fastly

Powered by Signal Sciences

PRODUKTDATENBLATT

Fastly Next-Gen WAF

Übersicht: Architektur und Bereitstellung

Integrierte Web-App- und API-Sicherheit für jede Umgebung

Fastly bietet die WAF mit den flexibelsten Bereitstellungsoptionen auf dem Markt und kann Ihre Anwendungen und APIs mit einer einzigen integrierten Lösung schützen, wo auch immer sie sich befinden – in Containern, auf Ihren eigenen Servern, in der Cloud oder auf der Edge. Profitieren Sie von einem umfassenden Schutz, ohne Abstriche bei der Performance machen zu müssen oder spezielles Personal zu benötigen: Fastlys Next-Gen WAF (powered by Signal Sciences) ist sofort einsatzbereit und so effektiv, dass 90 % unserer Kunden sie komplett im Blocking Mode betreiben.

Die Next-Gen WAF von Fastly bietet den proaktiven Schutz, den moderne Anwendungen brauchen, und lässt sich gleichzeitig in Ihre DevOps- und Security-Toolchains integrieren, wo sie Ihnen beispiellose Transparenz bietet. Unsere flexible Architektur kann Ihre Anwendungssicherheitsstrategie voranbringen, indem sie Dev-, Sec- und Ops-Teams Einblicke liefert, wo und wie Ihre Webanwendungen und APIs angegriffen werden.

Dieses Datenblatt bietet detaillierte Informationen über die hochperformante, patentierte Architektur der Fastly Next-Gen WAF sowie über die breite Palette an verfügbaren Bereitstellungsoptionen. Dieses Dokument ist in folgende Abschnitte gegliedert:

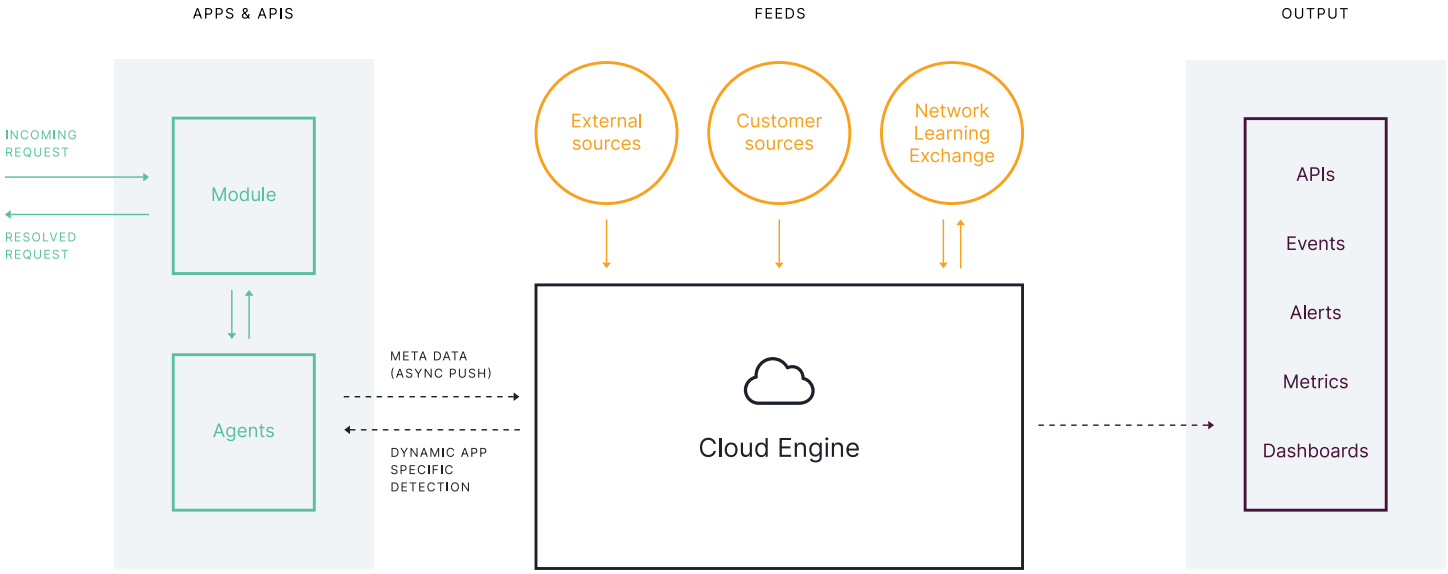
- **Architekturübersicht**
- **Bereitstellungsoptionen**
- **Integrationen in DevOps- und Security-Toolchains**

