Graham Mattingley

F5 BIG-IP Specialist and Virtual F5 Contractor

30+ years in IT and application delivery, 13+ of them on F5 BIG-IP.

graham.mattingley@gmail.com | Approxee, the virtual F5 contractor | approxee.eu

PROFILE

F5 BIG-IP specialist with more than thirty years in IT and application delivery, over thirteen of them focused on F5. One of the first individuals in the UK to complete the F5 Certified Technology Specialist exams, passing the F5 101 on its launch day, 14 December 2012.

F5 Certified Solution Expert in Security (401), the top of the F5 certification ladder, and an OWASP member. Deep experience in application security for multi-tiered systems, application resilience and failure testing, and performance optimisation.

Founder of Approxee, the virtual F5 contractor service. Also an experienced F5 trainer, having helped more than fifty UK students pass F5 exams, and comfortable presenting at board and CISO level.

CORE SKILLS

F5 BIG-IP	LTM, ASM / Advanced WAF, GTM / DNS, AFM, APM, SSLO, iRules / iControl
F5 Distributed Cloud (XC)	Application Security, Secure Multi-Cloud Networking
Security and applications	OWASP, PCI DSS, Application architecture and resilience, WAF policy design
Adjacent	Citrix NetScaler, .NET / TCL, ASP / MVC, HTML / JS / CSS, Oracle, Azure, AWS

CERTIFICATIONS

- F5 Certified Solution Expert, Security (401)
- F5 Certified Technology Specialist: LTM, ASM, DNS, APM
- F5 Certified Administrator, BIG-IP
- F5 Distributed Cloud (XC) accreditations, 2025

21 F5 exam passes since 2012, with every specialist exam recertified three to four times. OWASP member.

EXPERIENCE

Access and Application Security Platform

09/2024–01/2026

A major European petrochemical company

Faced significant broken access control (OWASP A01) and authentication (OWASP A07) issues. We designed and built a complete access platform on F5 APM to protect their critical applications, integrating both cloud and on-premises Active Directory as identity sources and using SAML together with APM, AFM and ASM. We implemented two-factor authentication on F5 APM via the Google and Microsoft authenticator apps, forwarded logging to a SIEM, and applied full OWASP mitigation on the ASM. We also coded and implemented a custom API for service integration and a phased roll-out of the service; the API was called by APM to validate users.

F5 APM · F5 XC · AFM · ASM · SAML · Active Directory · 2FA / MFA · SIEM · Custom API · OWASP A01 · OWASP A07

Global DDoS and Bot Mitigation Strategy

Mid 2025

A confidential engagement, via a global IT services company

Engaged by a global IT services company to define the DDoS and bot mitigation strategy for their client, a major global enterprise. Our role was to advise and design: we produced the strategy document, built a proof of concept, and delivered a live demonstration of how the firm's public-facing internet sites would be protected against their DDoS and bot mitigation concerns and the wider issues affecting those sites. The engagement also included OWASP and ASM training, along with business-as-usual (BAU) and support.

DDoS mitigation · Bot mitigation · Strategy and design · Proof of concept · Public-facing sites · ASM · OWASP training · BAU support

F5 BAU Support and OWASP

03/2025–08/2025

A global insurance company

A six-month business-as-usual (BAU) engagement managing the F5 support ticket queue for a global insurance company. The F5 estate had been in place for some years and carried a good deal of legacy configuration, so alongside day-to-day support we were able to recommend a number of improvements. We reduced ticket response times, which built greater confidence in F5 support among the application and security teams. The engagement also included a significant OWASP element, covering both implementation and training.

BAU support · F5 support queue · Estate review · OWASP · OWASP training · ASM

Zero-Downtime F5 TMOS Upgrade

Mid 2025

An aerospace company

A standard F5 upgrade project across three data centres, taking four F5 devices from TMOS 14 to TMOS 17, which requires a two-stage upgrade path. The work relied on zero downtime, which the multiple data centre setup made straightforward to achieve. It involved a large programme of planning meetings covering what we would do, how we would test it and how we would carry it out, with some of the work done out of hours. Because the data centre environments were not identical, different issues surfaced on TMOS 17 and required a good deal of mitigation work. Overall we delivered everything, and the customer was very happy.

F5 upgrade · TMOS 14 to 17 · Zero downtime · Multi-data-centre · Out-of-hours · Migration testing

Four-Year ASM / WAF Programme

07/2019–08/2023

A global financial messaging network

A four-year retained contract for a global financial messaging network, renewed on a six-monthly rolling basis. The first phase was to implement ASM policies across all of their internet-facing websites, 78 in total, and move them into blocking mode. Technically this was straightforward, though delivered with the caution and rigorous change control you would expect in banking. Following that success, we were retained to provide a similar service on the internal messaging system, which is business-critical: it carries financial messaging data across the global banking system. We delivered that successfully as well, and the work included training services for both BAU and new services. Everything was achieved over the four years.

