



Jsme Progress

ale jsou věci, co se nemění

Pavel Minarik

VP, Technology

15.9.2022, Partnerské dny

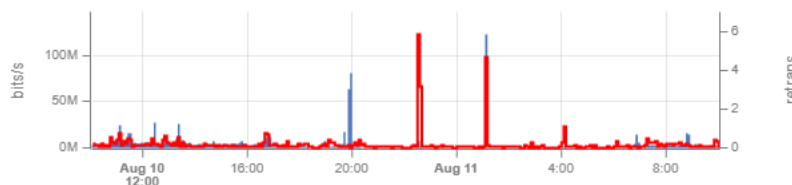


Last 24 hours (generic time span)



Structure of Overall Traffic

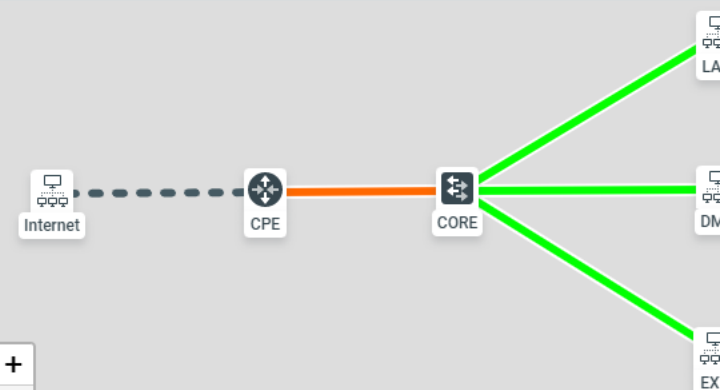
Last 24 hours (generic time span)



| Source | Maximal bits/s | Bits per second | Bytes | AVG RTR |
|-------------|----------------|-----------------|-----------|---------|
| (localhost) | 122.73 Mb/s | 3.62 Mb/s | 36.41 GiB | 0.2 |
| | 122.73 Mb/s | 3.62 Mb/s | 36.41 GiB | 0.2 |

Logical Topology

Last 24 hours (generic time span)



2022-08-10 10:03 - 2022-08-11 10:03

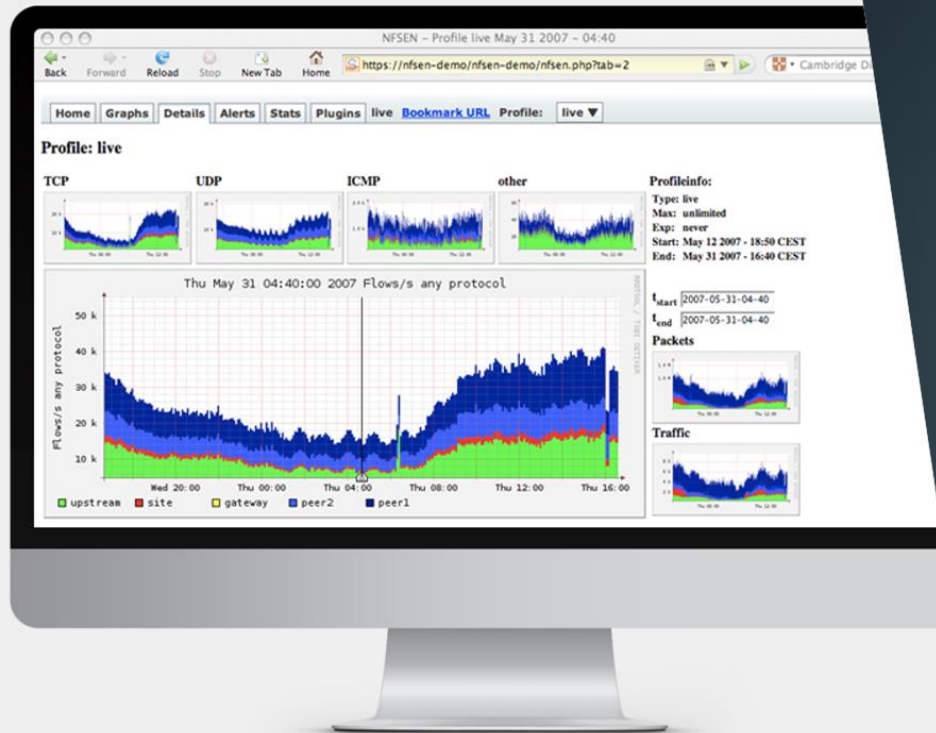
Last 24 hours (generic time span)

| Collection | Command and Control | Exfiltration | Impact |
|------------|---------------------|--------------|--------|
| | 0 | 3 | 2 |

Last 24 hours (generic time span)



Technologická a produktová vize řešení Flowmon



Transition from NetFlow & IPFIX experts



to NetSecOps Leader
providing Instant Business
Value



**FlowMon
Configuration Center**



**FlowMon
Monitoring Center**

 **inveaTECH**

Plugin3
Not installed.

 **inveaTECH**

Plugin4
Not installed.

 **inveaTECH**

Plugin5
Not installed.

 **inveaTECH**

Plugin6
Not installed.

 **inveaTECH**

Plugin7
Not installed.

 **inveaTECH**

Plugin8
Not installed.

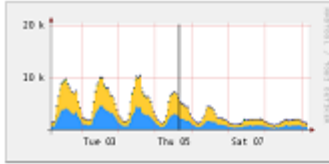
Choose the FlowMon Configuration Center to configure the FlowMon probe.
Choose FlowMon Monitoring Center to view and analyze collected IP flows.

 **inveaTECH**

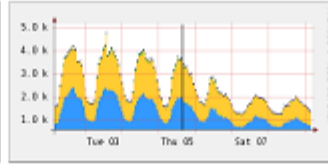
© 2007-2011 INVEA-TECH a.s. All Rights Reserved.

Profile: live

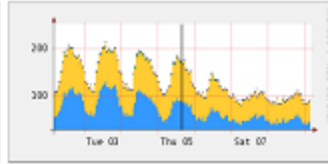
TCP



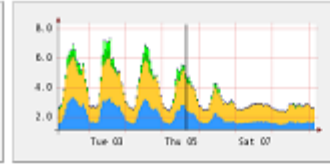
UDP



ICMP



other



Profileinfo:

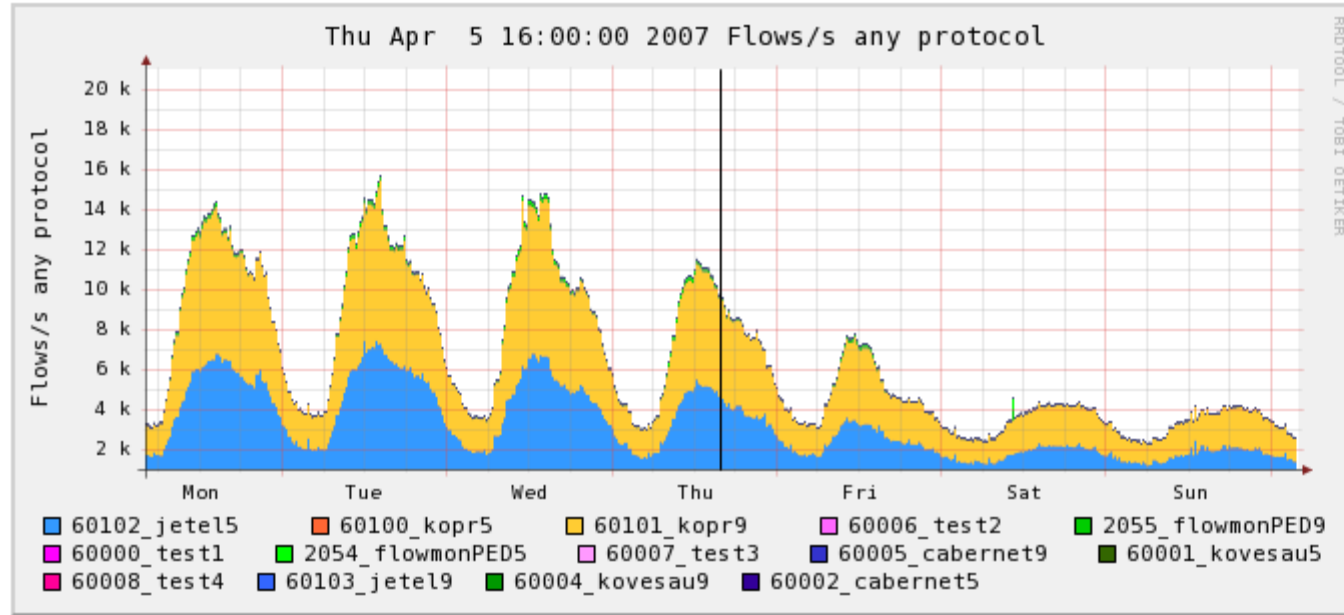
Type: continuous

Max: 1.0 TB

Exp: never

Start: Mar 07 2007 - 07:05

End: Apr 16 2007 - 15:25

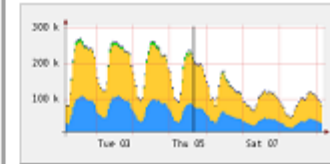


t_start 2007-04-05-16-0

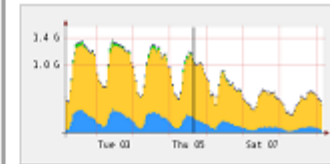
t_end 2007-04-05-16-0

Reset Timeslot

Packets



Traffic



Select left ▾ Mark

Display: 1 week ▾ << < | ^ > >> >|

Lin Scale Stacked Graph

Log Scale Line Graph

From 1 day ago To Now SET INTERVAL

- Dashboard
- Reports

DEFAULT OPERATIONAL ISSUES SECURITY EVENTS

Hosts with Top Data Transfers

| ANY IP ADDRESS | DEFAULT BYTES: INPUT |
|--|----------------------|
| 1 bizon.flowmon.com | 165.64 GIB |
| 2 89-185-224-89.static.masterinter.net | 154.15 GIB |
| 3 192.168.11.49 | 106.00 GIB |
| 4 192.168.9.20 | 101.24 GIB |
| 5 192.168.3.242 | 59.41 GIB |
| 6 192.168.70.32 | 37.66 GIB |
| 7 192.168.120.101 | 15.26 GIB |
| 8 192.168.3.84 | 12.87 GIB |
| 9 192.168.7.1 | 12.83 GIB |
| 10 192.168.11.50 | 12.03 GIB |
| Blacklisted | 0 |
| Total | 613.41 GIB |

