

CASE STUDY

How a Biotech Company Keeps Employees Safe When Working From Home

Since the onset of the COVID-19 pandemic, dedicated teams at international biotech company QIAGEN have been working around the clock to develop tests for the SARS-CoV-2 virus. The company focuses on testing solutions for diagnostic labs and researchers, as well as genomic services and genome sequencing for academic researchers.

Throughout the race to bring COVID-19 under control, Fortinet has helped secure vital data—both individual information and aggregated research results—across QIAGEN's 45 locations around the world and data centers on three continents.

“We do a lot of R&D; our IP [intellectual property] is one of our most important assets,” says Jonathan Martin, director of global IT infrastructure. “My team is responsible for securing our company’s data—from IP to financials to our customer database and our privileged communications. We need to be able to assure our executives and lab technicians that no unauthorized users are going to access all that crucial information.”

Security First at the Network Edge

In 2017, Martin and his team needed to replace edge security companywide. Their legacy firewalls were approaching end of life. The team evaluated a number of alternatives.

“We were not interested in following our legacy vendor’s roadmap,” Martin says. “As we evaluated our options, we liked several things about Fortinet. “We liked that Fortinet is focused on Security-Driven Networking, which seamlessly integrates networking and industry-leading security to simplify the hybrid IT architecture,” he adds. “With some other vendors we considered, we worried that after buying the product, we would start learning about piecemeal security add-ons that would require us to add more SKUs, driving the price higher than expected.”

The IT infrastructure team also liked the product features in the FortiGate Next-Generation Firewalls (NGFWs). “We wanted an application-aware firewall,” Martin says. “We wanted to start using IPS [intrusion prevention system] technology, antivirus scanning, and web filtering immediately. We also wanted to have SD-WAN [software-defined wide-area networking] incorporated into our edge devices, to make it possible to deploy SD-WAN in the future, with minimal effort.” QIAGEN is now interested in trying Fortinet Zero Trust Network Access (ZTNA), hoping to add this to its solution when it is ready.

Once Martin’s team selected FortiGate firewalls for QIAGEN’s network edge, they worked with Fortinet Professional Services to properly size their security solution. Fortinet also worked with the QIAGEN procurement team to make sure all the



“Fortinet has been a fantastic partner, particularly in overcoming the challenges around getting the firewalls installed in certain locations. They went above and beyond in ensuring that we were successful in this major deployment.”

– Jonathan Martin, Director, Global IT Infrastructure, QIAGEN

Details

Customer: QIAGEN

Industry: Healthcare

Location: Hilden, Germany

Business Impact

- Minimizes brand and competitive risks by protecting crucial intellectual property (IP), financial, and customer data
- Optimizes productivity of business users by minimizing latency connecting to the corporate network or internet via VPN

details of the complex transaction were managed properly. The biotech company does business everywhere from Europe and North America to developing and emerging countries in Africa and Asia. In some of those countries, tax policy and regulatory differences around asset imports created challenges.

"We faced some challenges in how to structure the deal and get the equipment installed," Martin reports. "Fortinet was very flexible in helping us. This was the start of a very solid relationship between QIAGEN and Fortinet."

Streamlined Management of the Security Fabric

Now, each QIAGEN location globally is protected by a pair of high-availability FortiGate firewalls. QIAGEN business users experience minimal latency across the WAN as a result of the edge security. "We sized everything right for our traffic and capacity expectations," Martin says. "We have been moving data into Microsoft Azure over the past couple of years. This means we have been pushing more and more traffic through a larger surface to the cloud. Still, we have not seen any major impact on our firewalls' CPU usage."

FortiManager and FortiAnalyzer (collectively known as the Fortinet Fabric Management Center) streamline management of edge security throughout the network, enabling the team in Germany to oversee the global infrastructure. "FortiManager is easy for us to use," Martin says. "It provides single-pane-of-glass management, which helps ensure that our firewalls have the same configuration everywhere around the world. The Fortinet solutions are well-integrated, which means we have more visibility across the network. And we can push out code to our firewalls from a centralized portal, so we can quickly and easily distribute fixes to remediate any issues."

Once the network edge security was in place, QIAGEN turned to FortiClient to achieve similar benefits for the company's endpoints. "That was our plan when we selected Fortinet for firewalls," Martin says. "We wanted to eventually deploy an all-in-one solution to handle security at our remote endpoints. Since rolling out FortiClient, we have had a consolidated security posture, whether a user is on a laptop or at a desk in the office."

Chris Fire, senior manager of service and solution network data for QIAGEN, appreciates having a single security operating system underlying all the solutions in the Fortinet Security Fabric. "Having FortiGate firewalls and FortiClient on all our endpoints makes it easier for us to upgrade," he notes. "Because they are both Fortinet solutions, we can be sure that when we move to a new version, it will still align with our other security systems. That makes it easier to manage and control our upgrade life cycles."

Business Impact (contd.)

- Frees up IT staff time by providing easy-to-use, single-pane-of-glass management tools
- Minimized impact of COVID-19 work-from-home policies on employees, by enabling rollout of companywide VPN access within two days

Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiClient

Services

- Fortinet Professional Services

"We are very satisfied with the Fortinet solution. All the components are doing what they are supposed to do, and we are better able to mitigate threats on a day-to-day basis."

- Chris Fire, Senior Manager, Service & Solution Network Data, QIAGEN

The Fortinet solution has also improved QIAGEN's confidence in its security. "We are very satisfied with the Fortinet solution," says Fire. "We have enabled IPS and web filtering. All the components are doing what they are supposed to do. We have not seen any glitches or issues in terms of our corporate attack surface, and we are better able to mitigate threats on a day-to-day basis."

Making Work-From-Home Security Work

Supporting QIAGEN's rapidly expanding COVID-19 testing business was not the only challenge Martin's team faced in the pandemic. Like many other security groups around the world, they had to protect a workforce that suddenly became highly distributed. "Because we were already using FortiClient, we were a little bit ahead of the game," Martin says. "All our users already had a VPN [virtual private network] client, and many of them were already familiar with using it."

"The challenge with COVID was that instead of using the LAN [local-area network] bandwidth we had built, all of a sudden everybody went home and started using FortiClient," Martin continues. Fortunately, the Fortinet solutions were easy to reconfigure. "We were able to push out configuration changes very quickly," Martin says. "We got them all finished within a day or two, because we did not have to log onto a bunch of different boxes, inspect configs, and push changes to the clients. Making changes in FortiManager saved us a lot of time."

Forging a Relationship

Since QIAGEN rolled out the Fortinet solution, Martin says, "The support has been really good globally. Just having a single firewall vendor with global reach has been very helpful. We know that if a firewall goes down in Malaysia, for example, we will get the same support we would have for a firewall problem in Virginia."

He believes QIAGEN and Fortinet have forged a sturdy relationship. "Fortinet has been a fantastic partner, particularly in overcoming the challenges around getting the firewalls installed in certain locations," Martin says. "They went above and beyond in ensuring that we were successful in this major deployment."

