AWS Leitfaden zur Entscheidungsfindung

AWS WAF oder AWS Shield?

AWS WAF oder AWS Shield?: AWS Leitfaden zur Entscheidungsfindung

Table of Contents

AWS WAF oder AWS Shield?

Machen Sie sich mit den Unterschieden vertraut und wählen Sie den aus, der am besten zu Ihnen passt

Zweck	Um Ihnen bei der Entscheidung zu helfen, ob AWS WAF oder ob Ihre AWS Shield Anforderungen an einen Sicherheitsservice für Webanwendungen erfüllt werden.
Letzte Aktualisierung	17. September 2024
Abgedeckte Dienste	• AWS WAF • AWS Shield

Einführung

AWS WAF(Web Application Firewall) und AWS Shieldkann Ihnen helfen, Ihre Webanwendungen vor verschiedenen Arten von Cyberangriffen wie Distributed Denial of Service (DDoS) -Angriffen und anderen Sicherheitslücken in Webanwendungen zu schützen.

- AWS WAFkonzentriert sich auf den Schutz Ihrer Webanwendungen vor gängigen Web-Exploits. Wird verwendet AWS WAF , um anpassbare Web-Sicherheitsregeln zu erstellen, um bösartigen Datenverkehr zu filtern, vor Angriffen wie SQL-Injection und Cross-Site Scripting (XSS) zu schützen und andere zu integrieren. AWS-Services
- AWS Shieldist ein verwalteter DDo S-Schutzdienst. Wird verwendet AWS Shield , um die ständige Erkennung und automatische Risikominimierung zu aktivieren und sich vor häufigen DDo S-Angriffen auf Netzwerk- und Transportebene zu schützen.

AWS Shield Advanced AWS Shield schützt zwar vor groß angelegten Angriffen auf Netzwerkebene, aber Sie können einer Ressource eine AWS WAF Web-ACL zuordnen, um Schutz auf Anwendungsebene zu gewährleisten. AWS WAF bietet detaillierteren Schutz vor anwendungsspezifischen Sicherheitslücken. Verwenden Sie beide Dienste zusammen für eine mehrstufige Verteidigungsstrategie, die Ihre Anwendungen vor einer Vielzahl potenzieller Bedrohungen auf verschiedenen Netzwerkebenen schützt.

Im Folgenden finden Sie einen Überblick über die wichtigsten Unterschiede zwischen diesen Diensten.

Kategorie	 AWS WAF	 AWS Shield
Hauptzweck	Schützt vor Exploits in Webanwendungen (wie SQL-Injection oder XSS)	Schützt vor DDo S-Angriffen (wie SYN- oder UDP-Floods)
Schutzschicht	Anwendungsschicht (L7)	Netzwerk-, Transport- und Anwendungsschichten (L3/L4/L7)
Bereitstellung	Muss explizit eingerichtet werden	AWS Shield Standards chutz für alle Kundenkonten enthalten
Anpassung	Hochgradig anpassbar mit benutzerdefinierten Regeln	Aktivieren oder deaktivieren Sie AWS Shield Advanced mit Optionen zur Aktivierung der automatischen Abwehr von Schutzmaßnahmen auf Anwendungsebene DDo S
Verwaltete Regeln	Beinhaltet AWS verwaltet e Regeln und Regeln von Drittanbietern	Nicht zutreffend
Preismodell	Pay-as-you-go Die Preisgest altung basiert auf der Anzahl der Regeln und Anfragen	AWS Shield Standard im Preis enthalten; AWS Shield für Advanced fallen zusätzliche Kosten an

Kategorie	 AWS WAF	 AWS Shield
Reaktionsteam für Angriffe	Nicht zutreffend	Verfügbar mit AWS Shield Advanced (DDoS Response Team rund um die Uhr)
Überwachung in Echtzeit	Ja	Ja
Verkehrsinspektion	Ebene der Anfrage	Auf Paket-Ebene

Unterschiede zwischen und AWS WAF AWS Shield

Erkunden Sie acht Hauptunterschiede zwischen AWS Shield und AWS WAF, die sich auf die Schutzebene, die Bereitstellung, die Anpassung, die verwalteten Regeln, das Preismodell, das Team zur Bekämpfung von Angriffen, die Echtzeitüberwachung und die Überprüfung des Datenverkehrs beziehen.

