

Kemp Flowmon: Uniting Netops And Secops

A Broadband-Testing Report



First published July 2021 (V1.0)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk Internet: HTTP://www.broadband-testing.co.uk

@2021 Broadband-Testing

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors.

Please note that access to or use of this Report is conditioned on the following:

- 1. The information in this Report is subject to change by Broadband-Testing without notice.
- The information in this Report, at publication date, is believed by Broadband-Testing to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. Broadband-Testing is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.
- 3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY Broadband-Testing. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY Broadband-Testing. IN NO EVENT SHALL Broadband-Testing BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
- 4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.
- 5. This Report does not imply any endorsement, sponsorship, affiliation or verification by or with any companies mentioned in this report.
- 6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or Broadband-Testing is implied, nor should it be inferred.



TABLE OF CONTENTS

i
TABLE OF CONTENTS
BROADBAND-TESTING2
EXECUTIVE SUMMARY3
UNITING NETOPS AND SECOPS4
PRODUCT OVERVIEW5
KEMP FLOWMON: USE CASES6
Secops – Ransomware (anomaly detection)
IN CONCLUSION14
Figure 1 – Ransomware Scenario
Figure 2 – Vulnerable Targets From Vertical TCP SYN Scan
Figure 3 – RDP BlueKeep Vulnerability Revealed
Figure 4 – Anomalous Behaviour Signals8
Figure 5 – Wireshark Packet Capture: Payload Content Analysis
Figure 6 – Kemp Flowmon ETA/TLS Dashboard9
Figure 7 – Kemp Flowmon ETA/TLS Dashboard: Analysis of key length and ALPN)
Figure 8 – Kemp Flowmon Dashboard: Bandwidth Monitoring
Figure 9 – Kemp Flowmon Dashboard: Drilling Down Into More Info
Figure 10 – Kemp Flowmon Dashboard: Identifying Spike Source
Figure 11 – Kemp Flowmon DNS Dashboard
Figure 12 – Kemp Flowmon DNS Errors Highlighted
Figure 13 – Kemp Flowmon DNS Flow Analysis
Figure 14 – Kemp Flowmon DNS Detailed Analysis14



BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do... The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk



EXECUTIVE SUMMARY

- Network performance and security are not isolated instances of IT; they directly impact on each other and are completely interactive. However, historically network operations (Netops) and security operations (Secops) have effectively been siloed, which is both inefficient and counter-productive
- Networks in the cloud era are becoming increasingly complex in terms of topologies, as the hybrid (On/Off Premises) approach becomes increasingly common. In turn, this makes it more difficult to manage, secure and optimise those networks.
- In the event of either a performance or security issue arising, on a hybrid network especially, locating the problem can take days, weeks or even months, or is simply untraceable without the right tools to hand. In the event of it being performance-related, this can result in significant down-time, meaning \$\$\$\$. If, however, the problem is a security breach, then by the time the problem has been identified, it may have resulted in business-damaging data loss or worse.
- For this reason, Kemp Technologies, whose technology is used to optimise application and data delivery globally, recently acquired Flowmon, providing the company with these very tools. So, this report is focusing on exactly what the Flowmon technology offers with some sample use cases.
- From capacity planning to application delivery optimisation, the Netops element of the Flowmon technology provides 24x7 monitoring and analysis, with real-world use of the over-hyped Artificial Intelligence (AI) at the heart of this, rather than AI simply being a marketing offensive.
- Tied directly in with the network monitoring and analysis is the Secops element alerting on network behaviour anomalies and possible cyber-attacks, with the ability to deep dive into the problem and rapidly identify a threat or other cause of behavioural change.
- In bringing together the worlds of Netops and Secops, not only is the Flowmon technology providing the means to optimise and secure the network 24x7, but it also results in de-duplication of IT time, effort and expenditure, thereby reducing bottom line spend. It's what you might call the ultimate win win scenario! More to the point, it also shows how, what was once seen as a "nice to have" or "insurance policy" is now essential technology, as those networks grow ever more complex.

UNITING NETOPS AND SECOPS

It's not being over the top to say that, in many cases, IT has got itself into something of an unholy mess.

The bolt-on approach to building networks over the best part of the past three decades has brought with it many problems, not least visibility. Many companies - regardless of size, geographical spread and status - simply do not know what applications, devices and even users are on their network. They don't necessarily even know where their extended network actually is, not least due to all forms of outsourcing over those decades, culminating in cloud-based deployments in the past few years. This immediately presents two obvious dangers: potential performance nosedives and security vulnerabilities – and, with them, a seemingly invisible network to track. Add in the Work From Home/Anywhere factor that the pandemic has forced on companies and the gravity of the situation is deeper than ever.

At the same time, and for far too long, IT has been creating islands of technology and resource, so tasks and data that should be shared are split between different teams and individuals who seldom communicate with each other. The result is a huge void in terms of visibility and understanding of what is on the network and how to manage and secure applications and data between the different IT teams – Netops, Secops, Devops... Not only does this create major potential problems in optimising and securing the network; it also results in duplication of effort, a lack of synchronisation and potentially excessive IT spend – all the while actually making the end user experience worse!

