

# App & API Protector

In today's connected world, protecting web applications and APIs from the wide range of emerging and evolving threats is critical for business success. However, securing digital interactions amid cloud journeys, modern DevOps practices, and constantly changing applications introduces new complexities and challenges.

Deploying an all-encompassing web application and API protection (WAAP) solution strengthens your security posture by adaptively updating protections and proactively delivering insights on targeted vulnerabilities.

**Akamai App & API Protector** is a single solution that brings together many security technologies, including web application firewall (WAF), bot mitigation, API protections, and distributed denial-of-service (DDoS) protection. App & API Protector is recognized as a leading WAAP solution for swiftly identifying and mitigating threats beyond the traditional WAF to protect entire digital estates from multidimensional attacks. The platform is easy to implement and use, provides holistic visibility, and automatically implements up-to-date, customized protections via Akamai Adaptive Security Engine.

## Extend WAF security with Akamai App & API Protector Hybrid






Built to secure distributed applications, App & API Protector Hybrid extends Akamai's proven, core WAF capabilities beyond our platform for consistent security across applications and APIs deployed in various environments, including on-premises, multicloud, and off-CDN infrastructures.

## The power of adaptive security

App & API Protector goes beyond rulesets with the Adaptive Security Engine. With this innovative technology, security protections are continually and automatically updated, with customized policy recommendations implemented in a single click. The Adaptive Security Engine provides modern protection by combining machine learning, real-time security intelligence, advanced automation, and insights from more than 400 security professionals and threat researchers. Adaptive Security Engine is unique because it:

- Analyzes the characteristics of every request in real time at the edge for faster detection
- Learns attack patterns by using both local and global data to make customer-specific protection adjustments
- Adapts to future threats, which ensures updated protections even as attacks evolve

### Benefits for your business

-  **Trusted attack detection**  
Evolve with the threat landscape; protect against established and emerging threats, including DDoS, botnets, injections, application and API attacks, and more
-  **One product, broad protections**  
Maximize your security investment with a solution that includes WAAP, bot visibility and mitigation, DDoS protection, security information and event management (SIEM) connectors, web optimization, API acceleration, and more
-  **Hands-off security**  
Alleviate time-intensive manual maintenance with automatic updates and proactive self-tuning recommendations powered by Akamai Adaptive Security Engine
-  **Ease of use**  
Use the improved UI design to simplify onboarding and comprehensive security operations, which are aided by setup and troubleshooting guides
-  **Unified visibility**  
Analyze your full scope of security metrics in a single dashboard or proactive discovery report via the shared telemetry of Akamai's security solutions



Adaptive Security Engine alleviates the burden of time-consuming, manual tuning with zero-touch updates for a nearly hands-off experience. At launch, this technology was proven to increase detections by 2x and reduce false positives by 5x. Recent updates to our machine learning-powered algorithms now reduce false positives by an additional 4x. Security professionals can be heroes again, with more time to focus on enabling secure — and customer-friendly — digital business operations.

## New: Behavioral DDoS Engine

The new Behavioral DDoS Engine both strengthens and simplifies application-layer DDoS defense and is powered by machine learning. Behavioral DDoS Engine's behavioral- and anomaly-based detection algorithms look at various traffic dimensions like country source, network fingerprint, and other HTTPS request attributes to create tailored protections and provide a hands-off approach against application-layer DDoS attacks.

Behavioral DDoS Engine's use of machine learning improves the efficacy and decision-making on traffic dimensions for use in creating traffic profiles or baselines. The scoring mechanism for different sensitivity levels considers the risk appetite of your business for detecting attacks and minimizing false positives.

**Leading attack detection** — As your digital environment grows, so does the depth and breadth of your protections as an Akamai customer. In addition to the automatic updates and adaptive self-tuning that Adaptive Security Engine delivers, App & API Protector provides analyst-recognized leading detections for DDoS, bot, malware, and more attack vectors. Confirm your Akamai protections against emerging and advancing CVEs with our threat research tool.

**Application security** — App & API Protector features a full suite of defenses and customizations to allow security to be tailored to your organization's needs. Effective capabilities like Client Reputation, client lists, novel attack detection, and more give you the advantage against adversaries while simplifying security operations. The Akamai WAAP solution's advanced application-layer defenses fight back against DDoS, SQL injections, cross-site scripting, local file inclusion, server-side request forgery, and other attack vectors.

**DDoS protection and granular rate controls** — Recognized as a market-leading DDoS solution, App & API Protector provides DDoS protection on multiple fronts. It starts by instantly dropping network-layer DDoS attacks at the edge for risk mitigation and resource savings. Then, it automatically detects and mitigates sophisticated Layer 7 DDoS attacks at the edge for hands-off and real-time protection against the evolving landscape of DDoS threats. Granular rate controls customize your DDoS defense specifically for your traffic and attack profiles.

**Bot visibility and mitigation** — Gain real-time visibility into your bot traffic with access to Akamai's directory of known bots. Investigate skewed web analytics, prevent origin overload, and create your own bot definitions to permit access to third-party and partner bots without obstruction. Expanded bot controls, including browser impersonation detection, conditional actions, and crypto challenges, are now included in App & API Protector.

## OWASP Top 10

Akamai mitigates risks in both the OWASP Top 10 and the OWASP API Security Top 10. Learn more about how App & API Protector and Akamai security protect customers from large, common, or emerging threats.

To learn more about Akamai's protections against the OWASP Top 10, [download the white paper](#).





