SOLUTION OVERVIEW

# Security Automation for DevOps with F5 Advanced WAF

KEY CAPABILITIES

- Declarative API-based deployment and configuration enables integration with DevOps tools and workflows
- Enables SecOps to manage and deliver security as “code” using easily readable JSON files for DevOps
- Ingestion of OpenAPI files support automated configuration of API security
- Integration with Webhooks (e.g., Slack, Teams) enables increased DevOps collaboration and advanced automation capabilities
- Ability to share base security across applications and custom controls per app via modular policy
- Ability to share policy objects across policies via reference to shared files

**Applications are at the center of digital strategy among modern organizations.** According to F5 Labs research, enterprise organizations manage an average of 983 applications, which often span across multiple clouds and data centers. Modern applications are generally designed with distributed architectures and built using agile development practices down to the component level. This framework for continuous integration and continuous delivery (CI/CD) enables DevOps to manage the software lifecycle with both speed and efficiency. With time to market as a primary KPI (key performance indicator), DevOps has adopted modern workflows and automation. Security, however, is often left out of the CI/CD workflow.

The absence of application security controls in the DevOps workflow means that they are not tested alongside the application code. As a result, application-security defects may not be discovered until operational testing is performed near the end of the development cycle, where addressing flaws is much more costly. The impacts may include significant delays in time to market, higher remediation costs, or inadequate security controls.

Introducing security testing earlier in the CI/CD process is the most efficient solution for addressing the gap between the application and security teams. The challenge is to do it with scale and efficiency, which requires both cultural and technology shifts that emphasize operational security testing as part of the application development phases.

F5® Advanced Web Application Firewall™ makes it possible to integrate operational application security testing early in the development pipeline. This allows comprehensive testing of both functional specifications and security policies early in the pipeline. The DevOps team can now discover security defects, either with the security policy or the application itself, while the application is still developing. When the team finds errors, they can perform remediation more efficiently and at a significantly reduced cost.

## Security as a Code

Integrating application security into the development pipeline is facilitated by using declarative APIs. These API commands can be used as part of the automated development pipeline to deploy and configure Advanced WAF. The automation can be instrumented through the tools that DevOps teams are already using, such as GitLab, Jenkins, and Bitbucket.

WAF security policies can also be applied to existing WAF instances using the same automation processes. Security policies can be defined as a simple JavaScript Object Notation (JSON) file. The file can include a pointer to the name and location of the WAF policy, typically in a repository such as GitHub.

## KEY BENEFITS

- Helps bring apps to market faster with lower cost and higher security efficiency
- Shifts security testing “left” in the application development pipeline for more cost-effective remediation
- Bridges the operational gap between SecOps and DevOps

## RESOURCES

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

Using this framework, the SecOps team can create, publish, and maintain security policies easily consumed by the development teams. Policies can vary depending on the application. For example, the SecOps team can have a baseline policy for applications that protect against the OWASP Top 10, which defines the most critical security risks to web applications. Other policies can be published for applications that require additional controls, which could include applications that handle sensitive data or perform financial transactions. The development team consumes these policies, just as they consume other pieces of application code.

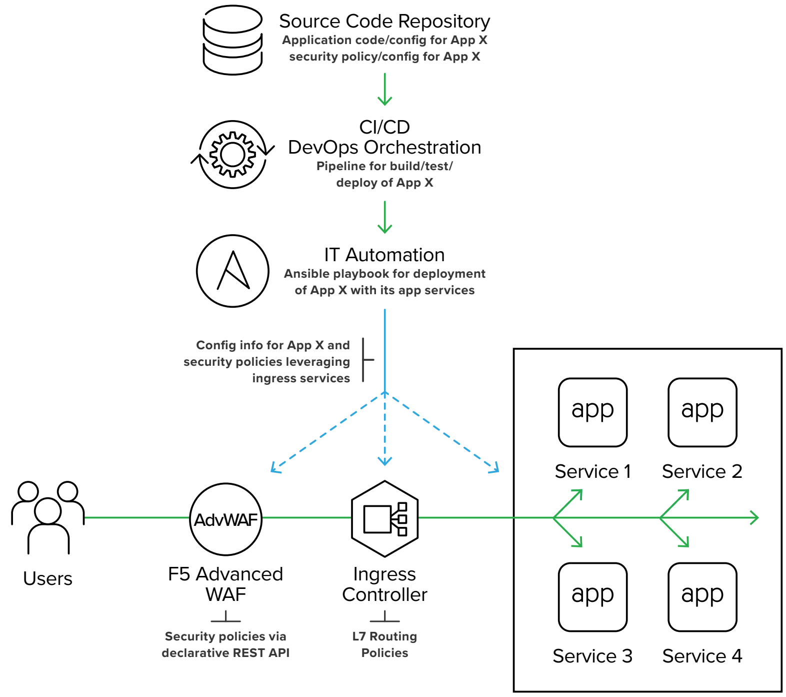

**Figure 1:** Organizations can use declarative APIs to integrate application security into the automated development pipeline to deploy and configure Advanced WAF.

Changes to the security “code” are automatically integrated, applied, tested, and built by the CI/CD pipeline automation toolset. This approach shifts security controls further left (earlier) in the CI/CD pipeline, enabling security to be a shared responsibility throughout the process. Just as with any other part of the application, this ensures consistent security implementation in all stages of the development lifecycle: development, test, quality assurance, and production.

Cross-functional DevSecOps teams can use additional ChatOps (e.g., Slack) integration capabilities to increase their efficiency and make sure they are always on the same page. However, ChatOps can go beyond just messaging and alerts. When integrated with the pipeline tools, ChatOps can provide real-time DevOps progress and even initiate pipeline actions such as updates to the Advanced WAF policy.