Flowmon Networks

Driving Network Visibility

Flowmon ADS ISP Models List

valid from 1.5.2017

ISP versions of Flowmon ADS are specially designed and optimized for internet service providers to increase network security and identify malicious activities in the backbone networks. These versions support sampling for reaching higher performance.

Flowmon ADS ISP		ISP 1	ISP 4	ISP 10	ISP 40	ISP 100	ISP 400
DATA PROCESSING	**Flow Data**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	External information	Reputation databases (IP, host names, domain names, URLs)					
EVENT REPORTING	**Reporting and alerting**	E-mail notification, PDF, Syslog, SNMP, Packer capture trigger, Script trigger					
	SIEM support	Using CEF (over syslog), SNMP trap					
PERFORMANCE INDICATORS	**Total performance (flows/s) after sampling**	5000	5000	10000	10000	15000	15000
	Designed for bandwidth	1 Gbps	4 Gbps	10 Gbps	40 Gbps	100 Gbps	400 Gbps
	Support for sampling	YES, on flow level					
	FCP instance	1	2	2	3	3	4
USER INTERFACE	**Event visualizations**	Dashboard, Details, Interactive, Evidence					
	Configuration change audit	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.

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.

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, reflection/amplification DoS/DDoS attacks, communication with potentially unsafe IP addresses including honeypot communication.

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.