AKAMAI PRODUCT BRIEF

App & API Protector

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

Deploying a holistic web application and API protection 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, bot mitigation, API security, and DDoS protection. App & API Protector is recognized as the leading attack detection solution, quickly identifying and mitigating threats beyond the traditional firewall 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 with 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 leveraging 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 TO YOUR BUSINESS

Trusted attack detection
Evolve with the threat landscape, protecting against established and emerging threats including DDoS, botnets, injections, API attacks, and more

One product, broad protections
Maximize your security investment with a solution that includes web application and API protections, bot visibility and mitigation, DDoS protection, 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

Ease of use
Improved UI design simplifies onboarding and comprehensive security operations, which are aided by setup and troubleshooting guides

Unified visibility
Akamai's single pane of glass delivers deep insights for determining traffic patterns and analyzing attacks using out-of-the-box or customized dashboards and proactive discovery reports

Akamai

More than app protection, gain API security

Akamai's industry-leading API security increases your protections by providing 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 denial of service (DoS), 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? All 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. 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 and 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, and 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 distributed denial of service (DDoS), bot, malware, and more attack vectors.

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

Bot mitigation visibility — Gain real-time visibility into your bot traffic with access to Akamai's expansive directory of more than 1,700 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. Increase your bot security controls with Akamai Bot Manager Premier to protect against credential stuffing, web scraping, mass account creation, inventory manipulation, and card cracking.

OWASP Top 10

Akamai mitigates the 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.

Download the white paper to learn more about Akamai's protection against the OWASP Top 10.

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, Page Integrity Manager, Account Protector, and Audience Hijacking Protector, can extend your in-browser security capabilities.

Adaptive Security Engine, the technology at the core of App & API Protector, improves detections by 2x while reducing false positives by 5x

Easy-to-use comprehensive security tool

Great security tools only work if you use them. Akamai is devoted to building a comprehensive and easy-to-use platform enabling productivity and strong protections.

Onboarding wizard — App & API Protector provides an easy-to-use wizard to onboard properties with integration and configuration workflows designed to streamline and simplify the onboarding process and ongoing learning.

Dashboards, alerting, and reporting tools — Access detailed attack telemetry, analyze security events, create real-time email alerts using static filters and thresholds, and leverage web security reporting tools that 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 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 UI is accessible via programmable APIs.

SIEM integrations — Security information and event management (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 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 ideal 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 with more complex application environments and advanced security needs. While 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 and understand improvements in accuracy before deployment. The Advanced Security Management option also includes additional configurations, rate controls, policies, custom 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 web application and API protection and managed attack support.

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

 | Support | | Published 1/23