

# Barracuda WAF-as-a-Service

Comprehensive Web Application and API Protection for  
your apps everywhere

Barracuda WAF-as-a-Service is a cloud-delivered WAF that provides comprehensive application security to your publicly hosted Web Applications and APIs. It provides unparalleled simplicity with a 3-step onboarding wizard, pre-built security policies, easy to navigate user interface and unlimited rulesets. Massively scalable and globally available, Barracuda WAF-as-a-Service can be deployed as a SaaS service or as WAF containers within your application deployments, providing both East-West and North-South protection.



## Gain comprehensive application security in minutes.

Barracuda WAF-as-a-Service puts you in complete control. Get up and running quickly and easily with a 3-step deployment wizard and preconfigured rulesets. Alternatively, take a more hands-on approach by creating, fine-tuning, and applying your own custom rulesets to the specific apps you choose. Either way, WAF-as-a-Service gives you a complete set of features and capabilities to ensure total application security.

## Unmetered Full-Spectrum DDoS protection for every protected app.

Full-spectrum DDoS protection capabilities give you total peace of mind, blocking the entire scope of application threats—much more than just the OWASP Top Ten vulnerabilities. And unlike other solutions, WAF-as-a-Service provides unmetered Layer-3 – 7 DDoS protection, to ensure uninterrupted availability of the apps your business depends on — comprehensive DDoS protection is built in, with no extra charges.

## Discover and protect your APIs.

Barracuda WAF-as-a-Service provides protection for your XML, JSON and GraphQL APIs. Configuring API security is complex and requires significant admin time. To reduce the burden on admins Barracuda WAF-as-a-Service's automated JSON API Discovery uses Machine Learning to identify API endpoints in application traffic and suggests automated security settings to protect them.

[www.pmddatasolutions.com](http://www.pmddatasolutions.com)

## Stop today's most advanced malicious bots.

Barracuda Advanced Bot Protection uses machine learning to continually improve its ability to spot and block bad bots and human-mimicking bots—while allowing legitimate human and bot traffic to proceed with minimal impact. The cloud-based Active Threat Intelligence layer uses crowd-sourced threat intelligence to identify & block emerging threats in near-real time. Included in this subscription are Credential Stuffing Protection and Privileged Account Protection capabilities to stop advanced Account Takeover attacks.

## Protect against dangerous client-side attacks.

Attackers exploit third-party scripts to perform client-side digital skimming attacks, such as Magecart, to steal PII and financial data directly from the browser. Barracuda WAF-as-a-Service offers Client-Side Protection, a feature that automates the CSP and SRI configuration, reducing admin overheads and configuration errors. In addition, detailed visualization and reporting provide administrators with a deep view into the application traffic.

## Enable granular access control and secure app delivery.

Barracuda WAF-as-a-Service features a hardened SSL/TLS stack that provides a secure HTTPS front end to your applications. It can secure both HTTP1.x and HTTP2 traffic. The built-in application delivery module enables server load balancing, content routing, caching, and compression. Barracuda WAF-as-a-Service also offers DNS security and Content Delivery Network (CDN) capabilities. Access Control capabilities include authentication and authorization for both web applications and APIs.

## Leverage powerful reporting capabilities.

Barracuda WAF-as-a-Service features a detailed dashboard that presents vast amounts of data in the form of actionable insights that help you make informed decisions. Detailed traffic logs are available for each request, along with firewall logs for attack traffic. The Active Threat Intelligence Dashboard provides deep drilldowns into Bot traffic and details about Client-Side Protection. In addition to on-board logs and reports, Barracuda WAF-as-a-Service also provides the ability to export logs to any Syslog or AMQP capable SIEM/SOAR system.

## Automate and orchestrate security.

Barracuda WAF-as-a-Service integrates with many popular third-party DevOps tools to ensure CI/CD processes are fully automated. Full-featured REST API seamlessly integrates with Puppet, Chef, Ansible, Terraform, Azure ARM, AWS CloudFormation, and more. Barracuda WAF-as-a-Service's REST API is built on OpenAPI specifications, making it easy to create automation scripts, and the official GitHub page has code samples for popular platforms and use cases.

**[www.pmdatasolutions.com](http://www.pmdatasolutions.com)**

#### Web Application Security

- 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 & Tarpits
- Auto-Configuration Engine

#### API Protection

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

#### Bot Protection

- Web Scraping Protection
- Advanced Bot Protection with Cloud-based Machine Learning (Requires ABP Subscription)
- Known Bot Database
- Bot Spam Protection (Referrer and Comment Spam)
- Form Spam Protection
- Credential Stuffing and Spraying Protection (Requires ABP Subscription)
- Privileged Account Protection (Requires ABP Subscription)
- Brute Force Attack Protection
- CAPTCHA Support
- reCAPTCHA v2/v3 Support

#### Client-Side Protection

- Automated Enforcement of Sub-Resource Integrity and Content Security Policies
- Deep visibility into resources and changes

#### Full Spectrum Unmetered DDoS Protection

- Volumetric DDoS Protection
- Application DDoS Protection

#### 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)

#### Logging and Reporting

- 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

**www.pmdatasolutions.com**

