Flowmon Solution

The Flowmon solution delivers the flow-based monitoring and network behavior analysis (NBA) for all organizations and all networks from 10 Mbps to 100 Gbps. It provides the statistics necessary for network monitoring, security, troubleshooting, IP accounting and billing, capacity planning, user and application monitoring, data retention law fulfillment and more. Flowmon solution includes autonomous probes, which generate statistical information on network traffic, collectors for the storage, display and analysis of this information and Anomaly Detection System for automatic detection of security issues like advanced persistent threats, targeted attacks or malware activities. Flowmon solution provides outstanding network visibility, security intelligence and compatibility with many network components and SIEM solutions.

Supported technologies in a nutshell

Flowmon Solution is compatible with all IP networks, devices and vendors. In addition Flowmon is capable of processing network traffic statistics in various flow standards and report events and incidents though various channels.

Network Monitoring

NetFlow v5/v9
NetStream, jFlow
IPFIX (NetFlow v9 template)
sFlow, NetFlow Lite (limited for NBA)

Event Reporting

E-mail notification
PDF reports
Syslog (CEF)
SNMP
User-defined **scripting**

Vendor compatibility list

Flowmon support includes but is not limited to support of following products. Note that software upgrade might be necessary to enable flow export features. The flow exporting capability might be affected by CPU load or limited in supported features (IPv6, MAC, TCP flags, MPLS, VLANs, etc.).

Sources of raw NetFlow/IPFIX data for Flowmon to analyze

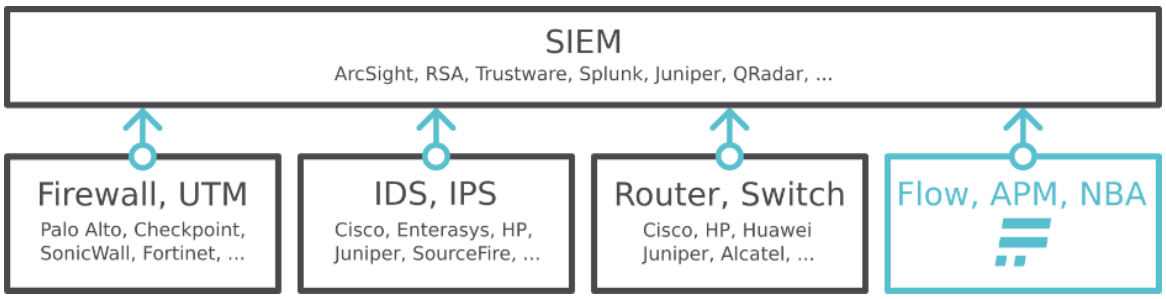
Network equipment (routers, switches)	
Alcatel	Router 7750 (cflowd v9, v10), Switch OS9000 series (only sFlow)
Brocade	Switches FastIron FSX, FESX, FGS, FLS, FWS, FCX series (only sFlow)
Cisco	Routers – all series (NetFlow) Switches – Catalyst 3750, 4000, 4500 with NetFlow module (NetFlow) Switches – Catalyst 3850, 6500, Nexus 7000, 7600 (NetFlow) Switches – Catalyst 2960 (NetFlow Lite)
Enterasys	N-series. DFE/S-series, X-Pedition SmartSwitch (NetFlow)
Extreme Networks	NetFlow v5/v9, PureView extensions not supported
HP	Switches 3500, 5400, 6200 (only sFlow), 9300, 9400 (NetFlow)
Huawei	Routers AR1200, AR2200, AR3200 (NetStream)
Juniper	MX, SRX, M, PTX, T routers (jFlow)
Mikrotik	RouterOS 2.9, v3, v4+ (NetFlow)
Nortel	Switches 5500, 8600 (IPFIX)
VMWare	Virtual Distributed Switch, VMWare 5.5 and higher (NetFlow), VMWare NSX
Network instruments (packet brokers)	
IXIA	All models supporting NetFlow/IPFIX
Gigamon	All models supporting NetFlow/IPFIX
Firewalls	
Checkpoint	Checkpoint Firewalls with IPSO 6.2 (NetFlow)
PaloAlto	PaloAlto Firewalls 6.0.3 and higher (NetFlow)
SonicWall	NSA series with SonicOS 5.8+ (NetFlow/IPFIX)

