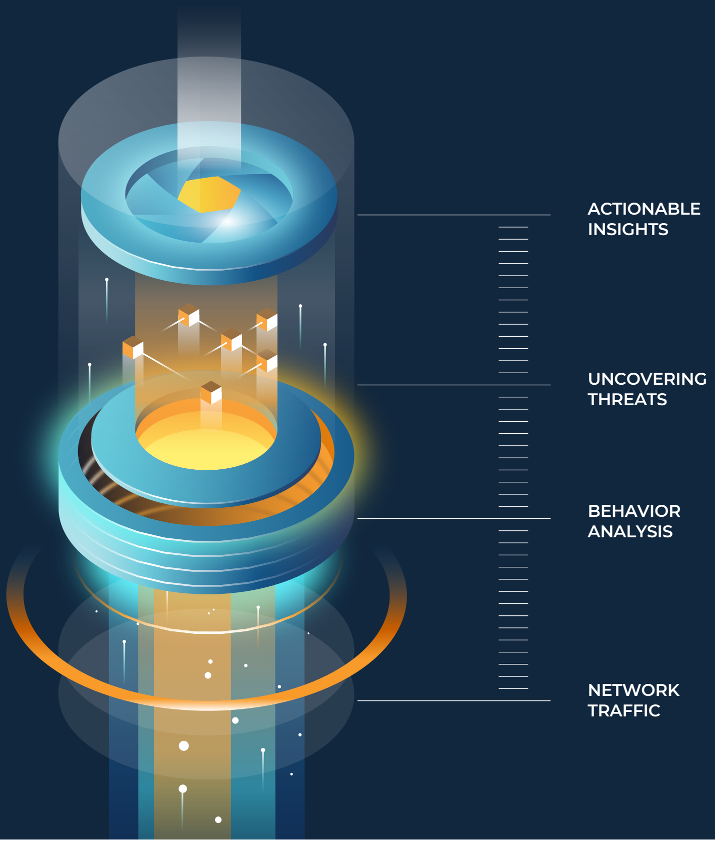
Progress® | Flowmon

Anomaly Detection System



Deal with security threats and operational issues confidently

Flowmon ADS (Anomaly Detection System) is a network security solution powered by an intelligent detection engine designed to complement traditional security tools. It seals the gap between perimeter and endpoint protection where attackers can often lurk. Unlike conventional solutions based on statistical detection, it uses behavior analysis algorithms to detect anomalies that are hidden in network traffic. These algorithms can reveal malicious behaviors, attacks against mission-critical applications, data breaches and a spectrum of indicators of compromise.

> “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

Confident action, **clear strategy**

Flowmon's detection capabilities combined with detailed analytics results in a solution that is useful throughout the incident lifespan:

Detection of insider threats
Whether incidents are caused by a careless user or malicious intent, protect your network from the inside.

Unknown threat detection
Thanks to behavior pattern recognition the system can discover unknown threats in early stages before any damage is done, providing zero-day protection.

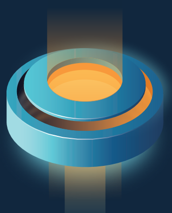
Incident investigation and response
Machine learning and data analytics work in unison to provide administrators with contextualized intelligence to reduce response time.

Troubleshooting and forensics
Flowmon ADS retains a wealth of information for deep post-compromise analysis and creates evidence for auditing and prevention purposes.

KEY FEATURES AND BENEFITS

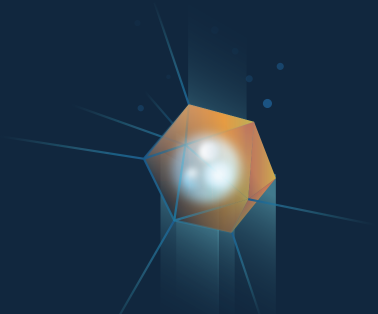
Automation

The solution detects threats immediately without placing the burden of interpretation on the user.



Noiseless insight

Flowmon provides accurate insight using sophisticated algorithms, machine learning, heuristics, and artificial intelligence.



Zero-day threat detection

Users learn about threats early due to behavior pattern recognition, which can detect anomalies in their infancy, preventing the danger from escalating.

Short incident response time

Incidents are detected in near real-time, providing context including information for remediation.

Integrations

There are many possibilities to integrate the solution with complementary security tools and platforms, whether it is through syslog, SNMP, email, REST API or custom scripts. Flowmon serves as a critical source of information to log management, SIEM, big data platforms, incident handling or response tools.

