Security Lab 9 - SIEM - Glasswire

Ana Herrera Flores

Fundamentals of Information Security: Cybersecurity (88252)

Table of Contents

Introduction

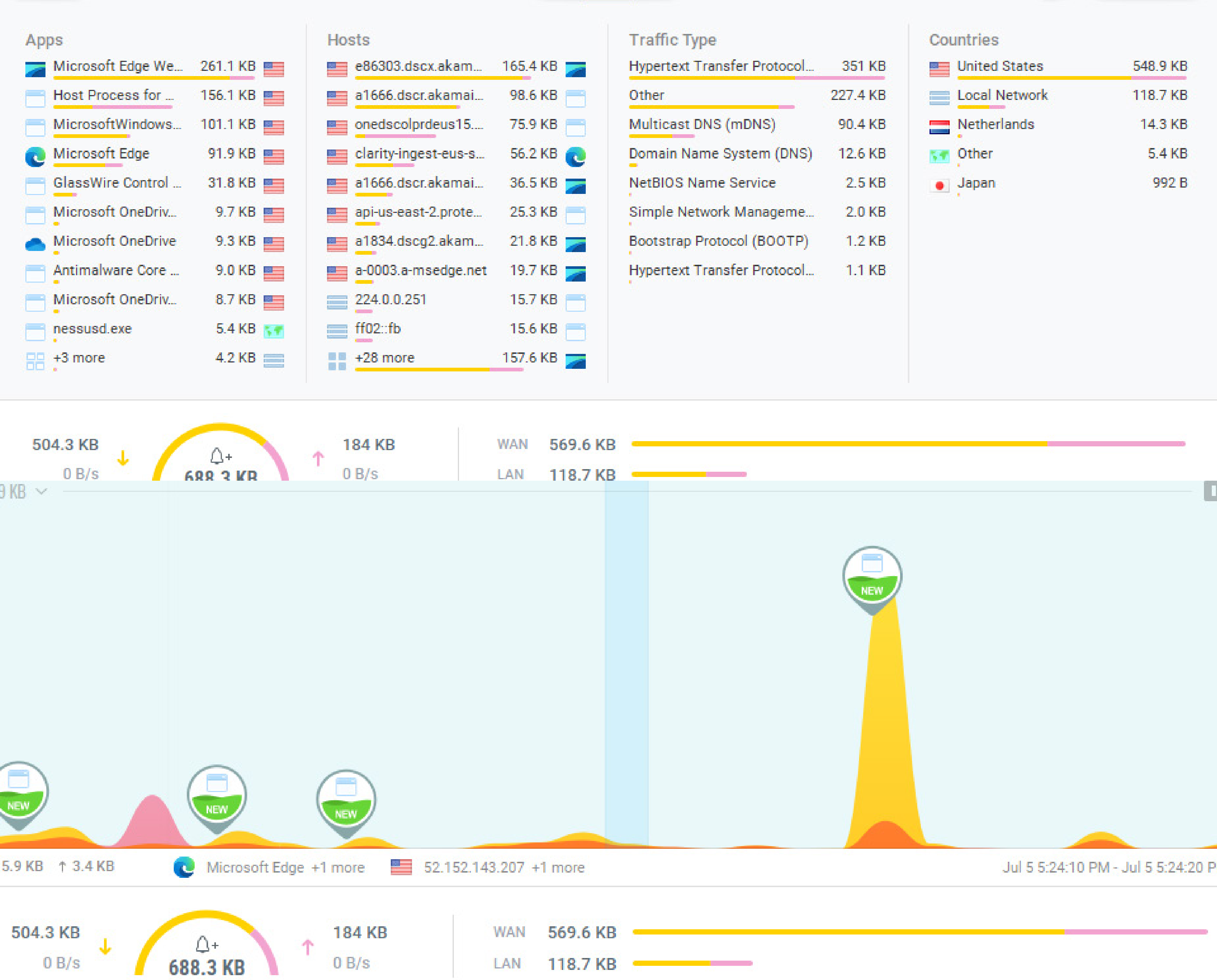
In today world humans spend a big portion of their time using devices to realize an uncountable series of activities, from paying bills to share pictures on social media . Every day, users access Internet without knowing what is happening with their devices or information. There are softwares that can help a normal user to monitor their network and to know if their information is secure. In this report we will take a close look to how GlassWire can give us a little bit more of knowledge about security and how to protect our devices.

