Web Application Protector

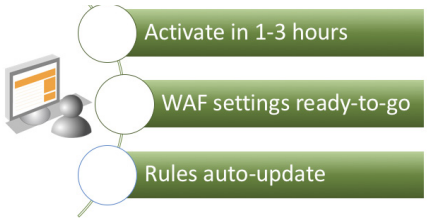
Protect your website against DDoS and web application attacks, while saving effort and overhead. Web Application Firewalls (WAFs) are often difficult to deploy and manage, especially for teams with limited security staff. Web Application Protector can help. Setup and management of the configuration settings is simple. Akamai's security research team continuously improves the protections available in the product, eliminating the need to decide what individual firewall rules to enable.

Most WAF Solutions

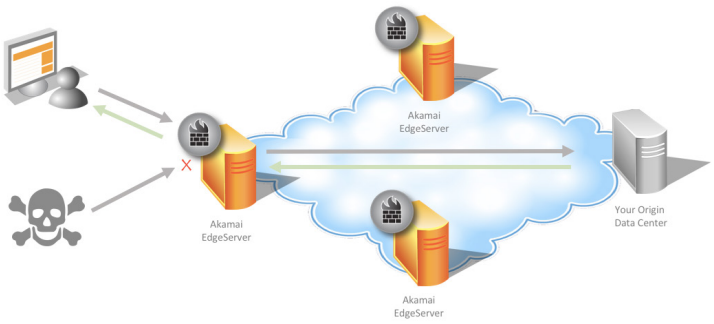
Require an IT Team and Vendor Service Team

Web Application Protector

Requires 1 person



Web Application Protector implementation is simple, but the service delivers robust protection that detects and mitigates application threats in HTTP and HTTPS traffic as they attempt to pass through Akamai's edge platform to reach your origin data centers. The platform specializes in accelerated web content delivery, so expect significant speed improvements too.



Protections Overview

This service protects against common web exploits with little need for tuning. When you do need to tweak some protections, it's easy to customize.

Network Firewall

Network Firewall lets you block or allow requests by IP address or geographic location. Akamai provides and maintains lists of known entities, like IP address ranges of popular cloud providers you may want to whitelist, or IPs related to nefarious traffic sources like The Onion Router (TOR), which hackers use to hide their identity. Geo-blocking lets you deny requests from specific countries or regions, like continents.

DoS Protection

Web Application Protector provides denial of service (DoS) protection through the following controls.

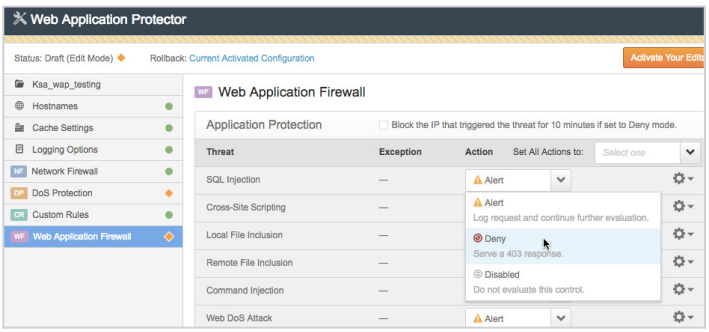
- **Layer 3/Layer 4 Protections** inspect packets and network connections to determine which requests to automatically block. This feature is always on for your protection.
- **Rate Limiting** lets you set thresholds to flag request traffic that's too fast to be from a human. Use the three profiles that Akamai provides, and you can create two of your own.
- **Slow POST Protection** lets you mitigate extremely slow requests that consume server connection resources.

Web Application Firewall

Akamai's security research team tracks the latest web threats and continually updates rules to keep up with the changing risk landscape. Web Application Protector includes an easy-to-manage ruleset that updates and deploys itself. The WAF protects against these six common attack categories:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- Command Injection (CMDi)
- Denial of Service Attack (DoS)

You can set actions by category. For example, if you've endured SQL Injection attacks in the past, you could specify that you want Web Application Protector to Deny requests that meet the criteria for this type of attack.



Custom Rules

Use Custom Rules to handle situations not covered by the WAF's application protection groups. You can define up to 10 custom rules. For example, you can configure a custom rule to inspect a request header for a specific value, and if found, deny the request.

Set Up Protection

Configure and deploy Web Application Defender in three simple steps.

Note: *These instructions assume that you have a delivery configuration set up with Akamai. If you don't, you can follow the same steps with just a few additional fields to complete. You'll find full details in the Web Application Protector user guide.*

Step 1: Setup

1. Visit https://control.akamai.com/ and log in.
2. From the menu, choose **Configure** ▸ **Web Application Protector**.
3. When asked if your hostnames are already part of a delivery configuration, select **Yes**.
4. Click **Get Started**.
5. Enter a descriptive name for the configuration
6. In **Add Hostnames to Protect**, enter additional hostnames you want to protect, like **`www.example.com`**. Separate entries with a space or return.
7. In **Customer Email**, enter the email address that should get Akamai notifications.
8. Click **Next**.

Step 2: Review

The review tab summarizes protections. When a request triggers a rule, you can have Web Application Protector generate an alert or deny the request. By default, actions in the DoS and WAF sections are set to alert. To start, you probably want to leave actions set to Alert. You can make changes later, when you have more information from Security Monitor reports. But, if you need to start blocking attacks right away, you can:

- Deny all requests that trigger rules by clicking the **Security Default Action** drop-down and selecting **Deny**.
- Deny for selected protection categories, by reviewing the DoS and WAF sections and changing the actions you want.

When you finish reviewing, click **Next**.

Step 3: Activate

Click **Activate**. Web Application Protector begins running through activation tasks. It takes 1-3 hours to deploy your site and security configuration across the Akamai Intelligent Platform.

©2017 Akamai Technologies, Inc. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission is prohibited. Akamai and the Akamai wave logo are registered trademarks. Other trademarks contained herein are the property of their respective owners. Akamai believes that the information in this publication is accurate as of its publication date; such information is subject to change without notice. Published 10/17.