Event logging, alerting, DDoS scrubbing and other integrations

SIEM systems and IT infrastructure monitoring products	
ArcSight	Enterprise Security Manager, native support through syslog/CEF
Enterasys	Security Information and Event Manager, native support through syslog
GFI	EventsManager, general support through syslog
Juniper	Security Threat Response Manager, native support through syslog
Q1 Labs	IBM QRadar SIEM, QRadar Log Manager, native support through syslog
RSA	enVision, general support through syslog
Trustwave	Trustwave SIEM, general support through syslog
Open sources	Nagios, Zabbix, Cacti, general support through SNMP
DDoS Mitigation devices and services	
A10	Thunder TPS
Corsa	Red Armor
F5	Big-IP, VIPRION, DHD
Radware	DefensePro using Vision version 3.30 and higher

Deployment scenarios

According to general recommendations and best practices in network security NBA should be deployed together with traditional signature based solutions (anti-virus, anti-malware or intrusion detection and prevention) to monitor the network traffic for unknown or unusual deviations from normal behavior that might indicate a presence of a threat.



Flowmon infrastructure independence

Flowmon solution is not tight to specific network components or vendors. Flowmon Probe connected to mirror port or deployed using TAP can measure any IP network.

Flowmon on Cisco infrastructure

NetFlow as original Cisco technology has a broad support in routers and switches manufactured by Cisco. Flowmon solution takes advantage of Cisco environment by processing the NetFlow generated by Cisco network components.

Flowmon with network instruments

Network TAPs and Packet Brokers act as a point in network where Flowmon can deploy Probes to see network traffic. Some of these network instruments are flow-enabled and may server as source of data for Flowmon Solution with no additional investments to Flowmon Probes.

Flowmon with IDS/IPS, UTMs or next-generation firewalls

Intrusion detection and prevention systems from vendors like Enterasys, Juniper, Sourcefire, HP, Cisco or next-generation firewalls from vendors like Palo Alto, SonicWall, Fortinet or Checkpoint are compatible with Flowmon solution and mutually complement each other. Sometimes are these solutions even flow-enabled and may serve as sources for Flowmon Solution.

Flowmon in virtualized infrastructure

Virtualization makes traditional network traffic monitoring close to impossible as the network traffic stays within the virtual switch. Flowmon VA (virtual appliance) Probes can provide unique visibility inside the virtualized infrastructure and measure the network traffic in a same way as applies to physical network components.

Flowmon with SIEM systems

Flowmon ADS is a reliable source of network related events for SIEM systems from Vendors like ArcSight, RSA, Trustwave, Q1, Enterasys or Juniper. As the events are generated they are automatically logged to SIEM using syslog transport protocol as a de facto standard.

Flowmon with DDoS mitigation devices

One of the most common approaches to protect from DDoS attacks is using in-line mitigation devices. Instead of deploying such a device on each uplink customers utilize Flowmon DDoS Defender's capability do passively monitor traffic, detect DDoS attacks and redirect the attack out of normal path into the mitigation device. This model brings ultimate flexibility, scalability and price-efficiency of DDoS protection. The same benefits apply to hosted/cloud scrubbing services.

Flowmon and Routing Control

For the purpose of DDoS attack mitigation orchestration and control Flowmon with DDoS Defender can divert the traffic using various techniques such as:

- Policy-based routing (ACL control for Cisco, Juniper and Alcatel-Lucent)
- BGP (iBGP/eBGP including remotely trigged black hole)
- BGP Flowspec

Routing control is usually used together with a third party mitigation equipment. For the list of supported mitigation equipment please refer to "Vendor compatibility list" section.

Flowmon with open source SNMP monitoring tools

Flowmon integrates with popular tools like Zabbix, Nagios or Cacti through SNMP (simple network management protocol). As the events are generated they are automatically reported through SNMP traps.