2018-03-05 11:00 - 2018-03-06 11:00

+ NEW WIDGET

Structure of Overall Traffic

| SOURCE | MAXIMAL BITS/S | BITS PER SECOND | DEFAULT BYTES: INPUT |
|---|----------------|-----------------|----------------------|
| 1 192.168.3.84 (int-probe.br.flowmon.com) | 310.8 M | 60.2 M | 605.87 GIB |
| 2 192.168.47.21 (localhost) | 54.2 M | 2.6 M | 26.17 GIB |
| 3 127.0.0.1 (localhost) | 703.1 K | 285.1 K | 2.87 GIB |
| Total | 314.8 M | 63.1 M | 634.90 GIB |

2018-03-05 11:50 - 2018-03-06 11:50

Overview

| PRIORITY | FLows | AVERAGE FLows | BYTES | AVERAGE BYTES | PACKETS | AVERAGE PACKETS |
|----------------------|-------|---------------|---------|---------------|---------|-----------------|
| 1 High priority | 1.2 M | 13.7 | 337.0 G | 3.9 M | 334.7 M | 3.9 K |
| 2 Medium priority | 1.4 M | 16.3 | 29.7 G | 342.6 K | 29.0 M | 334.7 |
| 3 Low priority | 2.2 M | 24.8 | 232.3 G | 2.7 M | 237.0 M | 2.7 K |
| 4 Legitimate traffic | 9.1 M | 105.1 | 82.7 G | 954.1 K | 141.5 M | 1.6 K |

2018-03-05 11:50 - 2018-03-06 11:50

+ NEW WIDGET


Hosts with Top Flows

| ANY IP ADDRESS | FLows |
|-----------------------------|---------------|
| 1 192.168.11.1 | 1.9 M |
| 2 192.168.9.17 | 1.1 M |
| 3 192.168.51.253 | 891.4 K |
| 4 192.168.70.253 | 595.4 K |
| 5 192.168.3.149 | 377.5 K |
| 6 192.168.70.64 | 316.7 K |
| 7 192.168.51.132 | 306.3 K |
| 8 prg03s05-in-f14.1e100.net | 305.4 K |
| 9 192.168.120.253 | 296.9 K |
| 10 192.168.9.14 | 290.9 K |
| Blacklisted | 0 |
| Total | 13.9 M |

2018-03-05 11:00 - 2018-03-06 11:00

+ NEW WIDGET


CLast 24 hours (generic time sp... 🔍 ⚙️)



Connected flow sources:
1 of 1

2022-08-10 10:00 - 2022-08-11 10:00

SLast 24 hours (generic time sp... 🔍 ⚙️)

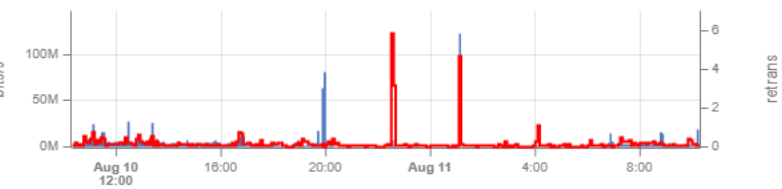


Excellent

[Show details](#)

2022-08-10 10:23 - 2022-08-11 10:23

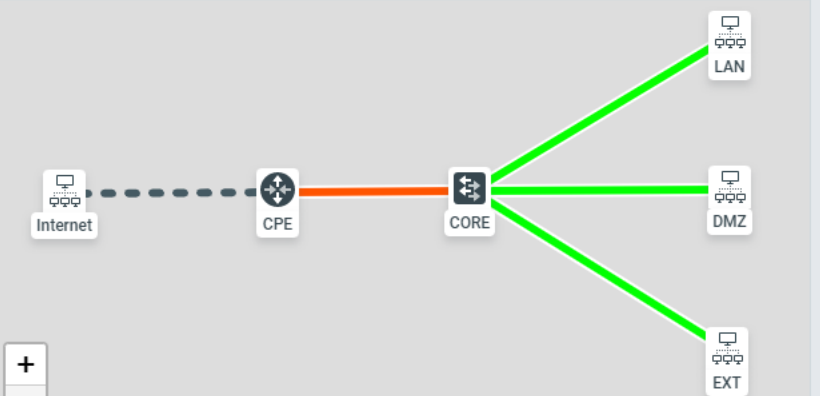
Structure of Overall Traffic Last 24 hours (generic time span) 🔍 ⚙️



| Source | Maximal bits/s | Bits per second | Bytes | AVG RTR |
|-------------------------|----------------|-----------------|-----------|---------|
| 1 127.0.0.1 (localhost) | 122.73 Mb/s | 3.68 Mb/s | 37.00 GiB | 0.2 |
| All traffic | 122.73 Mb/s | 3.68 Mb/s | 37.00 GiB | 0.2 |

2022-08-10 10:23 - 2022-08-11 10:23

Logical Topology Last 24 hours (generic time span) 🔍 ⚙️



2022-08-10 10:23 - 2022-08-11 10:23

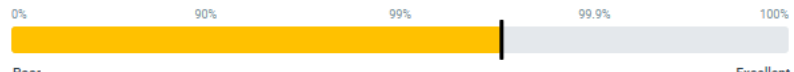
MITRE ATT&CK Matrix Last 24 hours (generic time span) 🔍 ⚙️

| Reconnaissance | Initial Access | Execution | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|----------------|----------------|-----------|-------------------|-----------|------------------|------------|---------------------|--------------|--------|
| 4 | 11 | 22 | 0 | 1 | 7 | 0 | 0 | 4 | 2 |

2022-08-10 10:23 - 2022-08-11 10:23


Structure of Overall Traffic Last 24 hours (generic time span) 🔍 ⚙️

99.7% Retransmission index



| | |
|------------------|------------------|
| AVG packets/s | AVG RTT |
| 530.6 | 34.332 ms |
| AVG SRT | AVG RTR |
| 78.243 ms | 0.2 |

Security status Last 24 hours (generic time span) 🔍 ⚙️




Critical priority events: 30

Security issues

[Show details](#)

Event overview by type Last 24 hours (generic time span) 🔍 ⚙️



| Event type | Name | Number of events |
|------------|---|------------------|
| 1 C | BLACKLIST Detection of communication with blacklisted IP addresses | 22 |
| 2 C | SSHDICT Advanced detection method revealing dictionary attacks on secured shell service | 7 |
| 3 C | DICTATTACK Detection of dictionary attacks on various protocols. | 1 |
| 4 I | SCANS Detection of TCP scans (SYN scan, FIN scan, Xmas scan, Null scan) | 4 |



actionable insights and automation

secure and transparent



time to value / ROI

digital environment



better balance

operations/tactics/strategy

people rule the network



integrating NetOps and SecOps

secure and transparent



**decentralized IT ownership
in hybrid and cloud environments**

digital environment



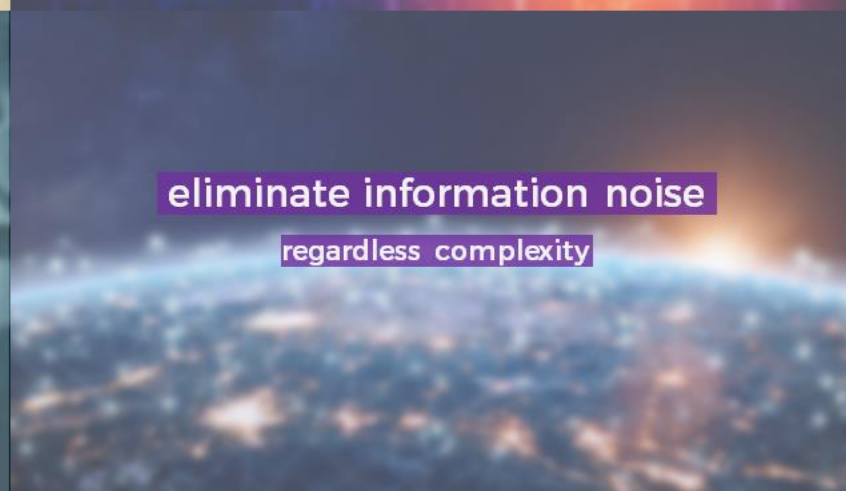
operator, analyst, expert, director

people rule the network



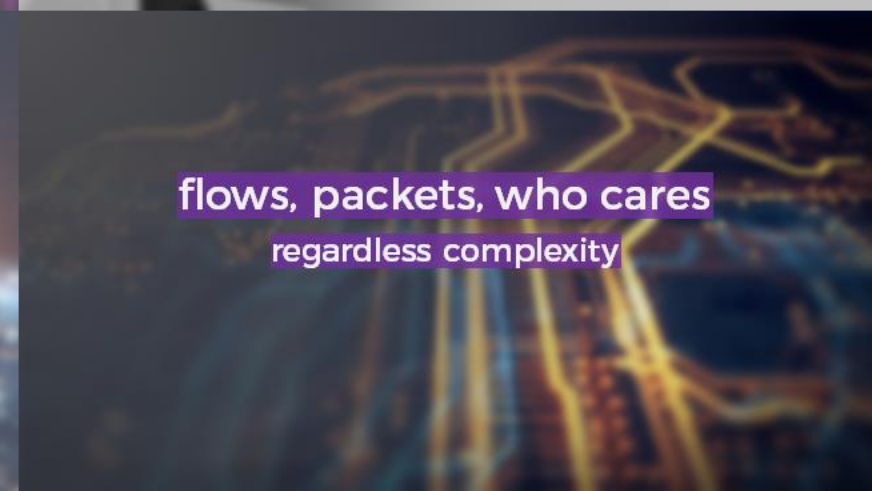
trending and prediction

secure and transparent



eliminate information noise

regardless complexity



flows, packets, who cares

regardless complexity

Flowmon in 2020

Flowmon 11: Insight at your fingertips

The dashboard overview consists of three main sections:

- Connected sources:** Last day (generic time span). Shows a network icon and the text "Connected flow sources: 3 of 3".
- All applications status:** Last day (generic time span). Shows a green cube icon and the text "Excellent" with a "Show details" link.
- Security status:** Last day (generic time span). Shows a shield icon and the text "High priority events: 8" with "Security issues" and a "Show details" link.