Layer of protection

AWS WAF

- Arbeitet auf der Anwendungsebene (Schicht 7). Es schützt Webanwendungen, indem es den HTTP/S Datenverkehr filtert und überwacht. AWS WAF schützt vor gängigen Web-Exploits wie SQL-Injection, Cross-Site Scripting (XSS) und Cross-Site Request Forgery (CSRF). Sie können benutzerdefinierte Regeln erstellen, um böswillige Anfragen anhand verschiedener Kriterien wie IP-Adressen, Abfragezeichenfolgen und Headern zu blockieren.

AWS Shield

- Arbeitet hauptsächlich auf der Netzwerk- (Schicht 3) und der Transportebene (Schicht 4). Es wurde entwickelt, um Distributed Denial of Service (DDoS) -Angriffe abzuwehren, die darauf abzielen, Netzwerkressourcen zu überlasten, wie z. B. SYN/ACK Überschwemmungen, UDP-Reflection-Angriffe und volumetrische Angriffe. AWS Shield stellt sicher, dass der Netzwerkverkehr, der Ihre AWS Ressourcen erreicht, auch bei Angriffen verfügbar bleibt. AWS

Shield Der Schutz analysiert die Muster des Netzwerkverkehrs und verhindert automatisch identifizierte Bedrohungen am AWS Netzwerkrand.

Deployment

AWS WAF

- Erfordert eine explizite Einrichtung und Konfiguration. Es kann auf mehreren bereitgestellt werden AWS-Services, darunter Amazon CloudFront, Application Load Balancer (ALB), Amazon API Gateway und. AWS AppSync Sie müssen Web-Listen ACLs (Access Control Lists) erstellen und mit Ihren Ressourcen verknüpfen und Regeln definieren, um bestimmte Webanfragen zuzulassen, zu blockieren oder zu überwachen. AWS WAF bietet anpassbare Bereitstellungsoptionen, mit denen Sie Sicherheitsrichtlinien an Ihre spezifischen Anwendungsanforderungen anpassen können.

AWS Shield

- Wird automatisch integriert AWS-Services und ist ständig aktiv, sodass keine zusätzliche Einrichtung für den Basisschutz erforderlich ist. AWS Shield Standard ist automatisch in allen AWS-Konten enthalten und schützt Ressourcen wie Amazon EC2, Elastic Load Balancing (ELB) CloudFront, Amazon und Route 53 Für einen erweiterten Schutz mit AWS Shield Advanced müssen Sie ihn explizit für bestimmte Ressourcen aktivieren. Die Bereitstellung erfolgt nahtlos, und nach dem Einschalten AWS Shield ist keine zusätzliche Konfiguration erforderlich.

Customization

AWS WAF

- Bietet umfangreiche Anpassungsmöglichkeiten. Sie können benutzerdefinierte Webanfragen ACLs (Access Control Lists) mit Regeln erstellen, die bestimmte Bedingungen für das Zulassen, Blockieren oder Zählen von Webanfragen auf der Grundlage von IP-Adressen, HTTP-Headern, Abfragezeichenfolgenparametern und mehr definieren. AWS WAF unterstützt verwaltete Regelgruppen von Drittanbietern AWS oder Drittanbietern, die weiter an Ihre spezifischen Anwendungsanforderungen angepasst werden können. Sie können auch ratenbasierte Regeln einrichten, um die Anzahl der Anfragen von einer einzelnen IP-Adresse zu begrenzen, und

diese AWS Lambda für eine erweiterte Prüfung und Beantwortung von Anfragen integrieren AWS WAF .

AWS Shield

- Bietet begrenzte Anpassungsmöglichkeiten. Bei AWS Shield Standard erfolgt der Schutz automatisch und ist nicht konfigurierbar. AWS Shield Advanced ermöglicht einige Anpassungen, z. B. die Aktivierung erweiterter Metriken und Benachrichtigungen, die Einrichtung von Health Checks und den Zugriff auf das AWS DDo S Response Team (DRT) für maßgeschneiderte Unterstützung bei der Schadensbegrenzung. Der Schwerpunkt liegt jedoch weiterhin auf automatisiertem DDo S-Schutz und nicht auf benutzerdefinierten Einstellungen. Sie können Ressourcen eine AWS WAF Web-ACL zuordnen, um den Schutz auf Anwendungsebene zu aktivieren.

