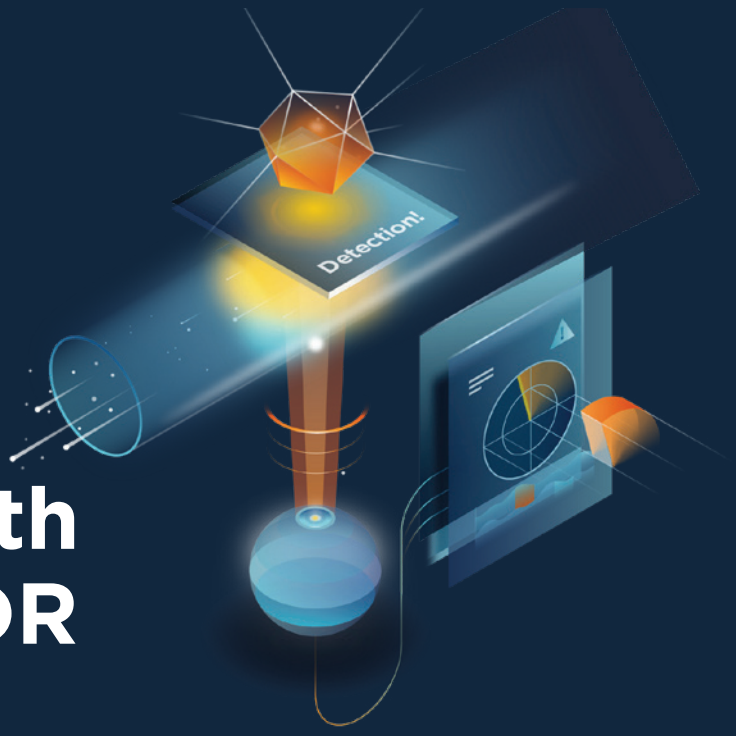
Flowmon Networks



Maximizing Investment into SIEM with Flowmon NDR

Even though SIEMs can usually utilize flow data as a source, doing this consumes license limits and duplicates the functionality of NDR tools. However, you can use an NDR tool to ingest flow data, process it using advanced algorithms and techniques, and detect events, which you can then feed to the SIEM. This approach can significantly reduce the budget and ongoing costs needed for the SIEM while still providing actionable threat information with comprehensive details.

50%

Clients report up to 50% savings on SIEM licenses

"Thanks to Flowmon 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."

Vittorio Cimin, CIO of Bricofer

Bricofer

FLOWMON

BENEFITS

Maximizing SIEM ROI

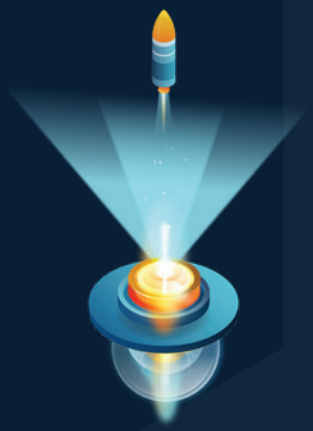
Instead of feeding the SIEM with a bulk of data, you can preprocess it using a specialized tool and only send what is relevant, thus saving on license costs.

Threat hunting time reduction

Events are presented in context to support real-time threat-hunting. Their circumstances are recorded in full for convenient post-compromise analysis.

Layered security

Cover the blindspots of your security solutions by deploying them in a complementary matrix. Let them make up for each other's shortcomings and reduce the likelihood of a successful attack.



Fast time to value

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

NDR tools convert the torrent of network telemetry data to a low number of events which are then exported to the SIEM, thus reducing the number of network logs the SIEM has to process and ultimately bringing significant savings, as SIEM pricing is typically based on the number of processed logs.

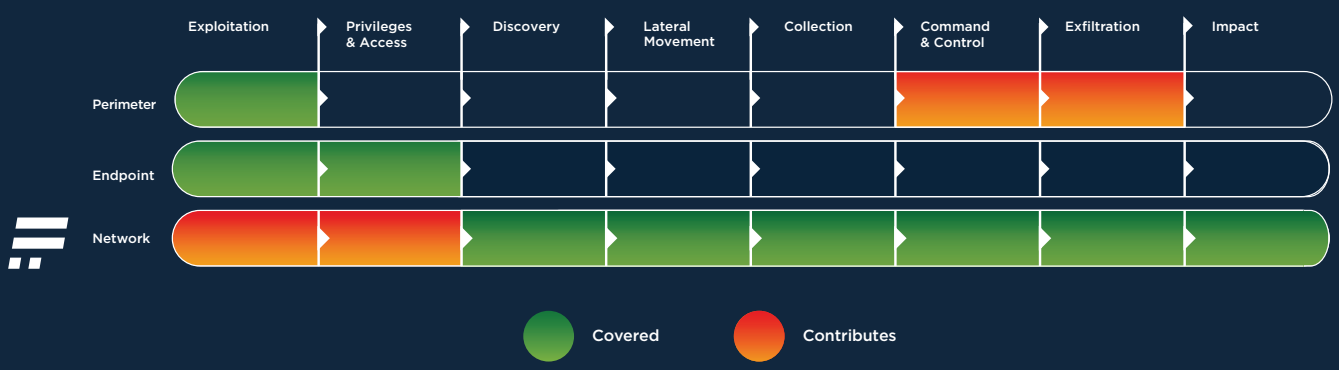
Flowmon is compatible with a wide range of SIEM systems. Integration and event delivery is based on standard syslog protocol or SNMP traps. Flowmon implements the industrial standard Common Event Format (CEF) to minimize deployment efforts. Furthermore, Flowmon supports REST API, custom-scripts, and other integration methods.

FLOWMON

FORTINET McAfee splunk> IBM QRadar ArcSight

How does it work?

The detection of unknown threats requires layered security consisting of several approaches that can pick up various anomalies and recognize them as indicators of compromise. Flowmon co-creates these layers alongside antivirus and firewall to monitor



Flowmon does not use just one detection mechanism, but several, all working at the same time. They cover a wide number of scenarios by examining the network from several points of view. Because the solution uses network traffic metadata, it delivers the same level of detection in encrypted traffic.

Data Source

- Proprietary Enriched Network Telemetry
- 3rd-Party NetFlow/IPFIX and Compatible Standards
- Raw Packet Data
- User Identity
- IDS Signatures
- Built-in and Custom Threat Intelligence

Detection

- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation

→ Threat and Anomaly Alerts

The **SOC Visibility Triad** is a concept created by Anton Chuvakin of Gartner, which postulates that deploying complementary security tools that make up for each other's shortcomings will significantly reduce the chances that an attacker will be able to achieve their goals. The Triad consists of three pillars; endpoint security (EDR), event logging and management (SIEM), and network detection and response (NDR).