Progress® | Flowmon

Network Troubleshooting and Forensics

Gain a deep visibility into your network.
Find and fix issues easily.

It takes more than just server uptime information to deal with outages, performance degradation or complaining users. Different IT teams draw insight from their separate tools and when an incident occurs, naturally, no one feels they are at fault. Precious time is then wasted by shifting blame instead of locating the root cause. The complexity of modern digital environments as well as the software-defined world of the cloud place obstacles in the way of full visibility throughout the environment.

"Thanks to Flowmon, we are provided with network visibility we previously lacked. Now we can identify the causes of network issues easier than ever before."

Masahiro Sato, CTO at SEGA

SEGA

Flowmon goes further than monitoring red/green status. It tracks individual user interactions with applications to give you an end-to-end understanding of the performance of the entire digital environment. It's a holistic approach that allows you to immediately identify what causes problems, which users and services are affected and who is responsible for remedy. Boosted by an AI-powered detection engine, Flowmon will transform your IT from reactive operations supporting business needs into a proactive enabler of your company's success.

BENEFITS

Automation

Cut the time spent on manual analysis and investigation to make room for strategic activities.

Proof of accountability

Own hard data to show which of the application delivery chain is at fault and who is responsible for remedy.

Reducing network visibility TCO

Avoid functional overlap and gain full visibility across your entire IT environment in one comprehensive solution.

Troubleshooting

Flowmon's noiseless insight will help you pinpoint the exact cause of degradations, so you may act before business is harmed.

Noise-free insight

Sifting through a featureless mass of disconnected information is no way to resolve incidents.

The level of visibility that Flowmon provides streamlines troubleshooting, which is key for the networking department to perform their mission-critical, but often reactive tasks. However, in order to support business initiatives more proactively and implement them in increasingly heterogeneous digital environments, administrators need to spend less time on routine and become more agile.

Flowmon's AI-powered analytical engine brings the automation they need to achieve this. It processes the mass of network traffic data, organizes it and presents it as distinct, meaningful events on the dashboard. Detected events are ranked by priority, allowing you to radically speed up investigation and response, and concentrate on what is important.

Flowmon provides a holistic view of all your network and cloud assets, and allows you to monitor everything centrally. Thus, rather than having multiple teams use different tools to arrive at several different conclusions, it draws a comprehensive picture of all traffic and enables all IT teams to coordinate and synchronize their efforts.

30 min

From deployment to dashboard insights

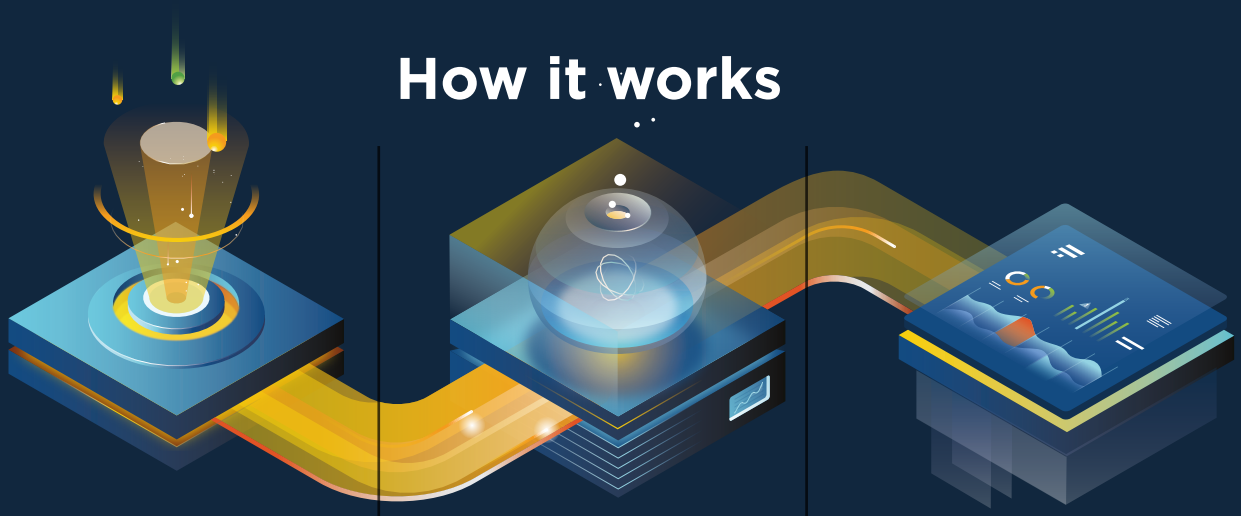
Day Zero

Respond to advanced persistent threats on Day Zero

16x

Up to 16x faster time to resolution

How it works



Gather
Use Flowmon Probes for enriched network and app data (L2-L7) or collect 3rd party NetFlow/IPFIX sources or other L3-L4 data.

Analyze
See statistics, visualize data, and drill-down to any communication for effective troubleshooting.

Report
The telemetry is displayed on a highly customizable dashboard with a wealth of presents, turning data into actionable intelligence.

Next-generation **network monitoring**

When a traffic anomaly occurs, you need to be able to reliably trace the root cause regardless of its character and location along the delivery chain. Traditional tools, which only focus on CPU and RAM utilization or the number of transferred packets, are unlikely to achieve this because their point of view is often far too narrow. You need a more sophisticated solution that provides full situation awareness instead of spear-fishing local symptoms.

Flowmon collects a variety of network telemetry data from your infrastructure, or uses passive network sensors to extract metrics on network and application performance, which it processes, sorts and analyzes. Using advanced analytical methods, it separates relevant information from the noise, detects events and visualizes them in customizable views.

- Unavailable services
- High latency
- Unusual network loads
- Misuse of a variety of communication protocols
- Use of non-compliance encryption
- Alien or unknown devices

The powerful detection engine combines machine learning with several other detection algorithms to be able to pick up even the most elusive anomalies and subtly disguised threats. Upon detection, the user is automatically alerted and predefined actions are triggered.

www.flowmon.com