THINK APP SECURITY FIRST

IS YOUR WAF KEEPING PACE

WITH TODAY'S THREATS?

As the threat landscape evolves, so must our security controls and countermeasures. Recent research from F5 Labs revealed that applications are the initial targets in the majority of breaches, suggesting that any app can be an attack vector. Cybercriminals are moving their tactics further up the stack using sophisticated application-layer exploits, as well as an emerging wave of automated, bot, and IoT-based threats that are quite capable of evading simple signature or reputation-based detection. **Yet, the majority of WAFs on the market today have remained largely unchanged, leaving the app-layer exposed, unable to proactively monitor and protect against evolving attack vectors.**

F5 ADVANCED WAF AT A GLANCE

Superior protections against credential theft and abuse.

The only WAF with comprehensive mitigation of web and mobile bot threats.

Layer 7 DDoS detection using machine learning and behavioral analytics for high accuracy.

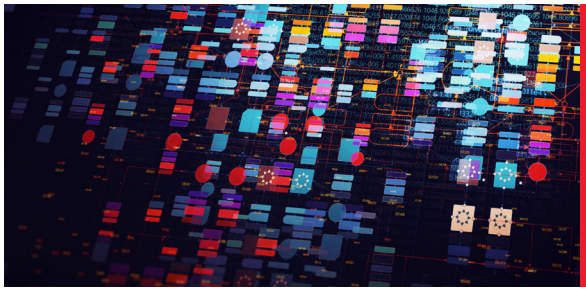
The market's most scalable WAF solution.

NOT ALL WAFS ARE CREATED EQUAL.

The most advanced perimeter threats for data loss or exfiltration occur at the application layer, rendering most next-gen firewalls (NGFW) and intrusion prevention systems (IPS) much less effective. At the same time, communications are moving to encrypted data channels not well-supported by NGFW or IPS, particularly at scale. To counter these newer threats, web application firewalls are specifically designed to analyze each HTTP request at the application layer, with full decryption for SSL/TLS.

There are a few things we know about the current threat landscape and how attacks go undetected:

- Most threats are automated in nature. Attackers automate scans for vulnerabilities. Distributed denial-of-service (DDoS) attacks are fully-automated to enable the kind of 1Tbps+ attack traffic volume that has become commonplace. Automation is difficult to detect because it often mimics good traffic.
- Credential stuffing is an automated attack that leverages billions of known username and password combinations from prior breaches. Use of stolen credentials was the most prevalent type of application attack of 2017, according to recent threat reports, and they are often "low and slow," to avoid detection as a brute force attack.
- Malware is pervasive and is used to exploit weaknesses in browsers and the users operating them. Limited detection and mitigation methods are available unless the client machine is managed by an experienced IT infosec team.
- DDoS attacks are not just volumetric in nature. Many attacks are designed to cause resource exhaustion somewhere in the application stack, the application servers, middleware, or back-end database. Detecting these conditions can be difficult since the traffic conforms to most standard input validation checks.



THESE ATTACKS BYPASS VIRTUALLY ALL TRADITIONAL WAF DETECTION MECHANISMS.

Simply put, these attacks bypass virtually all traditional WAF detection mechanisms since they often do not appear malformed in any way. A more advanced web application firewall is clearly needed to fight these threats.

An advanced WAF for today's advanced threats.

As we've shaped the direction of WAF in the past, so we do today with F5 advanced WAF technology. Focusing on today's constantly shifting threat landscape, F5 advanced WAF delivers proactive, behavioral-driven, automated, and integrated web and mobile protections.

F5 ADVANCED WAF SURPASSES OTHER VENDORS WITH NEW CAPABILITIES.

F5 ADVANCED WAF CAPABILITIES	OTHER VENDORS
ANTI-BOT PROTECTION FOR WEB AND MOBILE APPS Protection extends beyond signatures with client fingerprinting and server performance monitoring for all your apps.	Provide protection for only for web apps, not mobile apps.
LAYER-7 BEHAVIORAL DDOS Behavioral analysis with machine learning enables dynamic signatures to immediately address changing conditions, continually monitoring and adapting to proactively address potential threats.	Provide behavioral DoS that's more reactive, meaning updates require manual tuning to create new signatures that need to be deployed.
CLIENT-SIDE CREDENTIAL PROTECTION Account takeover protection stops credential theft and abuse with deep field encryption backed by obfuscation and evasion detection and comprehensive brute force mitigation.	Only offer credential stuffing feeds—blocking known malicious sites after credentials are compromised.

F5 provides perpetual, subscription, and utility billing options to give you the ultimate flexibility for deploying F5 advanced WAF in the cloud and the data center.

Learn more about how our unique advanced WAF capabilities set us apart by contacting an F5 WAF specialist today.