CASE STUDY

Healthcare Operator Protects Critical Applications in the Cloud With Fortinet's Security Platform

CASU (University Health Assistance Fund) is a private non-profit institution that provides health plans to employees of the UFMG (Federal University of Minas Gerais). Founded in 1992, CASU currently has 130 employees and more than 20,000 members who enjoy extensive medical coverage. Its infrastructure comprises a central office, two branches in Belo Horizonte that include a medical clinic, and four service units; one in the capital of Minas Gerais and three in the state's interior.

CASU decided to migrate its infrastructure to the Microsoft Azure cloud to ensure the constant availability of the members' information portal and the two service websites that integrate with the hospitals, as it was unfeasible to own and manage such a data center with the resources in place.

The healthcare organization deployed a hybrid environment with a data center at headquarters and all critical applications and loads in the cloud. "Our core business is to provide health insurance. There was no reason to invest so much in infrastructure if we could use the cloud," explains Tulio Lener, security and infrastructure coordinator at CASU. "Our portal must be available 24×7. The hospital's medical services are authorized in real time, while our associates are assisted, which is critical to communicate with our internal network. It cannot fail as this would cause a delay or even prevent service to our associates," he adds.

Cloud Protection for Business Security

With CASU's increasing use of the cloud, the IT team realized the need to secure their entire infrastructure in Microsoft Azure. CASU also needed to migrate some users who work with WVD (Windows Virtual Desktop), allowing access to the internet without any protection unless incorporating an extra layer of security. "Using the cloud without security leaves our server vulnerable on the internet. Furthermore, WVD is a critical environment since it is a user interface. Improving our security was critical, especially given the exponential increase in threats in the industry," says Lener.

With advice from NOWCY, a local Fortinet business partner, CASU implemented the FortiGate-VM (virtual machine) providing edge security to its entire cloud infrastructure, from servers to desktops. The Microsoft Azure solution is integrated into the headquarters and branch office communications network with Fortinet Secure SD-WAN technology, improving availability and providing a secure connection between the cloud and all business units. By segmenting the network and providing essential security features like content filtering and an IPS (intrusion prevention system), the FortiGate protects all applications and users within the cloud.

CASU
UFMG
CAIXA DE ASSISTÊNCIA À SAÚDE DA UNIVERSIDADE

"FortiGate's security features have brought great benefits to our management, including in terms of compliance, being one of the important actions we take to ensure that our associates' data is secure and available in accordance with the LGPD law."

– Tulio Lener, Coordinator of Security and Infrastructure, CASU

Details

Customer: CASU/UFMG

Industry: Healthcare

Location: Brazil

Business Impact

- Comprehensive security of cloud infrastructure and Windows Virtual Desktop users
- Visibility and monitoring of the entire Microsoft Azure environment, enabling proactive management both in the cloud and on-premises

"We chose Fortinet because we already had the FortiGate Next-Generation Firewall (NGFW) on our physical equipment, and we like and trust the solution. We even looked at other options but concluded that we would be safer with Fortinet. The implementation went very smoothly, with no impact to our operations and users," he says. "My team was incredibly pleased. We now have all our business-critical applications even more secured, such as our main website and partner portal, responsible for the entire exam and appointment booking process."

With the implementation, CASU began reaping the benefits of utilizing all the FortiGate NGFW features, from the most basic, like edge antivirus, to the most advanced, like scanning encrypted traffic. "We use 100% of the resources of a state-of-the-art firewall. From the point of view of security compliance, we reach 100% of the configuration," Lener celebrates.

A particularity of the CASU scenario is that, even with networks in different geographical regions, including Brazil and the United States, protection is adequate with a single firewall. In other words, both the WVD servers and applications in Brazil and those located in the United States are secured by the Fortinet platform.

"FortiGate's security features have brought great benefits to our management, including in terms of compliance, being one of the important actions we take to ensure that our associates' data is secure and available in accordance with the LGPD (Brazilian General Data Protection Law)," adds Lener.

Broader Cloud Visibility for Proactive Management

Another challenge for CASU's IT team was the poor visibility into their network within the cloud. Now, CASU has complete visibility into users inside and outside the network—all built on the capabilities of the Fortinet platform. Through monitoring by NOWCY's Security Operations Center (SOC), CASU relies on FortiManager to centralize network management and FortiAnalyzer to access more advanced incident logs and reports, powered by the FortiGuard Indicators of Compromise (IOC) Service that provides a database of more than a thousand indicators updated daily. In the event of a communication with a suspicious IP, the IT team can rely on the intelligence and automation of solutions with their analysis and context enrichment, leading to more effective decision making.

"Real-time network visibility and monitoring are a huge differentiator, allowing us to take proactive action and reduce our team's time spent managing network security," Lener shares. With Fortinet solutions and NOWCY management, CASU can now deeply and quickly verify suspicious behavior and applications from the inside out, reporting and log correlating all security events in the environment, both in the cloud and in the headquarters and branches. "We have already faced situations and managed to contain the threat at its source. That is where we realize the value of these solutions for our organization."

- Improved connection availability through Secure SD-WAN
- Compliance with the LGPD (Brazilian General Data Protection Law) and data protection of associates
- Better IT staff time management

Solutions

- FortiGate Next-Generation Firewall
- FortiGate-VM for Microsoft Azure
- Fortinet Secure SD-WAN
- FortiAnalyzer
- FortiManager
- FortiGuard IOC Service

> *"Visibility and monitoring are a huge differentiator, allowing us to take proactive action and reduce our team's time spent managing network security."*
>
> – Tulio Lener, Coordinator of Security and Infrastructure, CASU

www.fortinet.com

May 3, 2022 5:08 PM