F5 Advanced WAF

KEY BENEFITS

- Protect your web applications from vulnerabilities and web attacks
- Identify and mitigate automated attacks by bots and other attack tools before they cause damage
- Identify attacks using machine learning to detect and mitigate attacks with the highest level of accuracy

Web attacks are the leading cause of data breaches.[1] Despite the best efforts of secure application- and patch-management processes, half of all applications remain vulnerable, 24x7.[2] Web application firewalls (WAF) protect your applications from data breaches by fixing vulnerabilities and stopping attacks. F5® Advanced Web Application Firewall™ provides malicious bot protection, application-layer encryption, API inspection, and behavior analytics to help defend against application attacks.

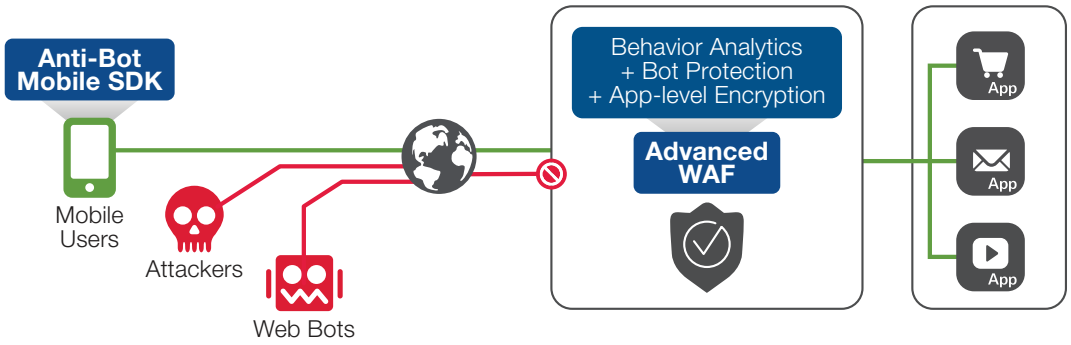
Attackers have embraced the use of automation to scan your applications for vulnerabilities, attack account credentials, or cause denial of service (DoS). F5's proactive bot defenses stop automated attacks and leverage a combination of challenge- and behavior-based techniques to identify and filter out bot traffic. By stopping bad bots, you can eliminate many of these opportunistic attacks.

Seventy-five percent of data breaches start with identity attacks. Advanced WAF includes F5 DataSafe to help encrypt data and credentials at the application-layer—without having to update the application. This encrypts the data as it passes through the Advanced WAF solution.

Behavior analytics are a requirement for detecting blended attacks. Many layer 7 distributed denial-of-service (DDoS) attacks are stealthy and may go undetected by traditional signatures and reputation-based solutions. Advanced WAF automatically learns the application behavior, then combines the behavioral heuristics of traffic with the server stress to determine DDoS conditions. This process provides the most accurate detection without false positives. Dynamic signatures are then created and deployed on the fly for real-time protection.

[1] Verizon's 2017 Data Breach Investigations Report. "Figure 33: Percentage and count of breaches per pattern (n=1,935)"

[2] 2017 Application Security Statistics Report—"half of all applications continue to remain vulnerable for 365 days a year"



CHALLENGES

- Automated attacks and bots overwhelm existing security solutions
- Malware and keyloggers steal data and credentials to gain unauthorized access to user accounts
- Application-layer attacks evade signatures and reputation-based security solutions

FOR MORE INFORMATION

- F5 Enterprise Solutions—Application Security
- F5 Anti-Bot Mobile SDK
- F5 DataSafe

F5 Advanced WAF Features

Proactive Bot Protection:

Proactively defend your applications against automated attacks by bot and other attack tools. This prevents layer 7 DoS attacks, web scraping, and brute-force attacks. Proactive bot defense helps identify and mitigate attacks before they cause damage to the site.

DataSafe:

Protect sensitive information from interception by encrypting data while it's still in the browser. DataSafe encrypts data at the application layer to protect against malware and keyloggers. This renders leaked credentials or data useless.

Behavioral DoS:

Behavioral DoS provides automatic protection against DDoS attacks by analyzing traffic behavior using machine learning and data analysis. By continuously monitoring server health and load, anomalies (performance slowdowns or traffic spikes) can be accurately detected and mitigated as needed.

Flexible Deployment:

Available as a purpose-built appliance, a cloud-ready virtual appliance, or part of the F5 Silverline service.

DC0318 | OV-SEC 253143946 | 0718