Progress® Flowmon®

Selling Progress Flowmon

SALES SHEET

What is Flowmon?

Flowmon is a network and security monitoring platform with AI-based detection of cyber threats and anomalies, and fast access to actionable insights into network and application performance. The solution supports cloud, on-prem and hybrid coverage with the market's fastest deployment time.

Buzzwords:

Network Performance Monitoring and Diagnostics (NPMD)		Network Detection and Response (NDR)	
Real-time monitoring & triage	Application availability & performance	Malware/ransomware protection	Zero-day vulnerabilities
Network traffic diagnostics	Root cause of performance degradations	Network detection & response	Compliance & risk management
Bandwidth cost	Scaling network	Threat intelligence	Cloud security
Network operating costs	Cloud resources management	Threat hunting & triage	Work-from-home security

Identify Your Customer:

1. Company owns and operates business or country-critical IT applications and infrastructure..
2. Company operates or stores sensitive data.
3. Company with wide and diverse network infrastructure that includes hybrid, cloud, branch offices, and remote workers.
4. Company experiencing rapid growth in employee, infrastructure, or capitalisation during last 6-24 month.
5. Company recovering from being breached or compromised in last 6-12 months.

Business Areas:

Government, Finance, Insurance, Manufacturing, Banking, Airports, Healthcare, Energy and Utilities, Education, Fintech, IT business, Retail, Food & Agriculture, Logistics etc.

Roles:

DECISION MAKER: CTO/CIO/CISO/CSO or IT deputy leaders and IT managers.

INFLUENCER: IT manager, IT/Network administrator, IT architect, Security architect.

(Best practice: involve client's technical staff for Flowmon evaluation asap)

Flowmon Customers:

KIA SEGA® TDK orange™ coop

Value Proposition:

1. Minimize breach impact – Monitor network traffic in any environment (Cloud, hybrid, or on-premises) to proactively alert on a compromise at an early stage, effectively reducing breach dwell time.
2. Decrease mean time to resolution (MTTR) and root cause analysis time, saving hours or even days, by extending visibility into network traffic.
3. Enjoy using just one tool and one user interface for availability, capacity, troubleshooting, compliance, and forensics, in any environment (Cloud, hybrid, or on-premises).
4. Increase tech staff efficiency with intuitive network monitoring tools that enable less experienced team members to carry out complex tasks.

Customer Pain Points:

1. Late detection of security breaches and failure to comply with regulations such as GDPR, HIPAA, and NIS can result in severe financial, legal, and reputational damage to a company. Relevant for: **C-level, Management; Value proposition: 1**
2. Business IT service outages or poor performance can cause significant financial losses and damage a company's reputation. Relevant for: **C-level, Management; Value proposition: 2, 4**
3. Network issues are becoming more complex, causing delays in troubleshooting and root cause analysis, which will increase operational costs. Relevant for: **Management, C-level, Techies; Value proposition: 4, 2, 3**
4. Network administrators are often responsible for network security (NDR) but lack the time and expertise to manage it effectively, resulting in security and performance monitoring issues. Relevant for: **Management, Techies; Value proposition: 4, 2**
5. Many other monitoring tools create alert noise that interferes with the engineer's visibility and response to critical issues. Relevant for: **Techies, Management; Value proposition: 3, 2**

Competition:

Cisco Stealthwatch	NDR	Vendor-specific product tied and sold predominantly with Cisco infrastructure components.
Darktrace	NDR	Attractive GUI but security analysts reporting limited detection capabilities and poor analytics.
Vectra	NDR	Enterprise SOC-optimized, yet due to performance and costs only scalable to mission-critical systems (focus on fortune 2000 customers, high-priced).
ExtraHop	NDR + NPMD	Optimized only for enterprises (cost, features).
Plixer	NDR + NPMD	Traditional NPMD vendor with premature security capabilities based on obsolete methods.

Discovery Questions:

1. How long does it take you to investigate and solve an outage?
2. Do you have plans to scale into cloud or hybrid infrastructure environment?
3. Do you have any detection capabilities to contain a ransomware attack?
4. How do you protect your network from zero-day attacks?

Objections Handling:

I don't need another detection tool, we already get too many alerts in our SIEM.

- SIEM is only as strong as its data sources. As most of the threats need network to operate, we connect the dots between seemingly unrelated events and help reduce the number of alerts, while increasing your awareness.

We do not have capacity to use such deep visibility technology.

- Most of the companies don't. It's ok to use the solution reactively when it red-flags some errors. Over time you'll learn that having such observability will lower the time you spend on infrastructure design, planning, operation and troubleshooting and gain more capacity for strategic activities and improvements.

We are moving infrastructure to the cloud and will have native cloud monitoring.

- We have many customers who have sped up the migration with Flowmon by uncovering and understanding their network systems and resources. Once their systems are migrated, Flowmon can measure user experience and optimize it which native cloud monitoring doesn't provide at all.