The reality is that network performance and security do not work in isolation but, instead, directly impact on each other. They therefore need to be managed as one, and not on an "as needed" basis, but 24x7 – IT never stops nowadays. Additionally, the landscape of IT – network topologies – are changing out of all recognition. A constant fear for companies currently is an inability to manage what appears to be a dramatic infrastructure change. Think back to IT of the 70s and early 80s – one or maybe two mainframe/midrange computers hosting a number of terminals and perhaps a smattering of PCs... That was not difficult to manage, even though in-fighting between what was then Datacomms and Telecoms made it harder than it should have been. Regardless, contrast that infrastructure with today's ever-changing hybrid structures, increasing numbers of remote users, any number of different endpoint devices, multiple xSPs.

Networks in the cloud era are becoming increasingly complex in terms of topologies, as the hybrid (On/Off Premises) approach becomes increasingly common. In turn, this makes it more difficult to manage, secure and optimise those networks – no one could even pretend that kind of contemporary IT footprint was easy to manage. It isn't; simply optimising and securing what might appear to be a healthy network is hard enough, but in the event of a performance or security issue arising? Panic, lots of finger-pointing and an inability to readily remediate the problem is a common scenario. In a best-case scenario this is likely to create expensive downtime and a reduction in productivity; the worst-case scenarios can potentially be business-threatening, especially in an era where many companies have been forced to reinvent themselves – digital transformation, adapting to new customers and new or different needs as a result of the pandemic – as if that weren't hard enough in its own right.



So, IT needs solutions; a hero technology to dig them out of these holes or, even better, make sure they are never formed in the first place. With Flowmon, Kemp Technologies' recent acquisition promises to potentially be that IT lifesaver, so let us take a look at what it offers those despairing Netops and Secops teams.

PRODUCT OVERVIEW

The basic premise behind the Flowmon technology is to provide a near instant way of monitoring and analysis of the network, from both a Netops and Secops perspective, using a combination of AI/Machine Learning (ML), heuristics and analytics, in order to both improve network performance and alert on incidents and potential threats.

Let's get straight to the point here. There have been many attempts in the past to provide some elements of what Flowmon is offering but, all too often, these potential solutions have taken weeks, or even months, to deploy, by which time it's simply too late. Basic deployment of the Flowmon solution takes no more than an hour from download. At that point it starts to monitor and analyse the network, taking a copy of everything flowing across it. With this baseline in place, it can then start to get smart and proactive – identifying any anomalies and alerting them, both for unencrypted and encrypted traffic. Basic tasks include the like of calculating the bidirectional round-trip time ((RTT) for a TCP SYN-ACK (request-response) to test for any latency and/or jitter in a connection, server response times and the retransmit rate. For example, simply by analysing the RTT versus the server response time, you can see whether a problem is manifesting itself on the network or at the server (or even both).

It is important to note that Flowmon does not inject unwanted additional synthetic traffic into the network in order to measure it, but simply uses the real traffic. Where it gets smart is where it uses the gathered performance date to apply network metadata run through ML algorithms to show anomalies such as attacks, misuse and strange behaviour patterns, including at the network perimeter, where the firewalls may have missed something – and they do. It also has full DDOS protection (in either notification or mitigation modes) and is effective up to 400Gbps. Traffic can be redirected to 3rd party scrubbing centres for cleaning if required. Equally, that "blue sky" between the perimeter firewalls and endpoints, that is all too often ignored, is covered off.

Again, it is important to note that this analysis is out of band, so there is no additional traffic or agents consuming resource – just complete transparency. However, the system can handle multiple data feeds making it ideal for MSPs managing a multi-tenant environment. At the same time, a simple deployment can all run on a single Virtual Machine (VM). Indeed, in smaller environments Flowmon might provide most of the required SIEM and APM elements itself. Everything runs on a purpose-built, hardened version of Linux, meaning no update requirement complications.

As is common nowadays, a central dashboard approach is used as the primary access to all the data and analysis which, by default, is kept for 30 days. Multiple dashboards – and reports – are available and all totally customisable. Reporting is interactive and based on a classic "drill down" approach to get deeper information. And there is plenty being collected – for example, DNS info alone has over 250 different fields to analyse.



While Flowmon performs the primary analysis, there are occasions where full packet capture and analysis is required; rather than this going 24x7 and generating unusable (and impossible to store) amounts of data, Flowmon uses an event-based, just in time packet capture approach, on an "as needed" basis, after which the PCAP can be downloaded and analysed with the ubiquitous Wireshark.

In addition to the intelligent collection and analysis, the system also simply black-list sites – there are seven databases in all and the lists are updated every six hours. Background information is also provided on all black-listed elements, such as a host or a URL. Data can also be fed into other systems with Syslog. Finally, Flowmon can carry out Deep Packet Analysis on a range of protocols, including DNS, DHCP, SMB, HTTP and SIP.

KEMP FLOWMON: USE CASES

Secops – Ransomware (anomaly detection)

No security threat has been more talked about over the past couple of years than ransomware. It has effectively become a multi-billion-dollar (or bitcoin!) industry in its own right and targets the most valuable commodity in the modern world – data.

Flowmon's secops' capabilities extend to identifying ransomware attacks, such as the following scenario which was based on a real customer case. It involves a compromised device after an attack on a Samba server for which an attacker has accessed a network via an RDP (Remote Desktop Protocol) server vulnerability, gained valid user credentials from a keylogger on a Windows server, in order to access the Samba server and grab data. The attacker then extracts the data in multiple chunks using the ICMP (ping) protocol, then encrypts the data still residing on the Samba server – classic ransomware. In the real-world case, the attacker then, naturally, fires off an email demanding a ransom payment, usually attaching a sample of the captured file as proof.



