AKAMAI PRODUCT BRIEF

Web Application Protector

Secure your digital business with little-to-no daily management

Web Application Protector is designed for companies looking for a more automated approach to web application and API protection (WAAP) and DDoS security.

Uncompromising Security, Greater Simplicity

Protecting your web applications and APIs can be a daunting task. Even the most seasoned security professionals can be challenged to keep up with the latest threats and update security protections in a timely manner. Organizations without dedicated in-house skilled operators can benefit most from a WAAP and DDoS solution that is easy to deploy, highly automated, and simple to maintain.

Web Application Protector

Web Application Protector is a cloud-based WAAP solution that is designed and purpose-built for simplicity and automation. Web Application Protector will help protect your applications and APIs from a wide range of network and application-layer threats with less effort and overhead. And since Web Application Protector is built on the Akamai Intelligent Edge Platform it comes prebuilt with performance capabilities that are designed to ensure your websites, web applications, and APIs perform their very best.

How It Works

With Web Application Protector, clients connect to your web applications through the most optimal Akamai edge server. Every server inspects web and API traffic to protect against DDoS, web application, and API-based attacks, while simultaneously allowing access to legitimate users. With well over 4,000 points of presence distributed across 940+ cities in 135 countries, Web Application Protector has the scale to stop the largest attacks, at the edge, before they reach your applications and APIs.

Web Application Protector simplifies the task of securing your organization with automated security protections. With visibility into thousands of attacks on the Akamai platform, our world-class security researchers use advanced machine learning algorithms to continuously analyze, refine, and update your security rules without requiring any human intervention.

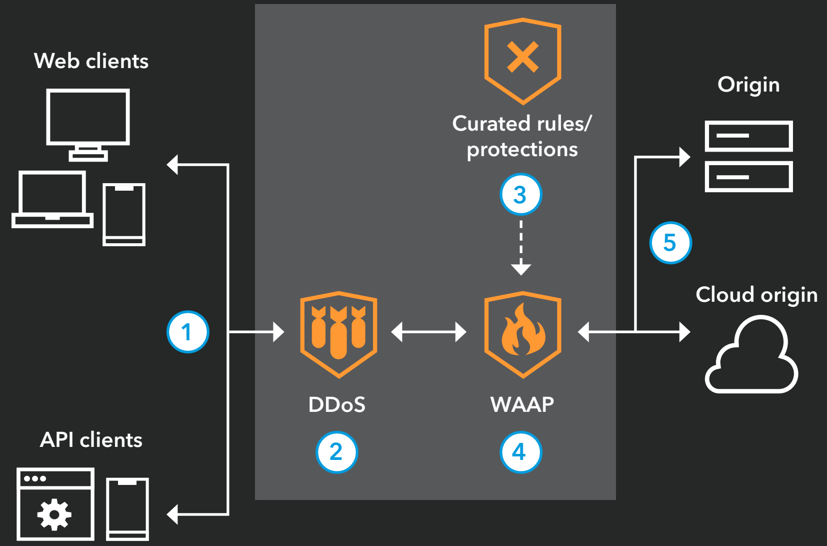
BENEFITS FOR YOUR BUSINESS

Operate more securely online – Protect your applications and APIs from a broad range of attacks to reduce the risk of downtime and data theft

Deploy quickly – Onboard and configure Web Application Protector's security protections in just a few clicks to secure your applications and APIs more quickly

Manage easily – Akamai continuously and transparently updates the included security protections to protect your digital estate with less effort

How It Works



1. Users and attackers all connect to your application through the closest Akamai server
2. Network-layer [L3/4] DDoS attacks are instantly dropped at the Akamai edge
3. Machine learning and heuristics-driven automatic updates are based on the evolving threat landscape
4. Web Application Protector blocks application-layer DDoS, web application, and API-based attacks
5. Reduce the risk of downtime and data theft by protecting your origin from attacks

Features

Application Firewall – Protects you from SQL injection, XSS, RFI, and other types of application-layer threats with an adaptive engine that replaces complex WAF rulesets with advanced detections and self-tuning that deliver superior protections with far less effort.

Performance and Delivery – Seamlessly scale to match traffic demands as they vary over time, distribute CPU and memory resources as required, deliver cached content from the edge, and provide continuous protection without interruption for the highest level of performance and delivery.

HTTPS Included – Web Application Protector includes a TLS or SSL certificate to deliver your secure content, help prevent data theft, and provide HTTPS security for your website and users free of charge.

Advanced Web Security Analytics – Access detailed attack telemetry and analyses of security events to evaluate what changes are needed to improve security protections and optimize configurations for your specific business needs.

Network (IP/Geo) Edge Firewall – IP/Geo controls let you block or allow traffic coming from a specific IP, subnet, or geographic area. This allows you to block malicious requests from specific IP addresses or traffic from The Onion Router (TOR), which hackers use to hide their identity.

Custom Rules – Web Application Protector offers a custom rule builder to quickly and easily generate custom rules that can be used to handle unique scenarios not covered by standard rules or to quickly patch new vulnerabilities.

API Discovery and Protections – Mitigate risks such as brute force attacks or credential stuffing by automatically discovering previously unidentified APIs, including API endpoints, definitions, resources, and traffic characteristics. Profile API traffic with simple “one-click” registration so you can spend less time worrying about constant API threats, and more time on ways to enhance your online business.

DoS Protection (Rate Controls) – Protect your applications and APIs from denial-of-service attacks by monitoring and blocking clients exceeding request-rate thresholds. Violators are automatically blocked to protect site origins.

Terraform, Open APIs, and CLI – Gain agility by simplifying and automating Web Application Protector functions through Akamai's Terraform provider, open APIs, or the Akamai command-line interface to integrate and customize based on your preferred methods.

Reporting – Web security reporting tools continually monitor and assess the effectiveness of your protections. You can create real-time reports to monitor daily activities, investigate attacks by type, and view reports on targeted APIs, DoS traffic, and more.

Real-Time Alerting – Create real-time email alerts using static filters and thresholds that can be easily configured to notify specific recipients only.

Site Shield – Provides an additional layer of protection that helps prevent attackers from bypassing cloud-based protections and targeting your origin infrastructure.

Other Solutions to Increase Protection

Bot Manager – Identify, categorize, and manage bots that are accessing your site. Automated algorithms use both bot and human behavior telemetry to detect and treat the most sophisticated bots.

SIEM Integration – Prebuilt connectors allow you to use on-premises and cloud-based SIEM applications like Splunk, QRadar, ArcSight, and more.

Page Integrity Manager – Protect websites from JavaScript threats – such as web skimming, formjacking, and Magecart attacks – by identifying vulnerable resources, detecting suspicious behavior, and blocking malicious activity.

Try Web Application Protector today at akamai.com/waptrial.