Gartner Peer Insights Customers' Choice 2022

Signal Sciences (jetzt Teil von Fastly) ist der einzige Anbieter, der vier Jahre in Folge mit dem Gartner Peer Insights Customers' Choice for Web Application and API Protection (WAAP) ausgezeichnet wurde, und eine der **am besten bewerteten** WAAP-Lösungen auf dem Markt mit einer Gesamtbewertung von **4.9/5** (Stand 31. Januar 2022[1], basierend auf 267 Bewertungen).

1: Die Inhalte von Gartner Peer Insights spiegeln die Meinungen einzelner Endnutzer wider, die auf ihren eigenen Erfahrungen mit den auf der Plattform aufgeführten Anbietern beruhen. Sie sind nicht als Tatsachenbehauptungen zu verstehen und stellen auch nicht die Ansichten von Gartner oder verbundenen Unternehmen dar. Gartner unterstützt keine Anbieter, Produkte oder Services, die in diesen Inhalten vorgestellt werden, und lehnt jede ausdrückliche oder stillschweigende Gewährleistung in Bezug auf diese Inhalte, ihre Richtigkeit oder ihre Vollständigkeit ab, einschließlich jeglicher Gewährleistung der Marktgängigkeit oder Eignung für einen bestimmten Zweck. Das Logo von GARTNER PEER INSIGHTS ist ein Markenzeichen und eine Servicemarke von Gartner, Inc. bzw. ihren Tochtergesellschaften und wird hier mit ausdrücklicher Genehmigung verwendet. Alle Rechte vorbehalten.

Architekturübersicht



Die Fastly Next-Gen WAF ist eine hybride Software-as-a-Service (SaaS)-Lösung, die im Wesentlichen aus drei Komponenten besteht.
Dieser von Signal Sciences entwickelte, patentierte Ansatz ermöglicht es uns, unsere Lösung einfach zu skalieren und selbst umfangreichste Anwendungen und APIs zu schützen, ohne dabei die Performance zu beeinträchtigen.

Agents

Leichtgewichtige Agents, die Sie über Ihre bestehende Infrastruktur bereitstellen, um Anfragen schnell und präzise zu analysieren und gegebenenfalls abzulehnen.

Modules

Optionale aber leistungsstarke Komponente, die zusammen mit unseren Agents für hohe Performance und Zuverlässigkeit sorgt.

Cloud Engine

In der Cloud gehostetes Analyse-Backend, das den Agent asynchron mit Informationen aus externen und eigenen Quellen anreichert, um dynamische, anwendungsspezifische Detections durchzuführen.

Agents

Agents bestehen aus einem kleinen Daemon-Prozess und sind darauf ausgelegt, extrem hohe Lasten zu bewältigen und gleichzeitig auf lokaler Ebene leistungsstarke, exakte Erkennungen durchzuführen und Entscheidungen zu treffen. Der Agent sammelt auch Metadaten zu den von ihm verarbeiteten böswilligen Anfragen und gibt sie an die Cloud Engine weiter. Wir schützen einige der am stärksten frequentierten Websites im Internet, wo Zehntausende von Agents gemeinsam Billionen von Produktionsanfragen verarbeiten, ohne die Performance von Apps oder APIs zu beeinträchtigen. Agents blockieren Angriffe, bevor sie auf Anwendungen oder APIs treffen, und bieten nicht nur Einblick in eingehende Anfragen, sondern auch in Serverantworten und Anomalien, die zeigen, wie sich die Anwendung verhält.

