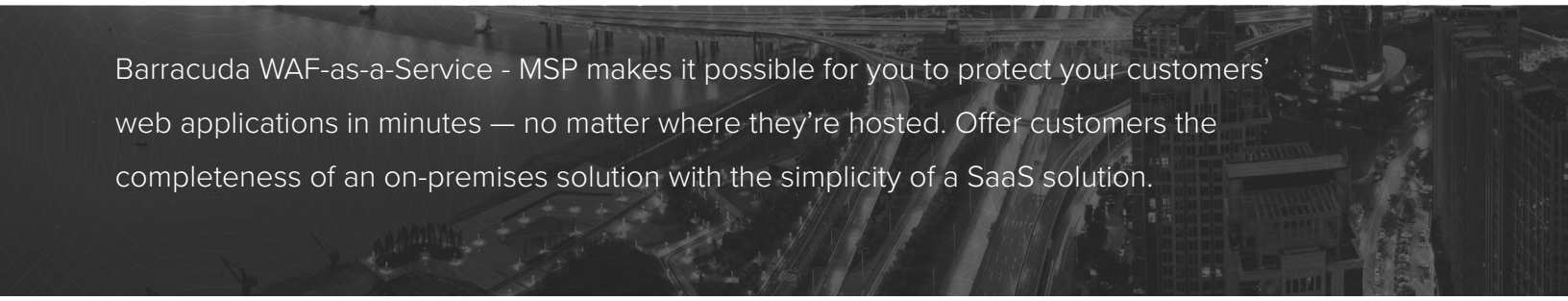
MSP Barracuda
Your journey, secured.

DATASHEET

Barracuda WAF-as-a-Service

Cloud-Delivered Application Security



Barracuda WAF-as-a-Service - MSP makes it possible for you to protect your customers' web applications in minutes — no matter where they're hosted. Offer customers the completeness of an on-premises solution with the simplicity of a SaaS solution.

A better approach

Managing specialized web application firewall (WAF) policies for your customers to ensure a perpetually robust application security posture can be a full-time job. Organizations that can't afford a fully-managed solution or to employ the required resources struggle to stay up to date on the latest attacks and protection measures needed to deliver consistent security and compliance. Barracuda WAF-as-a-Service offers MSPs a better solution to application security challenges.

Simplified setup and configuration

Remove the complexity of setting up and configuring an appliance or instance. Barracuda WAF-as-a-Service delivers comprehensive protection for your customers' web apps in minutes thanks to its simple five-step wizard.

Complete control over every component

Barracuda WAF-as-a-Service offers a level of control traditionally reserved for on-premises and public cloud solutions. Take complete control over every component, and fine-tune specific policies for each application's requirements. Building unique per-app policies for customers has never been simpler.

Automated vulnerability discovery and remediation

Barracuda Vulnerability Remediation Service is built into Barracuda WAF-as-a-Service and provides automatic vulnerability detection and remediation that can be scheduled, ensuring ongoing protection without administrative overhead.

Granular visibility

Barracuda WAF-as-a-Service helps you gain rich insight into customers' web traffic events and users. Detailed compliance reports help you easily understand each customer's security status at any given time by having complete visibility into all HTTP/S traffic.

Unmetered DDoS Protection

DDoS attacks disrupt the service availability of your customers' web apps, which can have a significant impact on business. Barracuda WAF-as-a-Service defends against the full spectrum of L3-L7 DDoS attacks ensuring the availability of your customers' web apps.

Key Features

Protections included

- All OWASP risks, including "Top 10"
- Brute force attacks
- Parameter tampering
- Cookie/form manipulation
- Forceful browsing
- XML attacks
- Application tampering
- Zero-day attacks
- SQL Injection
- Cross-site scripting (XSS)
- Form field meta-data validation
- Website cloaking
- Response control
- Web scraping prevention
- Granular policies to HTML elements
- Protocol limit checks
- File upload control
- IP whitelisting/blacklisting

Advanced protections

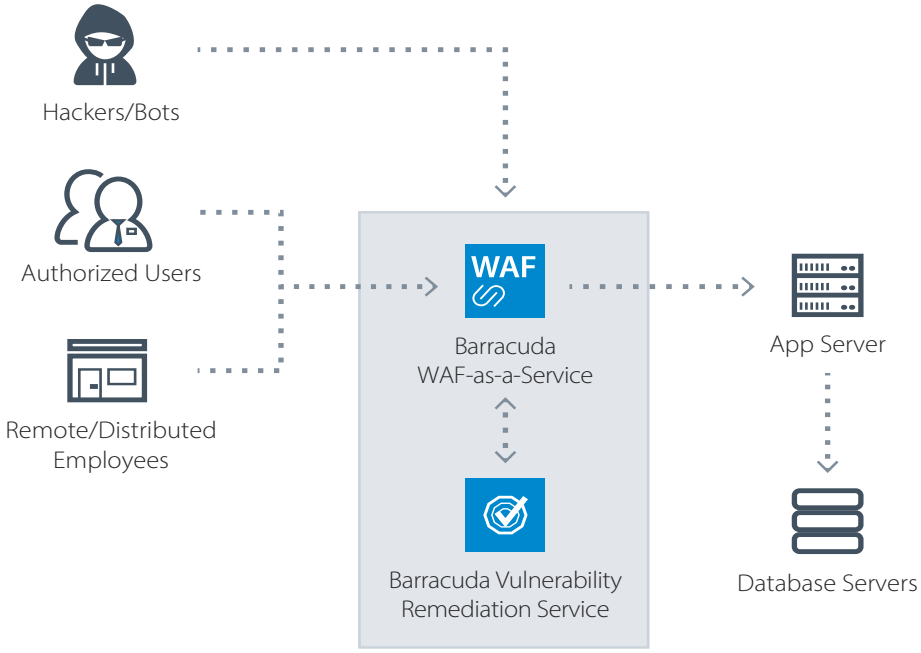
- Barracuda IP reputation database
- Heuristic fingerprinting
- CAPTCHA challenges
- Slow client protection
- ToR exit nodes
- Barracuda blacklist
- Unmetered L3-L7 DDoS protection

Application enhancements

- High availability
- SSL offloading
- Load balancing

-Support protocols

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



MSP Barracuda
Your journey, secured.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.
@BarracudaMSP | LinkedIn: BarracudaMSP | blog.barracudamsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com