



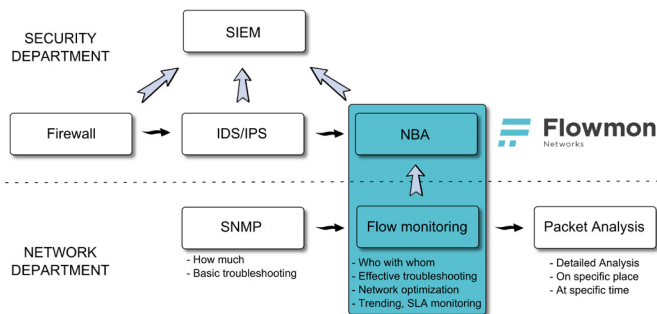
INTRODUCTION

Reliable and well secured network is of cardinal importance to any organization. Even minor network or breach to data or network infrastructure can cause financial liability, damaged reputation and customer aversion.

Network and security administrators are challenged daily managing a complex IT environment while facing an ever increasing advanced network attacks and threats. The use of leading edge tools provides the ability to manage the enterprise network in an effective and secure manner. A flow-based monitoring technology with Network Behavior Analysis (NBA) capabilities is currently being sought by enterprises worldwide.

NETWORK MONITORING

Flow-based monitoring (NetFlow or IPFIX standard and others) provides detailed inside view to network traffic with drill-down to the discrete traffic components. Providing effective administration, network troubleshooting and detection of internal and external security threats (including those which are undetectable by commonly available security tools) are just a few of the benefits.



Flow-based monitoring provides detailed information on inter-communication; timing, duration, frequency, protocol and data volume. These statistics enable real-time monitoring of network utilization, user activities and Internet use. Another benefits include threat detection and network forensics incident management. Continuous data analysis utilizing behavioral analysis technologies (NBA) enables detection of suspicious activities, anomalies, attacks or threats.

KEY BENEFITS AND FEATURES

- ▶ Detailed network visibility
- ▶ Network security enhancement
- ▶ Fast and effective network problems solving
- ▶ Detection of advanced threats and targeted attacks
- ▶ Identification of malware and potential data leakage
- ▶ Streamlined capacity planning and network optimization
- ▶ Simplified network management for administrators, increase in satisfaction of users and customers
- ▶ Detailed monitoring of users and services
- ▶ Benefits to all stakeholders – network and security administrators, CIOs
- ▶ Fast and non-invasive network deployment
- ▶ Based on NetFlow and IPFIX standards

FLOWMON SOLUTION

The Flowmon solution integrates flow-based monitoring and network behavior analysis (NBA), providing the ideal solution in assisting network and security administrators to manage, fix, optimize and secure the network.

Compatibility includes both types of networks – physical and virtual. Flowmon Solution is composed of a high-performance autonomous flow statistics generating **Flowmon Probes**, data storage **Flowmon Collectors** to display and analyze network traffic, **Flowmon ADS** (Anomaly Detection System) for automatic traffic security and operational incident detection, **Flowmon DDoS Defender** for volumetric attacks protection, **Flowmon APM** (Application Performance Monitoring) for HTTP/HTTPS applications and database performance monitoring and **Flowmon Traffic Recorder** for complete recording of data communication.

The use of network standards such as NetFlow and IPFIX, guarantees system expandability, scalability and easy integration with third party products.



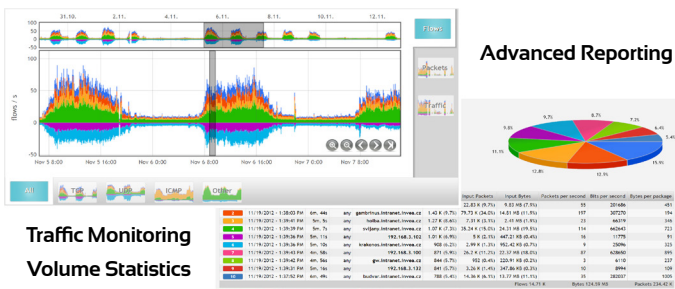
FLOWMON SOLUTION

The Flowmon solution provides **IP flow-based monitoring** to networks from 10 Mbps to 100 Gbps. It provides network monitoring, security, troubleshooting, IP accounting and billing, capacity planning, user and application monitoring, law fulfilling data retention, Network Performance Monitoring (NPM) and more. **The Network Behavior Analysis (NBA)** module enables automatic detection of operational and security events, undetectable by tools commonly in use (such as traditional network firewalls, antivirus, IDS/IPS).

A plug-and-play, of-the-shelf solution that integrates all modules necessary for network traffic, performance and security monitoring provides quick time to value and increase ROI.

NETWORK MONITORING

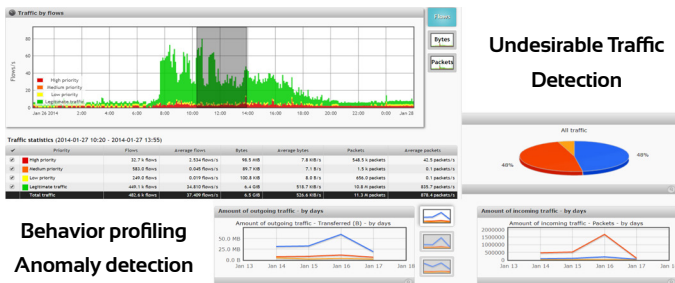
Detailed network traffic monitoring (NetFlow, IPFIX, sFlow) to organizations (SMBs, enterprises, government, academic organization, ISPs) provide needed complete network visibility.



Traffic Monitoring Volume Statistics

SECURITY MONITORING - NBA

Network Behavior Analysis (NBA) module uses automatic flow analysis to identify malicious activities, zero-day attacks and advanced persistent threats to increase network security.



Behavior profiling Anomaly detection

GARTNER

"NBA is about higher visibility to your network behavior to cover gaps left by signature based mechanism."

Network Behavior Analysis Update, GARTNER

BENEFITS OF FLOWMON SOLUTION

EFFICIENT NETWORK MANAGEMENT & PROCESSES

- ▶ Operational and configuration issues are detected and identified immediately – prior to causing nightshifts, downtime or disgruntle users/customers.
- ▶ Reduction in operational issues allows concentration on infrastructure optimization and provided services.
- ▶ Network monitoring processes as mandated by law or internal directives are fulfilled and automated.

SECURED INFRASTRUCTURE

- ▶ Infrastructure protection against new security threats (social engineering, inside attacks, data leakage, advanced persistent threats, sophisticated attacks, etc.).
- ▶ Security incidents are detected in real-time minimizing the risk and increasing time to resolution.
- ▶ Reduction in rouge software, services and network abuse.

COST SAVING

- ▶ Significant reduction of administrative overhead; Fast and efficient problem resolution.
- ▶ Lower financial impact of security incidents.
- ▶ Optimization of network application licenses, SLA and peering optimization, etc.

REFERENCES



ORDERING INFORMATION

Please contact Flowmon Networks or Flowmon Networks partner for pricing and additional information.

www.flowmon.com