Modules

Module laufen auf fast allen Webservern (NGINX, Apache, IIS und weiteren) und in fast allen Anwendungssprachen (.NET, Java, Python, PHP, .nodeJS und weiteren). Um Zuverlässigkeit und außerordentliche Performance zu gewährleisten, besteht das Module nur aus einigen hundert Codezeilen. Seine einzige Aufgabe ist es, Anfragen an den Agent weiterzuleiten und Entscheidungen vom Agent zu empfangen und durchzusetzen, die Anfrage an die Anwendung weiterzuleiten oder sie zu loggen/blockieren (je nachdem, welcher Modus in der Konsole festgelegt ist).

Cloud Engine

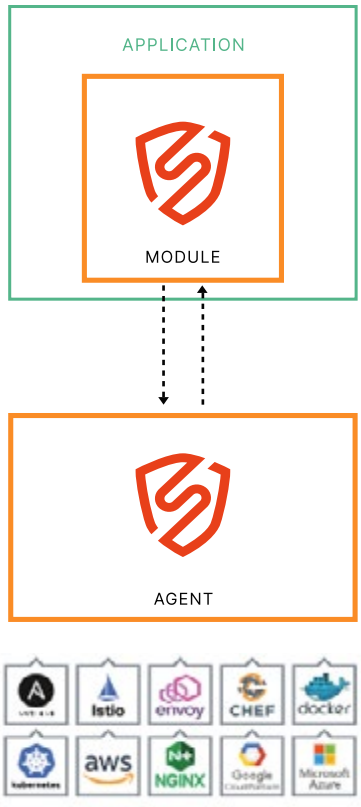
Die Cloud Engine sammelt und analysiert anonymisierte Angriffs- und Telemetriedaten von den vielen tausend Software-Agents unserer Kunden. Der Output der Cloud Engine wird von den lokalen Agents genutzt, um die Erkennung zu verbessern und aggressivere Blockierungsentscheidungen zu treffen. Die Entscheidungsfähigkeit der Agents wird durch unseren Network Learning Exchange (NLX) verbessert, der bestätigte bösartige IP-Quellen innerhalb der Managementkonsole weitergibt. So werden Sie vor verdächtigen Akteuren gewarnt, bevor diese eine Bedrohung für Ihre Anwendungen und APIs darstellen können. Zu den weiteren Feeds gehören zum Beispiel externe Listen bösartiger IPs und kundenspezifische IP-Listen, die allesamt zusätzlichen Anfragekontext liefern, der zur Entscheidungsfindung der Agents beiträgt. Diese Transparenz und dieser Kontext werden über unsere API und native Integrationen mit DevOps-Tools geteilt, die Ihr Team bereits verwendet, darunter Slack, PagerDuty, Jira und weitere, sowie Sicherheitstools wie Splunk, Elastic und Palo Alto Networks Cortex XSOAR. Metriken und Ereignisberichte für Ihren gesamten Anwendungs-Footprint sind auch über die Dashboards in unserer einheitlichen Managementkonsole leicht einsehbar.

Bereitstellungsoptionen

Native Bereitstellungsoptionen für Datacenter, Cloud, Container und Serverless-Umgebungen

Bereitstellungsoption 1: Cloud- und containernative Apps

Das Agent-Module-Paar lässt sich innerhalb weniger Minuten auf Ihrem Webserver, API-Gateway oder auf Anwendungsebene installieren. Unser Agent ist infrastrukturunabhängig, sodass Sie ihn überall dort einsetzen können, wo Sie ihn brauchen, ohne sich Gedanken über Abhängigkeiten von zugrundeliegenden Sprachen oder Frameworks machen zu müssen.



