



Live report from network & security operations

ITMK 2023

Pavel Minarik

VP, Technology

13th September 2023



IT teams are facing never ending challenges



Root-cause analysis

Troubleshooting

Performance issues

Bandwidth utilization

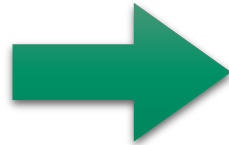
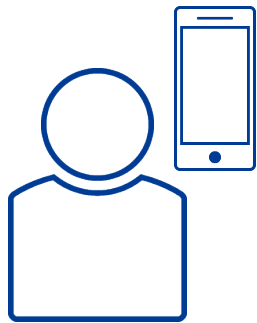
Infected devices

Security breaches

Mean time to repair

Repetitive pattern in IT operations

User complains about application {slowness, unavailability, etc.}



Network?



Device or server?



User?



Where is the problem?

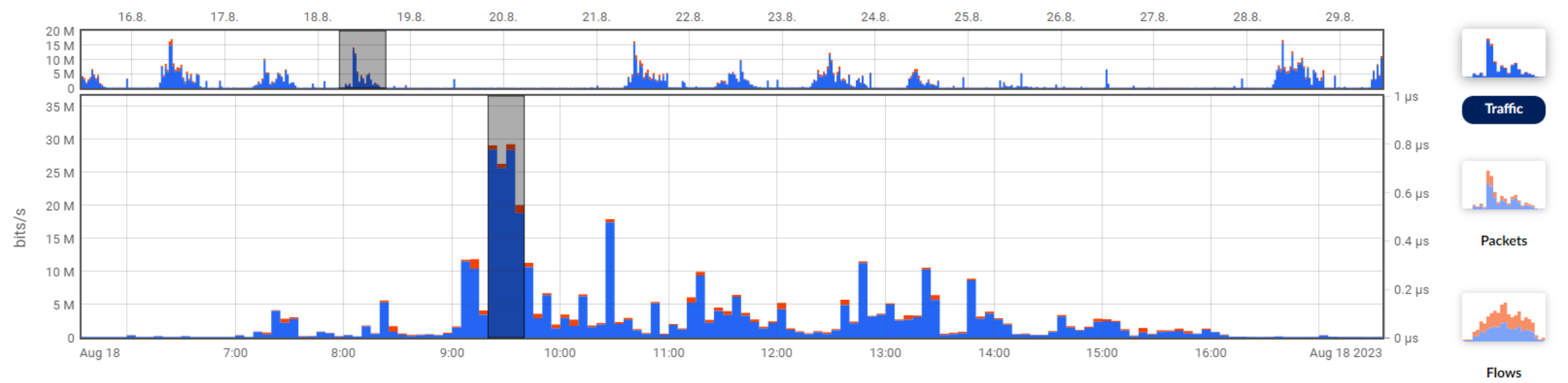


We have received a **network interface utilization** alert.
We need to find the root cause as it can slow down our network and impact users.

- Sources
- Profiles
- Analysis
- Report chapters
- Alerts
- Active Devices
- VoIP Traffic

INTERNET: 2023-08-18 05:35 - 2023-08-18 17:35

Profile: Internet Interval: Custom From: 2023-08-18 05:35 To: 2023-08-18 17:35 SET INTERVAL

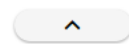


- All
- TCP
- UDP
- ICMP
- Other

CHANNELS (2 VISIBLE OF 2 TOTAL)

- Upload
- Download
- NPM Jitter
- NPM Round Trip Time
- NPM Server Response Time

