

Sint Franciscus Vlietland Groep protects patient confidential data

Real-time analysis with Bitdefender Network Traffic Security Analytics



In January 2015, the Sint Franciscus Gasthuis in Rotterdam and the Vlietland Ziekenhuis in Schiedam joined forces to form the Sint Franciscus Vlietland Groep. With a workforce of 4,600 employees including 250 medical specialists, the organization provides hospital care to the region's population in a safe and welcoming environment.

THE CHALLENGE

Since 2015, two hospitals in the Rotterdam region – the Sint Franciscus Gasthuis in Rotterdam and the Vlietland Ziekenhuis in Schiedam – joined forces to form the Sint Franciscus Vlietland Groep (SFVG). This merger also involved the integration of the two organizations' ICT infrastructures. The integration gave rise to a review and analysis of the current infrastructure, with security being the top priority.

Previously, the Sint Franciscus Gasthuis and the Vlietland Ziekenhuis both had their own separately managed security environments. For the ICT department, the merger prompted the search for a joint infrastructure that met the security requirements of both hospitals.

Peter de Boer, Head of ICT Management at SFVG, explains: "The merger of the two hospitals gave us sufficient reason to look at how we might raise our security to new and higher levels. What we needed was a malware detection option that was easy-to-use, so that management of the system would be less time-consuming.

"Protection of patient information is of paramount importance to us, so reliability – both in terms of the security provider and the solution – was an extremely important factor. Likewise, we feel it's important that the system provides us with useful information about issues which really require our attention."

THE SOLUTION

In planning a new infrastructure, the newly formed hospital organization opted for a security-by-design solution. The aim of SFVG's security-by-design vision was to take the overall security levels at the two locations into account when designing the infrastructure. Furthermore, SFVG also made specific demands.

In view of current threats, which are no longer only external in nature, the new security solution also needed to offer protection from within, the so-called 'insider threat.' The system needed to be able to detect threats at an early stage and to ensure that no sensitive information could be leaked.

Industry

Healthcare

Headquarters

Rotterdam, Netherlands

Employees

4,600

Results

- Avoided malware from shutting down hospital devices or impacting patient care
- Remained compliant with GDPR and other data privacy regulations
- Gained new level of visibility into network
- Identified ransomware and other malware attacks

What's more, it was important that the administrative burden was minimized and that the organization could act on its own when a threat was detected. "In identifying the security needs, we took into consideration the possible threats from malicious software that might find its way onto the network," according to de Boer. "We were looking specifically for new ways of detecting these threats. The best solution was a security solution that was able to identify network traffic moving from the inside to the outside."

SFVG is using Bitdefender Network Traffic Security Analytics to analyze outgoing traffic flows in real-time. Using insights from Bitdefender Threat Intelligence, NTSA notifies the security department as soon as malicious activity is detected in the network. NTSA provides information on where the malware is located, and what the organization can do to deal with the situation quickly and effectively. In contrast to other security solutions, the NTSA appliance does not look at the content of the network traffic but focuses on the metadata. As such, the privacy of the organization and sensitive data in the internal network are not put at risk.

THE RESULTS

SFVG achieved rapid implementation because of their proof-of-concept process. "Bitdefender provides malware detection which gives protection from the inside and operates in compliance with NFI guidelines. Bitdefender offers additional services that provide support in network administration and in organizing the security environment, thus cutting back on the administrative burden. We were able to complete implementation within just a few days by means of the proof-of-concept process, which we had already put through its paces. During this process, necessary technical measures for both hospitals were implemented, which enabled the NTSA to be quickly put into use," explains de Boer.

Bitdefender is a reliable security partner that meets our requirements. "We're extremely satisfied with the performance and detection speed of Bitdefender Network Traffic Security Analytics," adds de Boer. "Bitdefender's NTSA allows us to gain a new level of visibility into our network and spot ransomware and other malware attacks in an easy-to-use, time-effective manner. By analyzing network traffic at metadata level, the solution enables us to remain both compliant with GDPR and other data privacy regulations and avoid malware from shutting down hospital devices or impacting patient care."

"By analyzing network traffic at metadata level, the solution enables us to remain both compliant with GDPR and other data privacy regulations and avoid malware from shutting down hospital devices or impacting patient care."

Peter de Boer, Head of ICT Management, SFVG

Bitdefender Footprint

- Network Traffic Security Analytics (NTSA)

IT Environment

- VMware Horizon View
- VMware vSphere

Operating Systems

- Linux
- Microsoft Windows