What is GlassWire?

GlassWire is a free security tool by SecureMix LLC that monitors network activity. It offers graphic and real-time activity of your network as well as giving the user control about which apps can connect to the Internet. Some of the features are: visual network monitoring, internet security, GlassWire score, anomaly detection, management console, who's on your network, multiple server monitoring, bandwidth usage monitor, discreet alerts, evil twin detection, internet privacy protection, and RDP connection detection.

Visual Network Monitoring

Virtual Networking Monitoring offers two ways for the user to see the information of the network. One as a graph, and the other as a table. It shows the user which app visited which host, and in what country is that host located, as well as what protocol was used for that communication. Knowing this information can help users to know if the sites that they are visiting are communicating with secure protocols.



Apps	
Microsoft Edge We...	261.1 KB
Host Process for ...	156.1 KB
MicrosoftWindows...	101.1 KB
Microsoft Edge	91.9 KB
GlassWire Control ...	31.8 KB
Microsoft OneDriv...	9.7 KB
Microsoft OneDrive	9.3 KB
Antimalware Core ...	9.0 KB
Microsoft OneDriv...	8.7 KB
nessusd.exe	5.4 KB
+3 more	4.2 KB

Hosts	
e86303.dscx.akam...	165.4 KB
a1666.dscr.akamai...	98.6 KB
onedscolprdeus15....	75.9 KB
clarity-ingest-eus-s...	56.2 KB
a1666.dscr.akamai...	36.5 KB
api-us-east-2.prote...	25.3 KB
a1834.dscg2.akam...	21.8 KB
a-0003.a-msedge.net	19.7 KB
224.0.0.251	15.7 KB
ff02::fb	15.6 KB
+28 more	157.6 KB

Traffic Type	
Hypertext Transfer Protocol...	351 KB
Other	227.4 KB
Multicast DNS (mDNS)	90.4 KB
Domain Name System (DNS)	12.6 KB
NetBIOS Name Service	2.5 KB
Simple Network Manageme...	2.0 KB
Bootstrap Protocol (BOOTP)	1.2 KB
Hypertext Transfer Protocol...	1.1 KB

Countries	
United States	548.9 KB
Local Network	118.7 KB
Netherlands	14.3 KB
Other	5.4 KB
Japan	992 B