The "Create new dashboard" dialog box includes:

- A checked checkbox for "Choose from predefined dashboards".
- A search bar containing the text "Status".
- A dropdown menu with the following options: "Status", "NetOps", "SecOps", and "Application".
- "Create" and "Cancel" buttons at the bottom.

The user interface shows a top navigation bar with "Notifications 7", "English", and "admin Base tenant". The main content area features a sidebar with "Modules", "Tenants", and "admin" (with a user icon). The "Tenants" section is expanded, showing a list with "Base tenant" and "Base tenant/Tenant A". A "Log out" button is visible at the bottom left of the main content area.

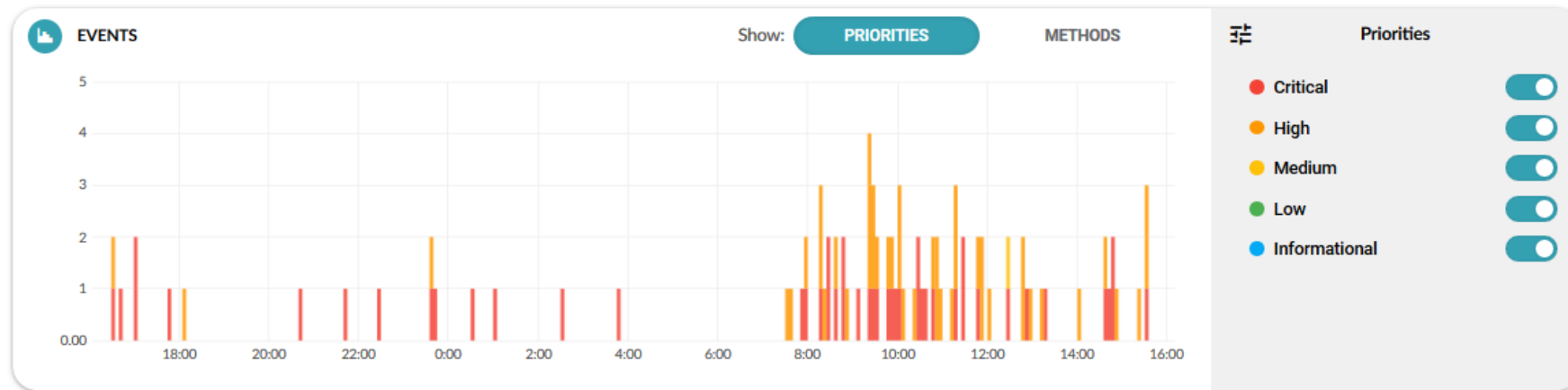


With the data from Flowmon, we can immediately move to resolve performance issues and make sure that degradations don't hinder our ability to deliver high-quality parts to our customers.”

Massimo Petrini
Factory manager



Flowmon ADS 11: Situational awareness

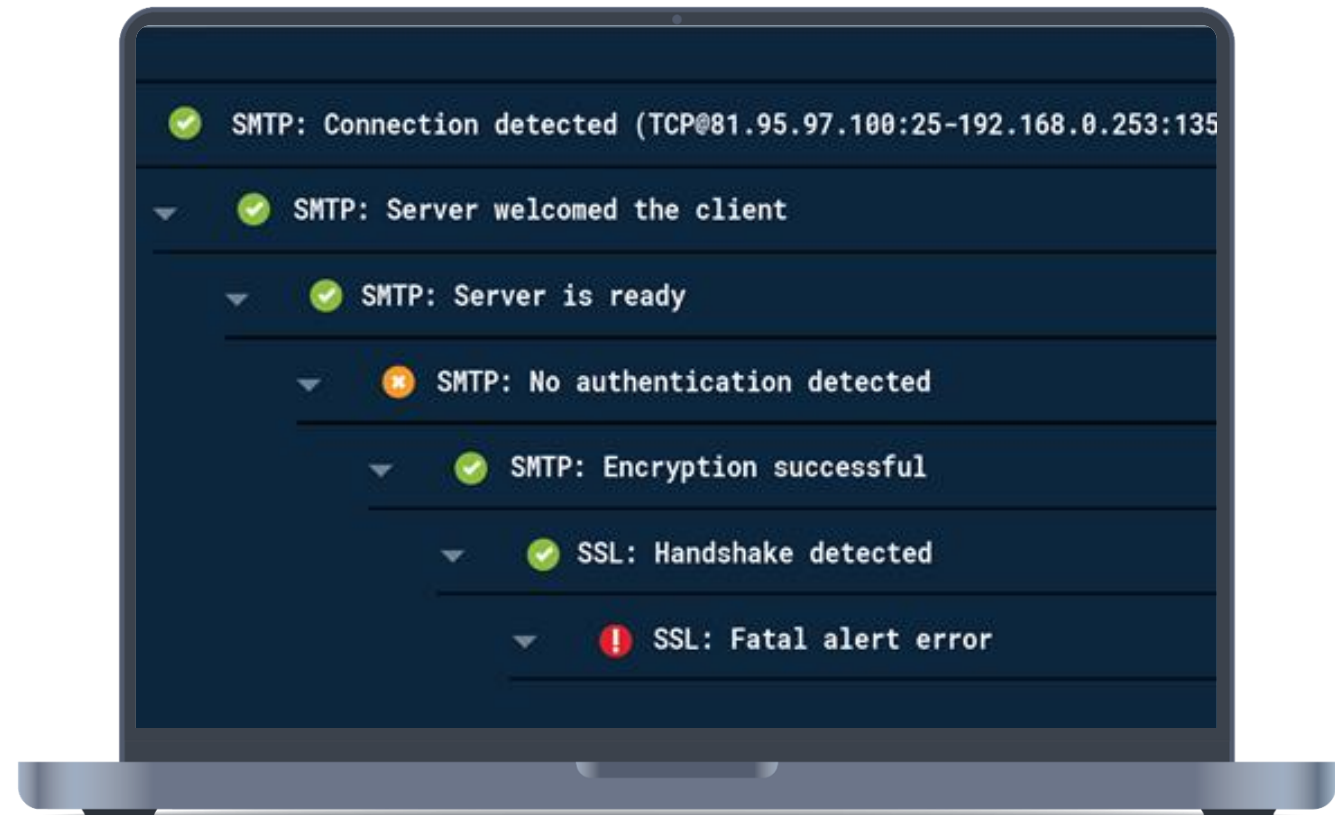


EVENTS BY PRIORITY 2020-02-12 16:05 - 2020-02-13 16:10 Overall events count: 92

| Priority | Event Type | Description | Count | Change |
|----------|------------|--------------------------------------|-------|----------|
| Critical | BLACKLIST | Communication with blacklisted hosts | 45 | +40.62 % |
| Critical | UPLOAD | Data upload anomaly | 2 | -50 % |
| High | DNSANOMALY | DNS traffic anomaly | 35 | |
| High | BPATTERNS | Flow-based behavior patterns | 8 | +60 % |
| High | ALIENDEV | New or alien device | 1 | |
| Medium | PEERS | PEERS method | 1 | |

Flowmon Packet Investigator introduced

- Augment flow-based monitoring with on-demand packet capture and analysis when required
- Built-in expertise and knowledge to automate root cause analysis and troubleshooting





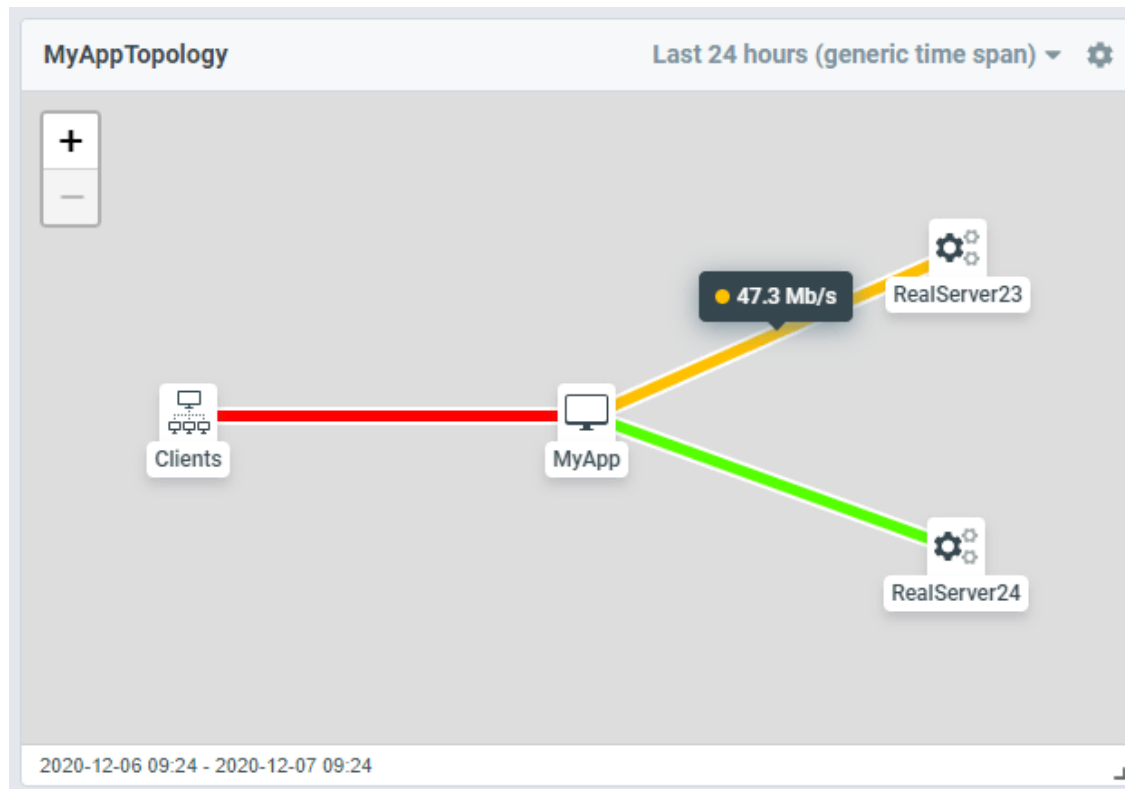
Flowmon Packet Investigator helps us to automate troubleshooting, which means we can spend less time in Wireshark PCAPs. Instead of going through packets manually, we know immediately what kind of issue we are dealing with and what the root cause is. Because we don't need deep knowledge of network protocols to use it, packet analysis is made available to every member of our IT team."