Figure 1 – Ransomware Scenario

So how does Flowmon capture this attack? First, using the Flowmon ADS (Anomaly Detection System), carrying out an ARP (Address Resolution Protocol) scan reveals an



event showing an ARP coming from an infected device (192.168.1.50) from the ARP scan table. There follows a Vertical TCP SYN scan to show discovered targets that might have vulnerable services that can be compromised.





Furthermore, an attack on the Windows RDP is discovered with a logged event relating directly to this. Deep diving into more detail, related intrusion detection triggers reveal an exploitation of the known BlueKeep security vulnerability on the RDP server.

	Type: Detail:			k (RDPDICT)		ole attack). Curr	rent statistics: at	tempts: 1. total upload: 5	.66 KiB, maximal upload: 5.66 KiB. Si	ingle attack.						
	Timestamp First flow:	73.02	2020-03-11 2020-03-11	6 08:00:00		EVENT EVIDEN	Event Captu MAC I User i	SOURCE: red source hostname: address: dentity: ED IOS EVENTS (2)	■ 192.168.1.50 (unknown) - N/A 08.00.27.13.b3.a1 - N/A			1	Probability: False positive: Detected by insta Data feed:		100 % No Default Default	
																_
	25			- 1								×	Search by source	ce IP 😑 Sea	rch by destination IP	s Vie
0	1			1								~	Search by source	ce IP 😑 Sea	irch by destination IP	
0	1	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2										~	Search by source	ce IP 📄 Sea	rch by destination IP	S VIE
0	1											*	Search by source	ce IP 📄 Sea	rch by destination iP	s Vie
0	1 175 150 125 20273 20015		7,48	2	20	7.52	754	75	756	800	8.02	804		e IP E Sea	eco	
0	1 175 150 125 20273 20015	7;46	7:48 SOURCE IP BASE FOR ACCERCINCE	5 SOURCE PORT	50 DESTINATION IP BALE FOR ACCERCISTICAL	7.52 DESTINATION PORT			256	LOG	802 LOG SOURCE INTERFACE	804				s Vie
0.0.0	1 175 125 0 20275 0 3	7:46	SOURCE IP	SOURCE	DESTINATION IP BASE FOR ACCRECATION	DESTINATION PORT	SIGNATURE ID	SIGNATURE BASE FOR AGGREGATION	7.58 j	LOG SOURCE IP	LOG SOURCE	BOI	OTHER INFO	8.06		

Figure 3 – RDP BlueKeep Vulnerability Revealed

In terms of the data extraction, it is noted that several different methods were triggered; a data upload anomaly, and an ICMP traffic anomaly (ICPM traffic with a payload – as the data was extracted – is an obvious anomaly to the Flowmon ADS, even though the packets were quite small and easily missed using purely manual analysis.





Figure 4 – Anomalous Behaviour Signals

However, as we now know there has been illegal access, we can use the aforementioned capabilities to use full packet capture and analysis on an "as needed" basis, using Wireshark to analyse the packet contents in full. This, in turn, reveals the actual content elements, including the filename and data contents.

