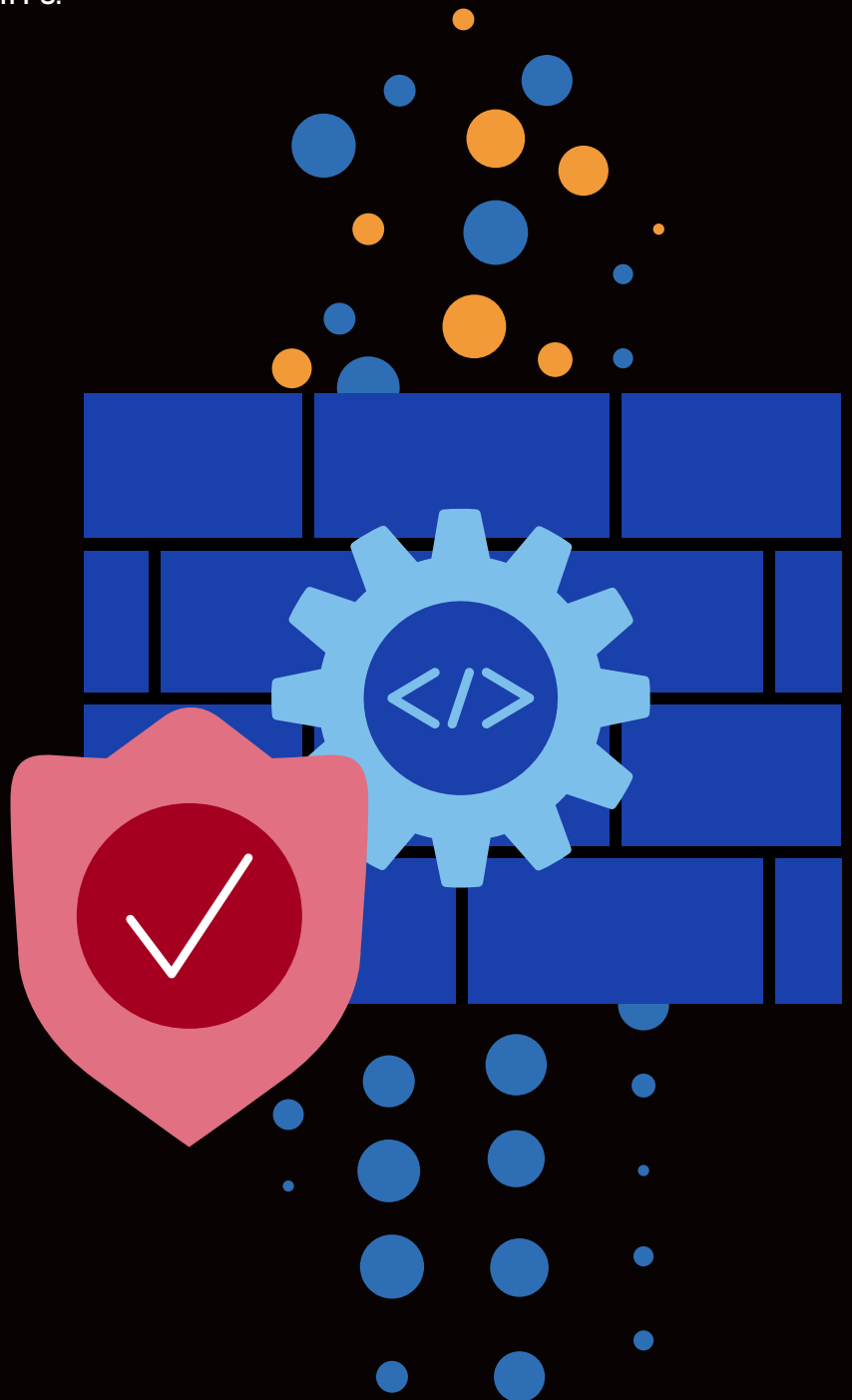


F5 Distributed Cloud Web Application Firewall (WAF)

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



Key Benefits

Easy-to-use, SaaS-enabled security

The SaaS-based F5® Distributed Cloud WAF is painless to setup, 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 the F5 Global Network and points of presence (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 25+ years of F5 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 SaaS-based WAF from F5 Distributed Cloud Services, leveraging F5's best-in-class advanced WAF technology.

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 SQL injections, cross-site scripting, L7 denial-of-service attacks, malicious bot traffic, and more.

Key Features

Flexible service options

Choose to deploy and manage on your own, or let F5 deliver as a managed service—deployed, maintained, and supported 24x7 by certified experts in our Security Operations Center (SOC).

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

Captures Common Vulnerabilities and Exposures (CVEs) plus known vulnerabilities and techniques identified by F5 Labs, including Layer 7 DDoS, bots, automated threats, and OWASP Top 10.

Advanced behavior engine

Leverages AI/ML to monitor and score client interactions, deciphering intent based on the number of WAF rules hit, forbidden access attempts, login failures, error rates, Malicious User Detection, and more to help identify an app's highest-priority threats.

Powerful custom rules engine

Enables micro-segmentation and advanced security at the application layer, utilizing IP reputation and allow/deny lists to block clients with known bad TLS fingerprints, ASNs from suspicious countries, and more.

With F5 Distributed Cloud WAF—a featured product in the SaaS-based F5® Distributed Cloud Web App and 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 F5 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.

The centrally managed F5® Distributed 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.

Threat intelligence from F5 Labs helps SaaS-based WAF customers stay on top of emerging threats.

Packaging F5 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 threats, and create customer signatures for your own tool to block/detect. Leverage more than 25 years of F5 expertise and experience.

Some key benefits of F5 Threat Campaigns:

- Mitigate threats cost-effectively by eliminating the need for internal threat hunting
- Proactively block attack campaigns to strengthen web application security
- Utilize real-time, automated tactical threat intelligence to help identify the individual actions of active attack campaigns
- Achieve near-zero false positive through F5 threat researchers to monitor attack campaigns

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

Key Features

IP reputation service

Easily allow or deny IP addresses based on threat categories or threat score using the F5 database of known malicious IP addresses.

Detects and prevents threat campaigns

Detects active attacks or campaigns that may pose a threat to apps.

Automatic attack-signature tuning

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

Simplify security operations with our AI assistant

Ask questions in natural language to obtain AI-powered insights that enhance security, help detect anomalies, and provide actionable recommendations in real-time.

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.

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 at the edge.

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.

