Flowmon ADS Models List

Rev. 1. 2

Flowmon ADS		Lite FPC-ADS-L	Standard FPC-ADS-S	Business FPC-ADS-B	Corporate FPC-ADS-C	Enterprise FPC-ADS-E
DATA PROCESSING	**Flow Data**	NetFlow v5/v9, IPFIX, NetStream				
	External information	WHOIS, IP reputation databases				
	Detection methods	Basic	Extended	Full feature		
	SIP anomaly detection	NO	YES			
EVENT REPORTING	**Reports**	E-mail		E-mail, SMS, Syslog, SNMP		
	SIEM support	NO		Using CEF (Syslog, SNMP)		
PERFORMANCE INDICATORS	**Performance (flows/s)**	<100	<1000	<2000	<3000	>3000
	Rough network size up to	<250 IPs	<1000 IPs	<5000 IPs	<10000 IPs	>10000 PCs
	FCP instances	1	1	2	3	>3
USER INTERFACE	**Event vizualization**	Dashboard, Details, Evidence	Dashboard, Details, Interactive, Evidence			
	Aggregated events	NO	YES			
	External tools	Diagnostics	Diagnostics, Geolocation (map view)			
	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.

Detection methods include consistency check of input data, detection of infected devices, detection of dictionary attacks on network services, anomalies of email communication and outgoing SPAM, port scanning, anomalies of DNS traffic, Telnet misuse, anomalies of ICMP traffic, unavailable services, high data transfers, anomalies in traffic at the network layer, DoS/DDoS attacks including so-called reflection/amplification attacks, communication with potentially unsafe IP addresses including honeypot communication.

Basic detection methods include detection of common behavior like port scanning, DNS or e-mail anomalies, P2P networks, data sharing, instant messaging, high data transfers, dictionary attacks, denial of service attacks, unavailable services, network latencies and more.

Extended detection methods is set of full feature detection methods excluding task-specific methods like sensor network monitoring or proxy traffic correlation.

Full feature detection methods include advanced detection methods like VPN, TOR, VoIP, TeamViewer traffic detection, IPv6 tunneling and more. Document with all Flowmon ADS detection methods is available to download in support portal.

Enterprise version might be customized by the means of processed data, external sources and detection methods, for more information please contact Flowmon Networks.

SMS notification requires SMS gateway provided by customer and external script prepared upon request by Flowmon Networks (in case of Flowmon license with Gold Support).

Performance is computed according to reasonable product configuration and corresponding resources on Flowmon Probe or Flowmon Collector.

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.

Gold support provides yearly support, including all updates and upgrades (new functionality), access to the web customer center, phone and email support in the English language during working hours (8x5), remote support via SSH, consultations with network and security technician.