SOLUTION OVERVIEW

Security & Network Visibility Assessment

Providing you with insight into how effective your current network security is at reducing risk while ensuring the best possible end-user experience.

UNDERSTANDING YOUR CURRENT SECURITY, PRODUCTIVITY & UTILISATION

Your IT infrastructure is constantly evolving, so too are the ever-prevalent security threats that are becoming more sophisticated and persistent. You are likely to have concerns that current security solutions may not be as effective as they once were, or the way that your network is optimised is not aligned to how it is being used today.

The NAK Network Security Assessment provides you with the deep insight you need to truly understand the security, performance and optimisation of your current network - flagging issues that can be corrected immediately and better informing you on future infrastructure decisions.

A HOLISTIC ASSESSMENT

Our assessment takes a holistic approach, analysing every aspect of the security and performance of your network to give you the insights you need.

Security

11,126
Application Vulnerability Attacks Detected

13
Malware and/or Botnests Discovered

17
High Risk Applications Detected

We enable you to understand how effective your current network security solutions are with insight into application vulnerabilities, which malware/botnets exist on your network, and pinpoint 'at-risk' devices on your network.

Productivity

330
Total Applications Detected

5
Total Proxy Applications Detected

5
Total Peer to Peer Applications

We provide you with visibility into how applications and web resources are used within your network. You gain insight into each category of application from IaaS/SaaS to non-business applications and flag where such applications are not operating in accordance with your policies.

Utilisation

40.5GB
Total Bandwidth Used

12.5
Average Log Rate per Second

58.0%
Percentage of SSL Encrypted Traffic

We provide you with insight into how your network security solution should be optimised for performance. We deliver visibility into throughput, sessions, and bandwidth during peak times to ensure that every line of defence is able to cope.

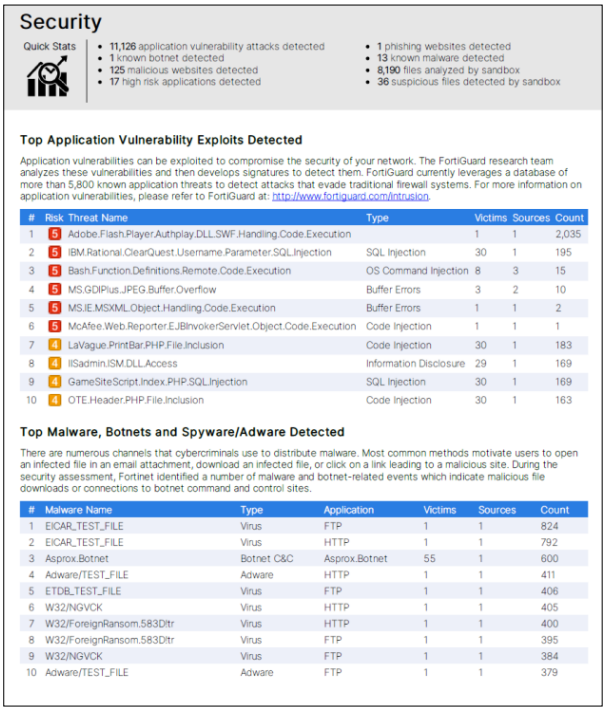
NAK
JOINING UP THE DOTS

INSIGHT & VISIBILITY TO INFORM DECISIONS

NAK is highly experienced in secure networks and as such, we know you are not looking for confirmation that something is not working right – you want actionable insight into how you can resolve issues and reduce risk. This is why our Network Security Assessment drills down on those areas that are critical for you.

Security

Utilising intelligence on threats and vulnerabilities we are able to leverage signatures to identify application vulnerabilities and exploits on your network. We provide you with a comprehensive list of malware, botnets and spyware that we detect as well as identifying your high-risk applications and at-risk devices and hosts.



Security

Quick Stats

- 11,126 application vulnerability attacks detected
- 1 known botnet detected
- 125 malicious websites detected
- 17 high risk applications detected
- 1 phishing websites detected
- 13 known malware detected
- 8,190 files analyzed by sandbox
- 36 suspicious files detected by sandbox