Apple a deplay film	194/x		and the first state of the			
ia. Tine		Source	Destination	Protocol	Length 3rds	
12_ 2020-03-16	07:59:23,74090	4 192.168.1.2	192.168.1.50	TCP	1514 445 + 56748	[ACK] Seq=5313 Ack=930
12. 2020-03-16	07:59:23,74102	9 192.168.1.2	192.168.1.50	TUP	1514 445 + 56748	[ACK] Seg=6761 Ack=930
12_ 2020-03-16	07:59:23,74103	4 192.168.1.2	192.168.1.50	TCP	1514 445 = 56748	[ACK] Seq=8209 Ack=930
	07:59:23,74103		192.168.1.50	TCP		[ACK] Seq=9657 Ack=930
	07:59:23,74103		192.168.1.58	TCP		[ACK] Seq-11105 Ack-930
	07:59:23,74137		192.168.1.58	TCP		[ACK] Seq=12553 Ack=930
	07:59:23,74137		192.168.1.50	TCP		[ACK] Seq=14001 Ack=930
	88:00:30,92164		1.0.132.227	10%P		request id-0x0000, sec
	08:00:30,97464		1.0.132.227	IOP		request id-0x0000, sec
	08:00:31,01629		1.0.132.227	IOb		request 1d=0x0000, sec
	06:00:31,06922		1.0.132.227	10.6		request id-0x0000, set
17 2020.01.16	88-88-11 13614	6.197.168.1.68	4 8 433 527	1/100	1AA7 Fran Inter1	ranart Litababbb ca
Ethernet II, Sr	c: PcsCompu_13:0	53:a1 (08:00:27:1	442 bytes captured 3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227			:36:bd)
Ethernet II, Sro Internet Protoco Internet Contro	c: PcsCompu_13:0 ol Version 4, S 1 Message Proto	63:a1 (08:00:27:1 rc: 192.168.1.50, col	3:b3:a1), Dst: Pcs0			: 36: bd)
 Ethernet II, Sri Internet Protoco Internet Control Type: 8 (Echo 	<pre>c: PcsCompu_13:) ol Version 4, Si 1 Message Proto (ping) request</pre>	53:a1 (08:00:27:1 rc: 192.168.1.50, col)	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227	:oepu_65:3		: 36: bd)
 Ethernet II, Sr. Internet Protoc. Internet Contro. Type: 8 (Echo 0000 08 00 27 65 	c: PcsCompu_13: ol Version 4, So 1 Message Proto (ping) request 36 bd 08 00 2	b3:a1 (08:00:27:1 rc: 192.168.1.50, col) 7 13 b3 a1 08 00	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45 00 'e5 '	Compu_65:3		: 36: 6d)
 Ethernet II, Sr. Internet Protoco Internet Control Type: 8 (Echo 0000 08 00 27 65 0010 05 94 00 01 	c: PcsCompo_13: ol Version 4, 5 1 Message Proto (ping) request 36 bd 05 00 2 00 00 ff 01 3	b3:a1 (08:00:27:1 rc: 192.163.1.50, col) 7 13 b3 a1 08 00 2 e3 c0 a8 01 32	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45:00 'e5 ' 01:00 2	Compu_65:3		: 36: 6d)
 Ethernet II, Sr. Internet Protoco Internet Contro Type: 8 (Echo 0000 08 00 27 65 0010 05 94 00 01 	c: PcsCompo_13: ol Version 4, 5 1 Message Proto (ping) request 36 bd 05 00 2 00 00 ff 01 3	b3:a1 (08:00:27:1 rc: 192.168.1.50, col) 7 13 b3 a1 08 00	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45:00 'e5 ' 01:00 2	65:3		: 36 : 6d)
 Ethernet II, Sr. Internet Protoc. Internet Contro. Type: 8 (Echo 0000 08 00 27 65 0010 05 94 00 01 0020 84 e1 00 00 0020 04 e1 00 00 	c: PcsCompu_13:1 ol Version 4, Si 1 Message Proto (ping) request 36 bd 08 00 2 00 00 ff 01 3 c7 99 00 00 0 65 20 64 66 0	b3:a1 (08:00:27:1 rc: 192.163.1.50, col) 7 13 b3 a1 08 00 2 e3 c0 a8 01 32	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45 00 'e5 ' 45 00 2	E Correct Correct Correct Correct Correct Correct Correct Correct		: 36: bd)
 Ethernet II, Sr Internet Protoco Internet Control Type: 8 (Echo 0000 08 00 27 65 0011 05 54 00 01 0010 05 54 00 01 0010 05 74 00 01 0010 07 70 23 75 0050 01 64 65 74 0050 22 20 51 64 	c: PcsCompu_13:1 ol Version 4, 5 1 Message Proto 0 (ping) request 36 bd 08 00 2 08 00 ff 01 3 c7 99 00 00 0 65 20 61 61 6 2c 20 61 61 6	b3:a1 (08:00:27:1 rc: 192.168.1.50, col) 7 13 b3 a1 08 00 2 e3 c0 a8 01 32 0 00 fc 6 f 72 65 c 6f 72 20 73 09	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45:00 'e6 ' 100 2 6d 20 74:20 [Dstum do 12	E 2 compu_65:3		:36:6d)
Ethernet II, Sev Internet Protoco Internet Control Type: 8 (Echo 0000 08 00 27 65 0010 05 40 00 00 0000 09 70 23 75 0000 01 09 70 23 75 0000 01 09 70 23 75 0000 01 09 70 23 25 0000 01 04 65 34 0050 72 20 61 64 0050 72 20 61 64	c: PcsCompu_13:1 ol Version 4, 5 1 Message Protoco (ping) request 36 bd 08 00 ff 01 3 cc 7 99 00 00 0 6d 20 64 6f 0 2c 20 61 6f 6 2c 20 61 6f 6 6e 74 65 67 0	$\begin{array}{c} b3:a1 \ (08:00:27:1\\ rc: 192.168.1.50\\ col \\ \hline \\ \end{array} \\ \hline \\ 7 \ 13 \ b3 \ a1 \ 08 \ 01 \\ 2 \ 03 \ col \ a5 \ 01 \\ 00 \ cc \ 64 \ 72 \ 55 \\ cf \ 72 \ 06 \ 67 \ 70 \ 55 \\ 160 \ 66 \ 57 \ 70 \ 65 \ 51 \end{array}$	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45 00	Compu_65:3		: 36: 6d)
Ethernet II, Sr Internet Protoco Internet Contro Type: 8 (Eche 0000 68 60 27 65 0110 65 94 60 61 0020 64 e3 04 60 10 0020 64 e3 04 60 0020 61 e4 e3 04 60 0020 61 e4 e3 04 60 0020 70 72 72 75 0020 71 74 0020 14 e3 04 60 010 64 65 74 0020 72 44 65 74 0020	c: PcsCompu_13:1 01 Version 4, 55 11 Message Proto (ping) request 36 bd 08 00 2 08 00 ff 01 3 c7 99 00 00 0 6d 20 6d 6f 6 2c 20 01 6f 6 66 70 00 73 6 6e 74 55 67 6 20 50 72 61 6	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	3:53:61), Dst: Pcol Dst: 1.0.132.227 45:00	Compu_65:3		: 36: bd)
