

**CASE STUDY**

How we supported a **major financial institution** to enhance their security posture, mitigate threats and protect customer data



A financial institution needed an expert partner to support them in enhancing their security posture and updating their F5 infrastructure



They faced various challenges around automating their F5 products, configuration consistency and planning future projects



Through a two-year managed service contract, we standardised all configurations and activated their web application firewall to provide active protection and monitoring against threats



As a result, they could better protect both web-based and mobile banking applications, mitigate threats and safeguard customer data

The client

A financial institution faced various challenges around F5 automation, configuration consistency, security posture and planned projects for open banking initiatives.

As an F5 Gold Partner and the UK's most certified F5 specialist, they sought our expertise and assistance not only to address these but also to improve their current cyber security infrastructure and the overall network traffic management of their F5 products.

Taking place between 2017 and 2020, we undertook an extensive project to provide a wholesale upgrade and update their F5 infrastructure, starting with open banking and home automation and later encompassing the entire F5 estate.

This included rolling out our managed services and successfully activating a web application firewall (WAF).



The challenge

The financial institution had been primarily using physical F5 devices.

However, their F5 configurations were inconsistent, as they'd used multiple external consultants to set up policies and experienced multiple changes in personnel in their in-house teams. This created a whole host of challenges around troubleshooting and policy management.

They also had previously purchased a WAF but had not set it up to realise its full benefits, leaving them vulnerable to cyber attacks.

Here's what we did.



What we did

We started by migrating the financial institution's F5 estate to a virtual platform, enabling capabilities for automation in the future. Our consultants then standardised all configurations, improving naming conventions, and testing the platform's compatibility.

We also fully implemented, correctly configured and activated the WAF so it provided active protection and monitoring against web attacks.

Following migration, we offered support for an additional three months remotely through training and configuration.



The Result

As a result of working with us, the financial institution could better protect both web-based and mobile banking applications, safeguarding customer data and mitigating potential cyber threats.

The new standardised configurations significantly enhanced their security posture and operational efficiency over the long term, as troubleshooting became much more straightforward and they could resolve security incidents promptly and effectively.

While our expert implementation and activation of the WAF provided powerful protection and monitoring against web attacks.

Over the course of a two-year managed services contract, our team of technical consultants also supported the financial institution to become fully self-sufficient in using its F5 devices.

We now proudly maintain a continued partnership with the financial institution and remain their preferred supplier for future F5-related services and initiatives.



Minimise your security risk. Maximise your return on investment.

We're the UK's most certified F5 and Fortinet specialists, with 30 years of industry-leading cyber security expertise.

Get in touch to learn more about how we help you secure your environment and get quicker ROI from your investment.

BOOK A MEETING

FORTINET



Gold
Unity Partner
Value Added Reseller



FullProxy

CASE STUDY

How we supported
a major financial
institution to enhance
their security posture,
mitigate threats and
protect customer data

