# Web Application Protector

## Automatisierter Schutz für Ihr digitales Unternehmen

Web Application Protector wurde für Unternehmen entwickelt, die einen stärker automatisierten Ansatz für Web Application Firewall (WAF) und Distributed Denial-of-Service (DDoS)-Sicherheit suchen.

Der Schutz Ihrer Webanwendungen und APIs kann ziemlich kompliziert sein. Selbst die erfahrensten Sicherheitsexperten haben oft damit zu kämpfen, mit den neuesten Bedrohungen mitzuhalten und die Sicherheits- und Schutzvorkehrungen immer rechtzeitig zu aktualisieren. Unternehmen ohne interne spezielle und qualifizierte Mitarbeiter können am meisten von einer WAF- und DDoS-Lösung profitieren, die einfach zu implementieren, hochgradig automatisiert und einfach zu warten ist.

## Web Application Protector

Web Application Protector ist eine cloudbasierte WAF-Lösung, die auf Einfachheit und Automatisierung ausgelegt ist. Web Application Protector schützt Ihre Anwendungen und APIs mit weniger Aufwand vor einer Vielzahl von Bedrohungen auf Netzwerk- und Anwendungsebene. Und da Web Application Protector auf der Akamai Intelligent Edge Platform basiert, verfügt es über integrierte Performancefunktionen, die dafür sorgen, dass Ihre Websites, Webanwendungen und APIs optimal funktionieren.

## Funktionsweise

Mit Web Application Protector stellen Clients die Verbindung zu Ihren Webanwendungen über einen optimalen Akamai-Edge-Server her, der sich in der Regel in Ihrer Nähe befindet. Jeder Server untersucht den Web- und API-Traffic, um sich vor DDoS-, Webanwendungs- und API-basierten Angriffen zu schützen, und gewährt gleichzeitig legitimen Nutzern den Zugriff. Mit mehr als 300.000 Akamai-Servern auf der ganzen Welt bietet Web Application Protector eine Größenordnung, mit der selbst größte Angriffe aufgehalten werden können – und das direkt an der Edge, noch bevor die Bedrohungen Ihre Anwendungen und APIs erreichen können.

Web Application Protector vereinfacht den Schutz Ihrer Organisation durch automatisierte Sicherheitsmodule. Unsere erstklassigen Sicherheitsexperten haben Einblicke in Tausende von Angriffen auf der Akamai-Plattform und nutzen fortschrittliche Algorithmen für maschinelles Lernen, um Ihre Sicherheitsregeln kontinuierlich zu analysieren, zu verfeinern und zu aktualisieren, ohne dass ein menschliches Eingreifen erforderlich ist.

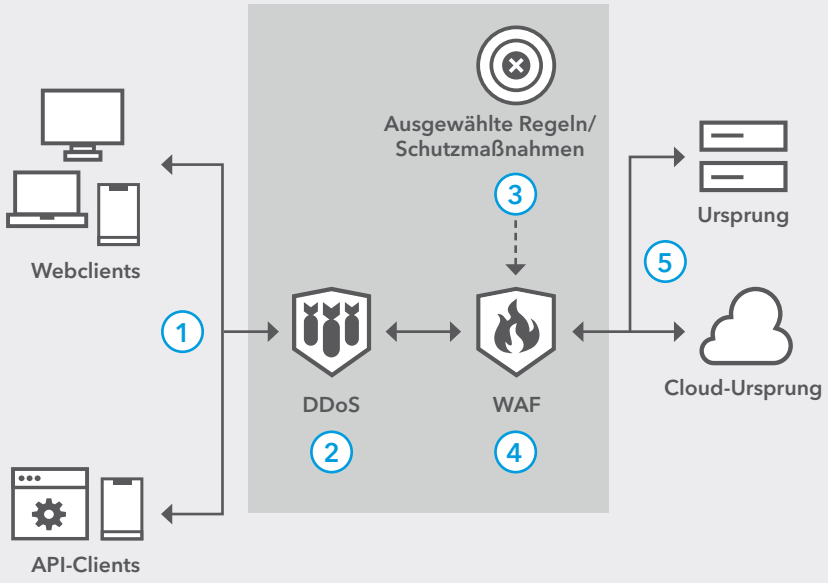
### IHRE VORTEILE

- **Höhere Onlinesicherheit –** Schützen Sie Ihre Anwendungen vor DDoS-Angriffen und Angriffen auf Webanwendungen, um das Risiko von Ausfällen und Datendiebstahl zu reduzieren
- **Schnelle Implementierung –** Konfigurieren Sie die Sicherheitsmodule von Web Application Protector mit nur wenigen Klicks, um Ihre Anwendungen schneller zu schützen
- **Einfache Verwaltung –** Akamai aktualisiert die enthaltenen Sicherheitsmodule kontinuierlich und transparent, um Ihre Anwendung mit weniger Aufwand zu schützen

# Web Application Protector

Automatisierter Schutz für Ihr digitales Unternehmen

## Funktionsweise




1. Nutzer und Angreifer stellen die Verbindung zu Ihrer Anwendung über den nächstgelegenen Akamai-Server her.
2. DDoS-Angriffe auf Netzwerkebene [L3/4] werden sofort an der Akamai Edge abgewehrt.
3. Automatische Updates, die sich auf maschinelles Lernen und Heuristik stützen, basieren auf der sich ständig entwickelnden Bedrohungslandschaft.
4. Web Application Protector blockiert DDoS-, Webanwendungs- und API-basierte Angriffe auf Anwendungsebene.
5. Reduzieren Sie das Risiko von Ausfällen und Datendiebstahl, indem Sie Ihren Ursprung vor Angriffen schützen.

