Customer

kofola
drinks. life. emotion.

Industry

Production of non-alcoholic beverages

Challenges

▶ A large computer network consisting of more than three thousand IP end points, 100+ independent LAN networks and two data centres.

▶ Legacy network monitoring was unable to provide the quality of important information needed for effective network management and security.

▶ From an operational-security point of view, it was necessary to deploy network monitoring solutions to provide information about network traffic, its structure and evolution over time.

Solution Benefits

▶ Network visibility including detailed awareness of user and device behaviour in the network.

▶ An increase in computer network security by controlled access to ICT resources.

▶ Effective network management, detection of wrong configurations and network troubleshooting.

Deployed Solutions

▶ Flowmon Collector

▶ Flowmon Probes

▶ Flowmon ADS

Kofola ČeskoSlovensko a.s.

Kofola is one of the most important producers of nonalcoholic beverages in Europe, with seven production plants in four markets across the region. The company produces a traditional Czecho-Slovak drink based on an original recipe, spring waters, syrups etc. It has more than two thousand employees.

Infrastructure

An internal ICT department must solve scores of tasks a day dealing with ordinary administration and maintenance of Kofola's systems. There is a heavy utilization of employees due to ordinary administration, a dynamically growing ICT environment and limited human resources. For these reasons the company decided to deploy better nework monitoring systems consisting of:

▶ Complete WAN monitoring for production plants and business branches.

▶ Detailed LAN monitoring of production plant infrastructure, data centres and headquarters.

▶ Better network visibility and efficiency, the detection of wrong configurations and troubleshooting.

▶ The possibility to trace back the initiators of operational-security incidents and anomalies.

Flowmon Solution Deployment

Kofola's requirements were met by a distributed Flowmon solution consisting of:

▶ Central 3TB Flowmon Collector

▶ Flowmon Probes with different monitoring ports, deployed in key localities to ensure detailed LAN visibility

▶ 10+ active elements exporting NetFlow data to the central collector

This solution was integrated with third-party DDI products (DNS, DHCP, IP address management) to ensure the maximum consistency of records (IP address against the domain name). Thanks to that, the following goals were achieved:

▶ Initiators of operational-security issues were identified unequivocally in real time. It is possible to identify both MAC addresses and connection locality (locality, active element, physical port)

▶ Unequivocal system communication trends monitoring, dynamically addressed by DHCP

Benefits

Milan Zmarzlak, Head of the ICT department at Kofola, summarizes Flowmon solution deployment:

Prior to Flowmon deployment, we had only limited chances to analyse system logs and statistics. These tasks are frequently covered by costly SIEM applications and dedicated human resources. The distributed Flowmon Solution fulfils our needs and helps us to handle the everyday management of our ICT environment. In addition, Flowmon provides us with effective troubleshooting. It is also important that this solution gave us a proactive tool for the debugging, redesign and planning of our ICT environment.