# **UK - FLOWMON Progress Campaign (Call Flow)**

***Goal: Prepare a messaging for VAD sellers to be able to identify Flowmon cutomers***

# **Preparation**:

Understand Network Visibility & Security technology landscape to identify Flowmon opportunities:

Flowmon is a network security and visibility solution, that complements your other security solutions like **”list securtiy vendors from preparation”**

1. Possible direction can be:
2. End point (AV / XDRs) and perimeter security (FWs, IDS, IPS..) with NDR
3. SIEM (SIEM = Security Information and Event Management - potential SIEM vendors , SPLUNK, ARCSIGHT, IBM Q-Radar)
4. FW – Firewalls, IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems
5. NAC (Network Access Control)
6. EDR (End Point Detection and Response)
7. SOAR (Security orchestration, automation and response

# **Call Out Script**:

1. "Hi is this Mr. RESELLER? This is (*Your Name*) calling you from [DISTI NAME] on behalf of the UK Sales team. Is this a good time to talk to you?”

***If NO,***

1. “Not a problem, Mr. RESELLER. Is there any good time to reach out to you?” *(Fix Appointment. Make sure you call back at the proposed time, and follow the below process)*

***If YES,***

1. “Firstly, thank you for being one of our valued customer. Today I’m calling you about cyber security solutions from Progress. Can I borrow a few minutes of your time to talk with you about how Progress Flowmon solution can streamline your network operations and secure your IT environment?

***If NO,***

1. “Not a problem, Mr. RESELLER. I can email you the information to your registered email address. However, I could walk you through the process if you could just spare a couple of minutes. *(If “NO” then thank the CUSTOMER and end call.* ***If Customer says, “Go Ahead”, or “OK”, then proceed with the next steps)***

***If YES,***

1. “That’s great to hear. At Exertis we offer great solutions to add onto what you’re already deploying to your customers.

## **Identifying Questions:**

* How has cloud adoption changed your monitoring capability for network performance and network security?
* How has the pandemic changed your ability to monitor the network, applications and users for performance issues?
* How do you currently detect zero day breaches inside your network?
* How do you detect lateral movement of a compromised device inside of your network?
* Encrypted traffic makes up nearly 90% of internet traffic. How do you currently detect threats inside encrypted traffic?
* Is there any existing experience of Netflow/IPFIX within the business?
* Any compliance reasons to keep full flow data for analysis?
* What insight do you currently have available to look at network telemetry and gain insight into what is happening?

## **Pitch Flowmon – What it is (Security Focus)**

Flowmon's visibility into the network traffic allows security operators to seal the gap left between perimeter (typically FW) and Endpoint and provide detection of cyber security threats like Ransomware, zero-day attack and insider threats. The great thing about Flowmon is that it leverages machine learning and artificial intelligence to recognize malicious behavior and is able to provide early warning of indicators of compromise, before it has a chance to impact the business.

(More info here - <https://www.flowmon.com/en/solutions/security-operations)>

## **Pitch Flowmon – What it is (Visibility Focus)**

Flowmon enables application and network visibility across on-prem, public and hybrid cloud environment.Flowmon provides network operations with a complete overview of network traffic, detailed insight & root cause analysis to ensure business reliability.

* **Benefits for customer:**
  + **Complete Insight** - Get outstanding visibility and easily monitor your on-prem, public and hybrid cloud environment
  + **Network and App Performance** - Be alerted about network and App performance deviation to ensure problem free end-user experience
  + **Troubleshooting and Analysis** - Identify and analyse root cause of network and App issues and simply measure SLA
  + **Anomaly Detection** - Leverage AI/ML for automated detection of network and user behaviour anomalies

(More info here - https://www.flowmon.com/en/solutions/network-and-cloud-operations)

## Alternative pitches - What is Flowmon Solution by Progress

**Option 1:**

Progress Flowmon is a network detection and response (NDR) solution that detects cyber security threats and anomalies hidden in network traffic. It focuses on minimizing your IT’s attack surface by bridging the gap between perimeter and endpoint security. Flowmon leverages artificial intelligence and machine learning (AI/ML) and employs multiple detection methods at once to uncover any hidden malicious activity. Thanks to the insight into the network traffic, Flowmon enables application and network visibility across datacenter, private or hybrid cloud environment, providing you with a holistic overview of your entire estate, detailed insights for troubleshooting and maximum operational stability and security.

**Option 2:**

Flowmon solution from Progress is an intelligent Network Monitoring & Analysis tool, that allows Network Operations teams troubleshoot and analyse network traffic to find and fix issues and ensure smooth uninterrupted business operation. Additionaly Flowmon is capable to detect hidden threats in the network traffic and provide early warning to Security operation teams.

**Option 3:**

Progress Flowmon is a cyber security solution that delivers better experiences for your customers through safeguard their data and overall business continuity.”

**Option 4:**

Flowmon detection and response solution allows Security Operation to detect anomalies and early indicators of compromise, that bypass traditional security solution. Flowmon leverages Artificial Intelligence (AI) and Machine Learning (ML) principles to uncover any hidden malicious activities.

***If NOT,***

1. “Would you like a member of the UK sales team to contact you to discuss more on what we’ve discussed, and how Progress Flowmon can work for your customers?”

***If NO,***

1. “This isn’t a problem Mr. Customer. If at a later date you would like to have a conservation around how Progress Flowmon can support your network visibility and cyber security needs, please don’t hesitate to get in touch with the UK Sales team at [DISTI EMAIL HERE]. Thank you for your time and have a good day.” **Hang up, and submit the data from the call.**

***If YES,***

“That’s great to hear. I’ll make a note for one of the UK Sales team to get in touch with you regarding these opportunities. Thank you for your time and have a good day**.” Hang up, and submit the data from the call. Inform the UK sales team.**

# **Additional Infromation:**

## Flowmon Key Value in bullets:

* Improve Your Network Security & Intelligence
* Track & analyze activity across your entire network
* Prevent breaches with AI-driven network detection & response
  + - Stop Ransomware attacks, Zero day attacks, Supply chain attacks and other malicious aktivity, before it has a chance to impact the business
    - Cover the security gap between perimeter & endpoint

Additional information about Flowmon

* + Flowmon is one of the 3 vendors in the market that is recognised by Gartner:
    - in NPMD (Network Performance Monitoring and Diagnostics) Market Guide
    - In NDR (Network Detection and Response) Market Guide
    - In other words: Flowmon is the technology leader in the Network Traffic analysis and anomaly detection.
  + Flowmon was recognised as Technology Leader in SPARK NDR Report
    - Download full report [here](https://www.flowmon.com/en/resources/ebooks/spark-matrix-ndr-2022)