Jan Kovarik
IT Center Coordinator



Flowmon in 2021 (part of Kemp Technologies)

Flowmon 11: Visualize, cooperate and share



Edit dashboards

My dashboards

| Name | Status | Predefined |
|--------------------|---------|------------|
| Status | Private | |
| NetOps | Shared | |
| DHCP (All Sources) | Private | ✓ |

Hidden dashboards

There are no hidden dashboards

Dashboard layout

Default Comfortable Compact

Create new dashboard



Flowmon gives KBC with its flow-based Network Performance Monitoring tool a great overview of the dataflow metrics in the network so that the network health can be easily assessed. In case of an issue the tool allows very fast and efficient troubleshooting by visualize the traffic that is causing the problem.”

Marc Daemen

Senior System Engineer



Flowmon ADS 11: Custom threat intelligence

Edit remote blacklist ×

Blacklist name

Description
The description field is optional and its value is used in the BLACKLIST event detail. If it is not provided, the name of the blacklist is used in the detail instead.

Assigned instances Default2 × Default × ▼

Type of blacklist
 CSV
Blacklist entries specified by CSV file
 MISP
Open source threat intelligence platform and open standards for threat information sharing

Remote URL

API key

Maximum days of valid records

Include records only for Intrusion Detection System

SAVE **CLOSE**

Flowmon ADS 11: MITRE ATT&CK framework

Dashboard Reports Configuration

MITRE ATT&CK SecOps +

MITRE ATT&CK Matrix Last 2 hours (generic time span) ⌵ ⚙

| Reconnaissance | Initial Access | Execution | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|----------------------|------------------------------|--------------------|-------------------|-------------------------------|-------------------------------------|------------------------------------|--------------------------------|--|---------------------------------|
| 12 | 0 | 0 | 0 | 12 | 5 | 0 | 2 | 3 | 16 |
| Active Scanning (12) | Drive-by Compromise (0) | User Execution (0) | Brute Force (0) | Network Service Scanning (12) | Exploitation of Remote Services (0) | Audio Capture (0) | Application Layer Protocol (2) | Automated Exfiltration (2) | Data Encrypted for Impact (0) |
| | External Remote Services (0) | | | Network Share Discovery (0) | Lateral Tool Transfer (5) | Data from Network Shared Drive (0) | Encrypted Channel (0) | Exfiltration Over Alternative Protocol (1) | Endpoint Denial of Service (14) |
| | Hardware Additions (0) | | | Remote System Discovery (12) | Remote Services (0) | Man-in-the-Middle (0) | Ingress Tool Transfer (0) | | Network Denial of Service (2) |
| | | | | | | | Protocol Tunneling (0) | | Service Stop (0) |
| | | | | | | | Proxy (0) | | |
| | | | | | | | Remote Access Software (0) | | |

2021-05-04 09:04 - 2021-05-04 11:04



Thanks to Flowmon ADS, we are able to reveal threats and malicious behavior within the internal network. And what is the most important experience - we have significantly reduced incident resolution times for both operational and security incidents."

Vittorio Cimin
CIO



Flowmon in 2022 (in Progress)

Flowmon 12: Multi-cloud network visibility

Native mirroring

- Functionality of the cloud platform to copy packets from virtual interfaces to monitoring appliances deployed in the cloud



Flow logs

- Traffic statistics generated in form of logs by the cloud platform as such
- Contain information similar to NetFlow v5



Google Cloud

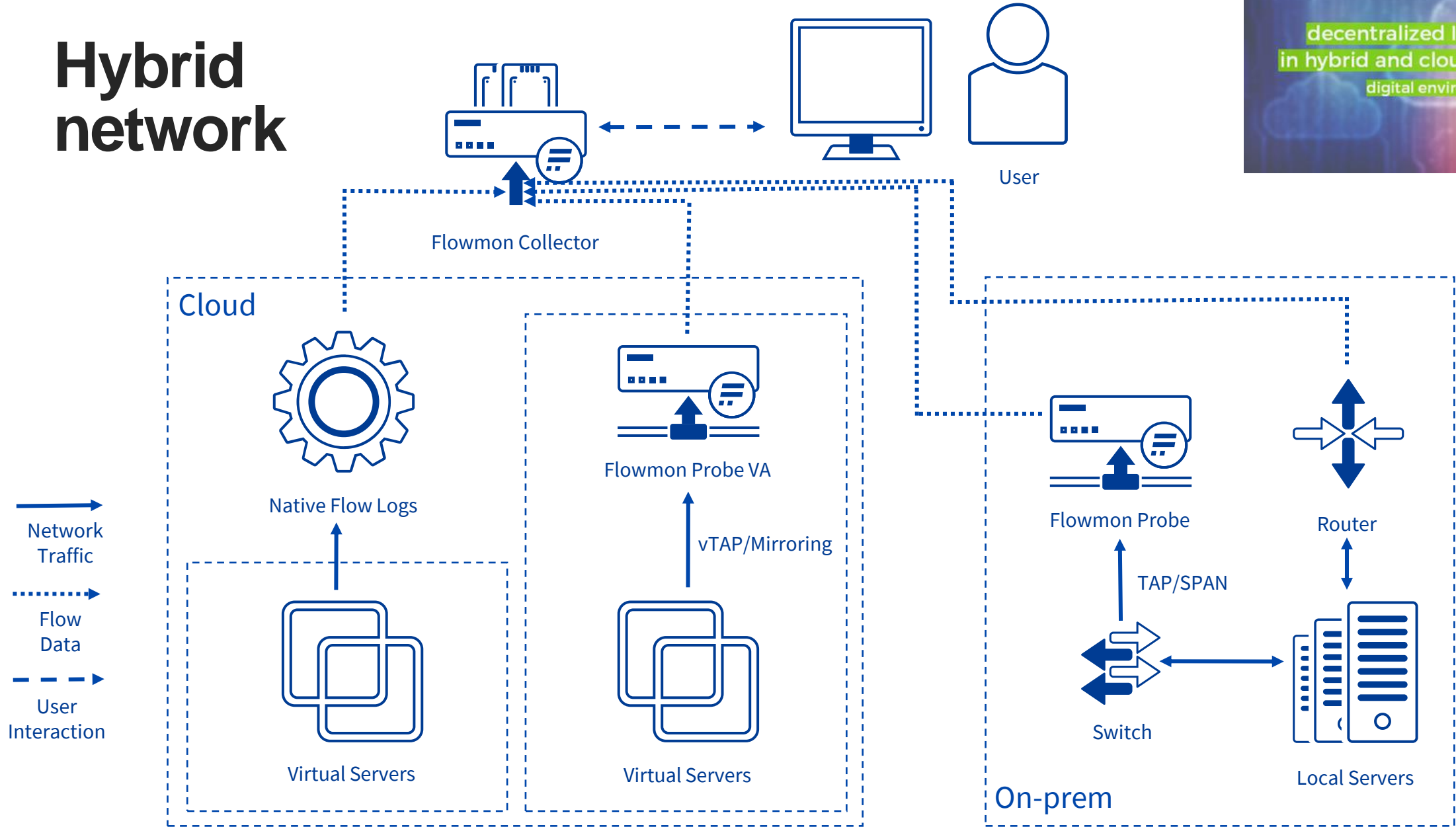


3rd party agents

- Software components installed on virtual machines to provide a copy of the traffic through tunnel
- Additional complexity, no longer passive



Hybrid network



Flowmon ADS 12: AI against cyber threats

Event #48745

Type Random domain name (RANDOMDOMAIN)
Subtype General
Reports the usage of randomly generated domain names. This kind of domain name is used to access to randomly generated domains.

Detail Access to randomly generated domains was detected. Domains: eqc49

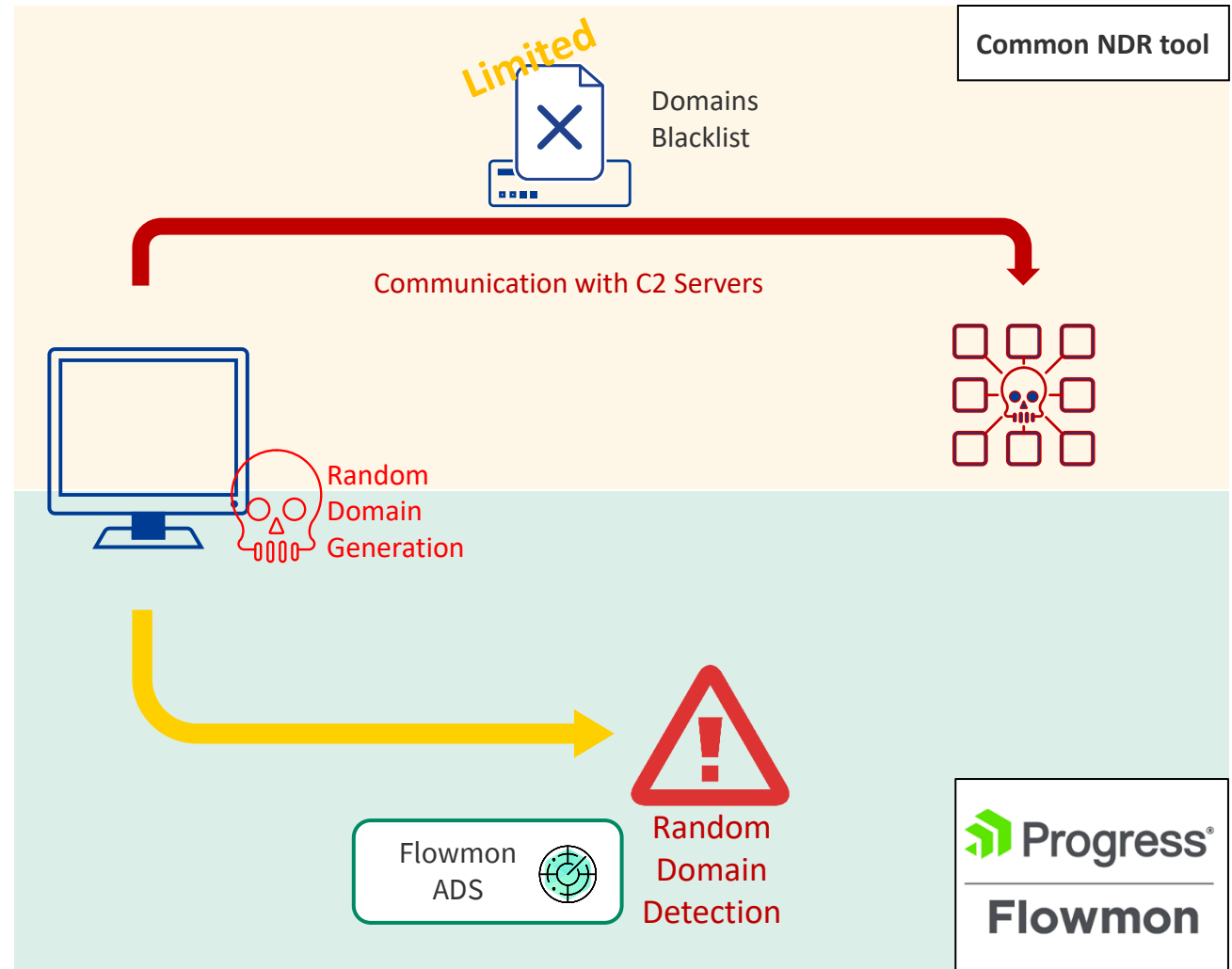
MITRE ATT&CK **Tactic** Command and Control >> **Technique** Dynamic Resolution

