Flowmon Networks

Driving Network Visibility

Flowmon ADS Model List

valid from 1.5. 2017

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	NO	Reputation databases (IP, host names, domain names, URLs)				
	Detection methods	Basic	Extended	Full feature including user defined behavior patterns			
	VoIP/SIP anomaly detection	NO	YES				
EVENT REPORTING	**Reports and triggers**	E-mail notification, PDF		E-mail notification, PDF, Syslog, SNMP, Packer capture trigger, Script trigger			
	SIEM support	NO		Using CEF (over syslog), SNMP trap			
PERFORMANCE INDICATORS	**Performance (flows/s) per FCP instance**	100	1000	2000	3000	4000	5000
	Rough network size (number of hosts)	250	1000	5000	10000	20000	50000
	FCP instances	1	1	2	3	3	3
USER INTERFACE	**Event visualization**	Dashboard, Details, Evidence	Dashboard, Details, Interactive, Evidence				
	Aggregated events	NO	YES				
	3rd Party integration	Web links, diagnostics (ping, tracert)		+ LDAP/AD query	+ McAfee ePO query		
	Configuration change audit	NO		YES			

FCP instance (flow collection & processing instance) represents the number of independent instances of flow data processing with the possibility of creating an instance of the detection method with a specific configuration. Each FCP can have its own configuration of flow statistics processing within the FCP. For Flowmon ADS Ultimate number of FCP instances and performance per instance can be adjusted.

SIEMs HP Arcsight, IBM Qradar, Enterasys or Juniper is supported natively (CEF message format). Integration with other SIEMs (Trustwave, RSA, etc.) is possible based on analysis of Syslog messages or SNMP notifications. Integration is not included in product price.

Flowmon Threat Intelligence is premium cloud-based service included in Gold support, obtains information about recent attackers, infected hosts or botnet command & control centers. This information is using for detection of suspicious network communications. Flowmon Threat Intelligence also updates behavior patterns of detection methods to detect unveiled current threats such as zero day vulnerabilities, etc. Flowmon Threat Intelligence is available for customers with valid Gold Support.

For list of detection methods available in corresponding version of Flowmon ADS please refer to detailed document “List of Flowmon ADS detection methods” available on Flowmon support portal after registration. Performance is computed according to reasonable product configuration and corresponding resources on Flowmon Probe or Flowmon Collector.

Flowmon Networks a.s.

info@flowmon.com