Ethernet II, Sr Internet Protoco Internet Control Type: 8 (Echo 0000 08 00 27 65 0010 05 94 00 01 0020 44 0 08 00 0020 44 0 08 00 0020 44 0 08 00 0020 44 0 08 00 0050 74 20 08 00 0050 74 20 20 40 0050 74 20 20 40 0050 04 60 64 20 0020 44 65 77 6	c: PcsCompu_13: 01 Version 4, 55 1 Message Proto (ping) request 36 bd 08 00 2 08 00 ff 01 3 77 99 00 00 0 66 20 64 6f 6 2c 20 61 6f 6 69 70 00 73 6 6e 74 65 67 6 20 59 72 61 6 20 59 73 65 6	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	3:b3:a1), Dst: Pcs0 Dst: 1.0.132.227 45 00	E 2 Lorent c tit ecteti c nec o ent 11 Corsus		:36:6d)
 Ethernet II, Sri Internet Protoco Internet Control Type: 8 (Eche 0000 08 00 27 65 00111 05 54 00 01 0020 34 e) 08 00 0020 34 e) 08 00 0020 44 e) 08 00 0020 54 e) 08 00 0020 64 e) 08 00 0020 64 e) 08 00 0020 65 e) 08 00	E: PesCompu_13:1 01 Vertion 4, 5 11 Message Protocol (glng) request 36 bd 08 00 2 36 bd 08 00 2 0 37 99 00 00 0 47 28 6.1 64 64 47 96 00 74 6 47 96 00 0 0 0 47 96 00 71 6 6 74 6.5 77 6 47 45 6.7 72 6.1 6 74 6.5 74 6 57 20 52 53 56 6 57 6 57 6 57 6 6 57 6 6 57 6 6 57 6 6 57 6 6 57 6 6 57 6 6 57 6	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	3:03:04), Dst: Peed Dst: 1.0.132.227 45:00	E E Cores F Cores F Cores F Cores F Cores		:36:bd)
Ethernet II, Sr Internet II, Sr Internet Protoco Internet Contro Type: 8 (Echo 0000 60 00 27 65 0010 65 94 00 01 0000 64 00 02 0000 64 00 00 0000 64 00 65 74 0000 64 0 64 2 0000 62 65 72 20 61 64 0000 61 65 73 0000 61 64 2 0000 61 64 2 0000 61 64 2 0000 61 64 2 0000 61 64 2 0000 61 64 2 0000	C: PcsCoepu_33: 01 Version 4, 5; 11 Version 4, 5; 15 bd 08 00 16 pcsoape pcsoape 15 bd 08 00 2 16 bd 08 00 2 16 bd 08 00 2 17 90 00 0 16 24 66 16 17 90 00 0 0 16 24 67 16 17 16 27 90 00 0 0 16 27 90 00 0 0 16 27 20 16 16 17 17 16 16 17 16 17 17 16 16 16 17 15 18 16 128 16 17 15	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	3:b3:a1), Dst: Pcol Dst: 1.0.132.227 45:00 **e6 * 42:00 22 45:00 22 40 20 22 40 22 40 40 22 40 40 22 40 40 22 40 40 22 40 40 40 22 40 40 40 40 40 40 40 40 40 40 40 40 40	Longu_65:3		:16:14() :
 Ethernet II, Sr. Internet Protoco Internet Control Type: 8 (Echo 0000 68 60 27 65 00110 65 54 60 61 00100 63 64 20 164 00100 63 64 20 164 00000 61 74 20 164 00000 72 20 51 64 00100 67 72 20 51 00100 72 20 51 64 00100 72 52 57 72 67 00100 72 65 77 66 00100 72 65 77 66 00100 72 65 77 72 67 00100 72 72 72 72 72 00100 72 72 72 72 72 72 00100 72 72 72 72 72 72 00100 72 72 72 72 72 72 72 00100 72 72 72 72 72 001	c: PcsCoepu_13: 01 Version 4, 53 01 Version 4, 53 11 Message Protocitic (ping) request 36 bd 68 00 06 00 67 01 36 bd 68 00 22 20 00 00 64 01 20 20 1.06 6 02 20 20 1.06 6 02 6 20 20 1.06 6 02 22 02 03 04 0 20 20 1.06 1.66 20 56 6 52 20 1.66 7 53 56 6 52 20 1.64 7 53 1.56 6 52 1.71 75 67 7 2 7 7 7 7 7 7 7 7 7 7 7 7 7 <td< td=""><td>$\begin{array}{cccccccccccccccccccccccccccccccccccc$</td><td>3:03:04), Dist: Peed Dist: 1.0.132.227 45:00</td><td>Loopu_65:1 Loopu_65:1 Loopu_65:1 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_65:1</td><td></td><td>:36:14() :</td></td<>	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	3:03:04), Dist: Peed Dist: 1.0.132.227 45:00	Loopu_65:1 Loopu_65:1 Loopu_65:1 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_7 Loopu_65:1		:36:14() :
 Ethernet II, Sri Internet Protoco Internet Contro Type: 8 (Eche 0000 68 60 27 65 0010 65 94 60 92 0020 64 e3 04 60 92 0020 69 24 e3 04 60 92 0020 69 24 e3 04 60 92 0020 70 72 72 72 0020 61 e4 e3 04 60 0020 70 72 72 72 0020 70 72 72 72 0020 61 e5 72 e6 0020 62 62 62 72 e7 0020 62 62 62 72 63 0020 62 62 62 72 63 0020 63 64 62 72 0020 64 62 62 72 0020 65 64 62 72 0020 65 64 62 72 0020 65 64 62 72 	c: PcsCoepu_13: 01 Version 4, 5: 12 Version 4, 5: 14 Version 4, 5: 15 16 00 02 00 00 01 request 15 16 00 02 2 00 00 01 00 00 16 26 64 0 22 26 16 67 20 54 54 56 20 54 56 67 20 54 56 67 20 54 57 51 20 54 57 51 52 54 57 61 52 54 54 61 50 56 64 61 53 65 64 62 20 55 62 65	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	3:b3:a1), Dst: Pcol Dst: 1.0.132.227 45:00	Compu 65:3 Compu 65:3 Communication Communicatio		:36:bd)
→ Ethernet II, Sri → Internet Protoco Internet Contro Trape: 8 (Echo 0000 08 00 27 65 0010 05 94 00 01 05 94 00 01 0020 44 00 10 0020 44 00 00 0020 45 00 00 0020 45 00 0040 01 65 78 0060 74 22 20 65 44 0060 74 22 20 65 44 0060 74 22 20 65 42 0060 07 64 22 20 0000 01 64 74 0000 01 64 72 65 0000 05 65 72 67 0000 05 65 72 0000 05 76 55 72	C: PestGeepu_13: 11 Version 4, 5; 12 Version 4, 5; 14 Message Protoco (ping) request 16 bd 00 00 2 00 00 ff 01 3 27 90 00 0 6 20 20 64 67 6 27 90 00 0 0 6d 20 64 67 6 27 20 53 65 6 20 53 65 65 24 42 21 53 65 65 24 42 71 20 55 65 74 20 65 74 2	$\begin{array}{c c c c c c c c c c c c c c c c c c c $	3:b3:a1), Dst: Pcol Dst: 1.0.132.227 45 00	Compu 65:3 Compu 65:3 Communication Communicatio		:16:14() :

