



CASE STUDY

Leading Latin America FinTech Company Relies on Fortinet Cloud Security Solutions



Founded in 2013, Nubank was established in São Paulo as a startup focused on solving problems in the financial services sector. They aimed to do this by revolutionizing the market through the use of technology and design. Today, with more than 6 million customers, 1,300 employees, and a branch office in Berlin, it is the largest FinTech company in Latin America. In addition to providing an international credit card without an annual fee, Nubank offers other products such as NuConta, a free digital account, and Nubank Rewards, a transparent benefits program with points that do not expire. All of these services are managed through an app where customers can solve any issue using their tablets and smartphones.

Due to its technology-first structure, Nubank can increase its capacity to leverage security resources deployed in virtual environments to prevent and mitigate cybersecurity threats.

Implementing Cybersecurity Solutions to Help with Performance

As Nubank is based entirely on a digital environment, network security has always been a concern and several precautions are taken on a daily basis to guarantee the security of customer information. The company's rapid growth has driven the search for new technologies capable of supporting the expanding number of employees—currently 1,300 and growing. When the relationship between Nubank and Fortinet began, Nubank also needed to find solutions that could support the Red Team and optimize communication with the AWS cloud environment.

“The increased number of employees resulted in latency issues, which is why we chose to deploy Fortinet solutions,” says Gabriel Diab, software engineer at Nubank Brazil. “We opted for FortiManager for the administration—we analyzed its feasibility for supporting future growth and an increasing number of locations. FortiManager was a key piece in the project to achieve more centralized administration. To complete this project's phase, we opted for the Fortinet Security Fabric, consisting of FortiGate, FortiSwitch, FortiAP, FortiAnalyzer, and FortiGate-VM—the virtual firewall for our Amazon Web Services (AWS) environment. It was as if we forgot all the network solutions we had been using until then and started the structure from scratch.”

“We practically forgot about everything we did before and started from scratch. In just five months, we managed to reorganize our environment.”

– Gabriel Diab, Software Engineer, Nubank Brazil

Details

Customer: Nubank

Industry: Financial Services

Location: São Paulo, Brazil

Solution

- FortiManager
- FortiAnalyzer
- FortiGate
- FortiGate-VM
- FortiSwitch
- FortiAP

Benefits of Choosing Fortinet

Even in their short partnership, Nubank has realized many benefits from the Fortinet deployment. For example, Wi-Fi availability has improved, the network is now more secure, and software engineers' latency time has decreased. The waiting time for opening a page also fell from 10 to 5 seconds and the teams now have more time to work on other projects.

"Nubank's main benefit from implementing Fortinet security solutions is the security itself," Diab relates. "Now, we have a record of activities of each user and engineer that uses one of our services, because the two solutions communicate with each other. This allows us to understand all the actions that are being carried out and represents an important security measure for us and our customers."

Next Step: Getting Ready for NAC

"This was the first step of a giant project we plan to implement, a goal we want to achieve here in Nubank," concludes Diab. "This project not only helped us learn the Fortinet technologies we deployed but also gave us experience that will help us in our next step—the implementation of a network access control (NAC) solution. Carrying out a NAC project without having done all this infrastructure work would not be possible. This was only the first step of many on the path to achieving our goal."

Business Impact

- Increased reliability and physical security for connected devices
- Optimized the IT team's time through improved communication with AWS
- Improved control over infrastructure, users, information, and future growth
- Centralized visibility and secure management for a wireless network environment
- Simplified executive and compliance reporting and auditing
- Faster connectivity improved quality of the internal team's day-to-day work



www.fortinet.com