Progress® Flowmon®

Flowmon ADS Specification

MODELS LIST

Valid from November 1, 2025

Flowmon ADS

Flowmon Anomaly Detection System (ADS) is a security solution that uses artificial intelligence and machine learning to detect anomalies hidden in the network traffic. It complements conventional security tools and creates a multi-layered protection system capable of uncovering threats at every stage of compromise. Traditional signature and rule-based detection approaches like firewall, IDS/IPS, or antivirus focus on securing perimeter and endpoints. Effective though they are in detecting initial infection by known malicious code or behavior, they offer no protection beyond perimeter and endpoint - a vast area where insider threats occur.

Exploiting this gap is the most common way of stealing data. Insider threats can only be uncovered by detecting the slightest anomalies that show indicators of compromise. Flowmon ADS can integrate with Suricata IDS operated on Flowmon Probes to extend and enrich the scope of detection capabilities and provide additional context to behavior-based anomalies and incidents. This specification **is valid for Flowmon ADS version 12.5 and newer versions.**

		Lite FM-ADS-SW-L	Standard FM-ADS-SW-S	Business FM-ADS-SW-B	Corporate FM-ADS-SW-C	Enterprise FM-ADS-SW-E	Ultimate FM-ADS-SW-U
Data processing	**Flow data**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	External information	AI-powered Flowmon Threat Briefings, Flowmon Threat Intelligence, whois, IP tools, weblinks					
	Behavioral detections	machine learning, adaptive baselining, behavior analysis, heuristics					
	IDS detections	built-in integration with Suricata IDS running on Flowmon Probes					
Event reporting	**Reporting and alerting**	e-mail, PDF/CSV, syslog, SNMP, packet capture trigger, script trigger					
	SIEM support	Using CEF (over syslog), SNMP trap					
Performance indicators[1]	**Stream data processing (flows/s)**	100	1,000	5,000	20,000	50,000	100,000
	Behavior patterns processing (flows/s)	100	1,000	5,000	20,000	25,000	25,000
	Data feeds	1	3	5	20	50	100
	Required memory (GB)	4	8	16	32	64	128
	Required CPU cores	1	2	4	8	16	24
User interface	**Event visualizations**	Event analysis tree, Timeline, Details, Evidence, Interactive					
	3rd Party integration	IBM QRadar App, LDAP/AD, McAfee ePO					

[1] Flows per second rate corresponds to unidirectional flow data before it is aggregated to bi-direction flow. Detection method configuration where there are high numbers of method instances and assigned active data feeds may lead to performance issues. The performance is declared for standard product configuration (all detection methods enabled, one method instance per method, proxy correlation disabled) while providing a required amount of memory for Flowmon ADS.

By enabling the proxy correlation, the performance can decrease up to 50% of the original value. Proxy correlation is available only for stream engine, and thus affects only stream data processing performance. Required memory refers to memory consumed by ADS only. It is recommended that the total memory of the Flowmon appliance is double the one for ADS. Insufficient memory allocated to Flowmon ADS does have an impact on detail of individual events as in memory rolling store for flow data does not provide sufficient history.

In case of insufficient memory Flowmon ADS will dynamically decrease the flow store capacity to continue data processing. Required CPU cores refer to CPU cores including hyperthreading allocated for ADS only. Providing less CPU cores may lead to performance degradation.

Total performance refers to the maximal number of flows per second processed on all active data feeds combined. For stream processing the limit is applied when the one-hour average value of flows/s exceeds threshold. For BPATTERNS processing the limit is applied when the 5-minute average value of flows exceeds the threshold. Therefore short flow bursts and traffic spikes will be processed, even if over the limit.

Behavior patterns (BPATTERNS) performance is the maximal amount of flows per second processed on all active data feeds assigned to this detection method. The performance is load balanced between data feeds equally, first flows in a 5-minute batch within the available capacity are processed. The limit is applied to the 5-minute data batches. BPATTERNS engine is based on batch processing of flow data.

Data feed is a receiver for flow data from Flowmon Collector. Data feeds provide logical separation of data from different network segments (e.g., LAN, DMZ) or different organizations (tenants). For a single Data feed, multiple instances of each detection method can be defined. Internal context and classifiers for each Data feed and method instance are computed and kept in isolation.

AI-powered Flowmon Threat Briefings is a premium cloud-based service included with Extended Support. Threat Briefings provide curated security intelligence updates about emerging threats, vulnerabilities, and attack campaigns. Each briefing includes a detailed description of the threat, associated vulnerabilities, root causes, and recommended mitigation measures. It also contains a list of indicators of compromise that can be used for automatic detection via the THREATS method or for retrospective analysis to assess past exposure.

Flowmon Threat Intelligence is a premium cloud-based service included in Standard and Extended Support. The service offers reputation data and indicators of compromise such as known attackers, infected hosts, or botnet command & control centers. This information is used as a basis for the detection of suspicious network communications via BLACKLIST method. Flowmon Threat Intelligence also updates Behavior patterns to detect known threats or zero-day attacks using behavior analysis principles.

About Progress

Progress Software (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and digital experiences with agility and ease. Customers get a trusted provider in Progress, with the products, expertise and vision they need to succeed. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at www.progress.com

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress