AKAMAI PRODUCT BRIEF

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 insight 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 protection, and distributed denial-of-service (DDoS) defense. App & API Protector is recognized as the leading WAAP solution for swiftly identifying and mitigating threats beyond the traditional WAF to protect entire digital estates from multidimensional attacks. The platform is easier to implement and use, provides holistic visibility, and automatically implements up-to-date, customized protections via Akamai Adaptive Security Engine.

The power of adaptive security

With App & API Protector, security protections are continually and automatically updated, with customized policy recommendations implemented in a single click. Adaptive Security Engine, the technology at the core of App & API Protector, provides modern protection by combining machine learning, real-time security intelligence, advanced automation, and insights from more than 400 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

Adaptive Security Engine alleviates the burden of time-consuming, manual tuning with zero-touch updates for a nearly hands-off experience, improving detections by 2x and reducing false positives by 5x. Security professionals can be heroes again, with more time to focus on enabling secure — and customer-friendly — digital business operations.

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 controls, DDoS protection, security information and event management (SIEM) connectors, web optimization, cloud computing, 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

Continuous innovation for application security

Akamai continues to innovate, providing new capabilities and extending protections in this customer-loved solution. Improved application-layer DDoS defenses include configurable rate accounting windows to protect against short bursts of DDoS, as well as enriched match conditions in rate limiting (like client reputation scores and TLS fingerprints). Unlike today's prevalent rate-limiting methods, our innovative new approach — URL protection with intelligent load shedding — helps detect and mitigate application-layer DDoS attacks according to origin-based rate throttling. Adaptive Security Engine has been enhanced to provide swift deployment of protections against emerging threats and high-profile CVEs. To improve bot controls, a new and innovative bot detection method called Browser Impersonation Detection, which uses a dynamic scoring model and machine learning, is now included as a part of Bot Visibility & Mitigation.

More than app security, gain API protection

Akamai's industry-leading API protections provide visibility to traffic across your digital estate, proactively revealing vulnerabilities, identifying environment changes, and protecting against hidden attacks.

The API Discovery capability alerts security teams to new, often unprotected, APIs that are connected by different lines of business. Akamai App & API Protector automatically discovers APIs every 24 hours based on a scoring mechanism that takes into account response content type, path characteristics, and traffic patterns. With API Discovery, 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
- Ensure API protection against DDoS, malicious injection, credential abuse attacks, and API specification violations
- Control sensitive data handling with App & API Protector's personally identifiable information (PII) reporting feature to remain compliant

The best part? API requests are automatically inspected for malicious code whether you choose to register them or not, providing strong API security the instant that App & API Protector is deployed. Akamai App & API Protector simplifies the complexity of estate-wide security operations, empowering security teams to increase alignment with development teams, line-of-business leaders, and executives.

App & API Protector's API data loss prevention capability lets you better secure PII and other sensitive data. Discover where PII may be leaked or used by APIs. Gain powerful visibility and control of sensitive data to keep your organization and customers safe.

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

DDoS protection — Recognized as a market-leading DDoS solution, App & API Protector instantly drops network-layer DDoS attacks at the edge and provides holistic defense strategies against application-layer DDoS attacks. You are not only protected from DDoS attacks but also from the traffic spikes of an attack — Akamai DDoS Fee Protection provides credit for any overage fees incurred because of a DDoS attack.

OWASP Top 10

Akamai mitigates risks in the OWASP Top 10 plus the OWASP API 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.

Improve detections by 2x while reducing false positives by 5x

Bot Visibility & Mitigation — Gain real-time visibility into your bot traffic with access to Akamai's expansive directory of more than 1,750 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. Browser Impersonation Detection, powered by machine learning, is now included in App & API Protector.

Malware protection — This add-on module can scan files before they're uploaded at the edge 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.

Site Shield — Prevent attackers from bypassing cloud-based protections and targeting your origin infrastructure with this customer-favorite product that is now included in App & API Protector. Other products in Akamai's security portfolio, Client-Side Protection & Compliance and Account Protector, can extend your in-browser security capabilities.

Easy-to-use comprehensive security tool — 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 detailed attack telemetry dashboard. Here, you can analyze security events, create real-time email alerts using static filters and thresholds, and use web security reporting tools to continually monitor and assess the effectiveness of your protections.

DevOps integrations — Enable rapid onboarding, create uniform management of security policies, centralize enforcement across cloud infrastructures, and improve collaboration between DevOps and security teams in a GitOps workflow to ensure your security always keeps pace with today's rapid development. Akamai APIs, which are also available in the form of a wrapper with an Akamai CLI package or Terraform, provide the ability to manage App & API Protector via code. Every action available in the user interface is accessible via programmable APIs. Security operations teams can also integrate WAF rule release or configuration activations alerts in IT service management tools, such as Slack information.

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

- mPulse Lite
  Get in-depth visibility into user behavior, address real-time performance problems, and measure the revenue impacts of digital changes
- EdgeWorkers
  Explore the benefits of serverless computing, including improved time to market and logic execution nearest to end users
- Image & Video Manager
  Intelligently optimize both images and videos with the optimal combination of quality, format, and size
- 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 usage. 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. Although automatic updates are recommended, this option provides a manual mode of operation that enables granular actions and the ability to activate updates when desired. You can also use Evaluation Mode to test new updates alongside current protections to understand improvements in accuracy before deployment. The Advanced Security Management option also 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 two levels of managed services — fully managed WAAP service and managed attack support.

To learn more, visit the App & API Protector page or contact your Akamai sales team.