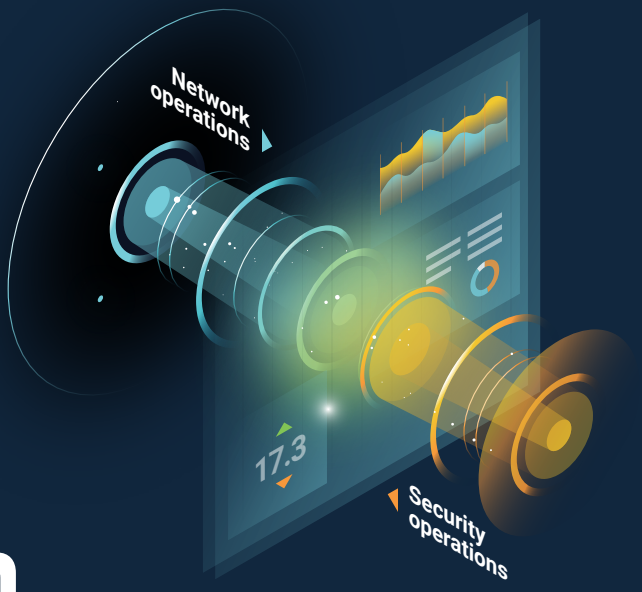
Progress® | Flowmon



NetOps and SecOps Cooperation

Even though they pursue different priorities, NetOps and SecOps share the same goal - ensuring secure and efficient business services. Forward-thinking leaders know how to break the walls that stand between them and bring out the value the two teams have for each other, making operations more agile, less risky and more cost-effective. Flowmon is a shared NetOps and SecOps tool that fosters this cooperation.

The traditional view is that NetOps and SecOps are independent silos with different technologies and processes. But in the event of data leakage, outage or performance degradation, it doesn't matter what the root cause is. What matters is resolving the incident as quickly and efficiently as possible so that business isn't harmed.

91%

of network managers formally collaborate with security group.

Source: A Guide to NetOps and SecOps Collaboration, An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™), 2019

84%

of network and security teams reported they lacked a shared data store

Source: A Guide to NetOps and SecOps Collaboration, An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™), 2019

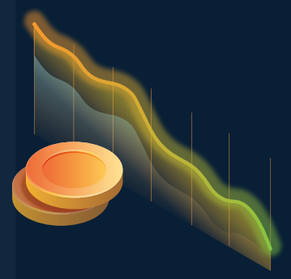
"The Flowmon solution is widely used in our company both by network and security engineers. Everyone receives the most important information necessary for their work."

orange™

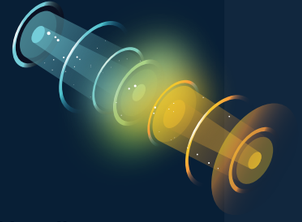
BENEFITS

One source of truth
The ability of both teams to access the same information via a shared platform enables them to piece together meaningful context and make decisions.

Fast time to value
Streamlined deployment, user enablement, predefined views, dashboards and reports. From deployment to data on the dashboard in just 30 minutes.

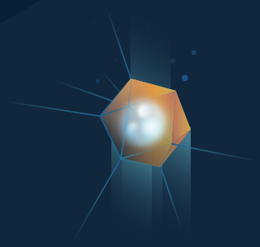


Optimizing spending
Merged procurement avoids purchasing multiple technologies with overlapping functionality and improves cost-efficiency in support, staff training and overhead.



Breaking silos
Common goals, such as safe infrastructure design, faster response time or automation can be achieved more easily if the priorities of both teams are kept in mind.

Risk reduction
The ability to enforce compliance policies, oversee unwanted behavior and evaluate data accesses in real time helps eliminate risk.



Breach impact minimization
Efficient cooperation on incident investigation and handling reduces response time to contain the threat in its early stages.

Shared values **streamline operations**

When NetOps and SecOps teams share a dataset and toolset, they gain the ability to make joint decisions and construct efficient security policies that do not affect performance. Moreover, coordination on tool spending and focus on shared data, use cases and technologies brings significant savings on purchase, support, training and staff overhead.

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

FORENSICS

Flowmon stores full traffic statistics for weeks or even months, and auto-triggers the recording of detected anomalies to provide full packet trace of the event. This provides a wealth of insight about the communication and enables post-compromise analysis of the incident.

RECOVERY

Flowmon helps to assess the attack scope and impact to draft a robust recovery plan. This includes identifying parts of the network which were compromised, assets and users affected, and what needs to be re-installed or recovered.

PREVENTION

While the NetOps team will appreciate Flowmon's data on network structure during sizing, capacity planning or performance management, SecOps teams will use the same data to identify non-approved service traffic

DETECTION

Perimeter and endpoint security can only protect against threats of known signature. The rest require a layered security model that can monitor the gap between perimeter and endpoint and pick up early indicators of compromise on the network level.

RESPONSE

When it comes to response, the SecOps team assesses the risk and decides how to mitigate, but it's the NetOps who carries it out on the network level. Flowmon helps with coordination between the teams and agreement on the remedial action, which is essential for faster time to respond.

Network Traffic Analysis for NetSecOps

Flowmon collects network telemetry data from a variety of sources including your existing network devices and its own sensors, in which case the process is passive and doesn't interfere with the network's performance. The data is then processed using machine learning, heuristics and advanced algorithms. Relevant information is extracted and visualized on the dashboard.

While NetOps teams benefit from insight into network traffic, which is essential for their ability to manage application performance and resolve emerging issues, SecOps layers their security strategy to detect unknown and insider threats (even in encrypted traffic). Together, they use shared data to make decisions on infrastructure design, enforce security policies across the entire IT ecosystem, investigate, assess impact and respond to threats and data breaches. Thanks to Flowmon, informed decision-making and prioritization are always supported by reliable intelligence.

User experience & app performance

Security analysis

Machine Learning

Network telemetry

On-demand Raw packet storage

Monitoring and Diagnostics for NetOps

- End-User Experience Monitoring
- Troubleshooting and Forensic
- Forecasting and Planning
- Cloud/Saas Performance

Erasing the silos between NetOps and SecOps

- Infrastructure Design & Deployment
- Incident Monitoring & Investigation
- Incident Response
- Policy Verification and Enforcement

Network Traffic Analysis for Secops

- Unknown Threat Detection
- Encrypted Traffic Analysis
- Detection of Insider Threats
- Volumetric DDoS Protection

www.flowmon.com