CASE STUDY VIVANTES

Protecting the Clinic´s Network and Sensitive Patient Data

Vivantes – Network für Gesundheit GmbH, seated in Berlin, optimizes network security and network management using macmon secure Gmbh´s macmon NAC solution, resulting in concise and comprehensive end-device monitoring, significant optimization of resources and reliable, future-oriented network security.

With a yearly turnover of €785 million and a staff of over 13,000 (as per 2010), Vivantes is Germany´s largest communal hospital group. It was founded by the city of Berlin, and in 2001 incorporated all hitherto communal hospitals. One of the challenges that thus arose was to merge and integrate a variety of heterogeneous IT landscapes.

The central ITK department is now responsible for the group´s network administration and network security. Around 19,000 network ports are available at 10 sites, supported by over 300 servers, 6500 end-user computers, 3000 printers, and over 700 IP telephones and 660 switches.

Vivantes clinical center, Berlin Friedrichshain

Protecting the Clinic´s Network and Sensitive Patient Data

Ensuring reliable network protection, and maintaining an overview over all active and passive devices in the network with all their heterogeneous hardware configurations was the main reason that Vivantes was on the lookout for a manufacturer-independent, reliable solution to protect its sensitive data and its network operation.

"We had clear expectations regarding network security" Rainer Paul, head of Vivantes GmbH´s IT systems is quoted. "We were looking for a system able to detect and lock out unauthorized hardware such as alien notebooks from the network. Reliable network protection was especially important given the sensitivity of patient-related data. We were also looking for ease of operation. In short, an exact overview of all end-user equipment in our network, with justifiable effort, was called for."

The ability to rapidly lock out or isolate unauthorized devices within the whole network was important. "To be able to quickly react, considering the size of the network, we configured our first Appliance with a Quad-Core CPU in this Project", says Marcel Mulch, software developer responsible at mikado soft (by now macmon secure gmbh) for the project. "Nowadays, that is standard configuration for an appliance."
Paramount for any NAC project is the initial population and subsequent maintenance of the reference list. Since the Matrix42 "Empirum" client management suite is implemented at Vivantes, it was simple to transfer asset data from Empirum to macmon via script. This script, originally developed for the initial implementation, is still put to good use when maintaining asset data.

Lothar Börner, Network team manager at Vivantes considers: "As far as network components are considered, we adhere to standards. This makes for ease of administration and procurement. Still, with our NAC solution we wanted

Rainer Paul,
Head of IT Systems
"macmon provides us with an overview over all devices connected to our network, across our complex IT infrastructure with over 10,000 nodes."

to be independent from any specific switch manufacturer. Since putting macmon into service, we can immediately detect patched but unused switch ports, thus greatly reducing the need for redundant equipment."

Concise End-Device-Monitoring, Reliable Network Control

Following extensive testing, Vivantes opted for macmon, macmon secure Gmbh´s NAC solution. "Our expectations regarding a solution easy to manage, quick to implement and catering to high security specification, were convincingly fulfilled. macmon convinced us that

it can successfully cope with the heterogeneous IT environment at Vivantes. In addition, we are now able to quickly detect and document any relocation of devices" adds R. Paul: "With more than 3000 printers deployed, it is a great relief to now be able to find leased devices previously considered as "missing".

Detection and classification of medical equipment, increasingly capable of being attached to the network, is an important task. "Initially, we classified these devices manually with the help of a network scanner. This task is now greatly simplified with the help of macmon´s Footprinting function", explains Nico-Alexander Walter, responsible for macmon administration.

Medical equipment

macmon helps hospitals ensure fulfillment of compliance requirements and supports in implementing standards regarding IT security management, such as the upcoming IEC 80001-1 norm governing risk management for IT networks in medical environments. macmon aids in ensuring strict discrimination between administrative and medical networks. Hospital certification along KTQ increasingly also requires IT security measures. According to Wolfgang Dürr, managing director at mikado soft, that is one reason why numerous hospitals and clinics rely on our product.

Conclusion

Implementing macmon delivered the desired results. The security situation was greatly enhanced and numerous tedious administrative tasks have been eliminated. All devices are now reliably detected and documented.

"macmon helped us to implement our security requirements in a short period of time without incurring high cost or effort. With macmon we feel well prepared to face future security challenges as well" sums up Rainer Paul, head of IT systems at Vivantes.

Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin | Germany
Phone: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu