SOLUTION OVERVIEW

Next-Gen WAF Leverages Threat Intelligence to Block Attacks

Protect web apps in any cloud, edge, and on-premises environment with a comprehensive WAF as a Service from F5.

KEY BENEFITS

Easy-to-use, SaaS-enabled security
The SaaS-based F5 Distributed Cloud WAF is painless to set up, deploy, manage, and scale with no hardware or software to deploy or maintain.

Protect applications closer to the source
Deploy across multiple environments, including different clouds, edge, and on-premises locations—and leverage F5 PoPs for policy enforcement wherever required.

Accelerate time to market
Reduce DevOps teams' dependency on SecOps to build policies to secure applications, enabling developers to deliver and release applications faster.

Reduce time to resolution in responding to threats
Customize and update policies per F5 Labs' threat intelligence, to safeguard apps and infrastructure from emerging attacks and thwart active attack campaigns and malware in real time.

Gain end-to-end observability and policy enforcement
Improve the efficiency of SecOps teams by providing visibility and unified security policies that are portable across clouds and environments.

Lower total cost of ownership
Maximize uptime and reduce TCO by leveraging F5's 25+ years of app security experience as a top WAF vendor.

Securing applications and infrastructure is demanding work. Tracking sophisticated, multi-vector attacks is extremely difficult. It takes experienced professionals, powerful tools, and vast expertise to do it well.

Still, there are enormous challenges, including:

- Inaccurate automated detection
- Costly and ineffective threat hunting
- Need for significant data and monitoring

Moreover, NetOps and SecOps teams at many organizations have been unable to keep up with the rapid pace of change. DevOps teams often view their NetOps and SecOps counterparts, and their security toolkits, as impediments that slow their progress. This has exacerbated the application security coverage gap that these enterprises face.

The proliferation of modern, microservices-based applications and APIs has expanded application attack surfaces—and traditional solutions are unable to provide consistent coverage. SecOps teams have been forced to rely on disparate, legacy security solutions, and as a result, their efforts net fewer returns than they would otherwise.

The result is often a higher total cost of ownership (TCO) and lower effectiveness against evolving attacks. The teams' stretched resources and ineffective tooling often mean their attack responses are conducted manually, creating an even greater burden on already-constrained resources.

The good news? With F5, an industry-leading provider, advanced WAF technology is more accessible and affordable than ever before and includes threat campaign protection to thwart potential attacks.

F5 Distributed Cloud WAF: Safeguard Your Apps Wherever They're Deployed

Protect web apps in any cloud, edge, and on-premises with a comprehensive WAF as a Service from F5 Distributed Cloud Services, leveraging F5's best-in-class Advanced Web Application Firewall.

A WAF safeguards web-based applications from a myriad of threats. It acts as an intermediate proxy by inspecting application requests and responses to block and mitigate a broad spectrum of risks—including hacking, zero-day exploits, L7 denial-of-service attacks, and more.

KEY FEATURES

Streamlined setup and management
Deploy through a simple user interface or automate via APIs, with best-practice default protections and the flexibility to add custom rules.

Robust attack-signature engine
The Distributed Cloud WAF signature engine contains more than 7,000 signatures for CVEs, plus known vulnerabilities and techniques identified by F5 Labs.

Advanced behavior engine
Client interactions are analyzed on how a client compares to others—the number of WAF rules hit, forbidden access attempts, login failures, error rates, and more.

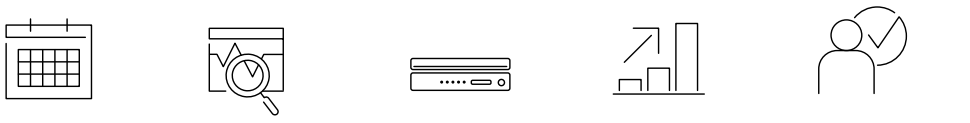
Powerful service policy engine
Utilize IP reputation and allow/deny lists, so you can block clients with known bad TLS fingerprints, with ASNs, from suspicious countries, and more.

Automatic attack-signature tuning
Easily determine if a signature-identified attack is really a threat, helping you reduce the number of false positives.

With F5 Distributed Cloud WAF—a featured product in the SaaS-based F5 Distributed Cloud Web Application & API Protection (WAAP) solution—you can seamlessly add multi-layer WAF protection to any application, regardless of where it's deployed. Implement and evolve protections as needed to combat common threats such as injection, cross-site scripting, software vulnerabilities, and more.

This WAF brings together best-in-class capabilities leveraging the Advanced WAF engine, with behavioral learning and machine learning adapted from F5 Distributed Cloud Services. It features a robust attack-signature engine and advanced behavior threat engine, and leverages threat intelligence from F5 Labs to keep pace with emerging threats in real time.

F5's centrally managed cloud platform offers adjacent benefits, such as easier audits, policy adherence for applications at scale, and assurance that policies are appropriate for the risks and threats that applications face.



Plan
Reap the benefits of dedicated, experienced F5 threat researchers.

Collect
Discover attacks using honeypots and other active monitoring tools.

Process
Use metadata and multi-vector threat intelligence to correlate the specific actions of an active attack campaign.

Analyze
Correlate and validate to provide accurate mitigation signatures and tactics.

Distribute
Leverage insights to proactively block attacks (e.g., prevention in place, tactics, attacker description, etc.).

Figure 1: Threat intelligence from F5 Labs helps WAF as a Service customers stay on top of emerging threats.

Packaging F5's Industry-Leading Security Expertise and WAF Technology

F5 has teams of researchers and engineers dedicated to application security, and our industry-leading expertise is packaged and available today to defend apps of every size and variety.

You don't need to build your own team of experts, collect and ingest threat data, track and monitor evolving/advanced threats, and create customer signatures for your own tool to block/detect. Leverage F5's more than 25 years of expertise and experience.

THIS WAF BRINGS TOGETHER BEST-IN-CLASS CAPABILITIES LEVERAGING THE F5 ADVANCED WAF ENGINE, WITH BEHAVIORAL LEARNING AND MACHINE LEARNING ADAPTED FROM F5 DISTRIBUTED CLOUD SERVICES.

Other important benefits:

- A cost-effective service model for confident risk mitigation
- Regular updates with accurate threat intelligence from F5
- Improved web application security with confidence and near-zero false positives
- Unique and flexible deployment options that will make implementation for your app a snap

Apps are the lifeblood of your business and the demands placed on them have never been greater.

Delivering superior digital experiences requires performant, effective, and scalable security wherever and however the needs of your business dictate. As applications become increasingly modular and distributed, your WAF needs to adapt to support these environments. The F5 Distributed Cloud WAF can be deployed wherever your apps are deployed, while being managed via a centralized SaaS infrastructure.

F5 delivers the security efficacy and ease of use sought by NetOps and SecOps teams today. Our innovative and accessible Distributed Cloud Platform can help organizations of all shapes and sizes reduce application protection coverage gaps and get consistent coverage across all apps in the cloud, on premises, and in edge locations.

Get started today. Contact an expert at sales@f5.com to arrange a free trial. For more information, visit our Distributed Cloud Services page at f5.com/cloud.