Progress® Flowmon®

Volkswagen Slovakia Implements Progress Flowmon to Provide IT Teams Insight to its Complex Infrastructure

CASE STUDY

Volkswagen Slovakia

INDUSTRY
Automotive

PRODUCT
Progress® Flowmon®

COUNTRY
Slovakia

"One of the most important initiatives we are implementing is the Zero Trust policy. Currently, standard security perimeters no longer exist. It is due to the increasing complexity through the usage of cloud services in both IT and OT environments, usage of IoT devices and increased complexity of computer and supply chain attacks."

Marian Klaco
Chief Information Security Officer, Volkswagen Slovakia

Challenge

Volkswagen Slovakia is one of the largest employers in its respective country with around 11,000 employees across two manufacturing plants.

Volkswagen Slovakia has a large IT infrastructure across its two locations. Its IT and operational technology (OT) departments are operating and monitoring 100,000 IP addresses, 8,000 user ID credentials and hundreds of automated machines. The growing complexity behind the IT and OT networks was pressing the auto manufacturer to start new strategies with security monitoring and detecting security anomalies.

"One of the most important initiatives we were trying to implement is the Zero Trust policy. Currently, standard security perimeters no longer exist," said Marian Klaco, Chief Information Security Officer, Volkswagen Slovakia. "It is due to the increasing complexity through the usage of cloud services in both IT and OT environments, usage of IoT devices and increased complexity of computer and supply chain attacks."

Volkswagen Slovakia were searching for a flexible security tool with the capability of enterprise-wide security monitoring. Since the complex IT and OT infrastructure offers a greater attack surface, the team wanted to proactively monitor it and effectively solve the issues.

After contacting Progress and doing due diligence and a Proof of Concept with Progress® Flowmon®, the company chose to deploy Flowmon company-wide.

Solution

There are a few specific products of the Flowmon solution which are used by Volkswagen Slovakia. The IT team utilizes the Flowmon Anomaly Detection System (ADS) to locate anomalies within network communication protocols. For example, if any inconsistent communication goes over proxy servers, Flowmon ADS is deployed to find, examine and remove any threats. Mr. Klaco notes how helpful this one capability of Flowmon has been to protect, monitor and secure their network infrastructure.

"Flowmon Anomaly Detection System (ADS) functionality helps us identify, investigate and eliminate anomalies in our network communication. It helps us identify malicious behavior in the usage of our systems and application. Due to fact that our infrastructure is complex it is necessary to be able to eliminate false positives in security monitoring and this is something Flowmon ADS does well."

Marian Klaco
Chief Information Security Officer, Volkswagen Slovakia

"Flowmon's functionalities help us identify, investigate and eliminate anomalies in our network communication. It helps us identify malicious behavior in the usage of our systems and applications," said Mr. Klaco. "Due to fact that our infrastructure is complex, it is necessary to be able to eliminate false positives in security monitoring, and this is something which Flowmon ADS can do well."

Flowmon Probe is another component being used by the IT departments to investigate traffic coming from applications, as well as capture network traffic for analysis. Specifically, Mr. Klaco and his team use Packet Investigator and its automated analysis capability to further examine any issues found in the captured traffic.

Results

Flowmon is now being widely used by the automotive manufacturer's IT service department, which consists of Network, Server, Endpoint Support and Security Operations teams. Other use cases for Flowmon include NetFlow collections, locating traffic from configuration management servers and checking-in on office and client activity. This has made for more efficient workflows locating and fixing security anomalies within the complex infrastructure.

"The complexity of our IT, especially OT networks, is increasing due to new product integration into production lines. For example, with predictive maintenance or conditional monitoring in production, automation of the existing production processes, integration of cloud services in production and so on," said Mr. Klaco. "All those activities are increasing demands on security operations to keep our infrastructure secure."

About Volkswagen Slovakia

Volkswagen Slovakia was founded in 1991 and is one of the largest foreign investors in the country. In 30 years of existence, more than 6,500,000 vehicles have left its doors for customers from all over the world. The Bratislava plant is also the only plant in the world that produces vehicles for four different car brands. Volkswagen Touareg, Audi Q7, Audi Q8, Porsche Cayenne, Porsche Cayenne Coupé, ŠKODA KAROQ, as well as Volkswagen up! and e-up!. For more information, visit sk.volkswagen.sk/sk

Implement Progress® Flowmon® to increase visibility into your own complex infrastructure and eliminate dangerous security threats to your company's IT department.