Barracuda WAF-as-a-Service

Protect every web app, hosted anywhere, in minutes

Deploying and configuring traditional web application firewalls (WAFs) can be prohibitively complex and time-consuming. Indeed, some simply install a WAF in default mode for compliance, and never configure it correctly — leaving them vulnerable to application-based threats.

You can deploy, configure, and get Barracuda WAF-as-a-Service up and running in just minutes. Pre-built templates protect your applications immediately, and an intuitive interface makes it simple to fine-tune specific policies. Full-spectrum DDoS protection ensures continuous application availability. And the built-in Barracuda Vulnerability Remediation Service automatically scans your applications and remediates vulnerabilities.

Simple yet flexible

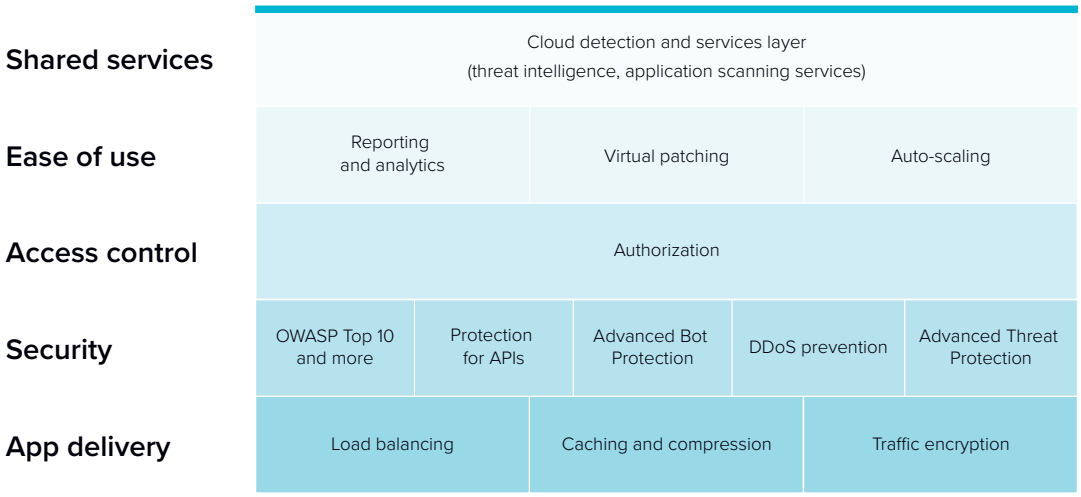
Barracuda WAF-as-a-Service features an easy-to-use, five-step onboarding wizard to ensure your applications are protected in minutes. Effective pre-built templates provide complete protection for most commonly used applications. Advanced users can easily assert granular control over specific elements to set customized security policies. Simply add the configuration element you want to fine-tune to the list of configuration components and adjust them to meet your specific needs.

Protection from next-generation attacks

The service is built on enterprise-proven technology that defends against OWASP Top 10 security risks, OWASP Automated Threats to Web Applications, and more, including zero-day threats. Advanced bot defense stops automated attacks such as web scraping, scalping, carding, bot spam, and credential-stuffing/ account-takeover attacks. Unmetered DDoS protection prevents both application and volumetric DDoS attacks. Rich analytics and intuitive reports help you document compliance.

Protection for next-generation apps

Regardless of where you host your apps — on-prem, in the cloud, in a container, or in a serverless environment — you get a REST API and the Barracuda Vulnerability Remediation Service, which scans for application vulnerabilities and remediates them with a single click. This ensures uninterrupted, optimized security even as you update your applications and deploy new ones in response to evolving business needs — without any additional administrative overhead.



API-driven and DevSecOps-ready

Protects against all these threats

- OWASP Top 10 Application Security Risks
  - Including SQL injections, XSS, CSRF, XXE, and more
- Advanced bots
  - Including the OWASP Automated Threats to Web Applications
- Credential-stuffing/account-takeover attacks
- API attacks for XML and JSON APIs
- Application and volumetric DDoS attacks
- Zero-day attacks
  - With a powerful positive-security model combined with smart-signature technology for negative security

Supported protocols

- HTTP/S/0.9/1.0/1.1/2.0
- WebSocket
- IPv4

Other advanced security features

- IP reputation protection
  - Including IP geolocation, and reputation feeds based on sensors in the field and other inputs
- File upload protection
  - Integration with Barracuda Advanced Threat Protection included
- Parameter tampering
- Cookie/form manipulation
- Forceful browsing
- Application tampering
- Form field meta-data validation
- Website cloaking
- Response control
- Granular policies to HTML elements
- Protocol limit checks
- Barracuda IP reputation database
- Heuristic fingerprinting
- CAPTCHA challenges
- Slow client protection
- ToR exit nodes
- Barracuda block list
- Unmetered L3-L7 DDoS protection

Barracuda®
Your journey, secured.