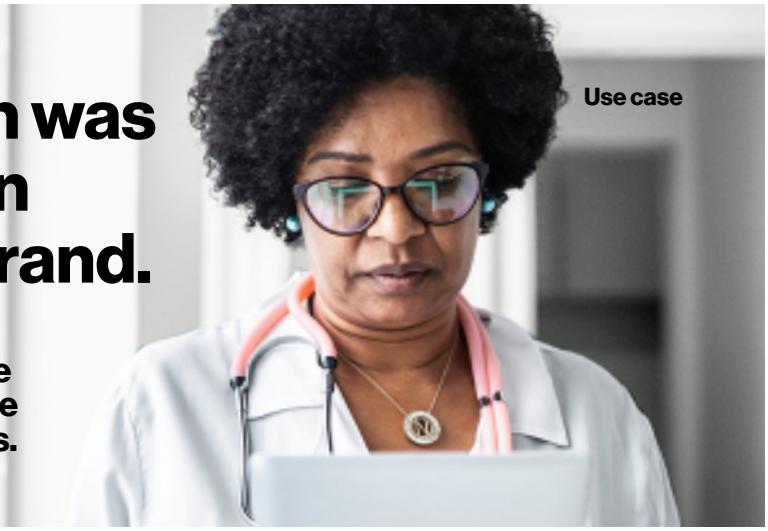
Why a SASE solution was the right prescription for this healthcare brand.



Use case

Deploying a Secure Access Service Edge (SASE) solution helped a large healthcare business optimize its security operations.

Protecting a unique healthcare brand

Healthcare companies are tasked with improving customer care while ensuring confidential patient data remains private. The larger the business, the greater this challenge becomes. As new business units emerge, it becomes increasingly difficult to ensure a consistent standard of security across the business.

This was the challenge facing a large, diversified healthcare company when it approached Verizon in 2020 to help execute a major multi-year corporate cybersecurity strategy. The company employs tens of thousands of staff globally, working across multiple business units, each with its own team, technologies and approach to security. The business had deployed a large and heterogeneous range of security solutions which resulted in many different processes in use and various organizational impacts: all of these factors having an impact on the company's cyber resiliency. It wanted to improve the employee experience, get the best from its technology investments and achieve security management excellence.

It needed to establish a new means of improving security while harmonizing processes and technology.

Laying the foundation

Working with Verizon, the business decided to take a phased approach to solving this problem, selecting one business unit for a trial project. This would allow the business to maintain more overall control over the optimization of their entire security platform, by incrementally integrating additional security features that proved successful within the business unit trial project.

The primary goal of this project was to deliver secure internet and business applications access across a user base of 30,000, located at hundreds of sites. The company partnered with Verizon due to its global network strength and supremacy in design, implementation and management of integrated network and security architectures. A consultative approach, strong partner ecosystem and ability to integrate between multiple vendors were also key. The business needed a guide with the experience and knowledge to avoid known pitfalls and respond to unforeseen challenges quickly.

The first step was appraising the customer's existing IT ecosystem. Working with the company's IT and Security teams, Verizon identified business and technology requirements and helped expose the feature limitations and implementation challenges presented by existing technologies.

Co-innovation and collaboration

The next task was sketching out the fundamentals of a new solution. It was agreed that Verizon Network-as-a-Service (NaaS) would provide the foundation, with Secure Access Service Edge (SASE) helping to enable users virtually anywhere to securely connect to business applications and all office and production sites.

One cohesive solution

This combined infrastructure marries networking and security in one tightly integrated solution. As a result, the business unit can now embrace hybrid working with confidence. Today, users across all 200 sites have secure internet and application access through their mobile devices; they can access IT resources on both physical and cloud-based servers, across all of business's offices and production locations.

The IT team is no longer juggling a host of vendors and solutions. They have one technology stack and one service desk. And with Verizon managing day-to-day security demands such as onboarding users and handling tickets between customer and vendor platforms, both the company's IT and security teams are liberated to focus on more strategic and high-value work.

With simplicity comes visibility and control. The business unit now has a better understanding of resource utilization and spending, which has helped security and IT teams to cut costs. Valuable systems and tools have been retained and optimized, to maximize return on investment. Meanwhile, redundant technologies were retired.

Perhaps most importantly, the business unit are no longer reliant on a shared infrastructure, which increased exposure and they're also in a much better position to align security policies with the group's overarching security team.

Looking to the future.

With Verizon having successfully helped the company optimize their operations, they have now progressed to the next phase of their security transformation. Verizon will now play the central role in further optimizing not only their security operations, but their entire platform. To accomplish this, Verizon will implement the gradual addition of more transformative security features, which will further integrate the SASE solution more into an MDR approach, including XDR and EDR.

Learn more:

To find out how a SASE solution can benefit you, contact your Account Manager or visit verizon.com/business/en-gb/resources/lp/secure-access-service-edge.

verizon business

© 2023 Verizon VZUC1700423