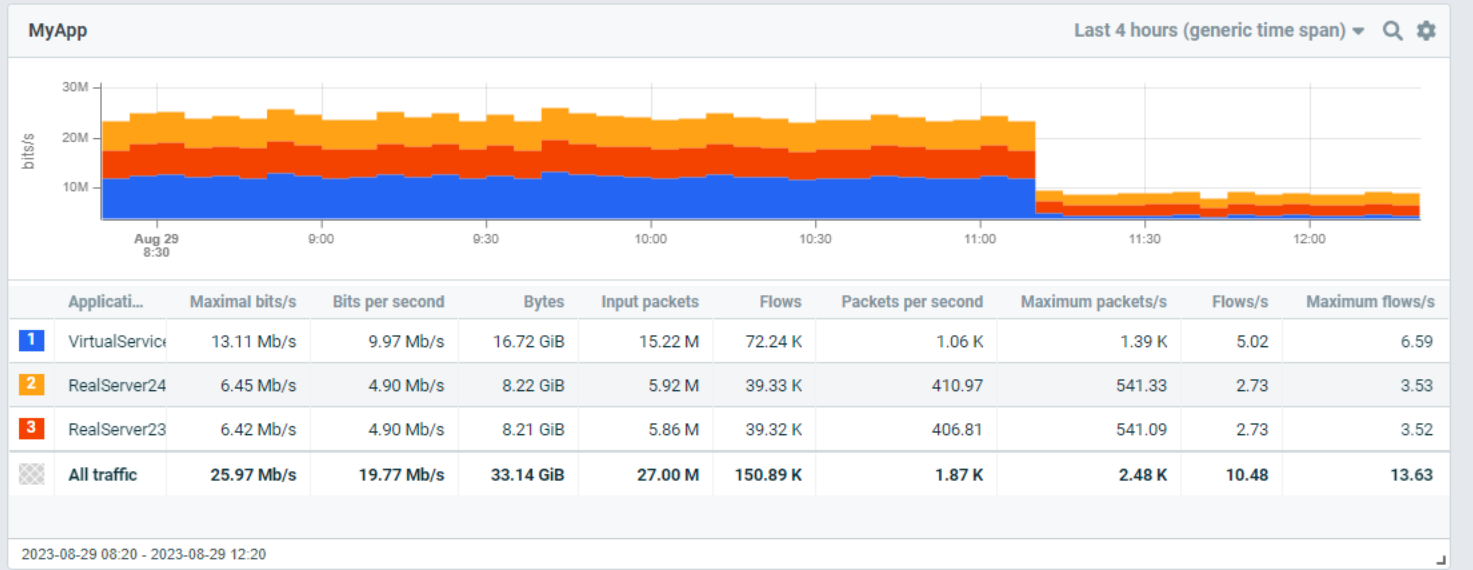
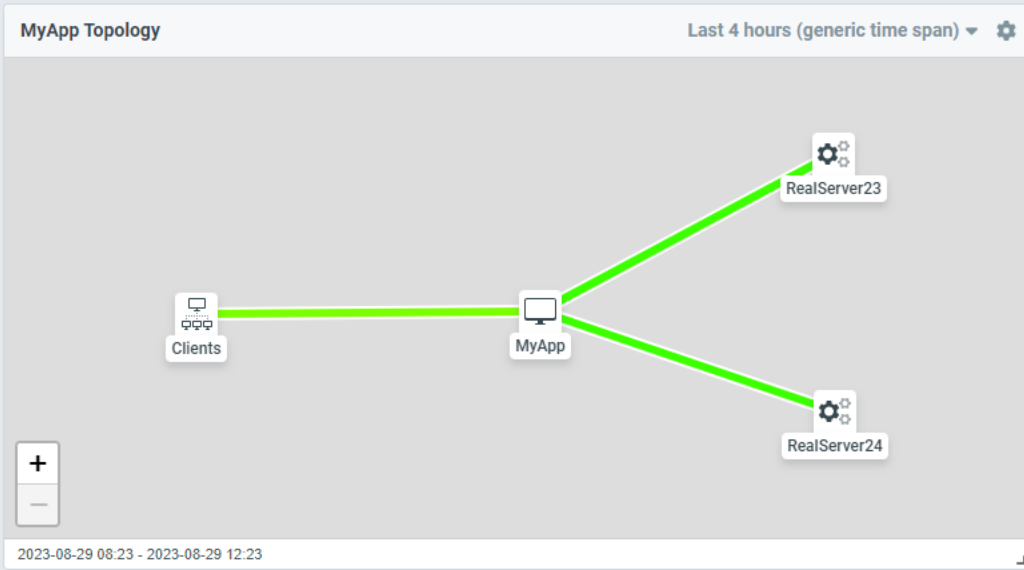
All None CHANGE DISPLAYED CHANNELS GET CHANNEL STATISTICS



Advanced analysis 2023-08-18 09:20 - 2023-08-18 09:40



After an order processing **system upgrade**, we are experiencing **performance degradation**. It impacts majority of users; it has attention of management, and the supplier blames our network.



VLast 4 hours (generic time spa...)

● **99.9%**
Retransmission index

0% 90% 99% 99.9% 100%
Poor Excellent

Bits per second
10.0 M

AVG packets/s
1.1 K

AVG RTT
0.614 ms

AVG SRT
124.131 ms

RLast 4 hours (generic time spa...)

● **99.9%**
Retransmission index

0% 90% 99% 99.9% 100%
Poor Excellent

Bits per second
4.9 M

AVG packets/s
406.8

AVG RTT
0.285 ms

AVG SRT
225.66 ms

RLast 4 hours (generic time spa...)

● **99.9%**
Retransmission index

0% 90% 99% 99.9% 100%
Poor Excellent

Bits per second
4.9 M

AVG packets/s
411.0

AVG RTT
0.308 ms

AVG SRT
1.292 ms

MyAppClients

Last 4 hours (generic time span)

Any IP address	Flows	Input packets	AVG RTT	AVG SRT	AVG RTR	Bytes
1 MyApp	77.02 K	16.23 M	0.627 ms	89.318 ms	0.0	17.83 GiB
2 client21.lan	55.84 K	11.90 M	0.509 ms	81.009 ms	0.0	12.93 GiB
3 client27.lan	21.18 K	4.33 M	0.935 ms	111.226 ms	0.0	4.90 GiB
All traffic	77.02 K	16.23 M	0.627 ms	89.318 ms	0.0	17.83 GiB



We experienced an issue with our UPS that should not have occurred, **yet no email notification was sent** by the UPS before the outage. It had been functioning properly in the past. What happened?