**API protections** — Akamai's industry-leading API protection increases your security by providing visibility to traffic across your digital estate, proactively revealing vulnerabilities, identifying environment changes, and protecting against hidden attacks. With App & API Protector's API capabilities, you can:

- Automatically discover a full range of known, unknown, and changing APIs across your web traffic, including their endpoints, definitions, and traffic profiles
- Easily register newly discovered APIs with just a few clicks
- Detect and mitigate attacks that target APIs, including DDoS, injection attacks, and specification violations
- Control sensitive data handling with App & API Protector's personally identifiable information reporting feature to remain compliant

**Performance and more from the largest global network** — Being on the Akamai platform provides customers with a competitive edge due to its unmatched global scale, offering real-time visibility into a significant portion of global internet traffic. This vast data enables Akamai to deliver actionable threat intelligence to help organizations stay ahead of evolving security threats and allowing for faster detection and mitigation of attacks across various environments. The platform also provides a proven performance increase and a 100% availability SLA.

**Malware protector** — This add-on module can scan files at the edge — before they're uploaded — to detect and block malware from entering your corporate systems as malicious file uploads. With no additional app or API configuration required, you free up the time you'd spend setting up protection in each system individually.

## Best-in-class defense with simplified security operations

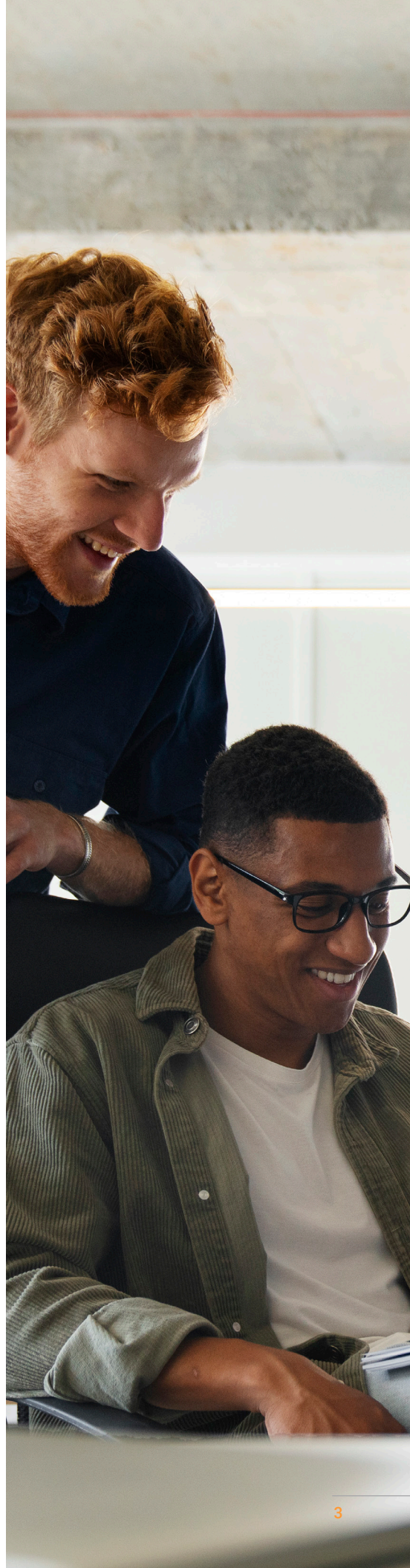
Key capabilities within App & API Protector improve the operational experience within your organization while improving the experience and performance for customers outside of it.

**Simple Start onboarding** — Great security tools only work if you use them. Akamai is devoted to building an easy-to-use platform that enables productivity and strong protections. You can onboard quickly with our Simple Start, or apply protections to new applications in just a few clicks.

**Dashboards, alerting, and reporting tools** — Web Security Analytics is Akamai's AI-enabled attack telemetry dashboard. Here, you can analyze security events, create real-time email alerts using static filters and thresholds, and use customizable reporting tools to continually monitor and assess the effectiveness of your protections across the Akamai platform.

**DevOps integrations** — Seamlessly integrate security into DevOps workflows with GitOps, ensuring that security aligns with fast-paced development. Akamai's APIs, available through CLI or Terraform, allow complete management of App & API Protector via code and match every action available in the user interface.

**SIEM integrations** — SIEM APIs are also available, and pre-built connectors to Splunk, QRadar, ArcSight, and more are automatically included with App & API Protector.



**Included solutions** — To increase visibility and performance, App & API Protector now features many of Akamai customers' most-loved products, including:

- **Site Shield**  
Prevent attackers from bypassing cloud-based protections and targeting your origin infrastructure
- **mPulse Lite**  
Get in-depth visibility into user behavior, address real-time performance problems, and measure the revenue impacts of digital changes
- **Akamai EdgeWorkers**  
Explore the benefits of serverless computing, including improved time to market and logic execution nearest to end users
- **Akamai Image & Video Manager**  
Intelligently optimize both images and videos with the ideal combination of quality, format, and size
- **Akamai API Acceleration**  
Boost your API performance by easily managing access, scaling for spikes in times of demand, and enhancing API security

Free tier offerings may have restrictions on use. Contact Akamai for more information.

## Advanced Security Management

The optional Advanced Security Management module has automation and configuration flexibility for those customers with more complex application environments and advanced security needs. The Advanced Security Management option includes additional security configurations, rate policies, security policies, application-layer DDoS controls, custom WAF rules, positive API security, and access to IP reputation threat intelligence (Client Reputation) out of the box.

## Managed Security Service

Standard support is offered 24/7/365 for all Akamai customers. In addition to on-demand professional services for consulting or single-project work, Akamai provides levels of managed services — fully managed WAAP service, managed attack support, and specialized security operations center support.



[Speak with an expert](#) to learn more.