Progress® | Flowmon

Detection of **Insider Threats**

Uncover suspicious behaviors.
Get insight.
Act immediately.

Insider threats range from oversights by careless users to social engineering attacks or sophisticated infiltrations with compromised credentials. Companies are well aware of how unpredictable and destructive these threats can be. This is why many invest heavily in education as the main form of prevention. Still, data exfiltration occurs, which calls for a well-defined plan for incident detection and response.

Flowmon is an actionable intelligence tool which detects indicators of compromise on the network level, where breaches can be tracked at their every stage. It uses several techniques simultaneously to uncover suspicious behaviors and provide immediate insight and alerting, as well as data for a thorough post-compromise analysis.

74%

of organizations feel vulnerable to insider threats.

Source: Insider Threat Report, AlienVault

20%

of organizations have well-defined incident response for insider threats.

Source: How to Build Incident Response Scenarios for Insider Threats, Gartner

> “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

Respond swiftly, **reduce risk**

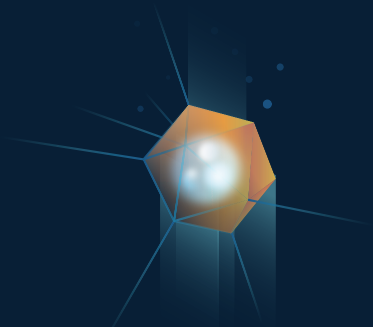
A good protection plan against insider threats consists of security-aware users and a clever combination of measures to tackle situations before, during, and after an incident.

Flowmon complements your existing systems, providing threat detection throughout the compromise life-cycle. It uses machine learning to give you insight into the network without noise or clutter, so that incident response is quick and straightforward. It shows precisely which assets have suffered damage and require repair. Data about previously encountered threats is stored for later analysis to test and refine incident response readiness. In this way, the solution reduces risk, improves prevention and makes sure the system is prepared for future challenges.

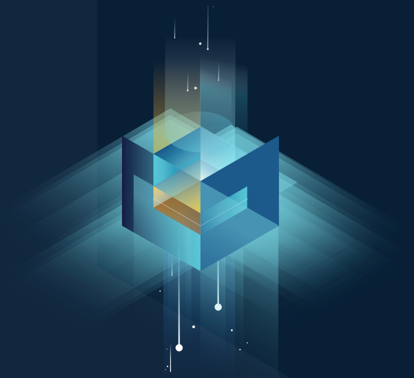
USER BENEFITS

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

Cut threat hunting time
Noise-free presentation of events enables real-time threat hunting and convenient post-compromise analysis.



Reduce risk
Prevent breaches by identifying non-compliant, high-risk assets and users.



Minimize breach impact
Flowmon monitors and analyzes network traffic to alert you to security compromises at early stages so that you may act before the danger escalates.

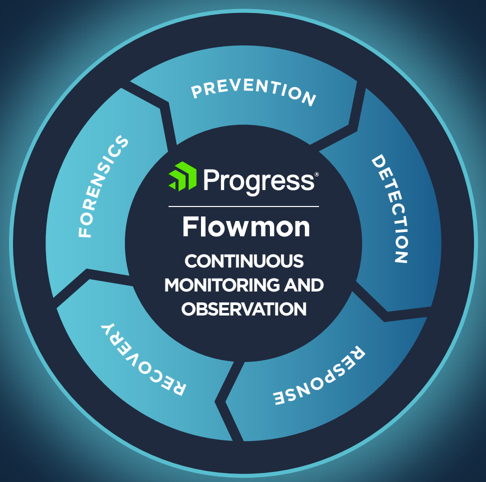
Breaking NetOps and SecOps silos
Coordination of effort between the two teams promotes prevention, improves detection and reduces response time.

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

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.



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.

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.

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.

30 min
From deployment to dashboard insights

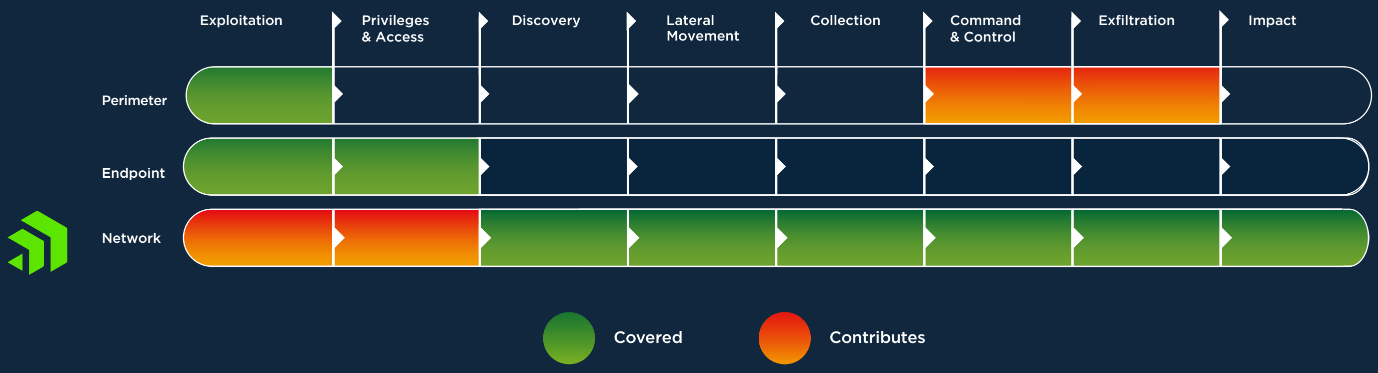
Day Zero
Respond to advanced persistent threats on Day Zero

16x
Up to 16x faster time to resolution

Layered security

The diversity of insider threats is reflected in the complexity of protection against them. It requires a layered security approach that stacks multiple points of view together to provide a holistic view of the incident scope and impact.

The layered security model consists of several approaches that can pick up various anomalies and recognize them as indicators of compromise. Flowmon co-creates these layers alongside data loss prevention or blocking measures and monitors the entire network, sealing gaps between the perimeter, endpoint as well as account.



	Exploitation	Privileges & Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Perimeter	🟩					🟥	🟥	
Endpoint	🟩	🟩						
Network	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Covered 🟥 Contributes

It does not rely on just one detection mechanism, but several, all working at the same time. They cover a large number of scenarios by examining the network from several points of view. For instance, threats that would escape detection by reputation databases will be revealed by machine learning.

Because the solution uses network traffic metadata for its analysis, it has no problem detecting threats with a consistent level of precision in encrypted traffic as well.

Once a threat is detected, the user is alerted and can immediately see the event and what it represents in the given context. This is key to immediate and deliberate decision-making and prioritization.

Flowmon can automatically trigger a response via integration with other security tools to block or quarantine the threat. The event is logged and recorded for full forensic drilldown; i.e. the examination of past insider threat incidents. These scenarios can then be used to test and hone incident response readiness through scenario planning or tabletop exercises.