

Barracuda API Security

Stop API attacks and improve customer experience.

[Barracuda Application Protection](#) is a comprehensive application security platform that provides powerful, easy-to-use security against Web Application and API attacks. Its built-in [API Protection](#) extends from API discovery, [OWASP Top 10](#), and zero-day attack protection to [bot protection](#), distributed denial-of-service (DDoS) [prevention](#), and access control. The platform is fully automatable for easy integration into DevOps environments.

How secure are your APIs?

The rise of digital transformation has contributed to an unprecedented growth in APIs. In fact, modern applications, DevOps, CI/CD pipelines, containers, and microservices speed digital transformation, and they all rely on APIs to send and receive data and for communication. Contributing to their proliferation is the API-first development approach. In this approach, application design and development start with defining the API.

As a result of this growth and changes in development methods, the majority of web traffic is API-based. And that kind of exposure makes APIs vulnerable to exploitation. In fact, Gartner predicts that by 2024, security incidents and breaches will have doubled. Also, OWASP has an [API Security Top 10 project](#) that focuses specifically on the top 10 vulnerabilities in API security, and it has been updated in 2023. The risk categories have been broadened because API management is complex, and because automated incidents are now a critical issue, they are addressed twice.

There's no question that APIs are woefully unprotected, often because organizations only protect public-facing APIs, leaving others unmonitored and unprotected.

Protect your APIs with Barracuda

Protect against the OWASP API Security Top 10 and more with Barracuda security solutions for your AWS-hosted apps and your APIs. Barracuda Application Protection solutions can analyze API traffic and payloads to enforce a wide variety of security policies that protect your APIs and their infrastructure. They can also find shadow and zombie APIs — the APIs you're not tracking or securing — and protect those as well. The following Barracuda capabilities offer a strong line of defense against API vulnerabilities.

Discovery

- ML-powered Continuous API Discovery
- Schema-based API Discovery and Validation

Protection

- OWASP Top 10, 0-day, DDoS, and Bot Attacks
- ATO and brute force protection
- AuthN, AuthZ, and Zero Trust enforcement
- East-West and North-South Protection

Visibility and Analytics

- Detailed Traffic Logs
- Attacks Logs
- Detailed reports
- Automate responses with SIEM/SOAR/XDR

Schema-based JSON and GraphQL API security

Protect your applications and infrastructure from issues in requests with JSON and GraphQL payloads. Barracuda Application Protection parses out the data, validates user inputs based on schema, and enforces other security checks to discover injection and other hidden attacks in the API payload. Control rules implemented for the URL/host require authentication before they can access the resource. Along with detecting and blocking denial-of-service (DoS), injection, and other suspicious requests, Barracuda Application Protection also offers GraphQL-specific solutions, such as preventing introspection queries and batching attacks that seek to bypass rate limits. In addition, East-West and North-South traffic can be protected using the included WAF containers, which are deployed to protected internal application traffic.

Protection against automated attacks

Barracuda's API security capabilities can control the rate of API calls, sending suspicious clients to a tarpit and forcing them to slow down their API-based communication. This protects against service downtime, slow response times, and DDoS. In addition to tarpits, Barracuda solutions can also enforce traditional rate control, which is particularly helpful in enforcing SLAs with misbehaving clients. With a lot of API traffic originating from bots and other automated tools, it is important to have the intelligence to identify and block unauthorized bots. [Barracuda Advanced Bot Protection](#) uses advanced machine learning models to detect and block them.

Machine learning-powered continuous API discovery

To ensure effective security measures, continuous discovery of APIs is crucial. Barracuda API security solutions provide API discovery by analyzing API traffic metadata. Using an intelligent engine and machine learning (ML), they uncover not only APIs deployed in production, but also unknown (shadow) APIs and those that are older and left unprotected (zombie APIs). Barracuda's ML-powered API discovery runs continuously, monitoring live traffic to API endpoints to discover these shadow and zombie endpoints. Once discovered, the solution automatically turns on security settings, reducing the threat surface and keeping unauthorized users out.

Strong authentication and authorization enforcement

A critical part of API security implementation is enforcing strong authentication and authorization. Barracuda Application Protection provides JSON Web Token (JWT) and client certification authentication support to achieve this enforcement, providing external and internal introspection. The solution checks for valid claims in the payload before checking the signature validation. Barracuda Application Protection is also capable of enforcing Zero Trust protection for your APIs – which is especially important when you have many microservices talking to each other.

Secure API delivery for your critical applications

A hardened TLS front end provides a secure access layer to your APIs. Content routing allows you to add newer API versions or rollout and test without configuring the entire API setup from scratch. You can also import either updated API contract documents or virtual patches from supported scanners. These imports enable automatic security configuration discovery for your new API endpoints. Add authentication and authorization to restrict API access to authorized users. You also have the option to extend the API security capabilities of Barracuda Application Protection to endpoints that are configurable through Swagger and OpenAPI specs. These advanced capabilities, which include extensive monitoring and logging, deliver comprehensive protection against various API vulnerabilities.

Gain full visibility into your applications and traffic.

Each request to your API is logged with all the headers and other details, making it easy for you to troubleshoot any issues. The reporting and syslog modules have multiple integrations, giving you quick and thorough visibility into traffic patterns and changes in behavior.

Barracuda Application Protection is available in two plans. Find the plan that's right for you.

CAPABILITIES	ADVANCED	PREMIUM
WEB APPLICATION PROTECTION		
OWASP Top 10 Protection	✓	✓
Smart Signatures	✓	✓
Zero Day Attack Protection	✓	✓
IP Threat Intelligence	✓	✓ (Cloud connected)
Geo-IP Intelligence	✓	✓
Data Leak Protection	✓	✓
Website Supply Chain Protection	Visualization only	✓
Anti-Virus for File Uploads	✓	✓
Advanced Threat Protection for File Uploads		✓
Risk-based Attack Detection		✓

CAPABILITIES	ADVANCED	PREMIUM
FULL SPECTRUM DDoS PROTECTION		
Unlimited Volumetric DDoS Attack Prevention	✓	✓
Unlimited Application DDoS Attack Prevention	✓	✓
Rate Limiting	✓	✓
DNS Security		✓
API SECURITY		
Protect JSON and GraphQL APIs	JSON	JSON + GraphQL
Schema-based API Discovery	✓	✓
ML-backed JSON API Discovery		✓
ML-backed Shadow API Discovery		✓
Unlimited API Rate Limiting Rules (Tarpit)		✓
ADVANCED BOT PROTECTION		
Basic Bot Protection — Web Scraping	✓	✓
Basic Bot Protection — Bot Spam Detection	✓	✓
Bot Signature Database	✓	✓
CAPTCHA Insertion and Challenges	✓	✓
Brute Force Prevention	✓	✓
Credential Stuffing Protection	✓	✓
Cloud-backed Active Threat Intelligence		✓
Privileged Account Protection		✓
ML-backed Bot Detection		✓
Client Identification and Control		✓
SECURE APPLICATION DELIVERY		
Content Delivery Network	✓	✓
Authentication, Authorization, and Access Control	Client Certificates and JWT	Client Certificates and JWT
Shared IP	✓	✓
Zero Trust Network Access		✓
Load Balancing with Server Health Monitoring		✓
Content Routing		✓
Containerized Deployment		✓
Per-App IP		✓

