Protection for Every App, Anywhere

F5® BIG-IP® Advanced WAF® protects applications and APIs from bad actors and automated threats trying to steal data, take over accounts, siphon resources (for example, cryptomining), and exploit zero-day vulnerabilities. Deployable across multi-cloud, hybrid, and on-premises environments in various forms, BIG-IP Advanced WAF provides a robust suite of sophisticated protections while enabling security automation for DevOps and AppDev.

KEY BENEFITS

Improve security posture and secure apps
Protect against the most common types of attack and streamline application security.

Bring apps to market faster with lower cost and higher security efficacy
Integrate security as code within apps being developed using a "shift left" approach that enhances automation and saves time.

Defend your apps from active attack campaigns
Receive security updates about the latest vulnerabilities and block ongoing threat campaigns with an optional F5 Threat Campaigns subscription.

Easily customizable to meet different security use cases
Guided configuration helps you create application security use cases that match your organizational needs, such as web app protection (comprehensive protection, behavioral DoS, bot protection) and API security.

Ensure government and industry compliance regulations
Complies with government and industry regulations to meet privacy and security requirements based on region.

Higher security efficacy via fine-grained controls
Independently manage security policies for microservices.

The Need for Apps and API Protection Wherever They're Deployed

Applications are more than just code. Applications are what connects businesses to their customers. Applications drive digital transformation. Applications drive business.

As organizations modernize their applications by adding new functionality, delivery points, and moving to an API-first approach, the need for advanced application security controls is more critical than ever. Modern applications are incredibly diverse in their architectures and delivery, where they reside, and their regulatory and protection requirements.

BIG-IP Advanced WAF meets theses needs with comprehensive application protection for a full range of app and API security requirements. BIG-IP Advanced WAF protects against common vulnerabilities (CVEs) and web exploits, targeted attacks, and advanced threats. BIG-IP Advanced WAF can be deployed wherever your apps are found—from complex hybrid and multi-cloud environments to on-premises and private clouds—and it's available as a full-featured, self-managed web application firewall.

F5 BIG-IP ADVANCED WAF

Today's applications require advanced security. BIG-IP Advanced WAF delivers sophisticated controls that mitigate automated application attacks, protect against known and zero-day vulnerabilities, and further detect and minimize the risk of attacks using F5 intelligent security threat services. In addition to standard app security capabilities, BIG-IP Advanced WAF offers protection for sensitive web form data, such as login credentials, app-layer denial of service (DoS) protection, defense against targeted threat campaigns (with an add-on subscription), proactive bot defense, and fine-grained controls for API security.

Common WAF Security

Web applications remain a top target for threats such as automated attacks, data exfiltration, and session tampering. BIG-IP Advanced WAF protects applications from common attack types, such as the OWASP Top 10 and SQL/PHP injection. BIG-IP Advanced WAF also defends against attacks targeting known CVEs and zero-day attacks.

BIG-IP Advanced WAF includes a dedicated OWASP Top 10 Compliance Dashboard that reflects the level of mitigation applied by your security administration against the latest version of the OWASP Top 10 vulnerability categories. The dashboard provides a security score relative to deployed policies to address the OWASP Top 10, enabling your security administrators to view each policy's coverage status and improve protections, if necessary. Security configuration can even be performed directly from the dashboard.

KEY FEATURES

Secures apps against common, known, and unknown (zero-day) attacks
Defends against common attack vectors, including known vulnerabilities (CVEs), OWASP Top 10, SQL/PHP injection, and more.

Protects credentials from theft
Prevents man-in-the-browser credential theft tied to app-level credential encryption.

Mitigates Layer 7 DoS
Behavioral DoS provides automatic protection against DoS and DDoS attacks by analyzing traffic behavior using machine learning (ML) and data analysis.

Safeguards APIs
Secures GraphQL, REST/JSON, XML, and GWT APIs, while also simplifying API protection profile configurations.

Delivers security as code
Leverages declarative APIs to shift security left in your software development life cycle (SDLC).