| | | | |
|-----------------------|---------------------|---------------------------------|--|
| Detection time | 2022-02-24 11:34:19 | Event source | |
| Last update | 2022-02-24 11:34:19 | Captured source hostname | |
| First flow | 2022-02-24 11:33:47 | MAC address | |
| | | User identity | |

TARGETS (1) COMMENTS (0) CATEGORIES (0) ATTRIBUTES EVENT

ALL IP ADDRESSES BY COUNTRY BY IP

51.254 (unknown) -



Specifikace



Flowmon ADS Models Specification

PDF, 567,8KB



Flowmon APM Models Specification

PDF, 557,7KB



Flowmon Collector Models Specification



Flowmon Compatibility Sheet

PDF, 229,1KB



Flowmon Architecture Overview



Flowmon Packet Investigator Models Specification

PDF, 556,3KB



Kolektor data retention

PDF, 235,5KB



PRIVATE

WhatsUp Gold and Flowmon CVP

Member

Weekly Digest



Zpětná vazba zákazníků a partnerů

MANAGEMENT

like to know?

Ask

Members (3+)



[Jason Alberino](#)



[Nichol Goldstei](#)



[Oleg Kupershm](#)

[View All](#)

Records (0)

Files (3+)

Terms

127KB • pdf

Event_Logs_Cheat_S...

[View All](#)

Kemp Support, how can we help?

The latest application delivery knowledge and expertise at your fingertips.

Search



Excelentní technická podpora

Master GEO

Multi-Tenant LoadMaster

Flowmon

Flowmon APM

Flowmon DDoS Defender

Kemp Support, how can we help?

The latest application delivery knowledge and expertise at your fingertips.



[Kemp Support](#) > [Submit a request](#)

My Activities

Requests

Contributions

Following

Please Select Your Product From the Drop-Down Below

Flowmon

CC(optional)

Add emails

Subject

Description

Please enter the details of your request. A member of our support staff will respond as soon as possible.

Geographical Location

EMEA

To help us direct your request to the correct team please select your geographical location from the list above.

Inquiry Type

Troubleshooting

Please indicate what type of inquiry the ticket is concerning.

Attachments(optional)

Flowmon > Spolupráce mezi NetOps a SecOps

Spolupráce NetOps a SecOps pro zdravější síť

Bezpečnostní oddělení má i přes zdánlivě rozdílné priority jeden společný cíl – zdravé a stabilní síť. Pokud odstraníte vzájemné bariéry, spolupráce mezi oběma týmy bude efektivnější, méně riskantní a nákladově efektivnější.



Maximalizace hodnoty integrací produktů

VYZKOUŠET TRIAL



Home

- Virtual Services
- Global Balancing
- Statistics
- Real Servers
- Rules & Checking
- Certificates & Security
- Web Application Firewall
- System Configuration

Network Telemetry

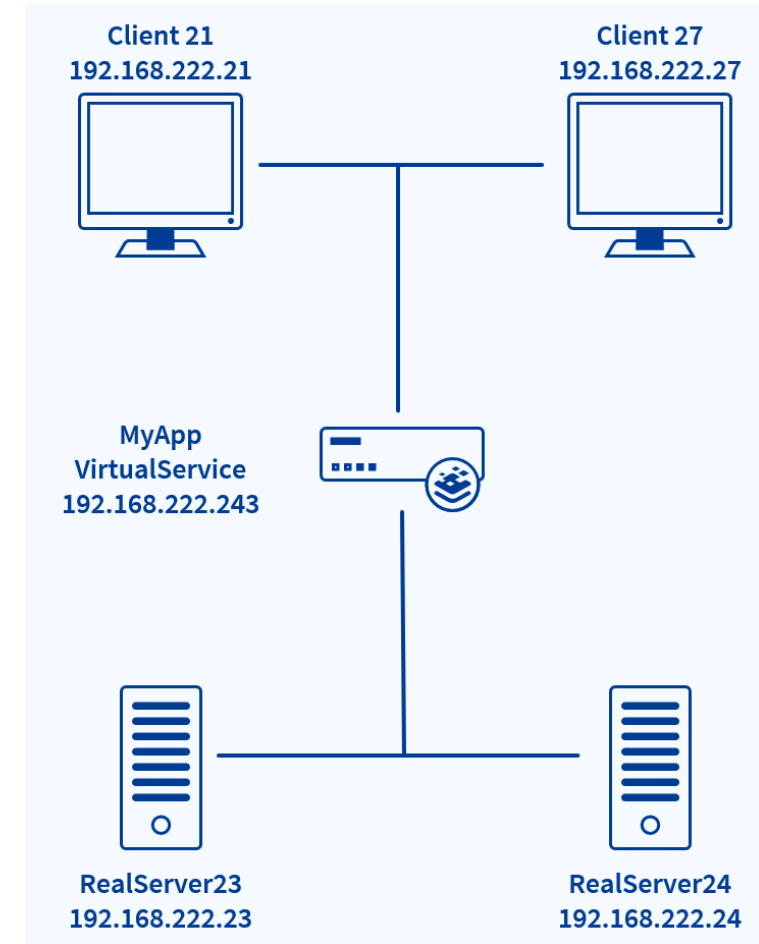
Help

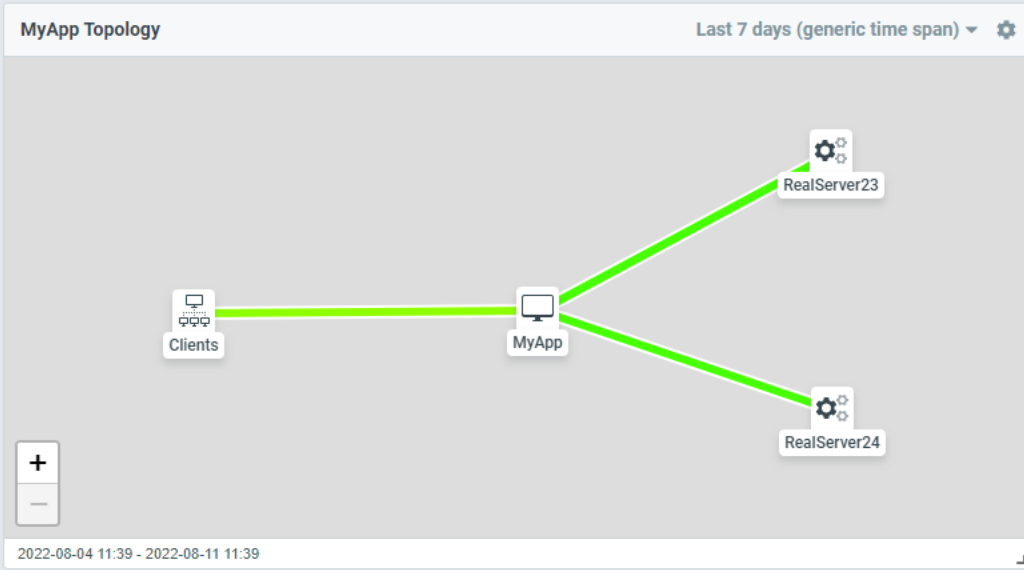
Network Telemetry requires the Kemp Flowmon Collector to collect the NetFlow / IPFIX application flow data. The Kemp Flowmon Collector is available here.

