

## AKAMAI PRODUCT BRIEF

# App & API Protector

In today's connected world, securing web applications and APIs from a wide range of threats – from web app business logic attacks and API abuse to bots – is critical for business success. However, securing digital properties amid cloud journeys, modern DevOps practices, and constantly changing applications and APIs introduces new complexities and challenges.

Deploying a holistic web application and API protection (WAAP) solution can strengthen your information security strategy and provide insight into emerging risks to target security gaps and stop web and API-based attacks.


Akamai App & API Protector is designed to protect entire web and API estates with a holistic set of powerful protections purposely built with customer-focused automation and simplicity. The simplicity of App & API Protector belies some of the most advanced security automation available today. Powered by a new adaptive security engine, App & API Protector brings together many industry-leading core technologies in web application firewall, bot mitigation, API security, and DDoS protection under a single solution that is actually easy to use.


## Adaptive Security That Self-Tunes


New multidimensional adaptive threat-based detections correlate threat intelligence across the Akamai platform with data/metadata from each web and API request to detect up to two times more attacks (with a 5x reduction in false positives) than our previous detection technology. Advanced decision-making logic that is tailored to your traffic stops both common and highly targeted attacks with incredible precision.


But no WAAP is 100% accurate, so App & API Protector is equipped with self-tuning capabilities designed to reduce operational friction and administrative overhead. All security triggers – both true attacks and false positives – are automatically analyzed with advanced machine learning (ML) for policy-specific tuning recommendations that can be easily accepted with just a few clicks.

## BENEFITS FOR YOUR BUSINESS

 **One Product, Broad Protections**  
Protect all your websites, applications, and APIs from a broad range of threats, including volumetric DDoS, automated botnets, and injection and API-based attacks, among others, from a single WAAP solution.

 **Frictionless Maintenance**  
Maintain strong security with automatic updates and alleviate alert fatigue with automatic self-tuning to help security teams focus on investigating real attacks and not chasing false alerts.

 **Do More with Less**  
Maximize your security investment with a solution that includes web application and API protections, bot visibility and mitigation, DDoS protection, SIEM connectors, web optimization, edge compute, API acceleration, and more.

 **Reduce Your API Attack Surface**  
APIs have become a dominant mechanism in the modern web that enable powerful web experiences, but could also expose back-end data and logic. Automatically discover and protect your APIs from vulnerabilities, including the OWASP API Security Top 10.



## Advanced API Capabilities

Automatically discover a full range of known, unknown, and changing APIs across your web traffic, including their endpoints, definitions, and traffic profiles. Visibility into APIs helps protect against hidden attacks, find errors, and reveal unexpected changes. Moreover, you can easily register newly discovered APIs with just a few clicks. The best part is: All API requests are automatically inspected for malicious code whether you choose to register them or not, providing strong API security by default.

With the advanced security management option, registered APIs can benefit from additional forms of protections, like the enforcement of API specifications at the edge.

## Bot Visibility and Mitigation

Monitor and mitigate bot attacks with integrated bot capabilities designed to detect and stop unwanted bots. Gain real-time visibility into your bot traffic with access to Akamai's expansive directory of more than 1,500 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. As your needs grow, you can easily upgrade to a full-featured bot management or account takeover solution with just a few steps.

## DevOps Integration

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. 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.

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.

## Maximum Protection and Performance

App & API Protector will seamlessly scale to match traffic demands as they vary over time, distribute CPU and memory resources as required, and deliver cached content from the edge to ensure continuous protection without interruption. In addition – since security should never hinder performance or development velocity – free tier entitlements to image and video optimization, API acceleration, and edge computing are also included.

### Additional Capabilities

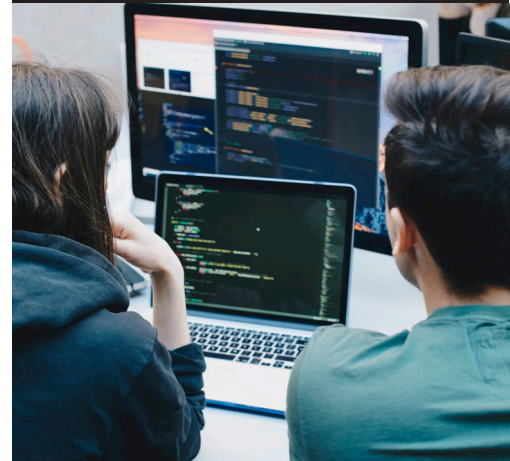
- **Automatic Updates** – Akamai threat researchers analyze more than 300 TB of daily attack data using ML to identify new attack vectors or permutations of existing ones. The security research team then automatically updates the adaptive security engine with the latest protections for the strongest possible security outcomes. Akamai-managed updates mean less administrative overhead and operational friction.
- **DoS/DDoS Protection** – Network-layer DDoS attacks are instantly dropped at the edge. Application-layer attacks, including those designed to exhaust resources, those that exploit vulnerabilities to impact availability, and those that target application logic are quickly mitigated within seconds. Akamai DDoS Fee Protection provides credit for any overage fees incurred due to a DDoS attack.

## Client-Side Protections



### 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



- **Network Lists** – 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 – for instance, The Onion Router, which threat actors often use to hide their identity.
- **Custom Rules** – Generate up to 100 custom rules using an easy-to-use rule builder to create and manage unique scenarios not covered by standard protections. For example, use custom rules to quickly patch unique application and API vulnerabilities (virtual patching).
- **Hostname Evaluation** – Safely add additional hostnames to an existing security configuration by first evaluating for potential impact and without taking protections offline. Existing protection settings, adjustment to rate controls, exceptions, or custom rules are automatically mirrored for the evaluation.
- **Response Actions** – Create and serve a wide range of response actions, including fully customized responses. You can send custom error messages, deliver brand pages with your own logo, or define and serve HTML-, XML-, or JSON-based responses, depending on your needs.
- **Site Shield** – Provides a layer of protection that helps prevent attackers from bypassing cloud-based protections and targeting your origin infrastructure.
- **Dashboards, Alerting, and Reporting Tools** – Access detailed attack telemetry and analysis of 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.
- **Simplified Onboarding** – 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.

## Advanced Security Management (*Optional*)

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 evaluate new updates alongside current protections to 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.

## World-Class Experts



### Managed Security Services

Offload or augment your security management, monitoring, and threat mitigation to Akamai security experts



To learn more, visit the [App & API Protector page](#) or [contact](#) your Akamai sales team.