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

BIG-IP Advanced WAF also supports modern application architectures, enabling security administrators to independently manage security policies for microservices, such as the ability to set transparency or blocking per microservice.

Layer 7 DoS Protection

Behavioral 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 signature and reputation-based solutions. BIG-IP Advanced WAF automatically learns the application's behavior, then combines the behavioral heuristics of traffic with the server stress to identify DDoS conditions. Dynamic signatures are then created and deployed for real-time protection. This process provides the most accurate detection while minimizing false positives.

API Security

APIs are the connective tissue of today's apps, delivering a steady stream of needed data and information. APIs provide access to business technologies that would simply be unattainable for many organizations. For instance, companies such as Uber can easily replicate Google Maps for a small cost with the Google Maps API, allowing Uber to provide valuable services to their customers. APIs are at the core of modern business and it's no surprise that the number of API-related attacks has also increased. Now more than ever, APIs require enhanced security.

API security failures have been the cause of some of the most recent high-profile API data breaches. Often API security is overlooked, and organizations don't properly implement authentication and authorization. Inadequate authentication and authorization security rank among the most common threats to APIs, according to OWASP's API Security Top 10. APIs are also susceptible to many of the same attacks that affect web applications. The attacks listed below aren't new, but all can be easily used against APIs:

- Injection and security misconfiguration are common web attacks that can also apply to APIs; but others, such as requests for invalid data types, can also lead to unauthorized data access.
- API endpoints are among the growing list of DDoS attack targets that can make an application unavailable to intended users (or other applications, in the case of APIs).

You can augment your API gateways with BIG-IP Advanced WAF to secure API management gaps, enabling API security for all use cases, whether for the edge or the API endpoint.

BIG-IP Advanced WAF's API security enables your organization to defend against API-specific risks with fine-grained controls for securing various APIs, including GraphQL APIs, XML, REST/JSON APIs, and GWT APIs. Advanced WAF's support for GraphQL is unique, with native

parsing of GraphQL traffic, allowing Advanced WAF attack signatures to be applied. This approach detects attacks in the appropriate segments of a payload and runs the signatures on those values. This will also stop false positives due to attack signatures running on the wrong parts of GraphQL requests.

F5 creates a GraphQL policy template and content profile as part of its Application Security Policy. An organization can configure the total length and value length of parameters in the content profile, limiting them according to policy. They can also configure the maximum structure depth, eliminating recursive GraphQL queries that lead to a DoS attack. Maximum batched queries can also be defined, limiting the number of different GraphQL queries in one HTTP request and the chances of malicious exploit.

DevOps and Security Automation

Modern applications are comprised of microservices and APIs and use open-source software, increasing risk and the threat surface area. With Agile development models in place, it has become difficult for SecOps to keep pace with application developers and for DevOps teams to implement security controls properly. Security controls may be implemented improperly or too late to be effective.

BIG-IP ADVANCED WAF PROTECTS APPLICATIONS AGAINST SOFTWARE VULNERABILITIES AND COMMON WEB EXPLOITS, AND DEFENDS AGAINST TARGETED ATTACKS, AND ADVANCED THREATS.

Current development processes are based on continuous integration/continuous development (CI/CD) principles, where security controls—especially WAF—are often placed at the end or out of the software development life cycle (SDLC). So, if DevOps runs into a failed test at the “Operate” stage toward the end of their SDLC, it’s treated as a security misconfiguration. This can create new or exacerbate existing tensions between your DevOps and SecOps teams. It will also force DevOps to return to their code, repair it, and then redeploy, operate, and monitor—creating additional cost, potentially missing time-to-market deadlines, and possibly reducing competitive advantage.

F5 aligns WAF policy construction and baselining into the development process to address this, leveraging an approach that enables both infrastructure and security policy controls to be provided as code in a declarative API. This allows BIG-IP Advanced WAF customers to automate both application deployment and WAF policies, as depicted in Figure 1.