504.3 KB ↓ 0 B/s

688.3 KB

↑ 184 KB 0 B/s

WAN 569.6 KB

LAN 118.7 KB

5.9 KB ↑ 3.4 KB Microsoft Edge +1 more 52.152.143.207 +1 more Jul 5 5:24:10 PM - Jul 5 5:24:20 P

504.3 KB ↓ 0 B/s

688.3 KB

↑ 184 KB 0 B/s

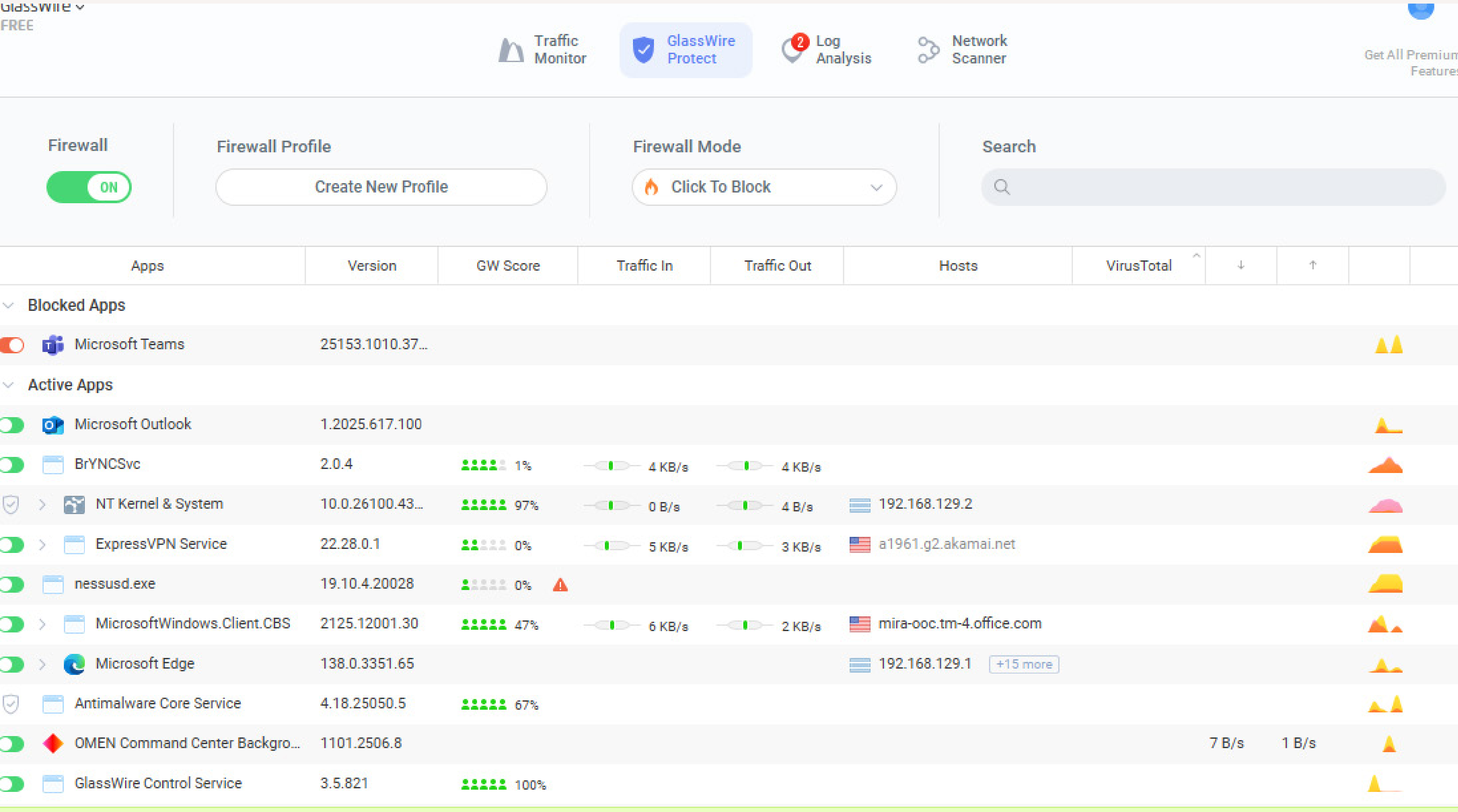
WAN 569.6 KB

LAN 118.7 KB

GlassWire Protect

Users have access to a diverse array of helpful tools on the GlassWire Protect dashboard.

1. A firewall adds an additional security layer; in *Firewall mode*, you can choose to prevent applications from connecting to the network.
2. Another features is the version used by the apps.
3. The GW Score indicates the percentage of Glasswire users who have engaged with a particular app over the last month.
4. Traffic In and Traffic Out.
5. Hosts.
6. We are able to detect any viruses infiltrating the system and identify their points of entry.
7. We can also observe the bandwidth consumption.