Figure 5 – Wireshark Packet Capture: Payload Content Analysis

It should be noted that all these events can be viewed on a timeline, which makes it easy to understand the processes involved in the attack and help prevent similar attacks in the future – that being the primary point of the analysis, of course.

Netops/Secops – Encrypted Traffic Analysis

One major potential problem area for companies is encrypted traffic; often given levels are mandatory for use within an enterprise, but how do you monitor and analyse that encrypted traffic to a) guarantee compliance and b) resolve those potential problems?

For these reasons, Flowmon provides an Encrypted Traffic Analysis (ETA) dashboard which we will now use to analyse – as an example – some TLS (Transport Layer Security) traffic. TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and VoIP.

	MySQL DB	QuS ETA/TLS	DNS Office	365 Soc	ial Networks O		Last 24 ho	urs- 0
Lit versions			Last 24 hours (prevents fo	ine spari) = Q.	Endpoints Using TLS V1.0		Last 24 Jours (generic)	(menpor) = 1
Meralder						0		
1000 2100 1022,2020.	10.0	10.00 10.00	- 10	1000	1000 C			100
TLE revenues		Manadousi Islan/w	Bio protected	Batter	My P attents P 1021624	Firms 27.5x.6	1000 packets 62100 K	111 17 M
nana.		2.2 M	228.00	228.58	8 11 a from all Coal from all	4.00.0	18130.8	156.4814
1.810		100.0 4	316.6	407.76 ket				
7L5X3		278	5.5	99.87 KB	support of the test stores	1.92.8	41.79.8	25.070
In the second		81 W	3.6	milies.		3.12.4	75.20.×	25.485
76313		294.8	1.9	20.00 HB	Ri pgththe-trivitiel	1.614	3687 K	22.275
I m.		141.1	2.1	14118	0 R 1820230	814	2122.5	10.955
Total		3.3 M	255.4 K	2.08.68	11 sige une voor stre 21 stef Jaarbank sant	tia	35.2 6 #	10.144
					vwd2x00x+164 3x100 ref	1348	22:15.8	15475
n-19-2017-20-2020-19-20-20-20-20-20-20-20-20-20-20-20-20-20-					S S Strategica Strategica Const		1723 K	15,214
S ALPN			Last 24 biture (generic ti	merenali - da	C Ch 142 100.0 M		15.42 K	14,541
					Column		4	
-					 144 	BUSK	DOL: NO.	425.281
					2004-943 0000-2000 942 0000			
The star is a second se	110	100 H-0	12.0	10.00	TLS Chent Key Longth		Last 24 fears (generic)	+ (Joseph area
TLENDE		Manual Man-	File are record	7,711				
NUTR		301.0W	38.04	200.87 HVE				
and the second se		16.14	1.0	114248				
NAT		.0	0	.0.				
WeRT								
Culf"					TLS Clevel key length	There	input perforts	. 19
8000					B 384	25.75 K	148.9	315.585

Figure 6 – Kemp Flowmon ETA/TLS Dashboard

As you'll note from the dashboard layout, the consistency of presentation runs throughout the Flowmon offering so, once you've got the hang of one element, the rest follow logically. In this case, at the top is a graph of TLS protocol usage differentiated by version. Next to it is a list of the top 10 endpoints using outdated TLS 1.0 – in other words, an instant viewpoint of devices using an obsolete, and therefore potentially vulnerable, encryption standard. No support equals vulnerable...

