fastly

Powered by Signal Sciences

HOJA DE DATOS DEL PRODUCTO

WAF de última generación de Fastly

Descripción general de la arquitectura y el despliegue

Seguridad unificada para aplicaciones web y API en todo tipo de entornos

Fastly ofrece el firewall de aplicaciones web (WAF) que tiene el despliegue más flexible del mercado. Además, protege tus aplicaciones y API dondequiera que estén alojadas (contenedores, entornos locales, la nube o el edge) con una única solución integrada. Disfruta de una protección exhaustiva sin renunciar al rendimiento ni tener que dedicar personal específico: el WAF de última generación de Fastly (con tecnología de Signal Sciences) funciona sin necesidad de configurarlo y es tan eficaz que el 90 % de nuestros clientes lo ejecutan en modo de bloqueo total.

El WAF de última generación de Fastly ofrece la protección proactiva que necesitan las aplicaciones modernas, al tiempo que se integra en tus herramientas de DevOps y de seguridad para ofrecerte una visibilidad sin igual. Nuestra arquitectura flexible permite reforzar la estrategia de seguridad de tus aplicaciones, ya que muestra a los equipos de desarrollo, operaciones y seguridad dónde y cómo reciben ataques tus aplicaciones web y tus API.

Esta hoja de datos explica la eficaz arquitectura patentada del WAF de última generación de Fastly e incluye información sobre la amplia variedad de opciones de despliegue. Este documento consta de las siguientes secciones:

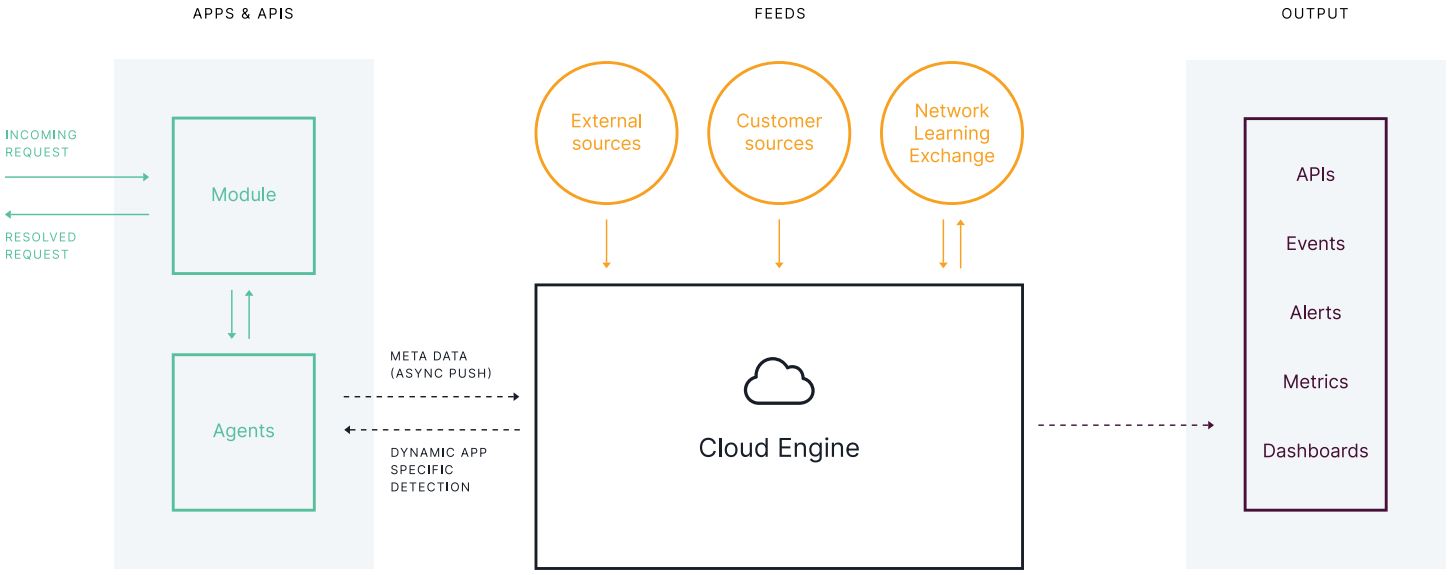
- **Descripción general de la arquitectura**
- **Opciones de despliegue**
- **Integraciones con herramientas de DevOps y de seguridad**

Gartner Peer Insights Customers' Choice 2022

Signal Sciences, que ahora forma parte de Fastly, es el único proveedor en recibir por cuarto año consecutivo el reconocimiento «Customer's Choice» de Gartner Peer Insights en protección de aplicaciones web y API (WAAP). Además, es una de las **soluciones WAAP mejor valoradas del mercado** con una valoración global de **4,9/5** a fecha del 31 de enero de 2022[1], sobre un total de 267 reseñas.