Firewall: ON

Firewall Profile: Create New Profile

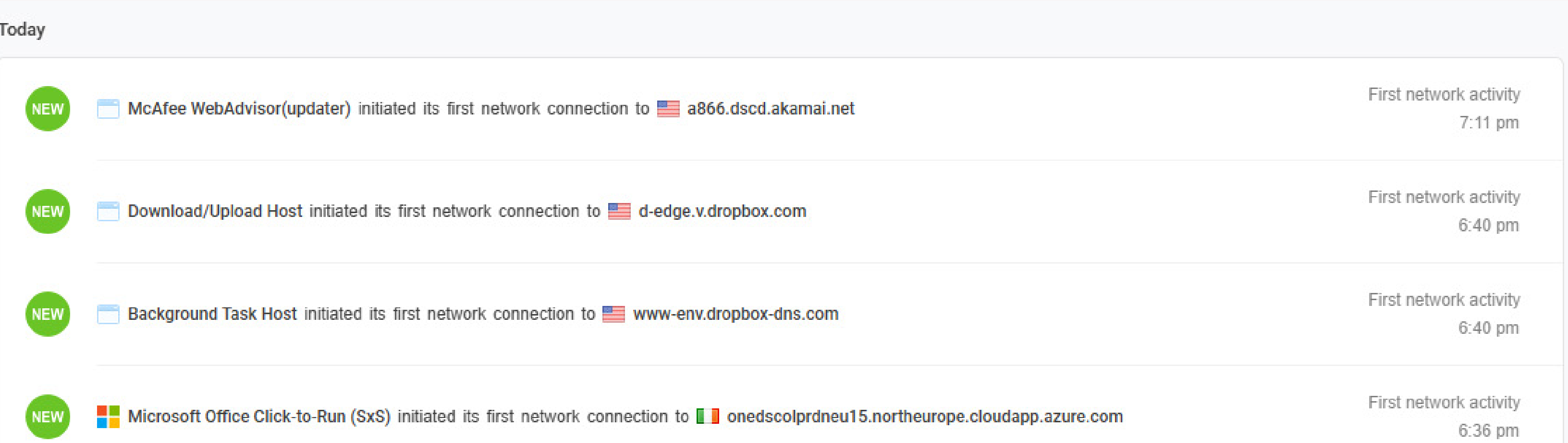
Firewall Mode: Click To Block

Search

Apps	Version	GW Score	Traffic In	Traffic Out	Hosts	VirusTotal	↓	↑	
Blocked Apps									
Microsoft Teams	25153.1010.37...								
Active Apps									
Microsoft Outlook	1.2025.617.100								
BrYNCSvc	2.0.4	1%	4 KB/s	4 KB/s					
NT Kernel & System	10.0.26100.43...	97%	0 B/s	4 B/s	192.168.129.2				
ExpressVPN Service	22.28.0.1	0%	5 KB/s	3 KB/s	a1961.g2.akamai.net				
nessusd.exe	19.10.4.20028	0% ⚠							
MicrosoftWindows.Client.CBS	2125.12001.30	47%	6 KB/s	2 KB/s	mira-ooc.tm-4.office.com				
Microsoft Edge	138.0.3351.65				192.168.129.1 +15 more				
Antimalware Core Service	4.18.25050.5	67%							
OMEN Command Center Backgro...	1101.2506.8						7 B/s	1 B/s	
GlassWire Control Service	3.5.821	100%							

Log Analysis

In the Log Analysis section, the application alerts you whenever there's a new event on your device, ranging from network connections to any irregularities. It displays the type of activity along with the timestamps of when these events took place.