ASM / Advanced WAF · WAF policy · Blocking mode · 78 sites · BAU support · Training · Retained (4 years)

F5 Application Onboarding and Enablement

2017–2022

A major energy and utilities company

A multi-year engagement, largely full time, implementing new services on the F5 for a major energy and utilities company as they rolled out applications at around two a week. This was not a BAU role: every application had to be implemented on the F5, which meant working closely with their developers, their security team and an in-house F5 team that was new to the platform. The core onboarding phase was delivered over around four months, covering the final twenty or so applications on the F5, and included BAU and new-service training. We have since returned twice to provide further training and support, covering BAU, application, and general OWASP and F5 ASM training.

F5 implementation · Application onboarding · New services · Team enablement · OWASP · ASM · F5 training

Wider F5 delivery, by sector

2012–present

Enterprise clients across multiple sectors

Alongside the specific engagements above, ongoing F5 application delivery and security across airlines, airport operators, tier-one banking, interbank and card payments, insurance, aerospace and defence, energy, media and global IT services. LTM, ASM / Advanced WAF, GTM / DNS, AFM, APM and iRules; WAF policy design and tuning; HA and DR design; PCI DSS and OWASP alignment.

LTM · ASM / Advanced WAF · GTM / DNS · AFM · APM · iRules · WAF policy · HA / DR · PCI DSS · OWASP

Application, network and security delivery

1990s–2012

Banking and telecommunications

More than thirty years designing and deploying critical applications and networks, spanning networks, security, databases, application delivery, and design and coding.

Networks · Security · Databases · Application delivery · Design and coding

F5 Trainer

Across career

Designed and delivered F5 training. Upskilled 20+ engineers to F5 300-level at a security services firm, and helped more than fifty UK students pass F5 exams.

F5 101–301 · Course design · Mentoring · Board / CISO level

These are a representative sample of real F5 engagements. Engagements of less than six months are not shown individually here.

SPECIALISMS

Software Development

My development experience goes back to 1995 and covers the full application lifecycle, from architecture and database design through to development, testing and production deployment. I have worked with traditional N-tier and full-stack architectures, domain-driven design and modern development practices, using technologies including SQL Server, MySQL and MongoDB. I have developed and supported live production applications, worked as part of development teams, and continued to adapt my approach as development standards, architectures and technologies have evolved.

Development as a Way of Thinking

I have always regarded development as a way of thinking rather than simply a way of writing code. The same skills used to design an application (understanding requirements, breaking complex problems into manageable components, defining interfaces, controlling state and data flow, testing behaviour and designing for failure) are the skills I apply to F5.

That applies whether I am developing automation, writing iRules, building APM access policies or designing the wider BIG-IP configuration. I do not regard F5 as simply a box sitting between a user and an application. I see it as an application delivery framework: something that can be designed, structured and engineered as part of the application architecture itself. My development background therefore has a direct influence on the way I approach F5 design, troubleshooting and automation.

Application Delivery and Resilience

I treat F5 as the outer layer of the application: a delivery, security, access and resilience framework rather than simply a device that sits in front of it. My approach is therefore to develop against the platform, not just configure it according to a product manual. I normally start by stepping back from the individual requirement, understanding what the application and business are trying to achieve, and then developing a strategy around what is possible, how it should be designed, and how it should operate in production. That design can then be reviewed with the wider team before implementation using AS3, automation, the CLI or the GUI, depending on what is appropriate for the environment.

That approach is supported by deep practical experience across the F5 platform. I have extensive experience of high availability, DSC and resilient application delivery, together with specialist expertise in ASM/WAF, application security, traffic management, application performance and access technologies including SAML. The important distinction is that I approach these areas with a developer mindset rather than a configuration mindset. I think in terms of architecture, behaviour, dependencies, failure scenarios, repeatability and lifecycle management, with the F5 forming an engineered part of the application delivery architecture rather than a collection of independently configured objects.

Application Security and OWASP

Application security is my first consideration in almost every F5 engagement. I do not treat security as something that is added after the application delivery design has been completed; it is part of the design from the beginning. My objective is always to provide the strongest practical level of protection while still allowing the application to operate as intended.

As an OWASP member, and having worked extensively with ASM/WAF, AFM and APM, I have a deep working knowledge of the OWASP threat model, common web application attack techniques, how those attacks present themselves in real traffic, and the controls available to mitigate them. This includes designing and tuning WAF policies, securing multi-tier applications, protecting authentication and access flows, and working within environments subject to standards such as PCI DSS. I have also taught OWASP courses and principles to some of the largest and most critical companies in the world.

One of the advantages I bring is the ability to work directly with application developers rather than treating the F5 as a separate security appliance. Having been a developer for around 30 years, I can discuss the underlying application behaviour, understand why a vulnerability exists, and work with the development team on the correct long-term remediation. At the same time, I can use F5 controls to provide an immediate mitigation where required, whether through ASM/WAF, AFM, APM, traffic policy, iRules or another appropriate mechanism.

That distinction is important. The objective is not simply to block an attack and close a ticket. It is to understand the vulnerability, recognise the attack path, apply an appropriate mitigation, document exactly what has been found and what has been implemented, and then work with the development team towards a permanent resolution. Security therefore influences almost every F5 design decision I make, whether the original requirement is security-related or not.

EARLIER CERTIFICATIONS

Cisco CCNA, CCNP and CCIE Written (2001), which led into the F5 and application security specialism that followed. Full F5 certifications are listed above.