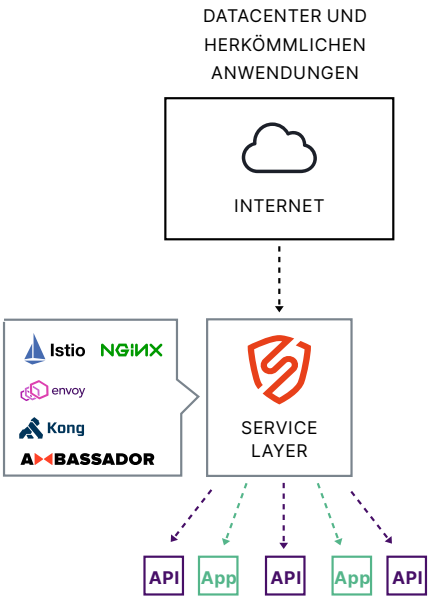
Implementierung in Kubernetes und Service Mesh

Neue Anwendungstools und Frameworks wie Kubernetes helfen Unternehmen beim schnellen Umstieg auf DevOps. Unternehmen veröffentlichen Code heute schneller als je zuvor. Fastly bietet flexible Bereitstellungsoptionen, die zu Ihrer Container-Strategie mit drei „Layers“ passen. Sie können unsere WAF also in Kubernetes installieren und haben dabei vier Bereitstellungsmethoden zur Auswahl. Außerdem sorgen unsere nativen Integrationen mit den Service Meshes von Envoy Proxy und Istio für Transparenz – sowohl bei Nord-Süd- (Client an Server) als auch bei Ost-West-Anfragen (Service an Service).

Installationsmethode	Layer 1: Ingress Controller	Layer 2: Mid-Tier Service	Layer 3: App Tier
Agent + Module im selben App-Container	✓	✓	✓
Agent + Module in verschiedenen Containern	✓	✓	✓
Agent im Reverse-Proxy-Modus im selben Container wie die App	✓	✓	✓
Agent im Reverse-Proxy-Modus im Sidecar-Container	✓	✓	✓

Fastly bietet umfassende Bereitstellungsoptionen für: kubernetes docker envoy Istio

