Barracuda
Your journey, secured.

Barracuda WAF-as-a-Service

Chroń każdą aplikację internetową, hostowaną w dowolnym miejscu, w ciągu kilku minut.

Wdrażanie i konfiguracja tradycyjnych zapór aplikacji internetowych (WAF) może być nadmiernie skomplikowana i czasochłonna. W rzeczywistości niektórzy po prostu instalują WAF w trybie domyślnym w celu zapewnienia zgodności z przepisami i nigdy nie konfigurują go poprawnie, co pozostawia ich podatnymi na zagrożenia oparte na aplikacjach.

Barracuda WAF-as-a-Service można wdrożyć, skonfigurować i uruchomić w ciągu kilku minut. Gotowe szablony natychmiast chronią aplikacje, a intuicyjny interfejs ułatwia dostosowanie określonych zasad. Pełne spektrum ochrony DDoS zapewnia ciągłą dostępność aplikacji. A wbudowana usługa Barracuda Vulnerability Remediation Service automatycznie skanuje aplikacje i usuwa luki.

Microsoft Azure Certified

ICSA labs CERTIFIED

Member of Microsoft Intelligent Security Association

Proste, a zarazem elastyczne

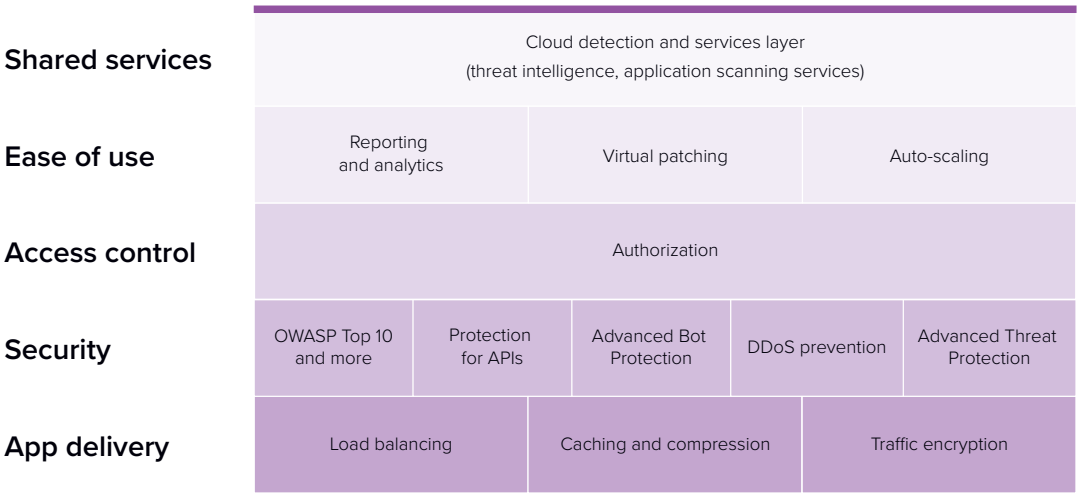
Barracuda WAF-as-a-Service posiada łatwy w użyciu, pięcioetapowy kreator włączania, aby zapewnić ochronę aplikacji w ciągu kilku minut. Efektywne, prefabrykowane szablony zapewniają pełną ochronę dla najczęściej używanych aplikacji. Zaawansowani użytkownicy mogą w łatwy sposób zapewnić sobie granularną kontrolę nad określonymi elementami, aby ustawić niestandardowe polityki bezpieczeństwa. Wystarczy dodać wybrany element konfiguracji do listy i dostosować go do konkretnych potrzeb.

Ochrona przed atakami nowej generacji

Usługa jest zbudowana na sprawdzonej w przedsiębiorstwach technologii, która chroni przed zagrożeniami bezpieczeństwa OWASP Top 10, OWASP Automated Threats to Web Applications i innymi, w tym zagrożeniami zero-day. Zaawansowana ochrona przed botami powstrzymuje zautomatyzowane ataki, takie jak skrobanie stron internetowych, skalpowanie, carding, spam botowy oraz ataki typu credential-stuffing/account-takeover. Nieopomiarowana ochrona DDoS zapobiega zarówno aplikacyjnym, jak i wolumetrycznym atakom DDoS. Bogata analityka i intuicyjne raporty pomagają udokumentować zgodność z przepisami.

Ochrona dla aplikacji nowej generacji

Niezależnie od tego, gdzie przechowujesz swoje aplikacje na miejscu, w chmurze, w kontenerze lub w środowisku bezserwerowym - otrzymujesz interfejs API REST oraz usługę Barracuda Vulnerability Remediation Service, która skanuje podatności aplikacji i usuwa je jednym kliknięciem. Zapewnia to nieprzerwane, zoptymalizowane bezpieczeństwo nawet podczas aktualizacji aplikacji i wdrażania nowych w odpowiedzi na zmieniające się potrzeby biznesowe - bez żadnych dodatkowych kosztów administracyjnych.



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 blacklist
- Unmetered L3-L7 DDoS protection

Barracuda®
Your journey, secured.