CASE STUDY

"Fortinet solutions have enabled us to meet our corporate directive of implementing comprehensive security measures without compromising the physicians' ability to share information and focus on their patients."

– Federica Gaddi,
AUSL information and communication technologies team
AUSL Reggio Emilia

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Modena

Italian Local Health Authority Optimizes Security and Productivity

Background

In Italy, the National Health System is run on a regional basis. Located in the country's northern area, the Province of Reggio Emilia covers 865 square miles and is home to over half a million residents. The province's Local Health Authority – the Azienda Unità Sanitaria Locale (AUSL) – consists of five satellite hospitals, 90 health and administrative branches, and employs almost 5,000 people. The authority's flagship facility – the Santa Maria Nuova Hospital – can trace its origins back to 1384.

Business challenge

The provision of secure, efficient communication between doctors, patients, and care locations is now an established practice in modern healthcare. A patient's right to have access to their own records has resulted in medical facilities becoming obligated to make information immediately accessible and delivered with uncompromising security.

Details

Customer Name: The Local Health Authority of Reggio Emilia
Industry: Healthcare
Location: Reggio Emilia, Italy

Business Impact

- Unified protection across 100+ facilities
- Centralized administration and monitoring
- Removed throughput and bandwidth constraints
- Facilitated secure, remote access for VPN-SSL users

In order to improve service levels for its patients, the AUSL Reggio Emilia had made the decision to eliminate paper reports and digitize all health records. In parallel with this, an escalating number of biomedical instruments were being brought online, creating a significant increase in load on the existing network.

It became evident that the legacy firewall was incapable of supporting the bandwidth necessary for the efficient exchange of data. Chandrashekhar Gadre, a manager in the AUSL information and communication technologies team, explained, "Supporting the escalating necessary levels of network throughput led to operational and performance problems.

"The existing systems were all independent and protected by traditional web-filtering firewalls. It was impossible to create profiles based on individual service needs. We could only perform basic differentiation using IP addresses and weren't able to prioritize based on the criticality of the type of service."

Requirements

To alleviate the inefficiencies of having multiple separate systems, the authority planned a consolidated central repository where all digital records and associated data would be stored. However, to function securely the new architecture required the utilization of VPN-SSL connections for staff to gain remote access to the information.

The exponential growth in the amount of digital clinical information being generated was accompanied by a commensurate advance in the potential for damage caused by a breach of that sensitive data. However, the AUSL possessed a very limited capacity to address alerts in a timely manner, and any downtime was a major inconvenience to both physicians and patients. The situation was further compounded by the number of different security products in the authority's environment, each requiring individual administration and proprietary expertize.

In addition, the IT functions of AUSL Reggio Emilia branch offices are frequently not operated by technical staff. Gadre commented, "It was essential to establish a centralized security capability from which we could coordinate all of our various locations." Any viable solution would have to be able to manage the AUSL's hundred-plus facilities from a single console.

The authority also stipulated that the final solution needed to be supplemented by a 24/7 monitoring and management service, with the ability to create an auditable record of repository data accesses.

Solution

After a period of extensive research, the AUSL Reggio Emilia selected Fortinet. The organization chose to deploy a pair of FortiGate 300C's, configured to provide failover redundancy, and more than capable of handling the traffic from every location. The next generation firewalls facilitate secure, remote access for staff using the mandatory VPN-SSL connectivity. Fortinet's 24-hour support provides round-the-clock monitoring of the environment. The constant presence of FortiGuard Labs guarantees that the authority is always protected by the very latest in threat intelligence.

Results

Deployment proved to be an easy task and was achieved without disruption to the users. AUSL elected to take a phased approach to activating the FortiGate's broad suite of features; culminating in the implementation of comprehensive anti-malware protection, web filtering, application control, WAN optimization, and an automated network vulnerability scan. All security-related functionality – delivered across the entire infrastructure – is administered by a single, centralized console.

One of the many benefits of the implementation is an optimized response time in the case of a breach. Now AUSL is equipped to do a rapid assessment of the threat and can easily identify the optimal mitigation strategy to deploy.

Federica Gaddi, a fellow manager in Gadre's organization, concluded, "Fortinet solutions have enabled us to meet our corporate directive of implementing comprehensive security measures without compromising the physicians' ability to share information and focus on their patients."

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

March 30, 2016