Flowmon Networks

Driving Network Visibility

Flowmon ADS Models List

valid from 1.6.2020

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 11.0 and newer versions based on a new stream-based detection engine processing the data on the fly.

Flowmon ADS		Lite FPC-ADS-L	Standard FPC-ADS-S	Business FPC-ADS-B	Corporate FPC-ADS-C	Enterprise FPC-ADS-E	Ultimate FPC-ADS-U
DATA PROCESSING	**Flow data**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	External information	Flowmon Threat Intelligence (reputation databases, indicators of compromise), 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	4.000	9.000	12.000	15.000
	Data feeds	1	1	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 values are designed for standard configuration (all detection methods enabled, one method instance per method) while providing a required amount of memory for Flowmon ADS. 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. The limit is applied when the one-hour average value of flows/s exceeds this 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.

Flowmon Threat Intelligence is a premium cloud-based service included in Gold and Platinum Support. The service offers reputation data and indicators of compromise such as recent 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.

Flowmon ADS ISP edition is no longer available and is replaced by the standard models as follows:

Flowmon ADS ISP version	Replacement
Flowmon ADS ISP 1 & Flowmon ADS ISP 4	Flowmon ADS Business
Flowmon ADS ISP 10 & Flowmon ADS ISP 40	Flowmon ADS Corporate
Flowmon ADS ISP 100 & Flowmon ADS ISP 400	Flowmon ADS Enterprise