Bereitstellungsoption 2: Datacenter und herkömmliche Anwendungen

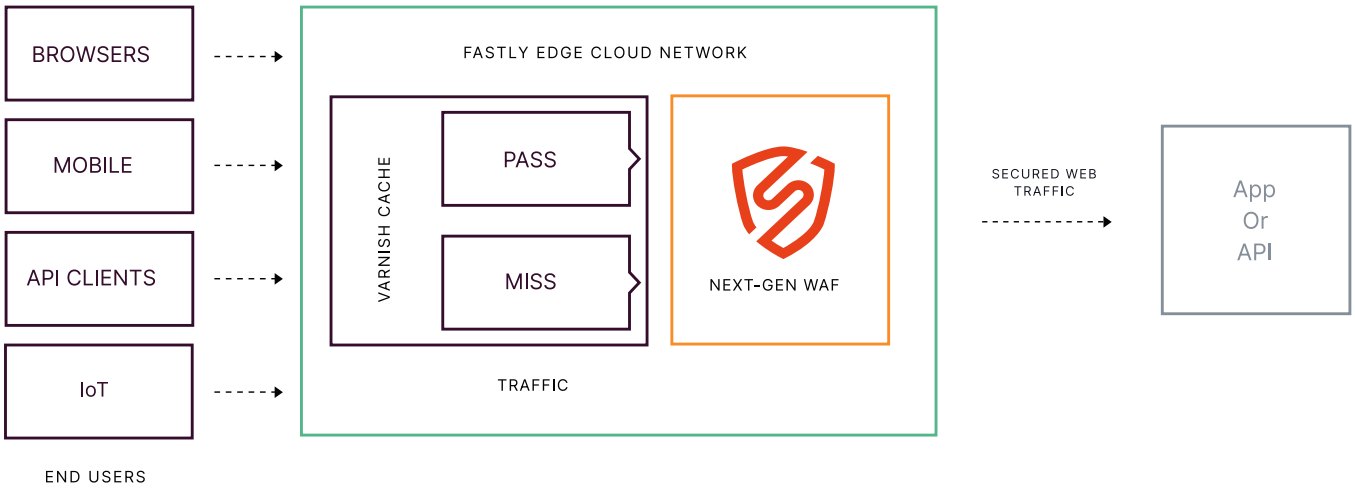


Kunden, die Schutz für herkömmliche oder in einem Datacenter bereitgestellte Anwendungen benötigen, entscheiden sich in der Regel für eine von zwei Bereitstellungsoptionen: Sie installieren Fastlys Next-Gen WAF, um den Traffic zu prüfen, bevor Webanfragen den App- oder API-Endpoint erreichen, oder sie installieren unsere Agents im Reverse-Proxy-Modus. Unser Module lässt sich zum Beispiel am Loadbalancer (HAProxy, NGINX) oder am API-Gateway (Ambassador, Kong, Cloudentity) installieren. Für Kunden, deren Anforderungen eine Installation am Loadbalancer oder API-Gateway nicht zulassen, kann unser Agent im Reverse-Proxy-Modus bereitgestellt werden. Beide Möglichkeiten bieten dasselbe Maß an Transparenz, verwertbaren Erkenntnissen und Warnungen.

Bereitstellungsoption 3: Auf der Edge

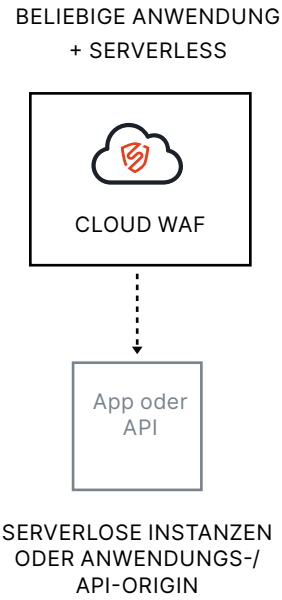
Fastlys Next-Gen WAF ist im Fastly Edge-Cloud-Netzwerk verfügbar und ermöglicht es Ihnen, Sicherheitskontrollen durchzuführen, während Sie Inhalte über Fastly ausliefern. Die Edge-Cloud-Bereitstellungsoption ist nahtlos in „Varnish“, den Caching Layer von Fastly, integriert.

Dies sorgt für Schutz und Beschleunigung in unmittelbarer Nähe der Nutzer durch Abschirmung der Origin-Systeme vor missbräuchlichen Angriffen bei gleichzeitiger erstklassiger Performance. Unsere Edge-Bereitstellung ist ideal für Kunden, die keine Software auf der bestehenden Infrastruktur installieren können und die Performancevorteile des globalen Content Delivery Networks (CDN) von Fastly nutzen möchten. Außerdem bietet diese Bereitstellungsoption zusätzliche Funktionen, einschließlich „always-on“ DDoS-Schutz für Layer 3 und 4 und TLS-Management.



Bereitstellungsoption 4: Cloud WAF

Mit Cloud WAF können Sie Webanwendungen, APIs, Microservices und serverlose Anwendungen schnell und einfach schützen – ohne in Ihrer Infrastruktur Software installieren zu müssen. Nach der Bereitstellung genügt eine einfache DNS-Änderung, um den Anwendungstraffic auf die Cloud WAF zu lenken und die Transparenz und den Schutz von Fastlys Next-Gen WAF für Ihre Anwendungen zu aktivieren. Sämtliche Webanfragen werden an unseren Cloud Enforcement Layer umgeleitet, wenn schädliche Anfragen erkannt und blockiert werden. Legitimer Traffic wird hingegen uneingeschränkt an Ihren Origin-Server weitergeleitet. Cloud WAF ist ideal für Kunden, die eine einfach zu verwaltende WAF hinzufügen möchten, ohne Änderungen an ihrem CDN-Layer vornehmen zu müssen.