KEY TAKEAWAYS

- Preemptively protect against credential attacks with F5 Leaked Credential Check
- Leverage the OWASP compliance dashboard that reflects the level of mitigation applied against the OWASP Top 10 security risks
- Guided configuration provides a simple, step-by-step utility to configure and deploy common WAF use cases
- Supports modern application architectures enabling security admins to independently manage security policies for microservices
- Effective threat hunting for ongoing attacks with significant monitoring with F5 Threat Campaigns
- Around the clock access to expert service and support

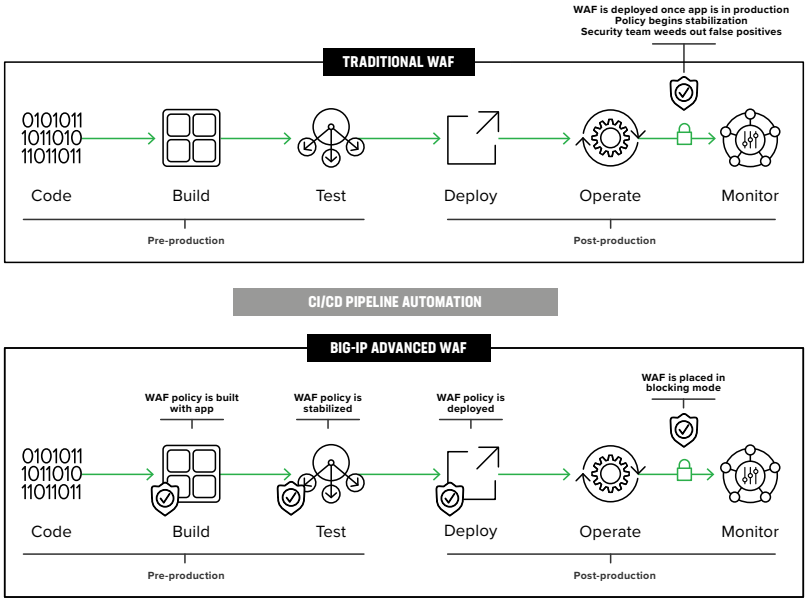

Figure 1: Incorporating WAF policy construction earlier in the development process reduces the risk of security misconfiguration late in the CI/CD pipeline.

And just like your application source code, BIG-IP Advanced WAF policies can reside in a code repository, enabling SecOps to own and maintain common security controls that can be integrated into the development pipeline just like any other piece of code. This approach helps DevOps and SecOps bridge operational gaps and bring apps to market faster with lower cost and higher security efficiency. Check out this Solution Overview to learn more about security automation for DevOps with BIG-IP Advanced WAF.

Threat Campaigns

F5 Labs research has shown that nearly three critical vulnerabilities are released daily. This can make it difficult for SecOps to empower their WAF to defend against targeted attacks. Advanced threats require an advanced WAF equipped with live, actionable threat intelligence to enable smarter security controls that automatically detect and block active attack campaigns.

F5 Threat Campaigns™ is an add-on threat intelligence subscription for BIG-IP Advanced WAF. The service provides intelligence that contains contextual information about the nature and purpose of active threat campaigns. It detects sophisticated attacks by leveraging metadata and multi-vector threat intelligence to correlate incidents of active threat campaigns. It is leveraged for high confidence risk mitigation and virtually eliminates false positives. A Threat Campaign subscription also includes bot signature updates to detect and prevent basic bot attacks.

Leaked Credential Check

The use of stolen, compromised, or misused credentials is one of the most aggressive and leveraged attack vectors. Your SecOps team needs to be able to preemptively protect against these attacks. BIG-IP Advanced WAF offers an add-on subscription, F5 Leaked Credential Check™, that prevents credential-based attacks by delivering automated detection and mitigation of leaked, breached, and fraudulent credentials. It also enables your SecOps team to perform various evasive actions, including blocking user access, when compromised credentials are used. Check out the Leaked Credential Check Solution Overview to learn how to safeguard your organization against account takeover (ATO) via leaked credentials.

