



BovenIJ Hospital improves security as part of their connected-care strategy

Why BovenIJ Hospital seeks to provide the right care in the right place

BovenIJ Hospital, a regional hospital in Amsterdam Noord, is committed to providing the right care, in the right place. Connected-care programs, that link in-hospital and outpatient care, enabled by technology, are key to this approach – but having more people connecting into the hospital's network also poses a security risk. With their existing firewall nearing end of support, BovenIJ needed a new solution to secure their infrastructure and protect sensitive data.

How a new firewall lays a foundation for connected care

BovenIJ was looking for a partner that could implement and support the solution, and NTT was the best fit for these goals. It was agreed that the best way forward would be to replace the firewall infrastructure. Thorough preparation and consultation enabled a smooth transition.

What robust infrastructure enables BovenIJ to achieve

In addition to improved security and management, the new firewall is designed to support new locations and cloud-based applications as the hospital extends its connected-care network. And being able to meet high industry standards for protecting sensitive patient data gives the hospital a platform for increasing its reach in the region – giving more people access to care, in more locations.



'Technology plays a vital role in transforming our services and the care we provide to communities in our region. The nature of our work and information we deal with means security is not negotiable. Working with NTT, we have a security partner that understands what we need today in terms of knowledge and support that will support future initiatives in years to come.'

Richard van Leeuwen, Coordinator ICT Infrastructure, BovenIJ Hospital

Challenge

Why BovenIJ Hospital seeks to provide the right care in the right place

BovenIJ Hospital, a regional hospital in Amsterdam Noord, strives to be personal, connected and entrepreneurial. It's one of the 28 hospitals in the Samenwerkende Algemene Ziekenhuizen (Cooperating General Hospitals) (SAZ), an organization committed to providing affordable, high-quality care that contributes to the quality of life of residents.

Providing the right care in the right place is central to this approach and the move towards connected-care programs, enabled by technology. Wherever possible, care is relocated to the home – a practice that's convenient for patients and alleviates pressure on hospital resources.

Connected care is transforming the healthcare sector and driving hospitals to reimagine their roles as care providers. BovenIJ wanted to move towards a more connected, data-driven system that would enable them to offer services remotely – and reach more people in a wider area.

But having more people connecting into the hospital's network from networks outside its control posed a significant security risk. With their existing firewall nearing end of support and potential attacks a very real and ever-present threat, BovenIJ needed a new solution to secure the hospital's network infrastructure and protect its data.

Solution

How a new firewall lays a foundation for connected care

BovenIJ was looking for a partner with the right cybersecurity knowledge and expertise to implement and support the solution. To take the pressure of their own IT resources, they also wanted a low-effort, easy to maintain solution from a partner that could provide professional support, 24/7.

They compared various providers and solutions and contacted us directly for a proposal. In terms of both our project management, consultancy and managed services capabilities and the overall solution proposed, NTT was seen as the best fit for BovenIJ's goals. A solid proof of concept was part of the process.

Following a review of the hospital's security network infrastructure, it was agreed that the best way forward would be to replace the firewall infrastructure.

Thorough preparation and consultation with BovenIJ ensured we were able to switch over to the new system with minimal errors and disruption.

A key part of this preparation was understanding the legacy systems and the creation of processes to ensure the seamless migration of rules and processes.

Outcome

What robust infrastructure does for healthcare innovation

The firewall currently protects the hospital's internal network and data center, but has been designed for expansion and new technologies. As the hospital extends its connected-care network, the firewall will be able to cover new locations. It will also be able to accommodate cloud-based applications that will become part of this new, innovative form of patient care.

BovenIJ is managing the solution in-house and has the backing of a multi-year agreement with NTT to ensure they receive the support they need, when they need it. A central management platform provides a clear, central view of activity on the firewall. Manual log inspections have been replaced by dynamic, automated ones, freeing up resources and enhancing the overall performance of the firewall.

The introduction of new, connected-care programs that aim to extend further care to more people will see an even greater focus on data privacy, protection and security. BovenIJ's firewall solution not only protects their technical infrastructure, it also helps them meet high industry standards for protecting sensitive patient data – enabling the hospital to increase its reach in the region and give more people access to care, in more locations.



Which Technologies?

- Palo Alto Firewall

Which Services?

- Consulting Services
- Technical Services
- Managed Services
- Professional Services

Which Partners?

- Palo Alto