Barracuda Application Security

Comprehensive web application and API protection for your apps everywhere.

Barracuda Application Protection provides comprehensive, easy-to-use application security for your publicly hosted apps everywhere. With a simple three-step onboarding process and pre-built security policies, you can start protecting your apps with machine learning-backed security within minutes. Massively scalable and globally available, Barracuda Application Protection can secure any size of application. Barracuda Application Protection can be deployed as a SaaS service or as WAF containers within your application deployments, providing both East-West and North-South protection. Barracuda Application Protection runs on over 60 PoPs worldwide. Deploy your application on the PoP nearest to you to gain comprehensive protection without introducing any application latency. Applications can be deployed on multiple PoPs for redundancy and other needs.

Secure your websites and APIs with one comprehensive solution.

Stop OWASP Top 10 web and API attacks, volumetric and application DDoS attacks, and zero-day threats with a single comprehensive solution. APIs are the biggest threat vector for modern applications, and Barracuda Application Protection protects JSON and GraphQL APIs.

Stop DDoS and account-takeover attacks in their tracks.

Barracuda Application Protection includes unlimited full-spectrum DDoS Protection against volumetric and application DDoS attacks. The Advanced plan also includes credential stuffing and credential-spraying protection to protect against account takeover attacks. The Premium plan includes behavioral detection of ATO attacks with the Privileged Account Protection capability.

Gain ML-backed adaptive protections to stop the latest bots and emerging attacks.

Barracuda Active Threat Intelligence uses cloud-based ML to identify and block emerging zero days, automated bot attacks, and threats in near-real time. It is backed by proven ML models and crowdsourced threat intelligence from all our honeypots and installations.

Automatically discover and protect hidden shadow APIs.

Many applications deploy APIs for their backend and do not document them for admins, leading to compromises through these “shadow APIs.” Barracuda Application Protection uses ML to detect these API endpoints and automatically configure protections for them.

Simplify security with automated configuration tuning and signature updates.

Included Auto Configuration Engine helps admins tune their configuration by providing ML-backed configuration suggestions. Schema-based API discovery allows admins to quickly set up API security and automated signature updates ensure continued protection against emerging threats.

Enable DevSecOps teams to move fast, securely.

Barracuda Application Protection is built API first. This means that every configuration setting can be managed using APIs and a JSON-based configuration file, allowing for easy automation and management.

Gain deep visibility and automated response capabilities.

Barracuda Application Protection provides detailed logging and reporting for each request, allowing you to gain unparalleled visibility into your applications and attack traffic. In addition, the same APIs that are used for configuration can be used with SIEM/SOAR/XDR systems, allowing you to define your own automated responses to various attacks and events.

Extend protection to your internal apps with included Barracuda CloudGen Access.

Internal applications need more protection while exposed on the internet than ever before. The included ZTNA capabilities of the Premium plan allow you to seamlessly enable ABAC and other advanced login protection for these internal apps, further extending your security posture to the edge.

Complete N-S and E-W security for hybrid deployments with included containerized WAF.

Traditional WAF services can only protect traffic to and from the application to the client – they don’t offer full protection between various parts of the apps. Compromise of one microservice of an app can allow attackers to move laterally quite easily. Barracuda Application Protection includes a containerized deployment mode where you can deploy the same protections between your microservices, protecting them from intra-app attacks.

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		✓
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		✓

CAPABILITIES	ADVANCED	PREMIUM
AUTOMATION, REPORTING, ANALYTICS, AND SERVICES		
Log Export to SIEM	One export server	Multiple export servers
Auto Configuration Engine	✓	✓
Virtual Patching and Scanner Integration	BVM	BVM
Log Storage Duration	30 days	60 days
Configuration API Access	✓	✓
Configuration Snapshots	✓	✓
Advanced Reporting and Visualization		✓

Key Features

Web Application Protection

- OWASP Top 10 Web Application Security Risks Protection
- Geo-IP and IP Reputation (including public proxies and Tor Nodes)
- Smart Signatures
- Outbound Data Theft Protection (Credit Cards, SSN, etc.)
- Exception Heuristics
- File Upload Control
- Anti-Virus for File Upload Protection
- Advanced Threat Protection for File Uploads (Requires ATP Subscription)
- Website Cloaking
- Protocol Limit Checks
- Granular per URL/parameter policies
- Rate Control and Tarpits
- Auto-Configuration Engine
- Automated Enforcement of Sub-Resource Integrity and Content Security Policies (Client-Side Protection)
- Deep visibility into resources and changes (Client-Side Protection)

Full-Spectrum DDoS Protection

- Unlimited Volumetric DDoS Prevention
- Unlimited Application DDoS Prevention
- Unlimited Rate Control Rules

API Security

- Protection against OWASP Top 10 API Security Risks
- JSON Security
- GraphQL Security
- Schema-based API Discovery
- Machine Learning-based Automated JSON API Discovery

Advanced Bot Protection

- Web Scraping Protection
- Advanced Bot Protection with Cloud-based Machine Learning
- Known Bot Database
- Bot Spam Protection (Referrer and Comment Spam)
- Form Spam Protection
- Credential Stuffing and Spraying Protection
- Privileged Account Protection
- Brute Force Attack Protection
- CAPTCHA Support
- reCAPTCHAv2/v3 Support
- hCAPTCHA integration

Secure Application Delivery

- TLS/SSL Offloading
- Server Load Balancing
- Content Routing
- DNS Security
- Content Delivery Network Integration
- Dynamic URL Encryption
- HTTP/1.0, HTTP/1.1 and HTTP/2.0 Support
- WebSocket Support
- IPv6 Support
- Request and Response Control (URL Translation)
- Website Translations
- Caching and Compression

Identity and Access Control

- Client Certificates
- JSON Web Tokens
- Virtual Patching and Feedback Loops
- Barracuda Vulnerability Reporting Service (Free)

Automation

- Configuration API
- Configuration Automation Code Samples
- Github Integration
- JSON-based Configuration
- Snapshots

Reporting and Analytics

- Onboard Logging (Access Logs, Web Firewall Logs, and Audit Logs)
- On-demand and scheduled reporting
- Syslog Export
- AMQP/AMQPS Export

Additional Deployment Modes

- Containerized Deployment for close-in protection

Barracuda®
Your journey, secured.