Customer

GÉANT
Networks • Services • People

Industry

Research and Education

Challenges

- *High performance*
- *Vast pan-European network*
- *Detailed and accurate real-time and historical information*
- *Development of supplementary detection methods*
- *Integration into 3rd party ticketing tool*

Solution Benefits

- *Overall network traffic visibility and security*
- *Security as a Service to GÉANT's users*
- *Saving time and operational costs on incident reporting and handling*
- *Lifetime license only limited to performance of appliances*

Products

- *FlowMon Collectors*
- *FlowMon ADS ISP*

GÉANT

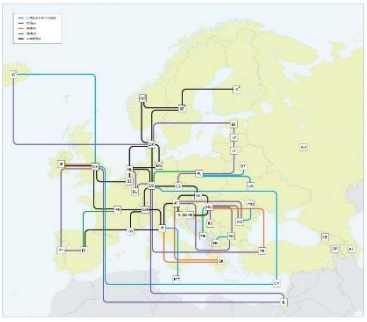
GÉANT is the leading collaboration on network and related infrastructure and services for the benefit of research and education, contributing to Europe's economic growth and competitiveness. A key part of this is the pan-European research and education network that interconnects European National Research and Education Networks (NRENs) on 1, 10, 20, 30, 100G lines and provides worldwide connectivity. Together they connect over 50 million users at 10,000 institutions across Europe. Operating at speeds of up to 500Gbps and reaching over 100 national networks worldwide, GÉANT remains the most advanced and well-connected research and education network in the world.

Infrastructure

High service availability and service quality operations are the key characteristics of GÉANT's infrastructure. Over 1,000 terabytes are transferred every day via the GÉANT IP backbone covering the entire Europe. 100 Gbps connectivity services are being operated across the core network that is designed to support up to 8 Tbps, ensuring the network remains ahead of user demand and the data deluge. GÉANT is using a variety of different router models at different versions and thus the entire environment is sensitive to precise integration.

The FlowMon Implementation

The goal of implementing FlowMon was to provide security reporting to GÉANT's users - represented by the 43 national research and education institutions. The scope of the solution is to discover attacks on network services, botnets, port scans, vulnerable services, infected devices and other malicious activity. It had been decided to integrate FlowMon into GÉANT's infrastructure by collecting flow data from existing backbone routers. To insure redundancy, two FlowMon collectors were deployed in parallel, hosting security intelligence module FlowMon ADS. Outputs from the system in the form of security events are exported to an automated ticket handling system, which notifies respective NREN's in the event of an incident being detected in their network. Customer specific development activities were carried to reflect the customers' needs for special detection methods. The entire solution was deployed in a matter of hours; followed by two months of custom development, customer testing and integration. Thereafter these activities transformed into the pilot program and the service officially went into production three months later.



Customer Review

Wayne Routly, Head of Information & Infrastructure Security at GÉANT, summarizes FlowMon solution deployment:

"We chose Invea-Tech, a vendor of Flow Monitoring and Network Behavior Analysis solutions, among a dozen different companies. After three months of intensive testing we were able to prove that FlowMon was the right product due to its performance, anomaly detection capabilities, scalability in GÉANT and its simplicity when managing and configuring. We are very keen that our users can see value in our security incident reporting and as such we have had tremendous interest in our new platform within NSHaRP."