

# AppSpider Defend

## WAF/IPS Virtual Patching

Generate effective custom WAF/IPS virtual patches without blocking desired traffic

- Why AppSpider Defend?
- Specifications



32% of vulnerabilities are fixed through virtual WAF patches.

-SANS Survey, 2015 State of Application Security: Closing the Gap

Today's organizations don't have the luxury of time when it comes to fixing web application vulnerabilities. In the time it takes for your security team to notify your development team that a code fix is needed, a site can be defaced, taken down, or have customer data stolen.

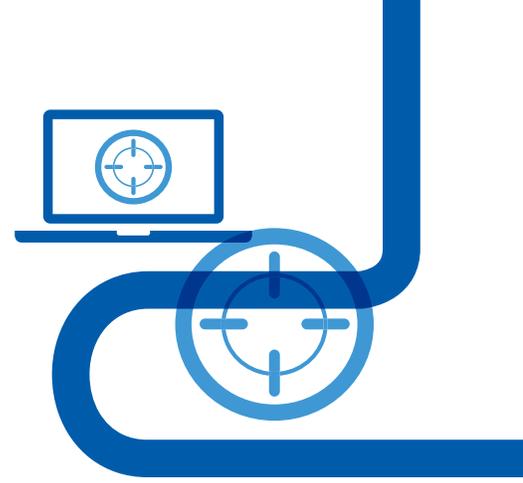
Using innovative automated rule generation, AppSpider Defend, part of AppSpider Pro, enables security professionals to patch vulnerabilities immediately – in a matter of minutes, instead of the days or weeks it can take to build a custom rule for a WAF or IPS; or the time it takes to deliver a source code patch. This allows developers to identify the root cause and fix it in the code – fast.

AppSpider Defend's virtual patches are uniquely accurate because they combine knowledge of the application, the vulnerability, and the WAF or IPS to create a highly effective filter that protects against the vulnerability, but doesn't block desired traffic.

### Why AppSpider Defend?

- **Ease** - Simply import the results of your AppSpider dynamic application security test (DAST) into AppSpider Defend, and generate custom rules that protect your web application from attacks on these vulnerabilities.
- **Accuracy** - Rely on AppSpider's knowledge of the application and the vulnerability to create strong, safe rules. Defend takes the AppSpider results and generates customized rules that target the application's specific vulnerabilities, which increases the WAF's accuracy and ability to protect WAF/IPS. These filters are able to pinpoint vulnerabilities without blocking desirable traffic.
- **Control** - Stay in control with the ability to review all of the vulnerabilities from your scan and quickly select which vulnerabilities to patch with AppSpider Defend's automatically generated highly targeted filters.

“WAFs are a highly recommended element of a security defense strategy, but it is also clear that even the best WAFs will miss attacks and thus are not adequate as the single element for protecting web applications. What is interesting is that the use of training tools combined with a tool like AppSpider Defend can dramatically increase their effectiveness and make them a far more useful part of an enterprise’s application security strategy.”



Larry Suto, Application Security Consultant  
*Analyzing the Effectiveness of Web Application Firewalls*

- **Quality Assurance** - As a safeguard, AppSpider Defend performs a quick re-scan once the filter has been applied to test for false-positives and ensure that the automated rule only patched the specific areas that were vulnerable.  
This enables you to quickly confirm both the effectiveness of the patch and that good traffic can continue to flow through as expected. By leveraging AppSpider Defend’s quick re-scan, you can eliminate the risk of false positives & false negatives and dramatically reduce or eliminate QA time.
- **Flexible Configurations** - AppSpider Defend allows you to optimally configure your WAF or IPS device to block web application vulnerabilities.
- **PCI Compliance** - Sophisticated accurate scanning technology with less manual configuration and training time. You will spend a lot less time configuring the scanner and training it to understand your application while having the utmost confidence that the results will have the best false positive and false negative rates available.
- **Broad Range of Integrations** - AppSpider Defend includes more integrations with WAF and IPS than any other solution available.

## Specifications

### Server hardware requirements

- Multi-core CPU
- 4 GB RAM
- 1 network interface card (NIC)
- 500 GB hard drive space

### Software requirements

One of the following operating systems:

- Microsoft Windows Server 2008 Editions x32/x64 bit
- Microsoft Windows Server 2008 R2 Editions x32/x64 bit

- Microsoft Windows Vista Ultimate, Professional, Enterprise, Home Premium x32/x64 bit
- Microsoft Windows 7 Ultimate, Professional, Enterprise, Home Premium x32/x64 bit
- Microsoft Windows 7 Ultimate, Professional, Enterprise, Home Premium SP1 x32/x64 bit
- Microsoft Windows 8 Professional x64 bit

### Additional requirements

- Rapid7AppSpider Pro
- Microsoft .NET Framework 4.5 Redistributable Package

## Available for the following WAF and IPS solutions:

### WAF:

- Barracuda
- ModSecurity
- DenyAll rWeb
- Imperva SecureSphere
- Akamai
- F5

### IPS:

- Sourcefire SNORT
- Secui Snort
- Nitro SNORT

Learn more about AppSpider at  
[www.rapid7.com/products/appspider](http://www.rapid7.com/products/appspider)