Analysis detail

Analyzed PCAP

smtp_for_webinar.pcap

Show the following protocols in the analysis report (1)

SMTP

EVENTS

STATISTICS

Tree options








Root events displayed after propagation of severity

PROPAGATE SEVERITY

COLLAPSE ALL

EXPAND ALL


Information: 0 Warning: 0 Error: 1

-  SMTP: SMTP connection detected (TCP@81.95.97.100:25-192.168.0.253:1357)
-  SMTP: Server welcomed the client
-  SMTP: Server is ready
-  SMTP: No authentication detected
 -  SMTP: Encryption successful
 -  TLS: Handshake detected
 -  TLS: Fatal alert error

Fatal alert error



The peers failed to negotiate a shared key material. Try connecting with different cipher suites one-by-one and check if any of them helps. If neither does, try to use a different protocol version.

Description	Fatal alert - 'bad_record_mac - Received a record with an incorrect MAC (Message Authentication Code).' (error code 20).
Protocol	TLS
Severity	error 
Flow	TCP@81.95.97.100:25-192.168.0.253:1357
TCP flow errors	No errors detected
Frame time	02.03.2018 19:40:34
Frame number	16
IP version	4
IP source	81.95.97.100
IP destination	192.168.0.253
IP proto	6
TCP source port	25
TCP destination port	1357
tls.alert_message.desc	20
Decoded error	bad_record_mac - Received a record with an incorrect MAC (Message Authentication Code).



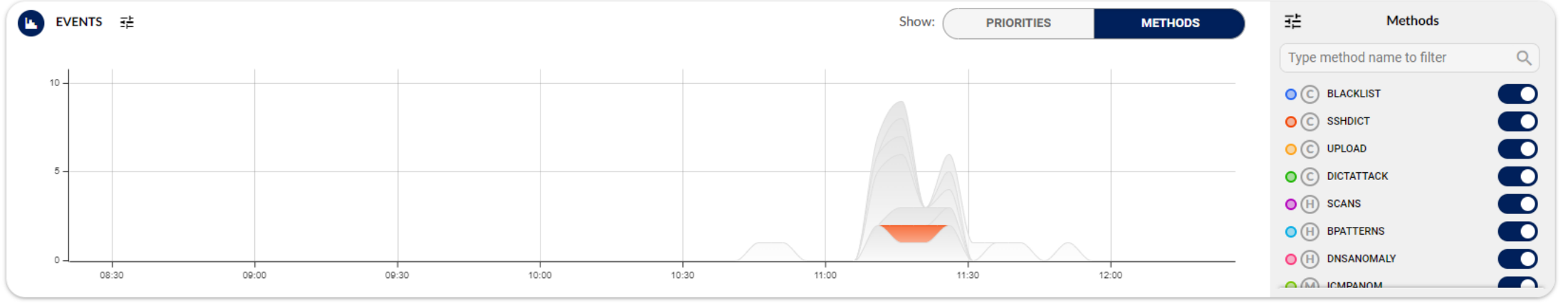


A threat actor contacted us, demanding ransom. We have one week to decide whether to pay, or they will disclose **sensitive data stolen** from our company HQ to the internet.

- Analysis
- Events
- Report Chapters
- Settings
- Logs
- About

Date: Last 4 hours | Perspective: Security issues | Data feed: - Unspecified - | Source IP: **APPLY**

FLOW processing status ✔



EVENTS BY PRIORITY Overall events count: 19

> BLACKLIST

▼ SSHDICT 1 ↑

1 events of the type SSHDICT from 1 source IP addresses detected

SOURCE IP ADDRESS	SOURCE IP FILTERS	EVENTS COUNT	RELATED EVENTS
> 192.168.255.1	ForBlacklist, LAN	1	☑ RELATED EVENTS

Showing 1 - 1 of 1

- > UPLOAD
- > DICTATTACK
- > SCANS
- > BPATTERNS

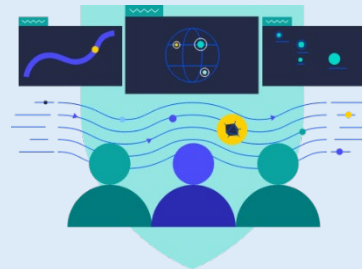
Flowmon Network Detection & Observability Platform

Progress® Flowmon® is a network and security monitoring platform with AI-based detection of cyber threats and anomalies, and fast access to actionable insights into network and application performance.

What makes Flowmon stand out

The solution supports cloud, on-prem and hybrid environments suitable for company-wide coverage, market's fastest deployment time and has been recognised by Gartner since 2010.

Security Operations



Early Detection & Warning
Threat Hunting
Incident Response
Breach Recovery

Network Operations



End-User Experience Monitoring
Troubleshooting & Forensics
Forecasting & Capacity Planning
Cloud/SaaS Performance

Think Scale

Think Hybrid