Managed rules

AWS WAF

- Bietet eine Reihe verwalteter Regeln, die auf Webanwendungen angewendet werden können, um sie vor gängigen Internet-Bedrohungen zu schützen. Diese verwalteten Regeln sind von Sicherheitsanbietern AWS oder Drittanbietern vorkonfiguriert und decken verschiedene Sicherheitsszenarien ab, z. B. SQL-Injection, Cross-Site Scripting (XSS) und bekannte schädliche IP-Adressen. Sie können diese verwalteten Regelgruppen abonnieren und auf Ihre Website anwenden. Sie bieten out-of-the-box Schutz ACLs, der regelmäßig aktualisiert wird, um neuen Sicherheitslücken und Bedrohungen zu begegnen. Verwaltete Regeln können individuell angepasst und mit benutzerdefinierten Regeln kombiniert werden, um Sicherheitsrichtlinien an spezifische Anwendungsanforderungen anzupassen. AWS WAF bietet außerdem verwaltete intelligente Funktionen zur Bedrohungsabwehr. Dabei handelt es sich um fortschrittliche, spezialisierte Schutzmaßnahmen, die Sie implementieren können, um sich vor Bedrohungen wie böswilligen Bots und Kontoübernahmeversuchen zu schützen.

AWS Shield

- Sie konzentrieren sich in erster Linie auf DDo S-Schutz und bieten keine herkömmlichen verwalteten Regeln. AWS Shield Standard wendet automatisch eine Reihe vordefinierter Schutzmaßnahmen gegen gängige Netzwerk- und DDo Transport-Layer-S-Angriffe an. AWS Shield Advanced verbessert diese Schutzmaßnahmen, bietet jedoch keine anpassbaren

verwalteten Regeln. Stattdessen bietet es fortschrittlichere Techniken zur Risikominderung und Zugang zum DDo S Response Team, das maßgeschneiderte Unterstützung bietet.

Pricing model

AWS WAF

- Verwendet ein pay-as-you-go Preismodell. Die Gebühren richten sich nach der Anzahl der von ACLs Ihnen erstellten Websites, der Anzahl der Regeln, die Sie in jeder ACL bereitstellen, und der Anzahl der Webanfragen, die nach den Regeln verarbeitet werden. Dieses Modell ermöglicht skalierbare Kosten auf der Grundlage der tatsächlichen Nutzung, sodass Sie nur für die Ressourcen zahlen, die Sie benötigen. Für verwaltete Regelgruppen, die von Drittanbietern AWS oder Drittanbietern bereitgestellt werden, fallen zusätzliche Gebühren an. AWS WAF bietet auch verwaltete Regeln für die Bot-Kontrolle und die Betrugsbekämpfung mit einem ähnlichen Preismodell pro Anfrage. AWS WAF bietet auch eine captcha/challenge Funktion, die nach der Anzahl der abgegebenen Captcha-Versuche und der abgegebenen Challenge-Antworten berechnet wird.

AWS Shield

- Hat ein gestaffeltes Preismodell. AWS Shield Standard ist ohne zusätzliche Kosten in allen Produkten enthalten AWS-Konten und bietet grundlegenden DDo S-Schutz. AWS Shield Für Advanced fallen eine Gebühr auf der Grundlage eines monatlichen Abonnements sowie zusätzliche Gebühren für Datenübertragung und Datenminimierung ab einem bestimmten Schwellenwert an. Dieses Abonnement beinhaltet den Zugriff auf das AWS DDo S Response Team (DRT) rund um die Uhr, erweiterte Angriffsdiagnosen und Kostenschutz bei Angriffen.

Attack response team

AWS WAF

- Im Service ist kein eigenes Team für die Reaktion auf Angriffe enthalten. Stattdessen bietet es Tools und Funktionen, mit denen Sie Sicherheitsregeln selbst erstellen, verwalten und anpassen können. Sie können den Datenverkehr überwachen und ACLs je nach Bedrohungslage in Echtzeit Änderungen an Ihrer Website vornehmen. Sie haben jedoch keinen direkten Zugang zu einem spezialisierten Support-Team für die Abwehr von Angriffen.

AWS Shield

- Bietet im Rahmen seines AWS Shield Advanced-Service Zugriff auf das AWS DDo S Response Team (DRT). Das DRT ist ein rund um die Uhr besetztes Expertenteam, das Sie bei der Abwehr und Reaktion auf Angriffe in Echtzeit unterstützt. Im Falle eines DDo S-Angriffs können Sie sich an das DRT wenden, um maßgeschneiderte Beratung und Unterstützung zu erhalten, um die Bedrohung effektiv zu bewältigen und zu mindern. Dazu gehören Anleitungen zu bewährten Verfahren, Vorfallanalysen und koordinierte Maßnahmen zur Minimierung der Auswirkungen auf Ihre AWS Ressourcen.

