Orange Swiftly Solves Multiple Pain Points for Their Security and Network Operations Teams by Scaling Flowmon

CASE STUDY

INDUSTRY
Telecommunications

PRODUCT
Progress Flowmon

COUNTRY
Slovakia

> "It's good to have as less tools as possible within the network, as multiple vendors will almost always add complexity. With Flowmon, we are solving two main areas that need this type of solution in one shot."
>
> **Henrich Snajder**
> Information Security Manager, Orange

Challenge

Orange Slovakia, the top Telco, ISP and Mobile provider in its country, is a subsidiary of the international telecommunications corporation Orange with a little over 280,000,000 customers worldwide. The company provides mobile solutions and support, including fiber optic connections for businesses.

Orange Slovakia has a massive IT infrastructure. And it does not stop there. Additionally, their infrastructure has millions of endpoints that need to be connected to their company-wide network at any given moment. However, having a sizable IT infrastructure creates its own series of troubles.

Orange's network operations and security operations teams wanted to meaningfully improve the overall availability and security of its network. Not only to provide better performance for millions of customers but also to take care of any lingering issues. For example, Orange Slovakia faced several security-related blind spots within its network. But no one in the company was equipped to fix these unseen areas, nor did they have the right tools to stretch across the company.

Orange Slovakia was deploying IT infrastructure monitoring tools with the help of a third-party vendor. While it had the capabilities Orange was looking for, it was not adaptable to the company's overall structure. Using multiple tools has created complex workflows for those working on the backend. Orange Slovakia began seeking a solution to gain better network visibility to resolve both operational and security blind spots, reduce the complexity of backend workflows and deploy efficient tools to manage it all. The company turned to Progress® Flowmon® and found it to be the usable solution for these scenarios.

Solution

When Orange Slovakia first implemented Flowmon as a one-stop solution, Henrich Snajder, Information Security, Orange Slovakia, pointed out observations previously unavailable to the security operations team. Security was noticing a massive surge of events. The number of alerts and notifications came as a surprise to the team. When it's monitoring and alerting capabilities expanded into various areas, including network parameters and data centers, Orange was now equipped with better techniques to find issues.

"It's good to have as few tools as possible within the network, as multiple vendors will almost always add complexity," said Snajder. "With Flowmon, we are solving two main areas that need this type of solution in one shot."

Security teams were enabled to develop an additional layer of security on their network. The 'single pane of glass' finally allowed Orange to analyze and figure out actionable responses to any network-related issue. It was easier to backtrack and discover where these issues came from.

Results

On a high level, Orange is utilizing Flowmon as an easy-to-use monitoring tool and continues to receive alerts from its numerous network assets and segments. In a more detailed sense, both user teams have found specific uses. Network operations has now found correlations between data traffic and its sources. This has allowed team members to double-check to see if data traffic is coming from the overhead. Snajder talks about how it has helped them during regular work hours.

"Network operations use Flowmon on a daily basis," said Snajder. "For example, they are monitoring the engineering network for planning and capacity to see the structure of different protocols in the network. They also use dashboards to get a visibility about network services and applications to locate outages to facilitate quicker responses to solve those problems."

Security operations, on the other hand, were able to contain the various problems related to the blind spots. But one aspect where they made improvements was the development of automated processes. Each team member can concentrate on finding outages and problems.

Before they implemented Flowmon, Orange was seeking to enhance its security. The company received more impactful features when Flowmon was finally deployed within its systems. Now, Snajder describes the implementation of Flowmon as a "Fundamental part of its technical stack and adaptive security architecture.

About Orange

Orange is also a leading provider of global IT and telecommunication services to multinational companies, under the brand Orange Business Services. In December 2019, the Group presented its new "Engage 2025" strategic plan, which, guided by social and environmental accountability, aims to reinvent its operator model. To learn more visit www.orange.com

Enable your IT team to never overlook abnormal security and data traffic issues with an in-depth network visualization for your company by deploying **Progress® Flowmon®**

Progress®