Top Application Vulnerability Exploits Detected

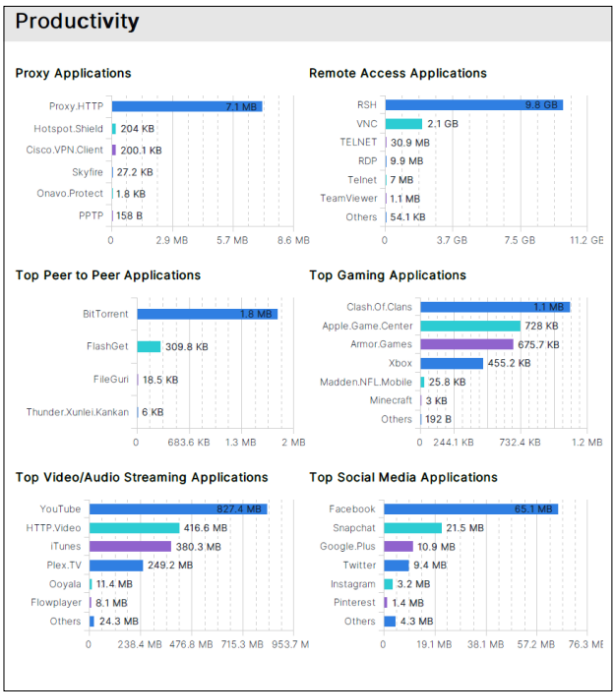
Application vulnerabilities can be exploited to compromise the security of your network. The FortiGuard research team analyzes these vulnerabilities and then develops signatures to detect them. FortiGuard currently leverages a database of more than 5,800 known application threats to detect attacks that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

#	Risk	Threat Name	Type	Victims	Sources	Count
1	5	Adobe.Flash.Player.Authplay.DLL.SWF.Handling.Code.Execution		1	1	2,035
2	5	IBM.Rational.ClearQuest.Username.Parameter.SQL.Injection	SQL Injection	30	1	195
3	5	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	8	3	15
4	5	MS.GDIPlus.JPEG.Buffer.Overflow	Buffer Errors	3	2	10
5	5	MS.IE.MSXML.Object.Handling.Code.Execution	Buffer Errors	1	1	2
6	5	McAfee.Web.Reporter.EJBInvokerServlet.Object.Code.Execution	Code Injection	1	1	1
7	4	LaVague.PrintBar.PHP.File.Inclusion	Code Injection	30	1	183
8	4	IISadmin.ISM.DLL.Access	Information Disclosure	29	1	169
9	4	GameSiteScript.Index.PHP.SQL.Injection	SQL Injection	30	1	169
10	4	OTE.Header.PHP.File.Inclusion	Code Injection	30	1	163

Top Malware, Botnets and Spyware/Adware Detected

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.

#	Malware Name	Type	Application	Victims	Sources	Count
1	EICAR_TEST_FILE	Virus	FTP	1	1	824
2	EICAR_TEST_FILE	Virus	HTTP	1	1	792
3	Asprox.Botnet	Botnet C&C	Asprox.Botnet	55	1	600
4	Adware/TEST_FILE	Adware	HTTP	1	1	411
5	ETDB_TEST_FILE	Virus	FTP	1	1	406
6	W32/NGVCK	Virus	HTTP	1	1	405
7	W32/ForeignRansom.583Dtr	Virus	HTTP	1	1	400
8	W32/ForeignRansom.583Dtr	Virus	FTP	1	1	395
9	W32/NGVCK	Virus	FTP	1	1	384
10	Adware/TEST_FILE	Adware	FTP	1	1	379



Productivity

Proxy Applications

Proxy.HTTP 7.1 MB
Hotspot.Shield 204 KB
Cisco.VPN.Client 200.1 KB
Skyfire 27.2 KB
Onavo.Protect 1.8 KB
PPTP 158 B
0 2.9 MB 5.7 MB 8.6 MB

Remote Access Applications

RSH 9.8 GB
VNC 2.1 GB
TELNET 30.9 MB
RDP 9.9 MB
Telnet 7 MB
TeamViewer 1.1 MB
Others 54.1 KB
0 3.7 GB 7.5 GB 11.2 GB

Top Peer to Peer Applications

BitTorrent 1.8 MB
FlashGet 309.8 KB
FileGuri 18.5 KB
Thunder.Xunlei.Kankan 6 KB
0 683.6 KB 1.3 MB 2 MB

Top Gaming Applications

Clash.Of.Clans 1.1 MB
Apple.Game.Center 728 KB
Armor.Games 675.7 KB
Xbox 455.2 KB
Madden.NFL.Mobile 25.8 KB
Minecraft 3 KB
Others 192 B
0 244.1 KB 732.4 KB 1.2 MB

Top Video/Audio Streaming Applications

YouTube 827.4 MB
HTTP.Video 416.6 MB
iTunes 380.3 MB
Plex.TV 249.2 MB
Ooyala 11.4 MB
Flowplayer 8.1 MB
Others 24.3 MB
0 238.4 MB 476.8 MB 715.3 MB 953.7 M