1: El contenido de Gartner Peer Insights se compone de la opinión de determinados usuarios finales que describen sus experiencias con los diferentes proveedores que están disponibles en la plataforma, y no se debe considerar una exposición de hechos, ni representa los puntos de vista de Gartner o de sus empresas vinculadas. Gartner no respalda a proveedores, productos o servicios descritos en este contenido, ni tampoco ofrece garantías, ya sean explícitas o implícitas, en relación con este, en lo que respecta a su precisión o su exhaustividad, ni siquiera garantías de comerciabilidad o idoneidad para una finalidad en particular. El logotipo de GARTNER PEER INSIGHTS es una marca comercial y una marca de servicio de Gartner, Inc. o sus empresas vinculadas y se utiliza aquí previa autorización. Reservados todos los derechos.

Descripción general de la arquitectura



El WAF de última generación de Fastly es una solución híbrida de software como servicio (SaaS) que tiene tres componentes principales. Este planteamiento patentado, obra de Signal Sciences, nos permite escalar sin complicaciones y dar protección incluso a las aplicaciones y API que mayor volumen de tráfico registran, sin que se vea afectado el rendimiento.

Agentes

Agentes ligeros que despliegas en tu infraestructura para realizar la detección y toma de decisiones con respecto a las peticiones con rapidez y precisión.

Módulos

Potente componente opcional que se sincroniza con nuestros agentes para garantizar altos niveles de rendimiento y fiabilidad.

Motor en la nube

Backend de análisis alojado en la nube que utiliza protocolos asimétricos para transmitir al agente datos recabados de fuentes externas y fuentes exclusivas, y con ello poder realizar detecciones dinámicas específicas de cada aplicación.

Agentes

Los agentes son procesos tipo daemon de pequeño tamaño diseñados para gestionar cargas extremadamente pesadas. Al mismo tiempo y en el ámbito local, realizan detecciones y toman decisiones que conllevan un alto grado de rendimiento y precisión. El agente recopila además metadatos sobre las peticiones maliciosas que ha procesado y los comparte con el motor en la nube. Protegemos varios de los sitios web que gestionan el mayor volumen de datos de toda la red mediante decenas de miles de agentes que procesan de manera colectiva billones de peticiones de producción. Los agentes bloquean los ataques antes de que puedan perjudicar al rendimiento de aplicaciones o API. Además, muestran no solo las peticiones entrantes, sino también las respuestas de los servidores y aquellas anomalías que sean indicativas del comportamiento de la aplicación.

Módulos

Los módulos se ejecutan prácticamente en cualquier servidor web (NGINX, Apache, IIS, etc.) y en cualquier lenguaje de aplicaciones (.NET, Java, Python, PHP, .nodeJS, etc.). El módulo ocupa solo unos pocos cientos de líneas de código para garantizar la fiabilidad y un grado extremo de rendimiento. Su cometido es doble: transmitir las peticiones al agente; y recibir y aplicar las decisiones del agente, ya sea para permitir que la petición llegue a la aplicación, se incorpore en el registro o se bloquee (en función del modo que se haya definido en la consola).

Motor en la nube

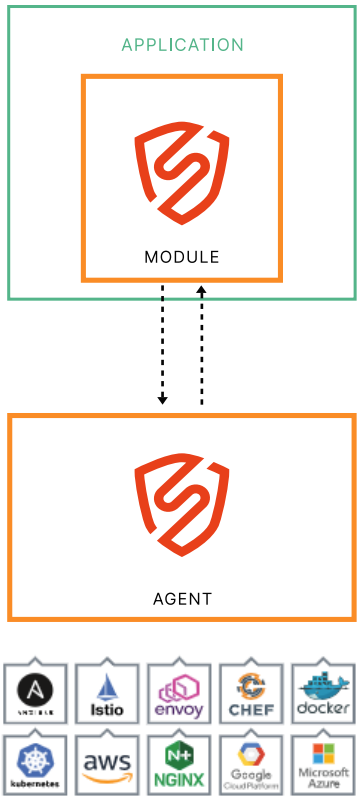
Este motor recopila y analiza telemetría y datos de ataques anonimizados procedentes de los miles de agentes de software distribuidos por toda nuestra base de clientes. El agente utiliza localmente la salida del motor en la nube para afinar las detecciones y tomar decisiones de bloqueo más agresivas. La toma de decisiones por parte del agente cuenta con el respaldo de nuestra tecnología Network Learning Exchange (NLX). Este punto de intercambio comparte en la consola de administración las fuentes de IP maliciosas que se hayan confirmado, lo que te alerta de la presencia de actores sospechosos antes de que se conviertan en una amenaza real para tus aplicaciones y API. Otras fuentes de datos posibles son las listas externas de IP maliciosas y las listas de IP personalizadas por los clientes. Toda esta información ofrece un contexto complementario para las peticiones, lo que, a su vez, suplementa la toma de decisiones que realizan los agentes. Nuestras integraciones nativas y con API comparten esta visibilidad y este contexto con las herramientas de DevOps que utilice tu equipo humano, como Slack, PagerDuty, Jira y otras, además de con herramientas de seguridad, como Splunk, Elastic y Palo Alto Networks Cortex XSOAR. Los paneles de la consola de administración unificada ponen a tu disposición métricas e informes de eventos correspondientes a todo el ecosistema de tus aplicaciones.