[Download Flowmon Collector](#)

Once the Kemp Flowmon Collector is installed and running, enter the connection details and select the relevant interfaces to enable this integration.

| Connection Details | | | | | | | |
|--|--|---|--|-------------------------------------|------|--------------------------|------|
| Collector Endpoint | <input type="text" value="192.168.222.242"/> Set Remote Address Validate | | | | | | |
| Global Settings | | | | | | | |
| Active Timeout | <input type="text" value="300"/> Set Active Timeout | | | | | | |
| Inactive Timeout | <input type="text" value="30"/> Set Inactive Timeout | | | | | | |
| Export Protocol | | | | | | | |
| NetFlow v9 | <input type="radio"/> | | | | | | |
| IPFIX | <input checked="" type="radio"/> | | | | | | |
| Advanced Settings | | | | | | | |
| Layer 2 values | Layer 3/4 values | Layer 7 values | | | | | |
| <input checked="" type="checkbox"/> ARP | <input checked="" type="checkbox"/> NPM | <input checked="" type="checkbox"/> DHCP | <input checked="" type="checkbox"/> VoIP (SIP) | | | | |
| <input type="checkbox"/> MAC | <input checked="" type="checkbox"/> Extended NPM | <input checked="" type="checkbox"/> DNS | <input checked="" type="checkbox"/> MSSQL | | | | |
| <input type="checkbox"/> VLAN | <input type="checkbox"/> L3/L4 extended | <input checked="" type="checkbox"/> HTTP | <input checked="" type="checkbox"/> PostgreSQL | | | | |
| | | <input checked="" type="checkbox"/> Email | <input checked="" type="checkbox"/> MySQL | | | | |
| | | <input checked="" type="checkbox"/> NBAR2 | <input checked="" type="checkbox"/> TLS | | | | |
| | | <input checked="" type="checkbox"/> Samba | | | | | |
| Activate Export of Application Flow Data Per Interface | | | | | | | |
| | <table border="1"><thead><tr><th colspan="2">Interface</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>eth0</td></tr><tr><td><input type="checkbox"/></td><td>eth1</td></tr></tbody></table> | Interface | | <input checked="" type="checkbox"/> | eth0 | <input type="checkbox"/> | eth1 |
| Interface | | | | | | | |
| <input checked="" type="checkbox"/> | eth0 | | | | | | |
| <input type="checkbox"/> | eth1 | | | | | | |





ViLast 7 days (generic time span) [Search] [Settings]

99.9% Retransmission index

0% 90% 99% 99.9% 100%

Poor Excellent

Bits per second
11.2 M

AVG packets/s
1.2 K

AVG RTT
0.679 ms

AVG SRT
3.144 ms

ReLast 7 days (generic time span) [Search] [Settings]

99.9% Retransmission index

0% 90% 99% 99.9% 100%

Poor Excellent

Bits per second
5.5 M

AVG packets/s
480.2

AVG RTT
0.291 ms

AVG SRT
1.359 ms

ReLast 7 days (generic time span) [Search] [Settings]

99.9% Retransmission index

0% 90% 99% 99.9% 100%

Poor Excellent

Bits per second
5.5 M

AVG packets/s
475.6

AVG RTT
0.279 ms

AVG SRT
1.433 ms

MyAppClients

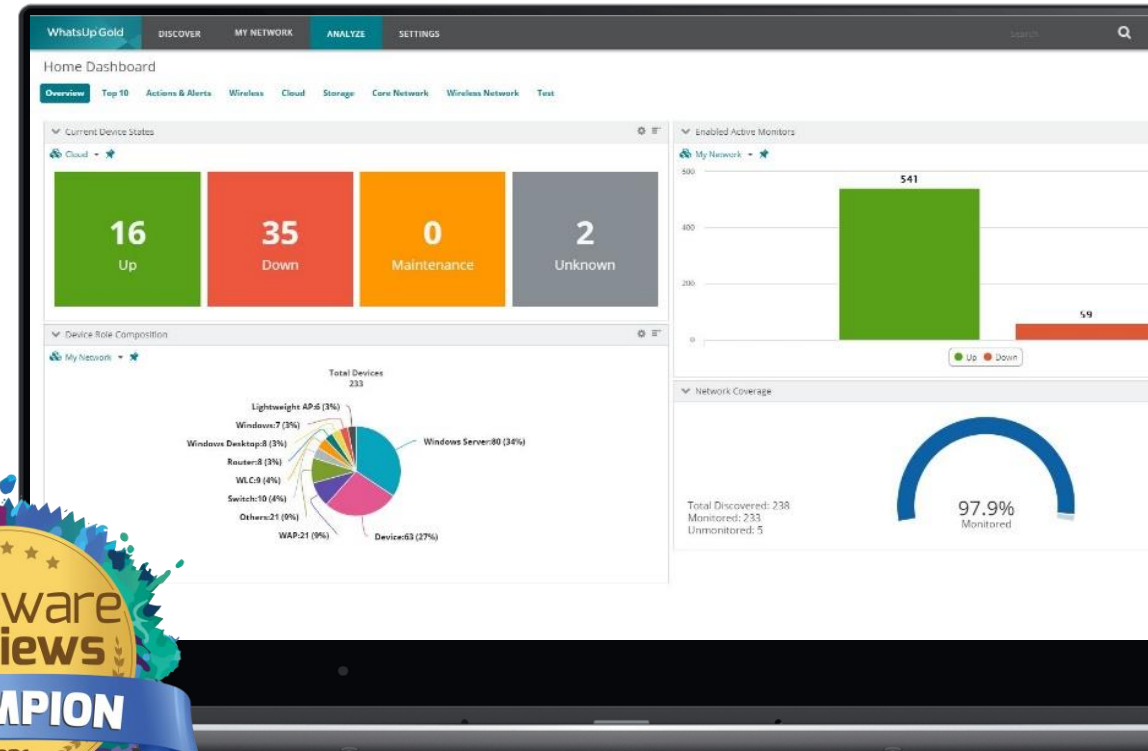
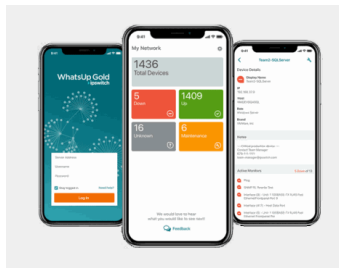
Last 7 days (generic time span) [Search] [Settings]

| Any IP address | Flows | Input packets | AVG RTT | AVG SRT | AVG RTR | Bytes |
|-------------------|----------|---------------|----------|----------|---------|------------|
| 1 192.168.222.243 | 3.41 M | 709.98 M | 0.677 ms | 3.143 ms | 0.0 | 788.31 GiB |
| 2 192.168.222.21 | 2.43 M | 512.21 M | 0.55 ms | 3.128 ms | 0.0 | 563.09 GiB |
| 3 192.168.222.27 | 974.48 K | 197.77 M | 0.996 ms | 3.18 ms | 0.0 | 225.22 GiB |
| 4 RealServer24 | 48 | 48 | 0 ms | 0 ms | 0 | 3.50 KiB |
| 5 192.168.222.50 | 3 | 3 | 0 ms | 0 ms | 0 | 134 B |
| 6 192.168.222.57 | 3 | 3 | 0 ms | 0 ms | 0 | 134 B |
| All traffic | 3.41 M | 709.98 M | 0.678 ms | 3.144 ms | 0.0 | 788.31 GiB |

WhatsUp Gold

Award-winning Network Availability and Performance At-a-Glance

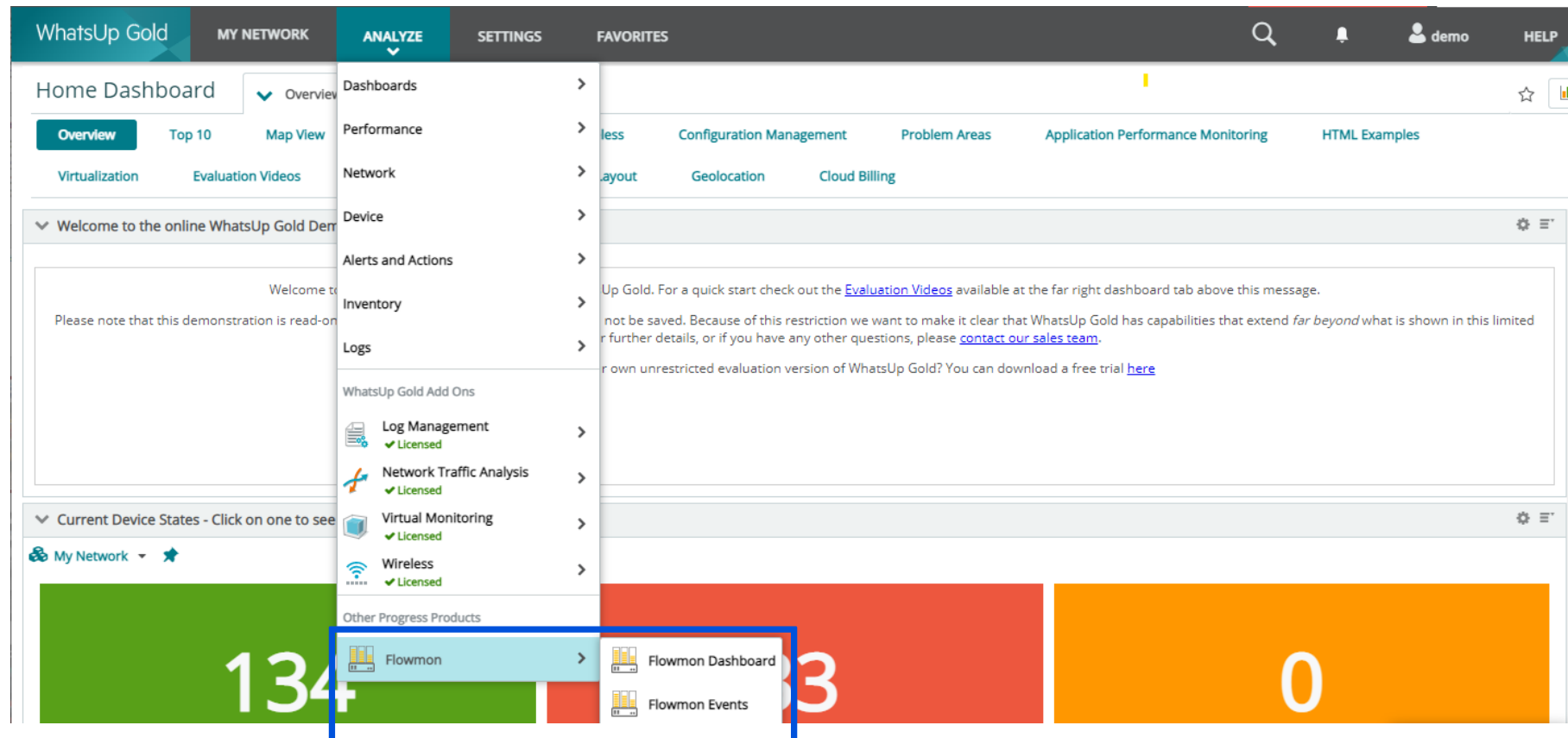
- See network status (what's up, what's down) at-a-glance
- Monitor everything connected to your network in context via a single, intuitive user interface
- Alert IT teams to network issues and **proactively find and fix problems fast**