Bot Defense

Attackers have embraced automation to scan your applications for vulnerabilities, attack account credentials, and launch DoS attacks. The BIG-IP Advanced WAF bot detection solution defends against drive-by bots and targets of opportunity hacking (such as vulnerability exploitation). For instance, bot defense in BIG-IP Advanced WAF leverages a combination of challenge- and behavior-based techniques to identify and filter out bot traffic. By stopping bad bots, you can eliminate many attack opportunities, defending your apps and protecting your customers.

Bot attacks are difficult to stop. Criminals retool to bypass defenses, rapidly solving CAPTCHAs and mimicking human behavior. To stay ahead of bots, F5 Distributed Cloud Bot Defense uses AI to achieve unparalleled, long-term efficacy and without increasing customer friction.

Distributed Cloud Bot Defense protects against a broad set of bot-based attacks, including credential stuffing, account takeover, fraud, and account abuse. Deploy Distributed Cloud Bot Defense through a connector that's right for your apps, with support services tailored to your needs, from self-service to managed service. BIG-IP Advanced WAF's bot defense and Distributed Cloud Bot Defense can also be combined to confidently mitigate against bots. For more information on advanced fraud and highly specialized bot defense techniques, please visit F5 Distributed Cloud Bot Defense.

The DataSafe Profile Feature

Most data breaches start with identity attacks. The DataSafe feature protects data and credentials entered into sensitive fields in your web application by encrypting data at the application layer on the client-side. Transport Layer Security (TLS) protects traffic in transit, while application-layer encryption protects users at the browser level, where TLS/SSL terminates. The extra layer of security provided by DataSafe defends your users from malware tampering and man-in-the-browser attacks.

BIG-IP ADVANCED WAF CAN BE CONFIGURED TO AUTOMATE MITIGATION FOR NEW AND ONGOING THREATS, WITH F5 BIG-IP ADVANCED WAF'S SECURITY AS CODE APPROACH BRINGING APPS TO MARKET FASTER WITH LOWER COST AND INCREASED SECURITY EFFICIENCIES.

BIG-IP Advanced WAF includes DataSafe to help encrypt data and credentials at the application layer without updating your application. It encrypts the data as it passes through BIG-IP Advanced WAF. It also addresses data integrity as it detects and prevents transaction data manipulation that may be caused by malware at the browser level. Additionally, possible violations are sent to BIG-IP Advanced WAF for further mitigation.

Integrated F5 BIG-IP Local Traffic Manager

Application delivery capabilities typically associated with F5 BIG-IP Local Traffic Manager™ (LTM), such as SSL offload and load balancing, are included in BIG-IP Advanced WAF. This ensures improved security monitoring and performance.

Why BIG-IP Advanced WAF?

Today's digital world is application-driven. And as organizations like yours continue to expand their web application portfolios and increase the use of APIs, the demand for application-layer and API protections will increase. BIG-IP Advanced WAF delivers robust security features that protect apps and APIs for many customers, securing against the broadest array of threats. BIG-IP Advanced WAF offers assured security where it is needed, deployable across multi-cloud, hybrid, and on-premises environments in various form factors (containers, virtual machines, chassis, blades, or appliances).

F5 WAF also forms the solid foundation for all F5's web application security services, including BIG-IP Advanced WAF, Silverline® WAF, F5 NGINX® App Protect WAF, F5 Distributed Cloud WAF, F5 Distributed Cloud Web App and API Protection (WAAP), and F5 BIG-IP Next™ WAF, all of which have been built on the robust F5 WAF engine. Leveraging one WAF engine allows F5 to deliver customers like you a simple, unified, consistent experience across F5's market-leading WAF portfolio.

Learn more about F5 BIG-IP Advanced WAF

- Visit the F5 BIG-IP Advanced WAF web page
- Visit the F5 Web App and API Protection web page
- Learn more about F5 Automation and orchestration toolchain
- Join the F5 technical community