

Quds Bank Achieves Full Network Visibility and Control to Bolster Security.



The customer summary

Customer name

Quds Bank

Industry

Banking and financial services

Employees

900

Summary

With more than 23 years' operating across the West Bank and Gaza, Quds Bank is constantly looking for ways to increase its cyber-security. Working in such a high-risk region, with frequent cyberattacks and more than 900 users, 70 sites (this covers; branches, offices, ATM locations, and remote sites) and thousands of devices, meant security across the network was a huge challenge. This was compounded by a lack of visibility of who or what was connecting to the network at any given time. By deploying Cisco ISE alongside Cisco AMP for Endpoints and Cisco Umbrella, Quds Bank now has stringent security policies in place and complete visibility and control across its entire network infrastructure. The Cisco Customer Success Team worked alongside the IT Team to ensure they could manage and control employee, guest and temporary access to the network from a centralised dashboard in real-time. This not only helps keep the network fully secure, but it also creates efficiencies by automating some manual processes and speeds up the time it takes to solve problems, all of which help to enhance the reputation of the bank.



Devices have been managed and secured

The challenge

Quds Bank, one of the largest banks in Palestine and with the Head Office in Ramallah, was established more than 20 years ago. Serving individuals and business customers throughout the West Bank and Gaza, the bank's services include personal banking, home and car financing and commercial loans. With a reputation for offering simple, secure and innovative solutions to customers, Quds Bank wanted to ensure the integrity of its network, both physically and technologically. However, with 40 branches around the West Bank and Gaza, 900 users and frequent cyberattacks in the region, it was a challenge for the bank to securely identify who was on their network and what they were doing. This uncertainty around the network presents a huge risk of virus and malware attacks, and regardless of the firewall protection the bank already had installed, monitoring external sites, users and end points was a time-consuming task. Given the political uncertainty in the region, the bank also needed to manage security from a centralised location and dashboard, rather than using manual intervention to resolve network issues.

The solution

Quds Bank wanted a solution that would not only help it achieve greater visibility over the network, but that would integrate with its existing solutions and be a straight-forward deployment with minimal issues for users and customers. Cisco Identity Services Engine (ISE) was selected for wired, wireless and VPN dynamic access policies that would help the bank enforce security while simultaneously giving full visibility and control over the entire network. Cisco ISE also allows the IT Team to see if devices connecting to the network are external, personal or corporate and define policies and access rights accordingly. Alongside Cisco ISE, Cisco AMP for Endpoint and Cisco Umbrella were also deployed to ensure Quds Bank had full, integrated security coverage. The AMP for Endpoint and Umbrella solutions protect the bank against threats and viruses and enable the IT Team to monitor, identify and resolve suspect files before they damage the network. With such an integrated solution, The Cisco Customer Success Team were engaged to ensure the bank received maximum value from the technology. The Success Team worked closely with the IT team, delivering in-depth training, webinars and sharing best practice to help overcome any adoption challenges.

“Before installing Cisco ISE I was blind on the network - I had no idea who was connected, or what kind of device they were connecting with. Now I have complete visibility and control, and I am able to monitor all our employees from the dashboard. With the added integration of AMP for Endpoints, Cisco Umbrella and Cisco Stealthwatch we have a very powerful, very efficient security architecture.”

Salameh Salameh

Manager Information Technology Management, Quds Bank

The impact

Cisco ISE has given Quds Bank visibility and control over its entire network, helping to mitigate and prevent any potential security risks. The organisation can now monitor everything that occurs in real-time – from what happens, to when it happens and who was involved – all from a centralised dashboard. The IT Manager and his team now have the ability to gather contextual information about users and devices to proactively enforce security policies across the network, shoring up the security for users, customers and guests. Combined with the integrated AMP for Endpoints and Cisco Umbrella solutions, it means Quds Bank can grant secure access to guests or temporary users, helping enhance its customer service reputation. Having the full solution from Cisco also means the bank can facilitate secure transactions across the network and beyond the perimeter, further helping to boost its credibility in the region.

Having network visibility has also increased efficiencies and speed up time-to-resolution of any problems. Now, with Cisco solutions and the help of the Customer Success Team, if there is a suspect file or device it can be isolated to protect the integrity of the rest of the network all from a centralised dashboard rather than previously when a team member would have to scour the network for the problem and then manually resolve the issue.



More than 3,000 devices have been managed and secured during the ISE installation process.