 Progress® WhatsUp® Gold

Flowmon NPMD/NDR Within WhatsUp Gold

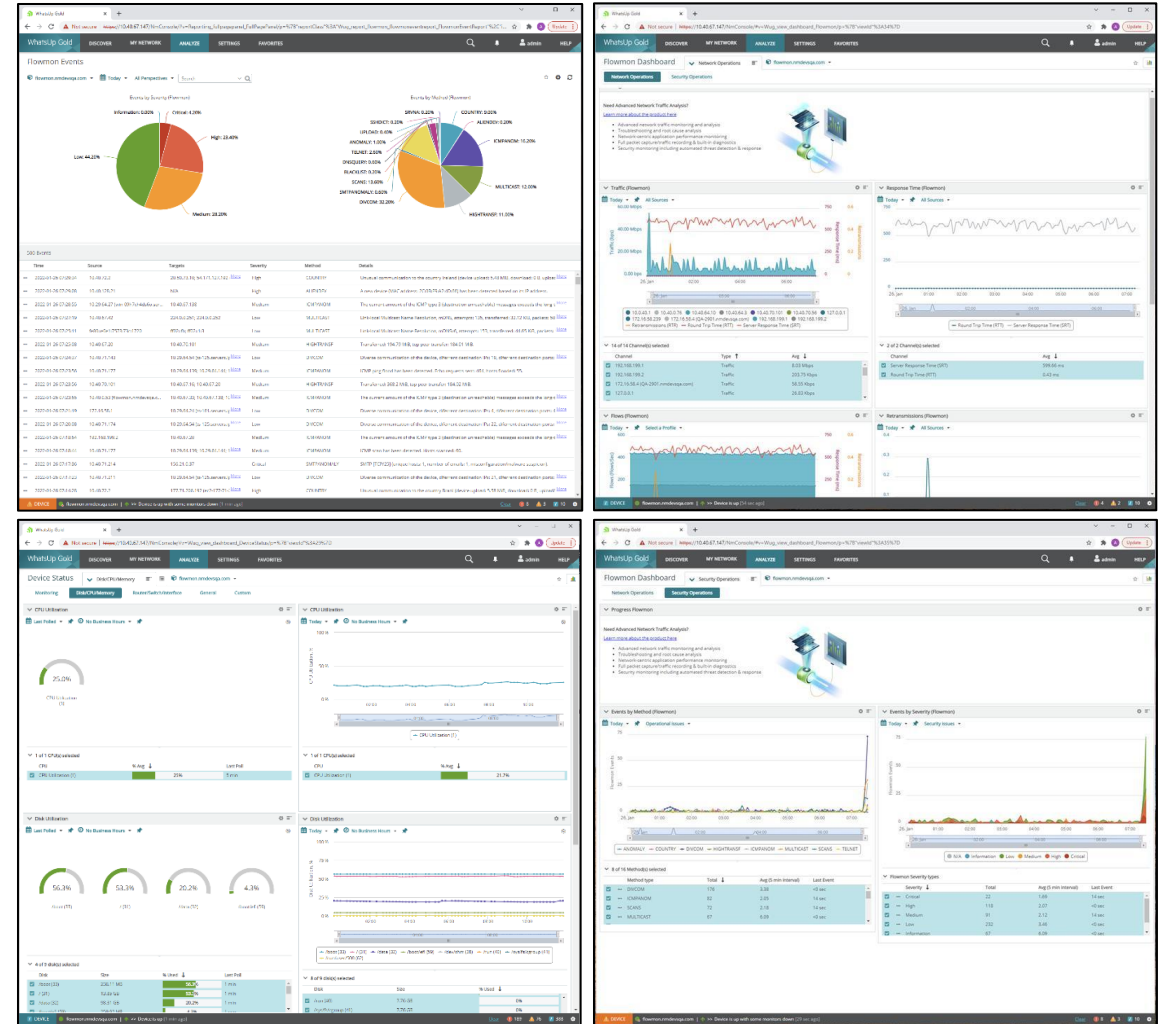
Display data from Flowmon's advanced network performance and traffic analysis solution – including network security detection and response capabilities – via the **Integrated Flowmon Dashboards** within WhatsUp Gold interface.



The Benefits of WhatsUp Gold & Flowmon

Add powerful new traffic analysis and security capabilities to WhatsUp Gold through Flowmon dashboards.

- **Convenience:** Gain access to advanced network traffic analysis while monitoring network issues
- **Speed:** Diagnose traffic issues faster and reduce MTTR through multiple views of network infrastructure, applications and traffic
- **Security:** Analyze encrypted traffic and detect ransomware insider threats and unusual behavior via Flowmon's more detailed traffic analysis





Flowmon Roadmap

As of September 2022

Disclaimer

All roadmaps are for informational purposes only, and the reader is hereby cautioned that actual product development may vary significantly from roadmaps

These roadmaps may not be interpreted as any commitment on behalf of Progress, and future development, timing and release of any features or functionality described in the roadmaps remains at our sole discretion

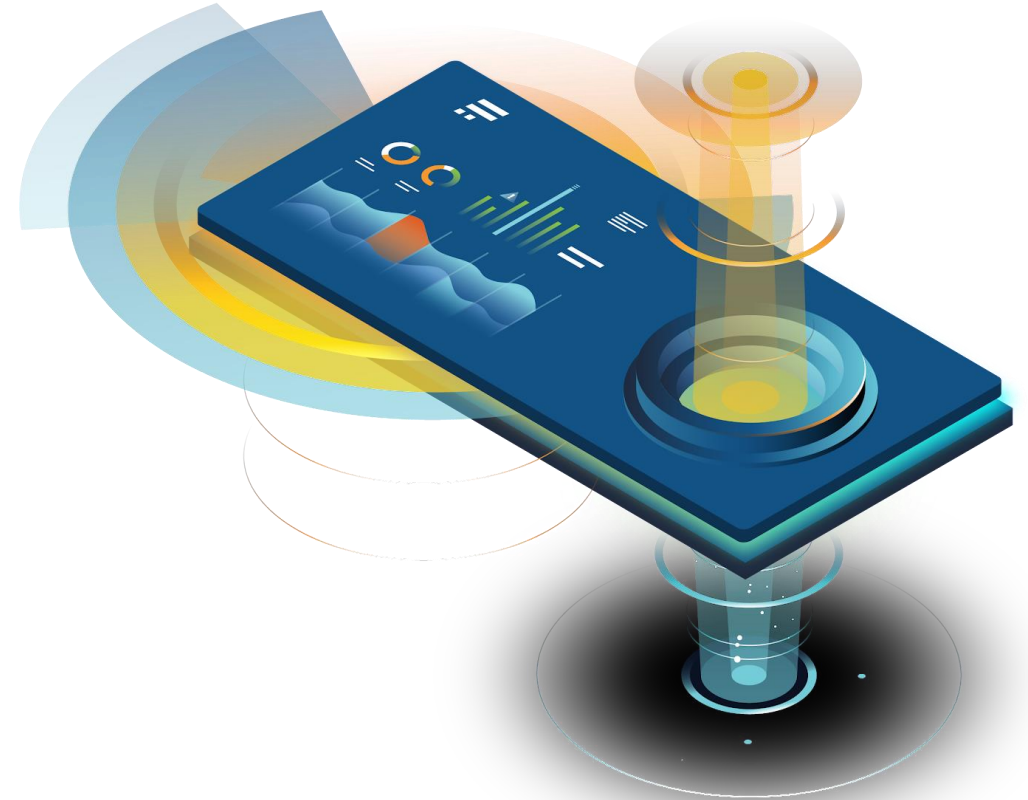
Flowmon 12.2 – est. Q1/2023

Flowmon 12.2

Focus on resiliency and stability of distributed architecture

Security improvements – in Flowmon solution and in the software delivery process too

Logging solution improvements for better supportability



Flowmon 13.0 – est. Q4/2023

Flowmon 13.0

New collector backend engine with native IPFIX support and 2x-7x performance gain

Prediction and trending on volumetric data and network performance metrics

Improved user documentation and way how it is available



Flowmon 13.0 – New Collector engine

New collector backend engine

- Completely new collector backend engine respects the most modern trends and will bring higher performance (est. 2x – 7x) by usage of massive parallelization and lot of other improvements
- Flexible design allows us to easily support various IPFIX flow items useful for different monitoring use-cases



Flowmon 13.0 – Prediction & trending

Prediction and trending

- Information about current and past situations in the network is not enough any more
- Predicting the future allows IT professionals to react proactively and to be prepared
- Predictions and trends will be available for both volumetric data and network performance metrics
- This will proactively help with situations like upcoming link saturation or gradual SLA degradations