Opciones de despliegue

Opciones de despliegue nativo para centros de datos, la nube, contenedores y entornos sin servidores

Opción de despliegue n.º 1: nativa de la nube y de contenedores

El par agente-módulo se instala en tu servidor web, en la puerta de enlace de la API o en la propia aplicación, en cuestión de minutos. Nuestro agente admite diferentes infraestructuras, lo que pone en tus manos la flexibilidad de desplegarlo allí donde lo necesites sin tener que preocuparte de dependencias de marcos de trabajo o lenguajes subyacentes.



Despliegue con Kubernetes y mallas de servicios

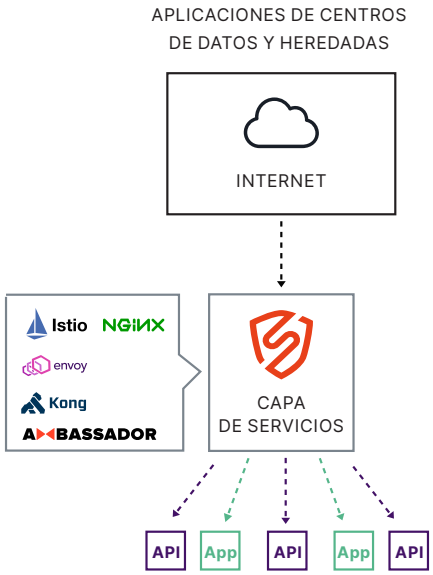
La aparición de nuevos marcos de trabajo y herramientas de aplicaciones, como Kubernetes, obliga a las empresas a prestar cada vez más atención a DevOps. Puesto que las empresas tardan cada vez menos tiempo en publicar código, Fastly ofrece opciones de despliegue flexibles que se adaptan a tu estrategia de contenedores. Para ello, ofrece tres «capas», donde puedes instalar nuestro WAF con Kubernetes, y cuatro métodos de despliegue. Además, gracias a nuestras integraciones nativas con las mallas de servicios Envoy Proxy e Istio, Fastly proporciona visibilidad de las peticiones norte-sur (cliente-servidor) y de las este-oeste (de servicio a servicio).

Método de instalación	Capa 1: controlador de acceso	Capa 2: servicio de nivel intermedio	Capa 3: nivel de aplicaciones
Agente + módulo en el mismo contenedor de aplicaciones	✓	✓	✓
Agente + módulo en contenedores diferentes	✓	✓	✓
Agente en modo de proxy inverso en el mismo contenedor que la aplicación	✓	✓	✓
Agente en modo de proxy inverso en contenedor sidecar	✓	✓	✓

