	5	HTTP.URI.Overflow		9	9	8,891
2	5	HTTP.Chunk.Overflow	Numeric Errors	3	4	4,562
3	5	IBM.Domino.iNotes.Buffer.Overflow	Buffer Errors	3	3	2,675
4	5	Minishare.HTTP.Server.Buffer.Overflow	Buffer Errors	1	1	2,278
5	5	MS.Windows.Message.Queuing.Remote.Buffer.Overflow	Buffer Errors	2	2	2,277
6	5	MS.SMB.DCERPC.WKSSVC.NetrJoinDomain2.Buffer.Overflow	Buffer Errors	2	2	2,226
7	5	MS.Windows.IGMP.Integer.Overflow	Numeric Errors	1	1	1,823
8	5	MS.Windows.RPC.DNS.Service.Buffer.Overflow	Buffer Errors	2	2	1,811
9	5	Sun.Solaris.rpc.ypupdated.Remote.Command.Execution	Code Injection	1	1	1,574
10	5	MS.Windows.PnP.Buffer.Overflow	Buffer Errors	1	1	1,173

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

User Productivity

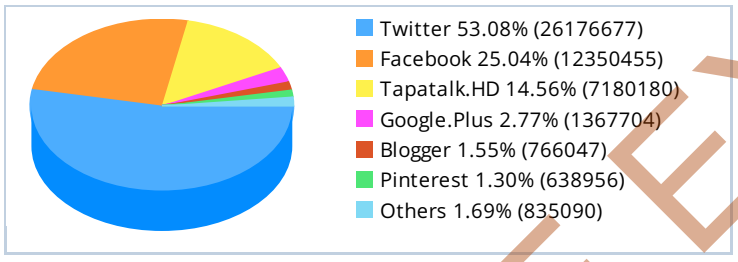
Application Usage

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 management. For application category details, see: http://www.fortiguard.com/encyclopedia/applications

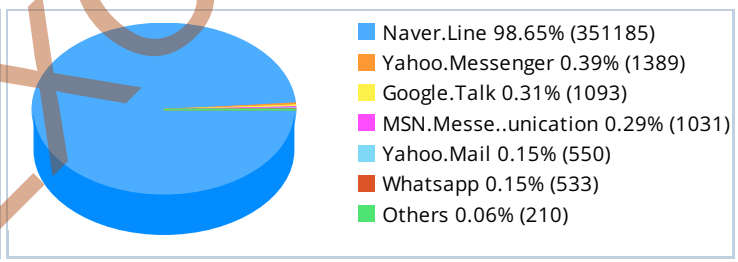


Understanding application subcategories can give invaluable insights into how efficiently your corporate network is operating. Certain application types (such as P2P or gaming applications) are not necessarily conducive to corporate environments and can be blocked or limited in their scope. Other applications may have dual purpose uses (such as instant messenger 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.

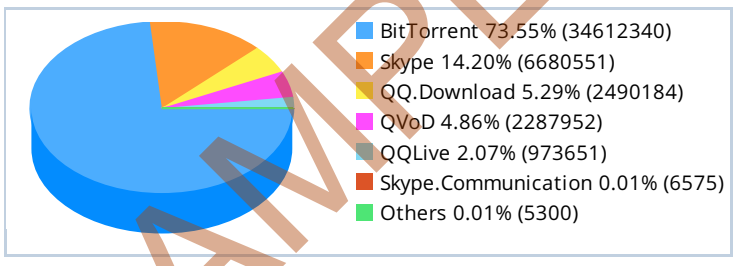
Top Social Media Applications



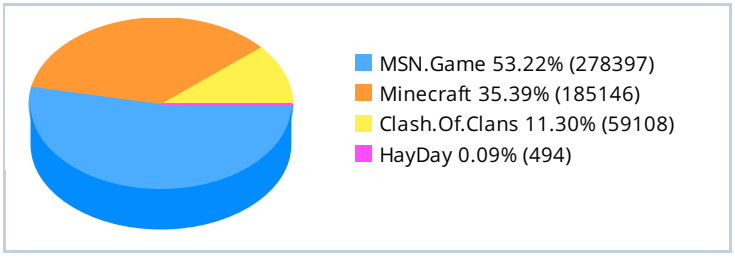
Top Instant Messaging Applications



Top Peer to Peer Applications



Top Gaming Applications

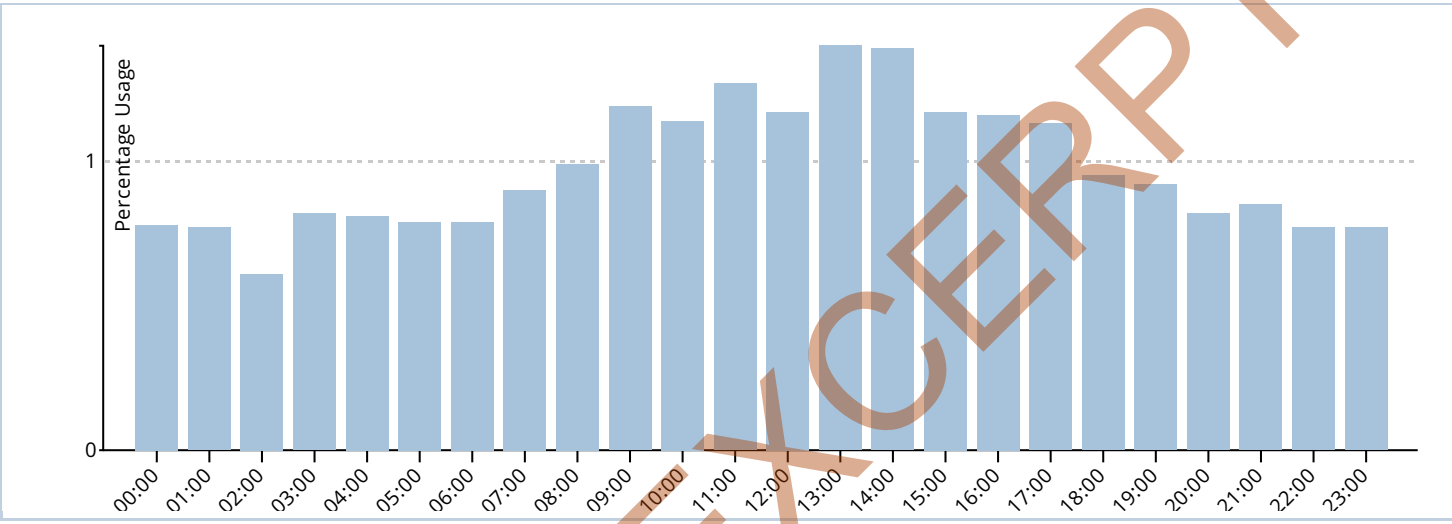


Network Utilization

Bandwidth and Sessions

Bandwidth usage is the primary indicator for throughput and capacity planning. FortiGates can analyze bandwidth by application usage or by host. In addition, looking at daily usage trends can assist with peak capacity planning.

Average Bandwidth Usage by Hour



Session averages on a a daily basis are useful for calculating throughput and proper sizing. It can help when determining peak planning as a typical enterprise will see more sessions being generated in the morning when the network is at its most active.

Average Session Usage by Hour