Real-time monitoring

AWS WAF

- Bietet Echtzeitüberwachung durch Integration mit AWS CloudWatch, sodass Sie Kennzahlen wie blockierte oder zugelassene Anfragen, Anforderungsraten und die Wirksamkeit bestimmter Regeln verfolgen können. AWS WAF bietet nahezu in Echtzeit Einblick in Web-Traffic und Sicherheitsereignisse im AWS-Managementkonsole OP APIs. Sie können benutzerdefinierte CloudWatch Alarme auf der Grundlage Ihrer AWS WAF Messwerte einrichten, um schnell auf potenzielle Bedrohungen oder ungewöhnliche Verkehrsmuster zu reagieren.

AWS Shield

- Bietet Echtzeitüberwachung hauptsächlich über AWS Shield Advanced. Es lässt sich integrieren AWS CloudWatch , um Metriken und Warnmeldungen im Zusammenhang mit DDo S-Angriffen nahezu in Echtzeit bereitzustellen. Sie können die Angriffsdiagnose, die Verkehrsmuster und die Wirksamkeit von Abhilfemaßnahmen überwachen. AWS Shield Advanced bietet außerdem detaillierte Berichte und Einblicke in Angriffsvektoren und skaliert automatisch als Reaktion auf Bedrohungen und bietet so Einblicke in die AWS-Managementkonsole

Beide Dienste bieten Dashboards zur Visualisierung von Angriffsmustern und Verkehrstrends. AWS Shield Die Überwachung konzentriert sich auf Anomalien auf Netzwerkebene und volumetrische Angriffe und AWS WAF bietet gleichzeitig tiefere Einblicke in Anfragen auf Anwendungsebene und die Effektivität von Regeln.

Traffic inspection

AWS WAF

- Untersucht den Datenverkehr auf der Anwendungsebene (Schicht 7) und analysiert den Inhalt der Anfragen. HTTP/S Es bewertet den Web-Traffic anhand benutzerdefinierter Regeln und sucht nach spezifischen Angriffsmustern wie SQL-Injection, Cross-Site Scripting (XSS) oder anderen schädlichen Payloads im Anfragetext, in den Headern oder in den URL-Parametern.

AWS Shield

- Konzentriert sich auf den Schutz vor DDo S-Angriffen und untersucht in erster Linie den Datenverkehr auf der Netzwerk- (Schicht 3) und der Transportebene (Schicht 4). Es untersucht nicht den Inhalt des Datenverkehrs auf Anwendungsebene (HTTP/S), sondern sucht nach Mustern, die für DDo S-Angriffe typisch sind, wie z. B. ungewöhnlich hohes Datenverkehrsvolumen oder Protokollmissbrauch. AWS Shield entschärft diese Bedrohungen automatisch ohne benutzerdefinierte Regeln oder inhaltsbasierte Inspektionen und stellt so die Verfügbarkeit von Angriffen sicher. AWS-Services

Verwenden Sie

AWS WAF

- Was ist? AWS WAF

  Erfahren Sie, wie AWS WAF Sie Ihre Webanwendungen überwachen und vor gängigen Web-Exploits schützen können.

  Erkunden Sie den Leitfaden

- Analysieren von AWS WAF Protokollen in Amazon CloudWatch Logs

  Richten Sie die native AWS WAF Protokollierung in CloudWatch Amazon-Protokollen ein und visualisieren und analysieren Sie die Daten in den Protokollen.

  Lesen Sie den Blog

- Visualisieren Sie AWS WAF Logs mit einem CloudWatch Amazon-Dashboard

  Verwenden Sie Amazon CloudWatch , um AWS WAF Aktivitäten mithilfe von CloudWatch Metriken, Contributor Insights und Logs Insights zu überwachen und zu analysieren.

Lesen Sie den Blog

AWS Shield

- Was ist AWS Shield?

  Erfahren Sie, wie AWS Shield Sie Ihre Webanwendungen vor gängigen DDo S-Angriffen auf Netzwerk- und Transportebene schützen können.

  Erkunden Sie den Leitfaden

- Erste Schritte mit AWS Shield Advanced

  Beginnen Sie mit AWS Shield Advanced, indem Sie die AWS Shield Advanced-Konsole verwenden.

  Erkunden Sie den Leitfaden

- AWS Shield Workshop für Fortgeschrittene

  Schützen Sie im Internet exponierte Ressourcen vor DDo S-Angriffen, überwachen Sie DDo S-Angriffe auf Ihre Infrastruktur und benachrichtigen Sie die entsprechenden Teams.

  Erkunden Sie den Workshop

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	Der Leitfaden wurde zuerst veröffentlicht.	17. September 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.