Fastly admite despliegues para: kubernetes docker envoy Istio

Opción de despliegue n.º 2: aplicaciones de centros de datos y heredadas

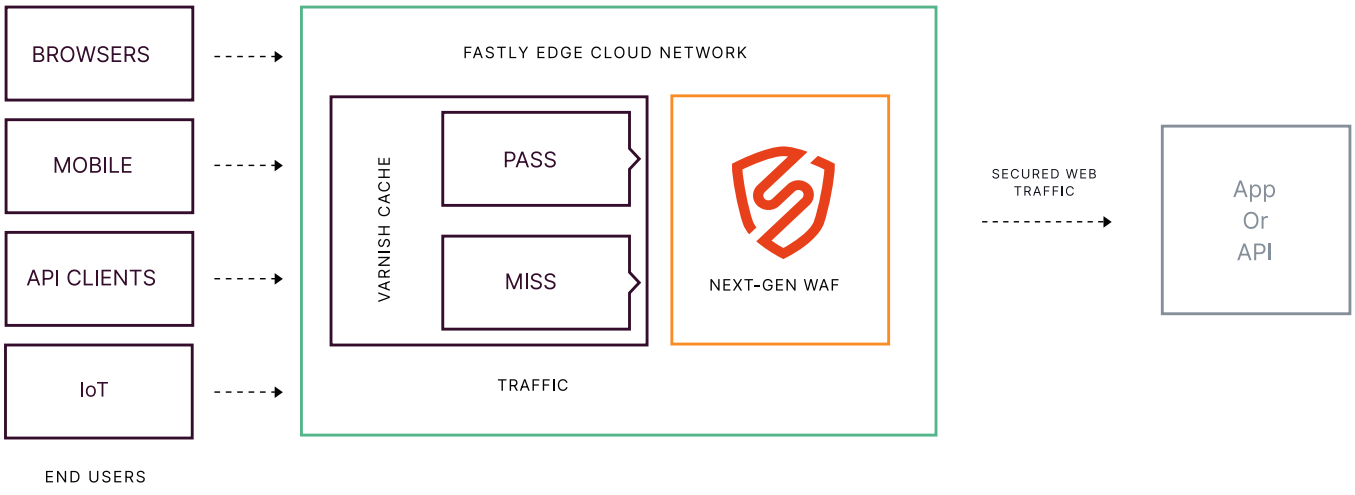
Los clientes que necesitan proteger aplicaciones heredadas o desplegadas en centros de datos suelen elegir entre dos opciones de despliegue: instalar el WAF de última generación de Fastly para que inspeccione el tráfico antes de que las peticiones web lleguen al punto de conexión de la aplicación o de la API, o bien instalar nuestro agente en modo de proxy inverso. Por ejemplo, nuestro módulo se puede instalar en el equilibrador de carga (HAProxy, NGINX) o en la puerta de enlace de la API (Ambassador, Kong, Cloudentity). Si los requisitos que manejan nuestros clientes impiden realizar instalaciones en el equilibrador de carga o en la puerta de enlace de la API, nuestro agente puede desplegarse en modo de proxy inverso. Ambas opciones de despliegue ofrecen el mismo grado de visibilidad, alertas y datos prácticos que el resto de nuestras opciones de despliegue y mantienen la paridad de funciones.



Opción de despliegue n.º 3: en el edge

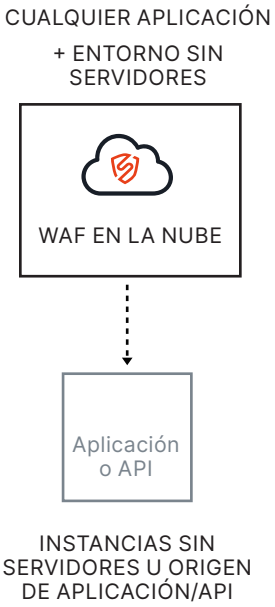
El WAF de última generación de Fastly está disponible en la red edge cloud de Fastly, lo que permite a los clientes implementar controles de seguridad dentro de los servicios de distribución de Fastly. La opción de despliegue en edge cloud se integra a la perfección con Varnish, la capa de almacenamiento en caché de Fastly.

De este modo, la protección y la aceleración se acercan más a los usuarios; los sistemas de los orígenes quedan protegidos frente al tráfico ilegítimo de los ataques; y, al mismo tiempo, se ofrecen unas prestaciones extraordinarias. Nuestro despliegue en el edge es ideal para los clientes que no pueden instalar software en su infraestructura y para los que quieren aprovechar las ventajas de rendimiento que aporta la red mundial de distribución de contenidos (CDN) de Fastly. Esta opción de despliegue ofrece otras opciones, como el servicio constante de protección frente a DDoS y gestión de TLS en las capas 3 y 4.



Opción de despliegue n.º 4: WAF en la nube

El WAF en la nube te permite proteger de manera rápida y sencilla aplicaciones web, API, microservicios y aplicaciones sin servidores, sin necesidad de instalar software en tu infraestructura. Una vez desplegado, solo tendrás que cambiar el DNS para que dirija el tráfico de las aplicaciones al WAF en la nube. Así, tus aplicaciones disfrutarán de la visibilidad y la protección que ofrece el WAF de última generación de Fastly. Todas las peticiones web se redirigen a nuestra capa de implementación en la nube, donde se detecta y se bloquea cualquier petición ilegítima. Al mismo tiempo, todo el tráfico legítimo se reenvía al servidor de origen de tus aplicaciones. El WAF en la nube es ideal para clientes que quieran añadir un firewall de aplicaciones web que sea fácil de gestionar y sin realizar cambios en sentido ascendente hasta la capa de su CDN.



