INTEGRATION BRIEF

Pinpoint and Protect Security Gaps in Your Applications

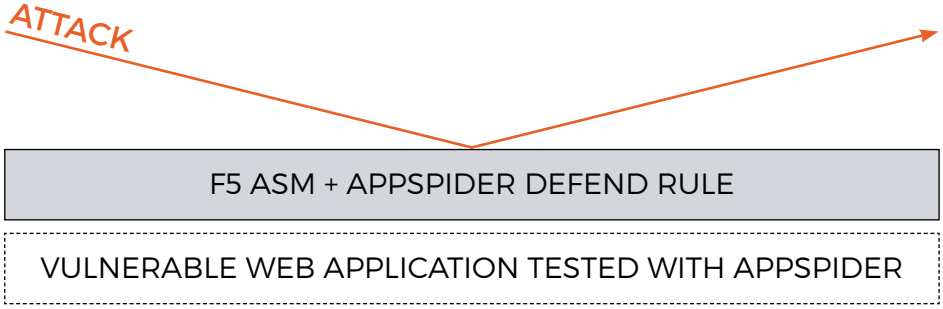
With F5® BIG-IP® Application Security Manager™ (ASM) and Rapid7 AppSpider

Organizations today are challenged to not just measure their application security risk, but also fix the vulnerabilities that create that risk. Unfortunately, it's not as simple as it sounds; many application vulnerabilities require code changes that can be costly and time consuming to implement, and entail constant back-and-forth between security and development teams to identify, validate, and fix. Sound painful? It often is.

That's why F5 BIG-IP® Application Security Manager™ (ASM) integrates with Rapid7 AppSpider to reduce the amount of time you're left exposed to attack while longer-term fixes are built and implemented.

HOW IT WORKS

AppSpider's Defend capability enables you to close security gaps in applications while the development team works to deliver a source code patch. AppSpider will generate Web Application Firewall (WAF) rules custom to the vulnerabilities that are identified. These virtual patches are tailored to specific vulnerabilities found in a target application so that the highest level of protection can be applied by the WAF. Through the integration with F5®'s BIG-IP® Application Security Manager™ (ASM), WAF rules generated by AppSpider can be immediately imported into F5 BIG-IP ASM for remediation that takes only minutes—not the days and weeks required by a source code patch. After the custom rule is enforced by an F5 BIG-IP ASM policy, AppSpider can also test the virtual patch and confirm the security gap is closed with its interactive attack replay feature.



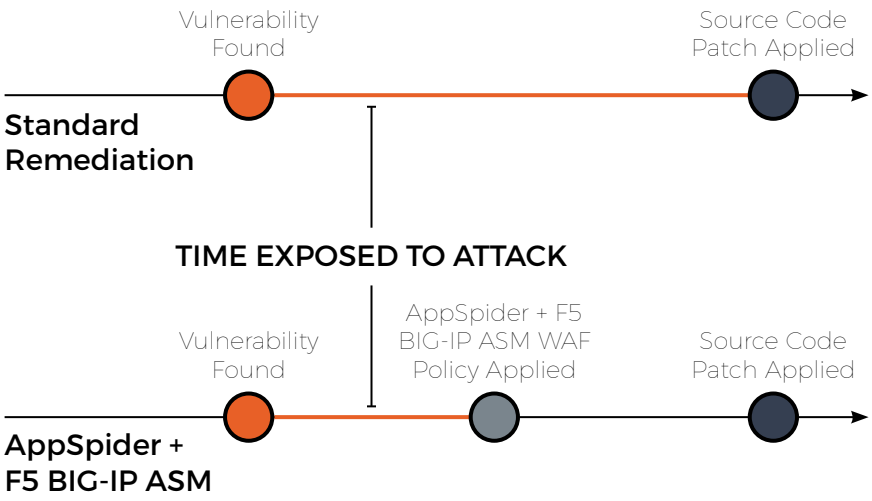
INTEGRATION BENEFITS

Reduce risk and save time by:

- Finding application security vulnerabilities in modern applications that include APIs and dynamic clients.
- Enabling them to remediate security vulnerabilities quickly with a virtual patch while development works on a source code fix.
- Providing the ability to test and validate virtual patches with AppSpider's interactive attack replay feature.

120617

Figure 1: AppSpider and F5 BIG-IP Application Security Manager (ASM) integrate to reduce the time vulnerable applications are exposed to attack.



Overview of the Integration Process

- Step 1: Conduct a Dynamic Application Security Testing (DAST) scan on the target application with Rapid7 AppSpider.
- Step 2: Review AppSpider scan results and confirm vulnerabilities. Validation is performed by reviewing recorded HTTP traffic and utilizing the interactive attack replay feature.
- Step 3: From the AppSpider Defend screen, load the XML AppSpider scan results and select "F5" as the WAF Rule output type.
- Step 4: In the F5 BIG-IP ASM configuration utility, import the WAF Rule generated by AppSpider into an Application Security policy, using the "Create a security policy using third party vulnerability assessment tool output" option.
- Step 5: Set policy enforcement mode to "Transparent" if attacks on the vulnerabilities should only be logged. Select "Blocking" to block these attacks.

SUPPORT

Please contact Rapid7 for support or assistance at +1.866.380.8113 or support@rapid7.com.

About F5

F5 (NASDAQ: FFIV) makes apps go faster, smarter, and safer for the world's largest businesses, service providers, governments, and consumer brands. F5 delivers cloud and security solutions that enable organizations to embrace the application infrastructure they choose without sacrificing speed and control. For more information, go to f5.com. You can also follow @f5networks on Twitter or visit us on LinkedIn and Facebook for more information about F5, its partners, and technologies.

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.