Flowmon
Networks

Flowmon Monitoring Center

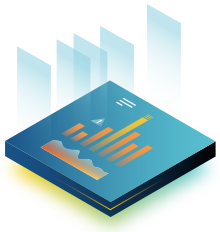
FLOWMON MONITORING CENTER

Flowmon Monitoring Center (FMC) is the beating heart of the Flowmon solution – a professional tool for effective network troubleshooting, performance monitoring and capacity planning. Instead of just the red/green infrastructure status, it helps users to understand user experience while keeping the amount of data noise and analytical work to a minimum.

Flowmon Monitoring Center

Provides insight for user experience monitoring, root-cause analysis and incident response.	Offers predefined widgets and charts that display statistics in an intuitive, easy-to-read way.
Allows advanced users to specify requests and filters on stored network telemetry data, to quickly and easily find particular communications, incidents or anomalies.	Saves time on incident investigation and data analysis.
	Is optimized for processing and filtering out important information and visualization of large amounts of network and application telemetry data.

Key Features and benefits



Predefined Views and Reports

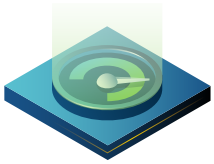
Flowmon comes with configuration templates for out-of-the-box functionality. In only a few clicks, the system automatically creates dashboards and reports for the user.

Hard Evidence

The solution creates a shared information space for all IT departments, so that they may collaborate, pool expertise together and make informed decisions without delay.

Transparent Network. Network

Hybrid and cloud traffic is monitored and visualized in near-real time, and presented in a single consolidated view as easy-to-read charts and graphs.

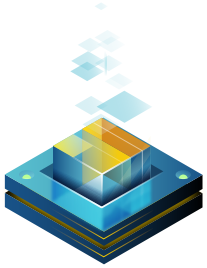


Optimization

Drilldown data is always available at hand, facilitating rapid analysis and identification of issues and bottlenecks. The data is neither sampled nor aggregated for the level of detail needed.

Reduced MTTR

Network administrators can perform troubleshooting and ticket resolution with far greater speed. Resolve up to 95% operational network issues from the same dashboard.



Customization

Data can be exported using the user's choice of tool. Widgets can be configured to show precisely what needs to be seen. No clutter, just clear data.

Use Cases

Network Performance Monitoring

Decisive intelligence to identify bottlenecks and resolve latency issues caused by networks, servers and applications.

Troubleshooting and Forensics

Next-generation network monitoring provides actionable insights into the network in order to find, analyze and fix issues easily.

Capacity planning

Comprehensive understanding of bandwidth usage to reduce the risk of services performance degradation and plan network capacity wisely.

Cloud monitoring

Traffic visibility to maintain SaaS apps performance. Flowmon tracks interactions between users and applications and reveals bottlenecks anywhere along the delivery chain.

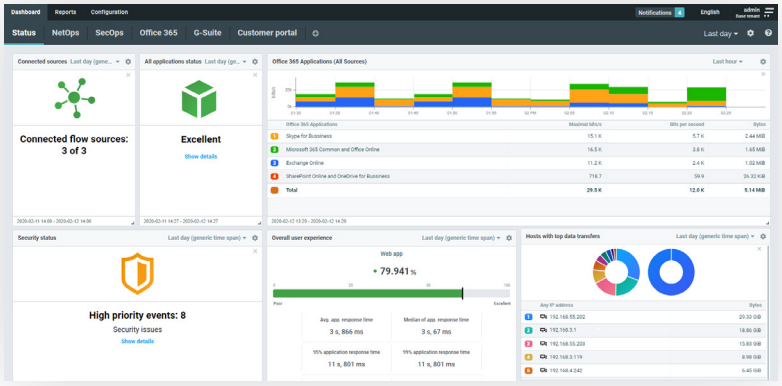
Encrypted Traffic Analysis

Scalable malware detection and cryptographic assessment of secured network sessions, which does not rely on decryption.

Streamlined Analytical Workflow

Clear Visualization

The face of FMC is the dashboard - a highly customizable interface designed for the visualization of traffic structure and performance metrics. It features flexible as well as custom widgets in order to make it possible for it to adjust to the user's every need.



Predefined views and dashboard

The solution can be configured out-of-the-box using predefined dashboards and the so-called configuration templates. They are presets designed to reduce configuration time down to only a few clicks. There are over a dozen basic templates reflecting the most common needs of users (Office 3U65, G Suite, social networks), including a number of enterprise protocols (DNS, DHCP,...) and media services.

Once a template is chosen, it automatically creates dashboards, widgets and reports and populate them with data to perfectly fulfil the purpose it was designed for.

The list of templates is continuously being expanded depending on the evolving user needs and IT trends.

Analytics - drill-down

Drill-down options are available from anywhere in the dashboard. Every widget, whether it is a traffic chart, graph or a list of alerts, can be displayed in an analytical view with for additional detail as well as sorting and filtering options (e.g. by protocols, time periods, or source/destination IP address). From there, it is possible to continue deeper, down to the level of flows or packets, with the ability to display very specific details, such as the activity of a chosen IP address, complete with information on active devices, vendors, or flow sources (where available).

The statistics are exportable at every level of the above-described drilldown.

Integrations

There are infinite possibilities to integrate the solution with complementary security tools and platforms, whether it is through syslog, SNMP, email, REST API or custom scripts. Flowmon servers as a vital source of information to log management, SIEM, big data platforms, incident handling or security automation tools. It maximizes the investment into network infrastructure equipment from a variety of vendors by enabling their use as a source telemetry data.

Logging and reporting

The system can feed log management or SIEM systems with comprehensive logging with context-rich syslog or SNMP messages for maximum visibility across the IT environment or logging events into ticketing tools automatically.

User identity

Flowmon can identify which user or hostname has taken part in an attack by collecting authentication system log data and correlating it. Any syslog-enabled authentication service or vendor is supported, including Cisco ISE, Microsoft Active Directory or LDAP.

Network telemetry

The system can leverage existing infrastructure as sensors that generate NetFlow, IPFIX, sFlow, jFlow or NetStream from network devices and other data sources such as public cloud platforms, firewalls, virtualization platforms and packet brokers.