Protección enfocada a la privacidad de los datos

Muchas empresas líderes en servicios financieros, atención sanitaria y otros sectores cuyas exigencias en materia de privacidad de los datos son rigurosas utilizan el WAF de última generación de Fastly, porque nuestra arquitectura es sólida y está diseñada pensando en la protección de datos. Todos los datos confidenciales se gestionan únicamente dentro del entorno del cliente. Además, al motor en la nube de Fastly se remiten únicamente fragmentos de las peticiones que el sistema marca como ataques o anomalías, y solo una vez que se hayan censurado u anonimizado.

En cuanto el agente identifica que una petición contiene un posible ataque o una anomalía, los datos confidenciales se censuran o anonimizan conforme a un conjunto de reglas plenamente personalizables. A continuación, el agente remite únicamente el parámetro censurado de la petición en cuestión que contiene la carga útil del ataque, además de otros fragmentos de la petición que son benignos o no confidenciales, como la IP del cliente, el agente de usuario, el URI, etc. En nuestro backend se recopilan únicamente metadatos de la respuesta, como códigos, tamaños y datos temporales de esta. Los clientes disponen de la capacidad de personalizar completamente las políticas y los campos de censura/anonimización de datos confidenciales. A fin de reforzar la protección, Fastly aplica la censura o anonimización automáticas de determinados tipos de datos que suelen ser confidenciales (p. ej., contraseñas, claves, GUID, datos personales o información sanitaria de carácter personal) antes de remitir la petición a nuestro backend.

Betterment

«Funciona sin necesidad de cambiar ningún ajuste, se adapta automáticamente al tamaño del sistema y nos ofrece una visibilidad estupenda, además de aportar seguridad a la aplicación».

Anson Gomes
Lead Security Engineer, Betterment

Integraciones con herramientas de DevOps y de seguridad

La mejor manera de aplicar una protección eficaz a aplicaciones y API es ofrecer el mismo conjunto de datos de seguridad a los equipos de desarrollo, operaciones y seguridad en las herramientas que ya utilizan. Fastly trabaja con las mejores herramientas y plataformas del sector con dos objetivos: ofrecerte alertas en tiempo real en las herramientas de DevOps y de seguridad que utilices; y facilitar a tus equipos el uso de nuestra telemetría de seguridad de producción con las herramientas y los procesos que tu entidad ya utiliza para profundizar en investigaciones y análisis.

Las integraciones no requieren hacer ningún tipo de ajuste, de manera que los equipos pueden poner en marcha o continuar la transición a modelos y arquitecturas de desarrollo modernos. Nuestras integraciones se llevan a cabo con un solo clic e incluyen los motores de alertas, aplicaciones de chat, sistemas de gestión de proyectos y sistemas de seguimiento de incidencias que suelen usarse en los campos del desarrollo y las operaciones.

Integraciones de plataformas y tecnologías

Integraciones de plataformas y partners

Ejecuta el WAF de última generación de Fastly donde quieras

WEB SERVERS

- NGINX
- Microsoft IIS
- Apache
- Apache Tomcat

IAAS

- Google Cloud
- Microsoft Azure
- aws

PAAS

- Microsoft Azure
- HEROKU
- Red Hat
- IBM Cloud
- VMware Tanzu

CONTAINERS

- kubernetes
- docker
- OPENSHIFT
- Istio
- envoy
- MESOS

CONFIG MANAGEMENT

- CHEF Progress
- Red Hat Ansible
- puppet
- SALTSTACK
- Terraform

Integraciones con fuentes de datos y partners

Intercambia datos del WAF de última generación de Fastly

DEVOPS TOOLCHAIN

- Jira Software
- DATADOG
- PivotalTracker
- VictorOps
- slack
- PagerDuty
- Opsgenie
- Microsoft Teams

SOC/SIEM

- splunk>
- elastic
- ELK Stack
- Radar
- sumo logic
- McAfee
- NETWITNESS
- ArcSight
- LogRhythm
- CISCO
- CORTEX XSOAR

Cómo empezar

Despliega un sistema de seguridad muy eficaz sin sacrificar el rendimiento.

Si quieres más información sobre nuestras soluciones de seguridad, echa un vistazo a nuestro sitio web o escríbenos a la dirección contacto@fastly.com.