How SASE gave a manufacturing company the building blocks for a secure future

Use case

By migrating to a Secure Access Service Edge (SASE) solution, a growing manufacturing business was looking for help to modernise defences, protect Operational Technology, enable digitalisation and cloud transformation—as well as simplify cybersecurity controls with a single security policy framework without compromising business resilience and continuity.

Protecting a growing manufacturing brand

Growing a business can be hugely lucrative–but it also brings added risk. As a company merges and acquires others, it inherits new systems, networks, and processes. Ensuring everything works securely and efficiently can be particularly challenging during growth. Guarding against cyberattacks, whilst improving sustainability as part of a transformation can seem like spinning multiple plates, but it's never been more important.

This was the situation faced by a UK-based manufacturing business when it contacted Verizon in 2019. The company was a long-time Verizon network customer, but as it grew, its security controls and detection services had become complex, fragmented and difficult to manage. Residual vulnerabilities that had been exploited in previous months and years were laying dormant and waiting to be activated by external bad threat actors. This resulted in several system intrusions, errors, social engineering and ransomware attacks that affected availability and productivity across multiple sites.

In response to these attacks, the business implemented global endpoint protection and rolled out over 140 physical firewalls. But the company it was using to manage its security did not have the global reach needed to maintain a stable, consistent standard and progress security improvement plans across 140+ business locations around the world.

Ransomware attacks remain dominant. In 2022, ransomware was present in 24% of all data breaches.[1]

verizon business

From stabilisation to innovation

After taking over management of the customer's network security environment, Verizon's first task was to stabilise, standardise and identify weaknesses in security rule sets and ensure cyber hygiene processes were embedded. Once this had been achieved, the Verizon team had a better understanding of the existing environment and could help the company take a more proactive approach to security. This was particularly necessary as the customer's physical firewalls were approaching the end of their serviceable life as it had previously taken the organisation over three years to roll out and deploy them globally.

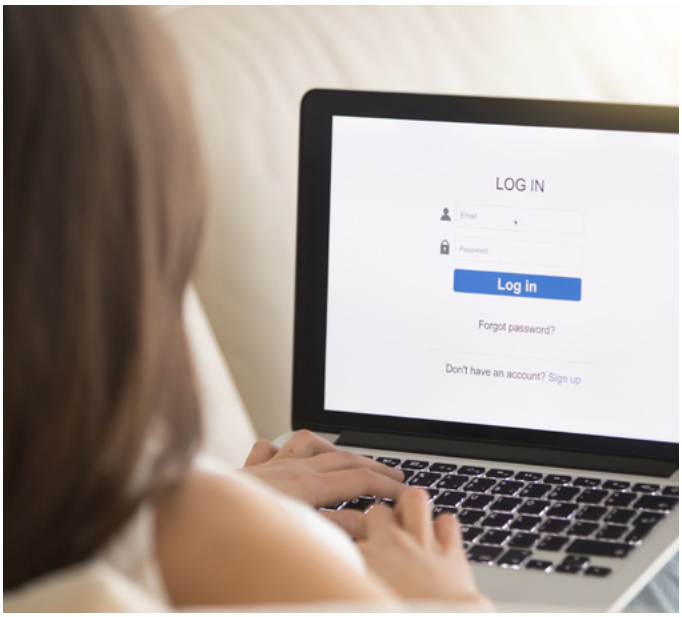
Because the business was already using Verizon's global MPLS network, migrating to a SASE environment was the logical next step. SASE combines network access, traffic optimization and security policies to give businesses a holistic and secure solution. This allowed them to detect security threats quickly and respond efficiently, giving users a consistent experience wherever they are. Zero trust network access was implemented, providing assurance that no 'thing' could access the network without being authenticated. It also allowed the customer to reduce its number of physical firewalls by leveraging cloud-based security services.

> **"With a single policy framework, Verizon was able to help simplify and standardise security controls improve visibility and reduce critical security incidents whilst improving business resilience that enabled a sustainable cloud transformation program to be deployed securely.**
>
> **Claudio Testa,**
> Security Solutions Executive, Verizon Business

In addition to helping the business keep track of any security vulnerabilities while building greater resilience, moving services to the cloud would help it meet rapidly shifting expectations for hybrid working. With human factors involved in 74% of data breaches,[1] a solution that protected credentials and maintained the highest security standards across devices, sites and even countries was crucial.

A collaborative approach to security

The Verizon team worked closely with the business to design and implement a holistic solution comprised of technology, consultancy and managed services to meet its specific short and long-term needs.



A greener and more secure solution

Reducing its reliance on ageing physical infrastructure allowed the company to simplify operations and boost security by reducing the vulnerabilities and attack surface that could be exploited by cyberattacks. The results are clear. With a significant reduction in ransomware attacks, the business's spend on cyber incident response and forensic remediation/clean-up activities was also reduced in the last year. Partnering with Verizon also helped improve the customer's sustainability, because a SASE solution consumes less power than an environment built up of dedicated hardware.

Looking to the future

With Verizon's help, the manufacturer now has a secure, cloud-based security environment that is managed across multiple sites around the world. The business has been able to modernise its security solution, reducing its attack surface and improving its availability and resilience. As the customer continues to grow and acquire new businesses, the flexibility of the SASE solution will enable it to integrate new networks and users quickly while keeping its security environment up-to-date and effective.

Learn more:
SASE Security Solutions

[1] 2023 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/en-gb/resources/reports/dbir/

verizon business