Today

NEW McAfee WebAdvisor(updater) initiated its first network connection to a866.dscd.akamai.net — First network activity 7:11 pm

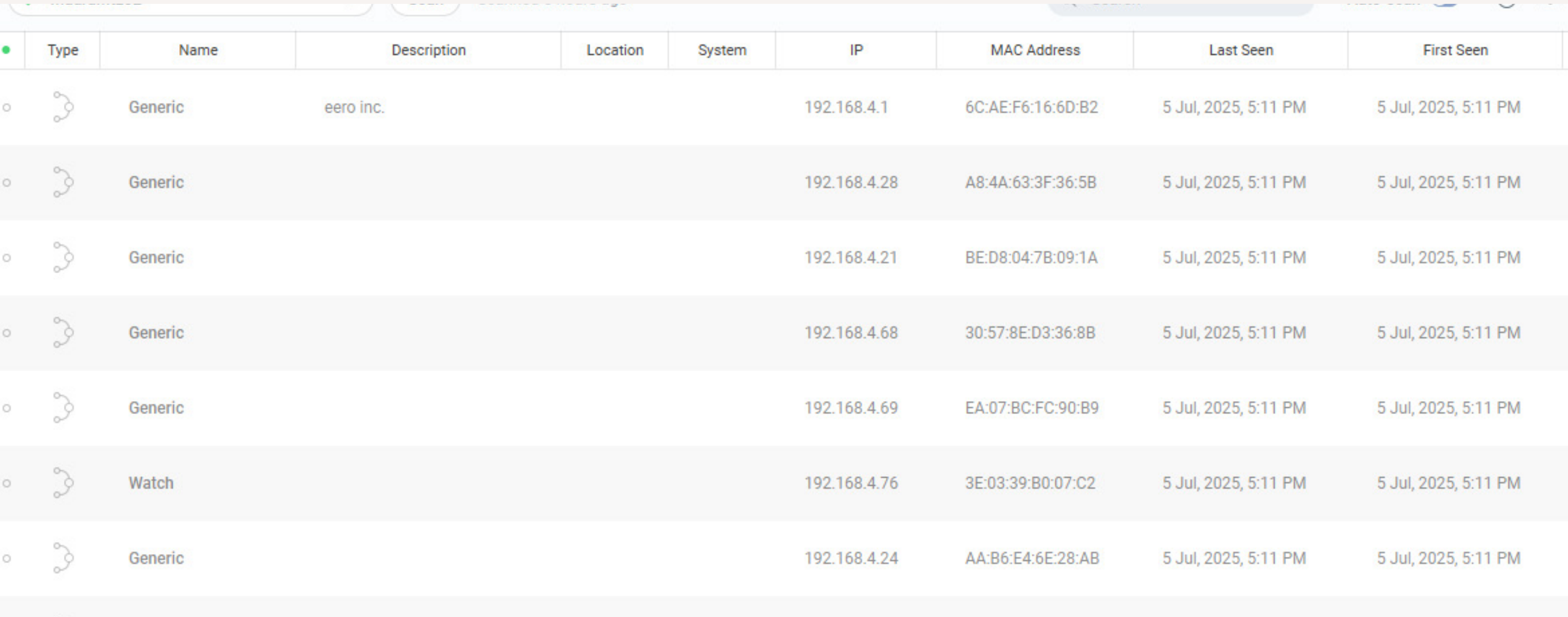
NEW Download/Upload Host initiated its first network connection to d-edge.v.dropbox.com — First network activity 6:40 pm

NEW Background Task Host initiated its first network connection to www-env.dropbox-dns.com — First network activity 6:40 pm

NEW Microsoft Office Click-to-Run (SxS) initiated its first network connection to onedscolprdneu15.northeurope.cloudapp.azure.com — First network activity 6:36 pm