One more, from this top level we can drill down using the **More info** menu to analyse in more detail, for example, the TLS-client key length and a chart of TLS ALPN (Application-Layer Protocol Negotiations).





Figure 7 – Kemp Flowmon ETA/TLS Dashboard: Analysis of key length and ALPN)

Here we can see exactly what versions of TLS are in use and to what extent. Using the **Advanced analysis** mode once more, we can then examine the potential problem area – the TLS 1.0 usage. By filtering on TLS 1.0, the results indicate that there is a device using the IP of 192.168.2.4 in the company using the obsolete TLS standard.

Obviously, not is this kind of discovery only important from a security standpoint, but also from a compliance perspective. Given the full TLS application-layer visibility, we could equally examine other potential problem areas such as the validity of TLS certificates, TLS issuer name and encryption algorithms. In each case, the search procedure is the same, just the content being analysed changes. Again, this emphasises the ease of use with the software; yes, ease of use is always a benefit, but when analysing traffic that might include ticking time bombs, saving seconds through speed of data discovery could be precious.

Netops – Bandwidth Monitoring (traffic spikes)

Traffic spikes are a common indicator of unusual or specific (time/day) behaviour patterns that need to be dealt with, since they are a primary cause of outages – note the household name casualties that have been much documented during the pandemic.

With Flowmon, our starting point to investigate potential spikes – in this case with Internet traffic – is naturally the dashboard. In this instance, the bottom half of the screen is showing top sources and destinations of inbound and outbound Internet traffic while the top half readily indicates a massive traffic spike that occurred between 15:00-16:00. Being so out of line with regular traffic flows, this would naturally merit investigation, for the reasons stated above.





whiteard Reports								Helfinsform 👔 English o	denn
tatus NetOps SecOps	Inet Traffic MySQL	DB QoS	ETA/TLS DNS	Office 365	Social Network	8 O		Last 24 hours -	•
Internet Uplink Utilization				aut 24 Troans (generic K	me spari) + 🗘 Inte	ernet Oplânk Utiliza	lon	1.441 24 hours (generic time spar)	() - ()
		1.1					e 97.45 Roman Prices	on index	ticebe
Splask Utilization	12.00		Mipolenii)	anda Dispersano arten 2.0	el Optes M 30,44 0 M		er second Avill pack 21 M 326.1		
Treat				0.0 K 01.7 0.7 M 2.5	K 933.01 MB M 21.40 GB		445 SIT 146.209 ms	.cv0.RTB 0.1	
101-16-18 III 57 - 2029-10-20-08-57					_ 200	1-10-19 00.07 - 2028 18	24951		
Top Source Autonemoue Systems	Last 24 hours (pararie line	e apari) = 10	Top Destination Autonomous 5	Systems	Last 24 hours (peneric 1	(ne ipian) + . 10	Tep Hostnames	Last 34 hours (generic time spar)	11 = 1
Inarth A3		Bytes	Devisation All		Bh per cete	ad fytee	HTTP Institute		Flow
Illeroseft Corporation	2.2 M		101 Public Company Limited	i i	212.3		even darupte ca		16.04
0cogie 110	492.9.6	601.00	Manaest Ourporation		\$4.3	101.42468	B0.180.78.102		12.143
PODdas	521.7 K	1.52.08	Masterinteret sco		\$5.4	LK 14339468	au download windows, publie com		5.12
		1.11.08	C dooglatts		25.5	K 72.54MB	O www.faotbook.com		4.17)
Auna Herndonii B.V.	1122.8								
Alama Homobonii 8.V Di Overge	1113 K		0 P004 #3		22.5	K 00.63 MB			3.724

Figure 8 – Kemp Flowmon Dashboard: Bandwidth Monitoring

At this point we can drill down, selecting a **More info** option from the drop-down menu, into analysis mode, where we can focus in on that spike and see that it is a result of an excessive number of downloads.



Figure 9 – Kemp Flowmon Dashboard: Drilling Down Into More Info

In the **Advanced analysis** window, a chart showed the first 10 IP conversations (i.e., aggregated connections between two hosts) in order of bytes transferred. From this, it was clear that communications between the pair of IP addresses **172.217.23.193** - **192.168.70.80** resulted in over 4GB of traffic being generated within three flows/connections. Simply right-clicking on one of the IP addresses gave us access to every single connection related to this communication, from which we chose **First 20 flows** from the dropdown menu.





Figure 10 – Kemp Flowmon Dashboard: Identifying Spike Source

From the list it was easy to see that the internet traffic spike was caused by a large download from an HTTP server. However, to short-cut the process further, we could have configured the system to alert us about any unusual situation arising, and this case would have resulted in an alert, as soon as that link saturated. Simply using **Alert view** we could review that spike as it happened in real-time, in greater detail. Essentially, what level of detail you wish to drill down into is all covered off – the more you dig, the more you find!

Netops – DNS Errors

Another major cause of application and data connectivity issues are DNS errors. From a user perspective especially, being unable to connect to regular application or site is both confusing and expensive in terms of potential loss of productivity. The classic scenario is the service management (helpdesk) team receiving a call or message to say a user cannot access an application or site – AKA a specific server in many instances. In this type of scenario, Flowmon provides a DNS dashboard, from which we can dig down into the problem.



