

DDoS Protection vs. WAF vs. Bot Management

DDoS Protection, WAF (Web Application Firewall) und Bot Management schützen Webseiten, Anwendungen und APIs vor schädlichem Webtraffic. Doch worin genau unterscheiden sie sich und welche Lösung schützt vor welchen Gefahren? Unser Kurzvergleich liefert Antworten und hilft Ihnen, die für Ihre Anforderungen passende Lösung zu finden.

 Merkmal / Funktion	 DDoS Protection	 WAF (Web Application Firewall)	Bot Management
Hauptziel	Schutz vor Überlastung durch schädlichen Traffic	Überwachung, Filterung und Blockierung von schädlichem HTTP/S-Traffic	Erkennung und Blockierung von automatisierten Zugriffen durch Bots
Primäres Schutzziel	Verfügbarkeit	Integrität und Vertraulichkeit	Integrität und Vertraulichkeit
Schützt gegen	DDoS-Angriffe • volumetrische Attacken mit hohen Bandbreiten oder Paketraten auf Netzwerk- und Transportebene • Attacken mit schädlichen Anfragen auf Anwendungsebene • Traffic-Spitzen durch Botnetze	OWASP-Top-10-Risiken • SQL Injection • XSS • CSRF • etc.	Automatisierte Angriffe • Scraping • Credential Stuffing • Account Creation & Takeover • Skewing • etc.
Verhindert	Ausfälle und Störungen durch Überlastung	Datendiebstahl, Manipulation, Spionage, unautorisierten Zugriff	Datendiebstahl, Manipulation, Spionage, unautorisierten Zugriff
Ebene im OSI-Modell	Netzwerkebene (Layer 3) + Transportebene, (Layer 4) + Anwendungsebene (Layer 7)	Anwendungsebene (Layer 7)	Anwendungsebene (Layer 7)

Merkmal / Funktion	 DDoS Protection	 WAF (Web Application Firewall)	 Bot Management
Erkennt Mensch vs. Bot?	✗ Nein	✗ Nicht primär	✓ Ja
Nutzt Verhaltensanalyse?	✗ Selten	○ Teilweise (z. B. durch Regeln)	✓ Ja (Machine Learning, Fingerprinting etc.)
Rate Limiting möglich?	✓ Ja (z. B. Requests pro Sekunde)	✓ Ja (per IP oder URI)	✓ Ja, inkl. dynamischer Regeln
CAPTCHA / Challenge-Funktionen	✗ Nein	○ Teilweise	✓ Ja (z. B. JavaScript Challenges, CAPTCHA)
Gute Bots erlauben?	✗ Kein Fokus	✗ Kein Fokus	✓ Ja (z. B. Suchmaschinenbots)
Empfohlen für	IT-Infrastrukturen, Webseiten, Webanwendungen, APIs	Webanwendungen, APIs	Webseiten mit Nutzerkonten, Webformularen, Exklusivinhalten, APIs

Fazit: Wer benötigt welche Lösung?

- **DDoS Protection** sichert die **Verfügbarkeit** Ihrer Website, indem Überlastungen durch hohe Bandbreiten oder Paketraten verhindert werden – essenziell für alle Online-Dienste.
- Eine **WAF** schützt die **Integrität Ihrer Webapplikation**, indem sie bekannte **Angriffe über das HTTP/-Protokoll blockiert** – besonders wichtig für interaktive und geschäftskritische Anwendungen, z.B. für Online-Banking, E-Commerce.
- **Bot Management** unterscheidet zwischen Menschen und Maschinen, **erkennt unerwünschte und betrügerische Bots** und schützt Ihre **Geschäftslogik** – wichtig für Login-Seiten, Online-Formulare und APIs, z. B. für E-Commerce, Ticketanbieter, Medienseiten.

Myra schützt, was zählt. In der digitalen Welt.

Sie wollen mehr darüber erfahren, wie Sie mit unseren zertifizierten Lösungen Ihre Anwendungen vor vielfältigen Risiken wie DDoS-Attacken, Bot-Netzwerken und Angriffen auf Datenbanken schützen können? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihre Organisation. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.