Sicherheit + Datenschutz

Viele führende Finanzdienstleister, Unternehmen des Gesundheitswesens und andere Unternehmen mit strengen Datenschutzanforderungen nutzen die Next-Gen WAF von Fastly wegen unserer soliden, datenschutzzentrierten Architektur. Sensible Daten werden ausschließlich innerhalb der Kundenumgebung verarbeitet, und nur bereinigte und redigierte Teile von Anfragen, die als Angriffe oder Anomalien gekennzeichnet sind, werden an die Fastly Cloud Engine weitergeleitet.

Sobald der Agent einen potenziellen Angriff oder eine Anomalie in einer Anfrage erkennt, werden individuell konfigurierbare Anpassungen vorgenommen, und der Agent sendet lediglich den einzelnen, korrigierten Anfrageparameter, der die Angriffs-Payload enthält, sowie einige andere nicht sensible oder gutartige Teile der Anfrage, wie Client-IP, User-Agent, URI usw. Unser Backend sammelt nur die Metadaten der Antwort, z. B. Antwortcodes, Größen und Zeiten. Wir bieten unseren Kunden die Möglichkeit, die Entfernung oder Bearbeitung von Richtlinien und Feldern ganz nach Bedarf anzupassen. Als zusätzlichen Schutz sorgt Fastly automatisch für die Anpassung gängiger sensibler Datentypen wie Passwörter, Schlüssel, GUIDs und aller Arten von personenbezogenen Daten oder geschützten Gesundheitsinformationen, bevor die Anfrage an unser Backend gesendet wird.

Betterment

„Fastlys Next-Gen WAF ist sofort einsatzbereit, lässt sich automatisch skalieren und bietet hervorragende Transparenz und Anwendungssicherheit.“

Anson Gomes
Lead Security Engineer, Betterment

Integration von DevOps- und Security-Toolchains

Der beste Weg zum Erfolg für einen effektiven Anwendungs- und API-Schutz besteht darin, Entwicklungs-, Operations- und Sicherheitsteams dieselben grundlegenden Sicherheitsdaten in den von ihnen bereits verwendeten Tools zur Verfügung zu stellen. Fastly arbeitet mit den besten Tools und Plattformen der Branche zusammen, um Ihre DevOps- und Sec-Toolchains mit Echtzeitwarnungen zu versorgen und sicherzustellen, dass Ihre Teams unsere Sicherheitstelemetrie für die Produktivumgebung innerhalb der aktuellen Tools und Prozesse Ihres Unternehmens für weitere Untersuchungen und Analysen nutzen können.

Ergänzende Out-of-the-Box-Technologien helfen Teams bei der Umstellung oder der Fortsetzung des Umstiegs auf moderne Entwicklungsmodelle und -architekturen. Unsere Ein-Klick-Integrationen umfassen die gängigsten Alarmsysteme für Entwicklung und Operations, Chat-Ops, Projektmanagement und Incident Tracking.

Technologie- und Plattformintegrationen

Plattformintegrationen und -partner

Setzen Sie Fastlys Next-Gen WAF überall ein

WEB SERVERS

IAAS

PAAS

CONTAINERS

CONFIG MANAGEMENT

Feed-Integrationen und -Partner

Senden und Empfangen von Daten von der Fastly Next-Gen WAF

DEVOPS TOOLCHAIN

SOC/SIEM

Erste Schritte

Ermöglichen Sie hochwirksame Security ohne Performance-Einbußen.

Um mehr über unsere Sicherheitslösungen zu erfahren, besuchen Sie unsere Website oder kontaktieren Sie uns unter sales@fastly.com.

Sales kontaktieren