## Funktionen

**Anwendungs-Firewall:** Verhindern Sie SQL Injection, XSS, RFI und andere Arten von Bedrohungen auf Anwendungsebene mit von Akamai verwalteten automatisierten Regeln. Diese verfügen über eine erweiterte Erkennungslogik, die sich dynamisch an die Eigenschaften eingehender Anfragen anpasst.

**DoS-Schutz (Ratensteuerung):** Schützen Sie Ihre Anwendungen und APIs vor DoS-Angriffen (Denial-of-Service), indem Sie Clients überwachen und blockieren, die Schwellenwerte für die Anfragerate überschreiten. Wer die erlaubte Anfragerate überschreitet, wird automatisch gesperrt, um die Ursprünge der Website zu schützen.

**Fortschrittliche Web Security Analytics:** Ermitteln Sie anhand detaillierter Telemetriedaten zu Angriffen und Analysedaten zu Sicherheitsereignissen, welche Änderungen erforderlich sind, um Ihren Schutz zu verbessern und Ihre Konfigurationen entsprechend Ihrer spezifischen Geschäftsanforderungen zu optimieren.

**Netzwerk-Edge-Firewall (IP/Geo):** Mit IP-/Geo-Kontrollen können Sie Traffic von einer bestimmten IP, einem bestimmten Subnetz oder einer bestimmten geografischen Region blockieren oder zulassen. So können Sie schädliche Anfragen von bestimmten IP-Adressen oder Traffic von The Onion Router (Tor) blockieren, den Hacker zum Verbergen ihrer Identität verwenden.

**Nutzerdefinierte Regeln:** Web Application Protector bietet einen nutzerdefinierten Regelgenerator zur schnellen und einfachen Erstellung individueller Regeln, mit denen Sie besondere Szenarien bewältigen können, die nicht durch Standardregeln abgedeckt sind. Auch neue Schwachstellen lassen sich so schnell beheben.

# Web Application Protector

## Automatisierter Schutz für Ihr digitales Unternehmen

**Performance und Bereitstellung:** Nahtlose Skalierbarkeit, um immer neuen Traffic-Anforderungen gerecht zu werden, CPU- und Speicherressourcen nach Bedarf zu verteilen, zwischengespeicherte Inhalte von der Edge bereitzustellen und unterbrechungsfreien Schutz für höchste Performance und Bereitstellung zu bieten.

**HTTPS enthalten:** Web Application Protector beinhaltet ein TLS- oder SSL-Zertifikat, mit dem Ihre Inhalte sicher übertragen werden und Datendiebstahl verhindert wird. Damit bietet es Ihrer Website und Ihren Nutzern kostenlose HTTPS-Sicherheit.

**Reporting:** Tools für die Berichterstellung zur Websicherheit überwachen und bewerten kontinuierlich die Effektivität Ihrer Schutzmaßnahmen. Sie können Echtzeitberichte erstellen, um tägliche Aktivitäten zu überwachen, Angriffe nach Typen zu untersuchen und Berichte zu gezielten APIs, DoS-Traffic und mehr anzuzeigen.

**Echtzeitwarnungen:** Erstellen Sie E-Mail-Warnungen in Echtzeit mit statischen Filtern und Schwellenwerten, die ganz einfach so konfiguriert werden können, dass nur bestimmte Empfänger benachrichtigt werden.

**Site Shield:** Eine zusätzliche Sicherheitsebene, die Angreifer daran hindert, cloudbasierte Schutzmaßnahmen zu umgehen und gegen Ihre Ursprungsinfrastruktur gerichtete Angriffe auszuführen.

## Weitere Lösungen für besseren Schutz

**Bot Manager:** Identifizieren, kategorisieren und verwalten Sie Bots, die auf Ihre Website zugreifen. Automatisierte Algorithmen nutzen Telemetrie sowohl für menschliches als auch für Bot-Verhalten, um auch die komplexesten Bots zu erkennen und zu abzuwehren.

**SIEM-Integration:** Dank vorgefertigter Konnektoren können Sie lokale und cloudbasierte SIEM-Anwendungen wie Splunk, QRadar, ArcSight und mehr verwenden.

**Page Integrity Manager:** Schützen Sie Websites vor JavaScript-Bedrohungen wie Web-Skimming, Formjacking und Magecart-Angriffen, indem anfällige Ressourcen identifiziert, verdächtige Verhaltensweisen erkannt und schädliche Aktivitäten blockiert werden.

Testen Sie Web Application Protector noch heute unter akamai.com/waptrial.

Akamai

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter www.akamai.com, im Blog blogs.akamai.com oder auf Twitter unter @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: August 2020