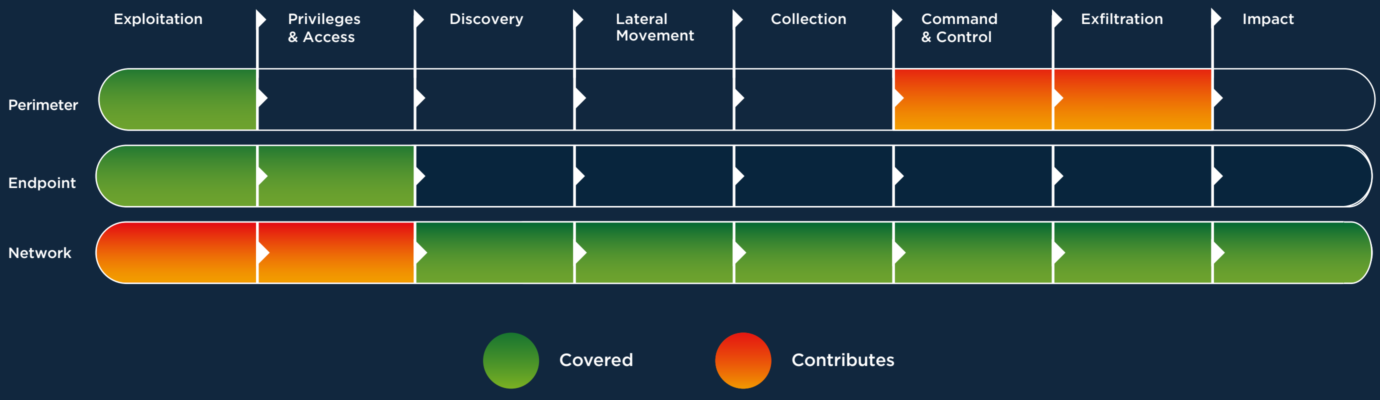
IBM · Google Cloud · Azure · cisco · vmware · Radar · aws

Juniper NETWORKS · Hillstone NETWORKS · ArcSight · Allied Telesis · ixia A Keysight Business · Gigamon

McAfee · FORTINET · splunk>

Advantage at every stage of compromise

It’s important to layer the security so that it is able to monitor the perimeter, endpoint, and network, and use a combination of detection approaches. Flowmon not only detects threats but enables response and forensic analysis.



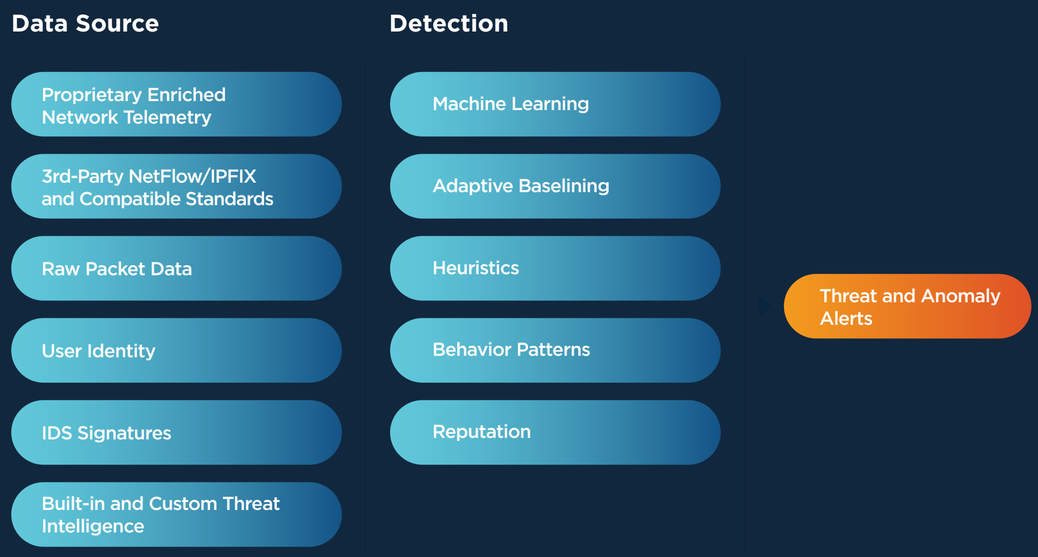
	Exploitation	Privileges & Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Perimeter	🟩					🟥	🟥	
Endpoint	🟩	🟩						
Network	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩

🟩 Covered 🟥 Contributes

How it **works**

1

Detection Process – Flowmon ADS uses several detection mechanisms that combine into one versatile capability that can examine network traffic from several points of view and thus cover a wider array of scenarios.



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

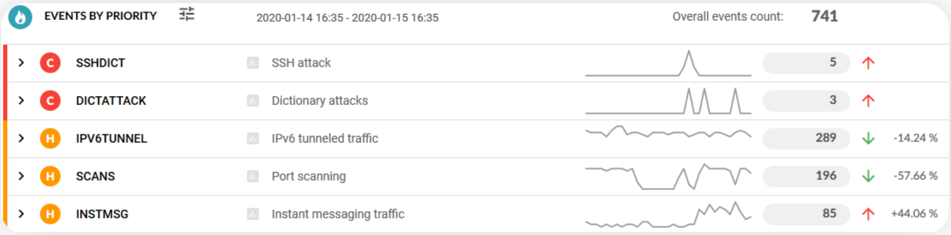
Detection

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

Threat and Anomaly Alerts

2

Report and Visualize – The analytical view provides context-rich visualization of attacks with drill-down analysis for a detailed understanding of what is happening.



EVENTS BY PRIORITY 2020-01-14 16:35 - 2020-01-15 16:35 Overall events count: 741

C	SSHDICT	SSH attack	5	↑	
C	DICTATTACK	Dictionary attacks	3	↑	
H	IPV6TUNNEL	IPv6 tunneled traffic	289	↓	-14.24 %
H	SCANS	Port scanning	196	↓	-57.66 %
H	INSTMSG	Instant messaging traffic	85	↑	+44.06 %

3

Segmentation and Prioritization – Incidents are ranked according to your priorities with an easy-to-use customization wizard that builds upon battle-tested out-of-the-box configuration.

4

Response – Flowmon ADS can be integrated with network access control, authentication, firewall or other tools for immediate incident response.

www.flowmon.com