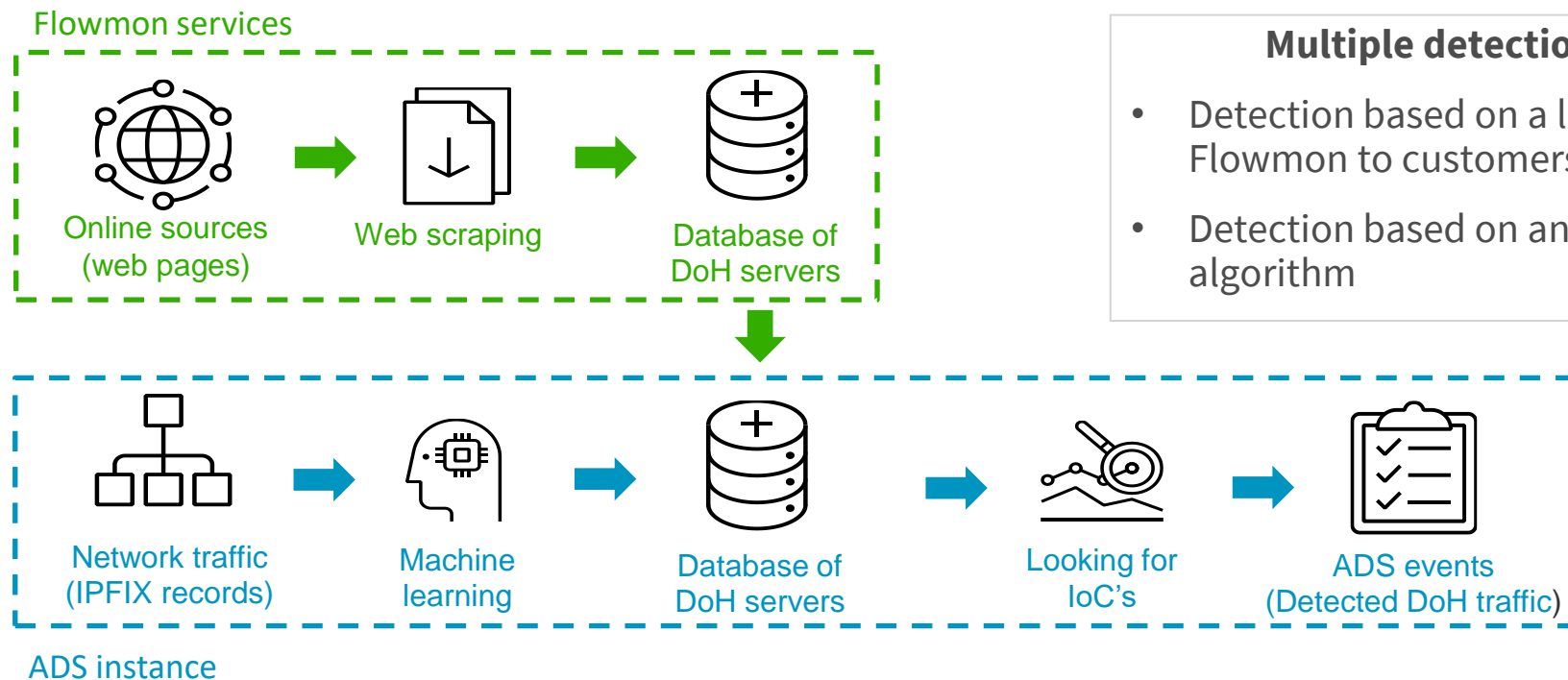


Flowmon ADS 12.1 – est. Q1/2023

Encrypted Traffic Analysis

Our new detection methods will uncover encrypted DNS servers attempting to hide from network monitoring tools

- **Detection of DNS over HTTPS (DoH)**



Multiple detection techniques

- Detection based on a list of IoCs provided by Flowmon to customers via services portal
- Detection based on an ML-based detection algorithm

Flowmon ADS 12.2 – est. Q2/2022

Initial multitenancy

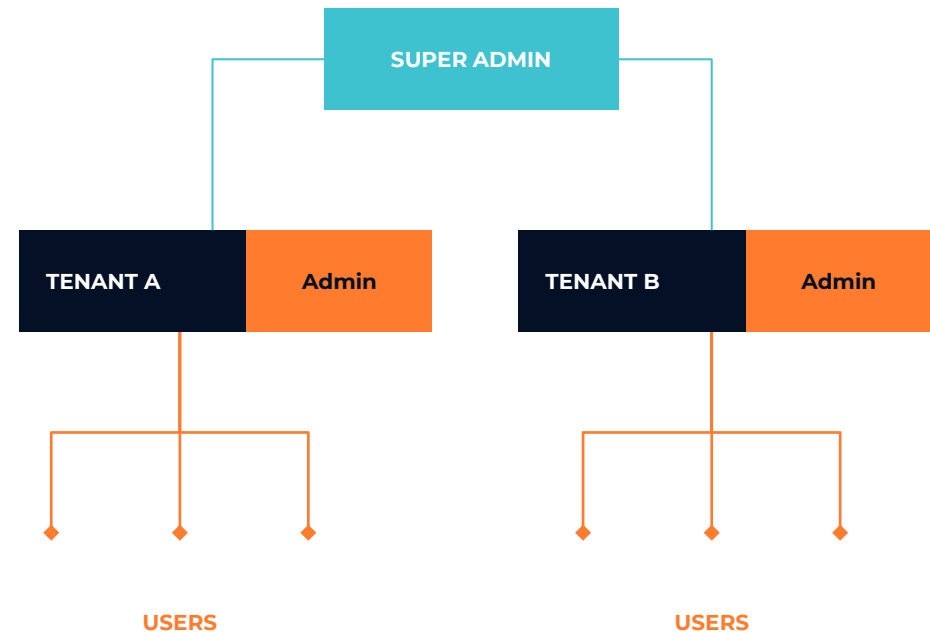
Initial multitenancy support

The First step for the MSP level multitenancy (support for Flowmon multitenancy)

- One shared appliance providing independent data spaces
- New admin layer of Tenant Admin to address per tenant user/role management

Initial ADS multitenancy support will not include several features available with Flowmon multitenancy, some options will only be available to a super admin user. (e.g., some configuration options)

Remaining features will be delivered in following version – ADS 13.0



Flowmon ADS 13.0 – est. Q4/2023

Flowmon ADS 13.0

Full multitenancy support

Anomaly detection for ICS/SCADA environments with a new set of detection methods

Improved detection accuracy and proxy correlation by adopting a new collector backend engine



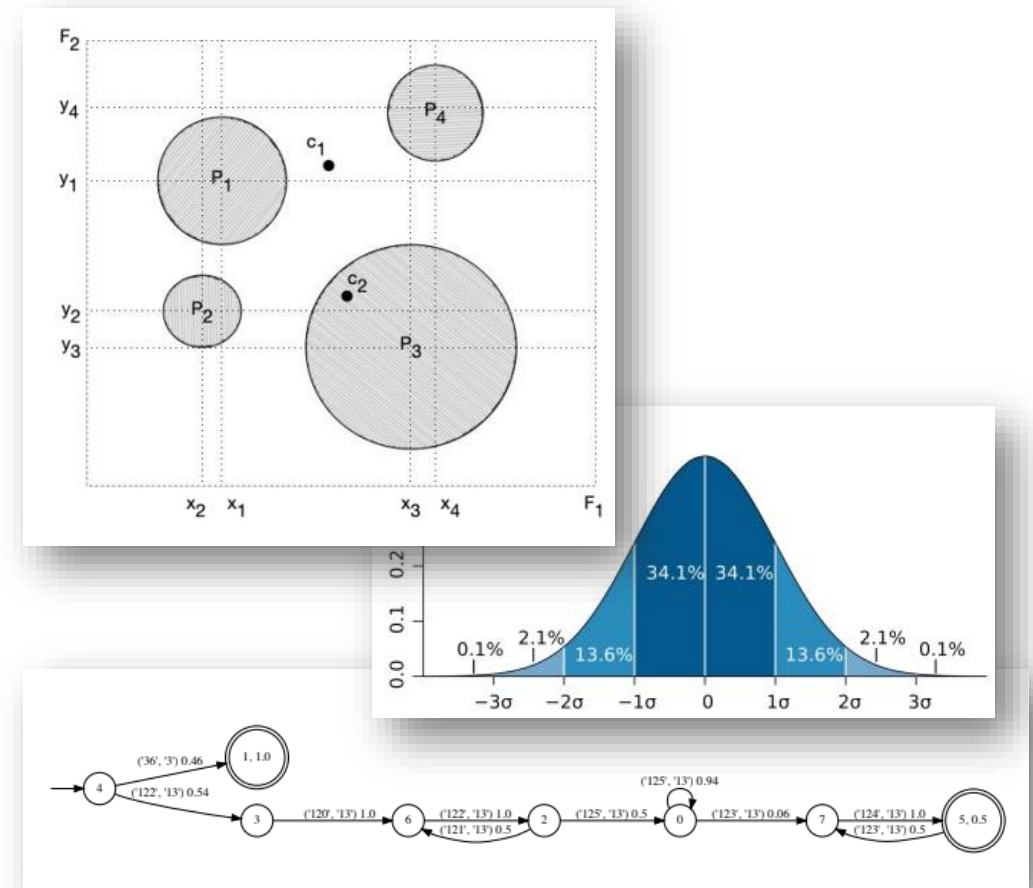
Flowmon ADS 13.0 – Security of ICS/SCADA

Anomaly detection for ICS/SCADA

Brand new methods for the detection of anomalies within various ICS/SCADA protocols including:

- MODBUS
- DNP3
- IEC104
- Goose

Anomaly detection based on clustering algorithms, probabilistic automata and statistical models



Flowmon ADS 13.0 – New backend adoption

New collector engine support

ADS support of the new Collector engine

Improved detection accuracy by reimplementing ADS preprocessing to the new collector engine

- More precise flow pairing, and deduplication
- More precise proxy correlation



Flowmon Asset Model for Configuration (teaser)

The screenshot displays the Flowmon web interface. The top navigation bar includes 'Dashboard', 'Reports', 'Incidents', 'Analysis', 'Users', 'Assets', and 'Configuration'. The user 'John Flowmon' is logged in. The left sidebar shows the 'Asset structure' with a tree view: All Sites > Nagano > DC > Datacenter > SAP > Flowmon > Web GUI, Service #1, Service #2. The main content area shows the 'Flowmon' asset structure with a table of assets:

| Name | Description | Tags | Modified |
|------------|---|----------------------|------------------|
| Web GUI | This asset serves as a primary service for Flowmon We... | Web, Brno, Marketing | 1 minute ago |
| Service #1 | Lorem ipsum dolor sit amet, consectetur adipiscing elit... | Database, Brno | 01/02/2020 08:20 |
| Service #2 | Aenean dictum nulla ligula, eu fringilla ipsum sodales n... | Database, Brno | 01/02/2020 13:30 |

The right-hand panel shows details for the 'Web GUI' asset:

- Type: Service
- Asset full name: Flowmon Web GUI
- Description: This asset serves as a primary service for Flowmon Web GUI framework and components. Lorem ipsum dolor sit amet, consectetur adipiscing elit.
- Parent asset: Flowmon (host)
- Asset filter: Any
- SrcFilter: -
- DstFilter: -
- Contacts: jan.pazdera@flowmon.com
- Views: All Traffic (In Traffic and Out Traffic are disabled because SrcFilter and DstFilter was not provided)
- Alerts: -
- Widget templates: All Traffic in last 7 days
- Created: -

A success message is displayed at the bottom right: 'Asset created' - Asset Web GUI was successfully created and is ready for use in Flowmon applications.

Application eXperience Fabric

New LoadMaster consumption model focused on simplicity, automation, workflows and user experience.

Cloud-native central management of whole LoadMaster fleet with automation of provisioning, central health monitoring and reporting.

Join CVP (Customer Validation Program) to provide feedback!

Future plans to expand and integrate Flowmon & Whats Up Gold for consolidated application insights and security.