Network Scanner

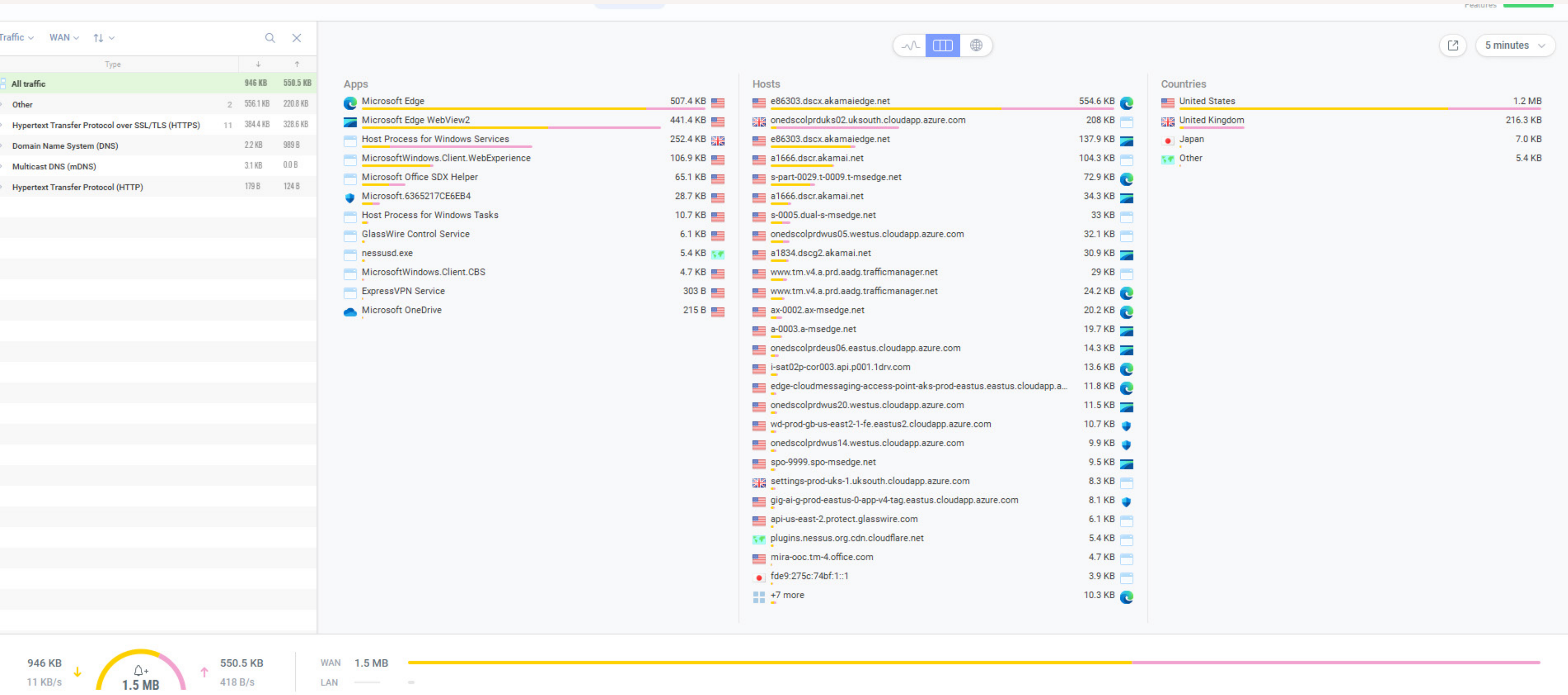
Another important function is the Network Scanner, which provides the user with the ability to view various details such as IP addresses, MAC addresses, and additional characteristics of all devices that are currently connected to your network.



●	Type	Name	Description	Location	System	IP	MAC Address	Last Seen	First Seen
○		Generic	eero inc.			192.168.4.1	6C:AE:F6:16:6D:B2	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM
○		Generic				192.168.4.28	A8:4A:63:3F:36:5B	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM
○		Generic				192.168.4.21	BE:D8:04:7B:09:1A	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM
○		Generic				192.168.4.68	30:57:8E:D3:36:8B	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM
○		Generic				192.168.4.69	EA:07:BC:FC:90:B9	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM
○		Watch				192.168.4.76	3E:03:39:B0:07:C2	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM
○		Generic				192.168.4.24	AA:B6:E4:6E:28:AB	5 Jul, 2025, 5:11 PM	5 Jul, 2025, 5:11 PM

Other Features

1. WIFI Evil Twin Detection: Get alerts of suspicious WiFi activity near you as a network with the same name as your network.
2. RDP Connection Detection: It notifies when there is RDP connection to your device in real time.
3. Internet Privacy Connection: See all devices that are connected to your network, when they connected, and when they leave.
4. Multiple Remote Server Monitoring: Keep an eye on your servers remotely.
5. Management Console: This feature lets you handle account-related endpoints efficiently.