Top Social Media Applications

Facebook 65.1 MB
Snapchat 21.5 MB
Google.Plus 10.9 MB
Twitter 9.4 MB
Instagram 3.2 MB
Pinterest 1.4 MB
Others 4.3 MB
0 19.1 MB 38.1 MB 57.2 MB 76.3 MB

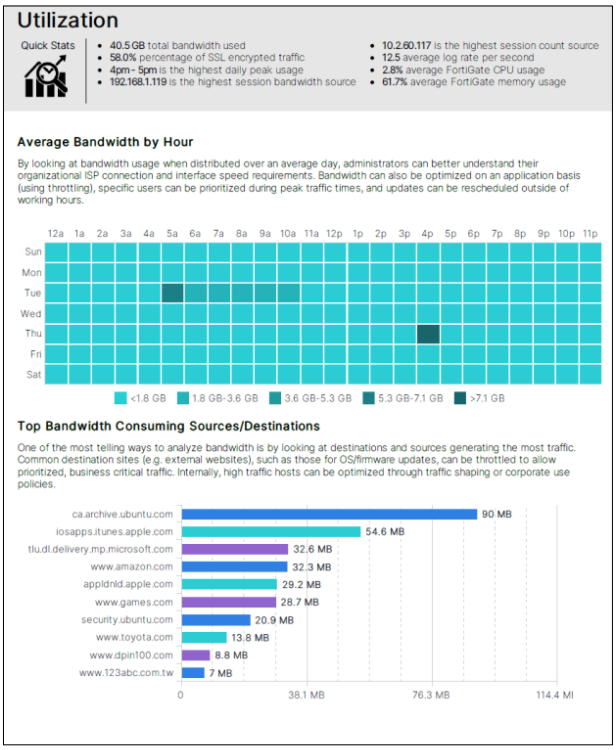
Productivity

It is a challenge for IT teams to truly understand the number of web-based applications and services that are being accessed across the network and the risk to data security that these poses. We provide you with detailed insights on the services being used across your network, the end-locations being accessed, and the network bandwidth being utilised.

NAK
JOINING UP THE DOTS

Utilisation

In order to secure your network, you need to understand and have the visibility into the utilisation of your network over time. We provide you with detailed insights into network utilisation; you can see what bandwidth is being consumed by which end destinations and how this fluctuates over the day and at busy times. This enables you to accurately define the bandwidth required through your security applications and appliances.



HOW DOES THE ASSESSMENT WORK?

As a Fortinet partner, we are able to utilise the market-leading FortiGate technology to analyse your network usage and security as well as Fortinet's comprehensive tools to provide you with the detailed insights you require.

The process is quite simple. Once you request the NAK Network Security Assessment, we set-up a FortiGate appliance that we provide you to connect behind your organisation's gateway firewall or at a branch office. The period we leave the appliance in place is determined by your environment; we can normally collect enough data in a matter of days, however, if you have significant fluctuation of traffic over the week, then we can leave this in place for 1-2 weeks.

Once we have the traffic logs, we analyse these and produce your specific Assessment report. We schedule a time convenient to you to walk you through the findings and then provide you with the full written report.

THE VALUE YOU GAIN FROM THE ASSESSMENT

The aim of the NAK Security Assessment is to provide you with the detailed visibility into how secure your current network is; to provide you real insight into potential issues and vulnerabilities you have and how these can be addressed and provide you with the actionable intelligence to make informed future network infrastructure and security decisions.

NAK
JOINING UP THE DOTS

KEY BENEFITS

By utilising the NAK Network Security Assessment, you are able to fully understand your security posture, the areas of vulnerability across your infrastructure and visibility into current threats.

Network Usage Visibility

To truly understand how your network is being utilised and the applications and traffic traversing your network.

Identify Vulnerable Applications

Highlighting those applications operating across your infrastructure that are high-risk in terms of potential vulnerabilities.

Detect Malware

Identifying any malware that exists across your infrastructure in order to take immediate action in blocking and remediating risk.

Understand Utilisation

Gain data-driven insight into your network utilisation and the requirements to secure this while delivering the required end-user experience.

Visibility of Web Applications

Visibility into the business and personal web-based applications being used across your network and the risk associated with these.

Compliance to Security Policy

Assess your security posture and activity against the security policies you have in place across your business.

WANT TO KNOW MORE

We would be more than happy to walk you through how we perform this quick but comprehensive security assessment of your network infrastructure, and how we are able to deliver significant insights to inform your security roadmap. Please do not hesitate to contact us:

0300 456 0471
enquiries@nak.co.uk
nak.co.uk

NAK
JOINING UP THE DOTS