Figure 11 – Kemp Flowmon DNS Dashboard



This dashboard gives us an overview of DNS traffic and DNS errors, with a breakdown of DNS servers handling the greatest load, devices getting the most DNS errors, and related information. In this instance we wish to investigate a potential server problem, so – in a similar fashion to the first scenario – we once again can drill down, selecting a **More info** option from the drop-down menu (DNS Errors in this case).



Figure 12 – Kemp Flowmon DNS Errors Highlighted

From the drill-down graph we can clearly see that the majority of errors are resulting from an attempt to connect to non-existing domains (orange) with periodic server failures (red). To analyse these errors in more detail we can then access a **First flows** menu, from which we can choose **First 20 flows** revealing a table of the flow data. In turn, from this we can see that seemingly the DNS server leasing the IP of 172.18.28.240 is the one experiencing the issues.

FLOWS	BYTES	PACKETS	TOS	TCP FLAGS	DESTINATION PORT	DESTINATION IP ADDRESS	SOURCE PORT	RCE IP ADDRESS	SOU	PROTOCOL	DURATION	START TIME - FIRST SEEN
1	57 B	1	Best Effort & Default		27555	□ ! 172.17.107.32	domain	172.18.28.240	Q1	UDP	0 s	2020-10-22 01:00:49.212
1	54 B	1	Best Effort & Default		11829	Dt 172.17.107.32	domain	172.18.28.240	0	UDP	0 s	2020-10-22 01:01:38.281
1	64 B	1	Best Effort & Default		56229	D: 172.17.107.32	domain	172.18.28.240		UDP	0 s	2020-10-22 01:01:43.830
1	55 B	1	Best Effort & Default		32314	D: 172.17.107.32	domain	172.18.28.240	•	UDP	0 s	2020-10-22 01:01:46.906
1	65 B	1	Best Effort & Default		23376	D: 172.17.107.32	domain	172.18.28.240	Q;	UDP	0 s	2020-10-22 01:01:47.149
1	67 B	1	Best Effort & Default		41142	Q 172.17.107.32	domain	172.18.28.240	ç,	UDP	0 s	2020-10-22 01:01:59.260
1	54 B	1	Best Effort & Default		54986	DI 172.17.107.32	domain	172.18.28.240	P:	UDP	0 s	2020-10-22 01:02:07.437
1	58 B	1	Best Effort & Default		15899	D: 172.17.107.32	domain	172.18.28.240	ç,	UDP	0 s	2020-10-22 01:02:18.056
Packets 8		ytes 474 B	B B	Flows 8								

Figure 13 – Kemp Flowmon DNS Flow Analysis

Digging deeper into the communications, we can dive into Layer7 stats, providing us with more DNS-related information including the type of the DNS message, the payload of those messages, and, at the heart of the problem, the DNS question names, which the DNS server has not been able to deliver



DNS RESPONSE DATA	DNS RESPONSE NAME	DNS QUESTION NAME	DNS QUESTION TYPE	DNS QUERY/RESPONSE	INATION IP ADDRESS	ss c	RCE IP ADDRESS	SOUR	START TIME - FIRST SEEN
		trace.org.sg	MX	Response	172.17.107.32	10 1	172.18.28.240	•	2020-10-22 01:00:49.212
		bmed.com	MX	Response	172.17.107.32	10 1	172.18.28.240	Q1	2020-10-22 01:01:38.281
		bestdealsalert.com	MX	Response	172.17.107.32	\$0 I	172.18.28.240	Фı	2020-10-22 01:01:43.830
		cl.uh.edu	MX	Response	172.17.107.32	10 1	172.18.28.240	-	2020-10-22 01:01:46.906
		canariastelecom.com	MX	Response	172.17.107.32	10 1	172.18.28.240	•	2020-10-22 01:01:47.149
		eproauctionreport.com	MX	Response	172.17.107.32	40 1	172.18.28.240	D:	2020-10-22 01:01:59.260
		f-mp.com	MX	Response	172.17.107.32	ŧ0 I	172.18.28.240	Q1	2020-10-22 01:02:07.437
		ida-dtek.com	MX	Response	172.17.107.32	10 1	172.18.28.240	-	2020-10-22 01:02:18.056
Flor		1							

Figure 14 – Kemp Flowmon DNS Detailed Analysis

IN CONCLUSION

Too many products and services within the world of IT are the classic invention of a solution looking for a problem.

In the case of Kemp Flowmon, we have the exact opposite. It exists because all the potential – and absolute – problem areas it targets and addresses already exist. In other words, it does what it says on the tin. And very efficiently too. The reality is that the contemporary hybrid network is unmanageable and impossible to secure using traditional methods. What the Flowmon technology brings to the table is what is required now – in 2021 – and onwards., as the IT infrastructure revisions continue apace for some years to come yet.

Moreover, it brings together the isolated worlds of Netops and Secops to create a far more secure, resilient and efficient way of managing a network. In so doing, helps enormously with the never-ending task of optimising and securing the network 24x7, reducing the excess of duplication in IT and thereby saving budget to boot. If that sounds like a must-have, then you'd be right on the money – highly recommended.