Type		↓	↑
All traffic		946 KB	550.5 KB
Other	2	556.1 KB	220.8 KB
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	11	384.4 KB	328.6 KB
Domain Name System (DNS)		2.2 KB	989 B
Multicast DNS (mDNS)		3.1 KB	0.0 B
Hypertext Transfer Protocol (HTTP)		179 B	124 B

Apps	
Microsoft Edge	507.4 KB
Microsoft Edge WebView2	441.4 KB
Host Process for Windows Services	252.4 KB
MicrosoftWindows.Client.WebExperience	106.9 KB
Microsoft Office SDX Helper	65.1 KB
Microsoft.6365217CE6EB4	28.7 KB
Host Process for Windows Tasks	10.7 KB
GlassWire Control Service	6.1 KB
nessusd.exe	5.4 KB
MicrosoftWindows.Client.CBS	4.7 KB
ExpressVPN Service	303 B
Microsoft OneDrive	215 B

Hosts	
e86303.dscx.akamaiedge.net	554.6 KB
onedscolprduks02.uksouth.cloudapp.azure.com	208 KB
e86303.dscx.akamaiedge.net	137.9 KB
a1666.dscr.akamai.net	104.3 KB
s-part-0029.t-0009.t-msedge.net	72.9 KB
a1666.dscr.akamai.net	34.3 KB
s-0005.dual-s-msedge.net	33 KB
onedscolprdwus05.westus.cloudapp.azure.com	32.1 KB
a1834.dscg2.akamai.net	30.9 KB
www.tm.v4.a.prd.aadg.trafficmanager.net	29 KB
www.tm.v4.a.prd.aadg.trafficmanager.net	24.2 KB
ax-0002.ax-msedge.net	20.2 KB
a-0003.a-msedge.net	19.7 KB
onedscolprdeus06.eastus.cloudapp.azure.com	14.3 KB
i-sat02p-cor003.api.p001.1drv.com	13.6 KB
edge-cloudmessaging-access-point-aks-prod-eastus.eastus.cloudapp.a...	11.8 KB
onedscolprdwus20.westus.cloudapp.azure.com	11.5 KB
wd-prod-gb-us-east2-1-fe.eastus2.cloudapp.azure.com	10.7 KB
onedscolprdwus14.westus.cloudapp.azure.com	9.9 KB
spo-9999.spo-msedge.net	9.5 KB
settings-prod-uks-1.uksouth.cloudapp.azure.com	8.3 KB
gig-ai-g-prod-eastus-0-app-v4-tag.eastus.cloudapp.azure.com	8.1 KB
api-us-east-2.protect.glasswire.com	6.1 KB
plugins.nessus.org.cdn.cloudflare.net	5.4 KB
mira-ooc.tm-4.office.com	4.7 KB
fde9:275c:74bf:1::1	3.9 KB
+7 more	10.3 KB

Countries	
United States	1.2 MB
United Kingdom	216.3 KB
Japan	7.0 KB
Other	5.4 KB

946 KB ↓ 11 KB/s
1.5 MB
↑ 550.5 KB 418 B/s
WAN 1.5 MB
LAN

Conclusion

GlassWire proved to be a valuable resource for day-to-day users, helping them understand and stay aware of security measures for their networks and devices. Offering real-time activity and network monitoring in a user friendly dashboard that almost everybody can understand. But does this tool have a real value as a security tool? Yes, while Glasswire is not a substitute for an antivirus, it enhances security and can detect threats coming from the network, acting as another line of defense.

Bibliography

1. GlassWire blog - https://www.glasswire.com/blog/
2. GlassWire website - https://www.glasswire.com/features/