CLOUDFLARE®

Protección de aplicaciones en la nube

Defensa en capas rápida, fácil de implementar y escalable ante DDoS, filtración de datos y bots maliciosos

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Protección de aplicaciones en la nube

Defensa en capas rápida y fácil de implementar para proteger ante DDoS, filtraciones de datos y bots maliciosos
Las empresas se enfrentan a presiones cada vez mayores para fortalecer su nivel de seguridad. Tres factores que contribuyen a esta presión son:

- Los atacantes son más fuertes, más sofisticados, y están mucho más motivados;
- La superficie de ataque crece debido a una mayor exposición de API públicas por parte de las aplicaciones, el incremento en la adopción de SaaS y el aumento de integraciones con aplicaciones de terceros;
- La intensificación del escrutinio público y gubernamental en materia de datos, privacidad y seguridad.

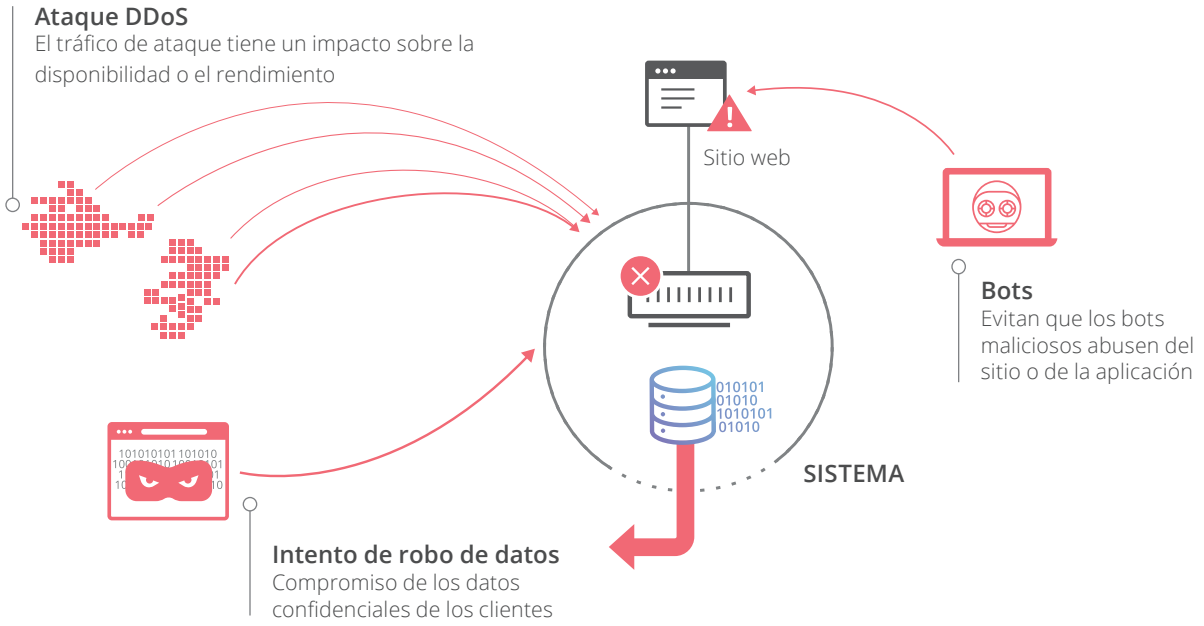
Los atacantes están aumentando la frecuencia y el volumen de ataques por denegación de servicio distribuido (DDoS). Aprovechan las redes de bots (botnets) y los millones de dispositivos de internet de las cosas (IoT) en línea, por lo que pueden cometer ataques volumétricos altamente distribuidos con más facilidad y mayor repercusión.

Además de enviar volúmenes más altos, los atacantes están empezando a centrarse más en la capa de aplicación que en la capa de red. Los ataques de capa de aplicación o «capa 7» son más difíciles de detectar, suelen necesitar menos recursos para causar la caída de un sitio web o aplicación e interrumpir las operaciones.

Los atacantes pueden monetizar sus intentos de provocar la caída de un sitio o robar datos confidenciales, por ejemplo, secuestrando sitios web a cambio de un rescate. Como resultado, y debido a las sumas pagadas como rescate por parte de las empresas objetivo, los atacantes están más motivados, organizados y presentes.

Con una mayor exposición, las empresas tienen que fortalecer sus defensas ante tres problemas y riesgos principales:

- Un ataque DDoS contra las aplicaciones, los sitios web y las API, que perjudica la disponibilidad o el rendimiento y provoca una disminución de los ingresos, costes operativos más altos y la degradación de la marca;
- Filtración de los datos confidenciales de la empresa y de los clientes, tales como información de identificación personal o propiedad intelectual, lo que resulta en la pérdida de clientes y la confianza que estos depositan en la empresa;
- Bots maliciosos que abusan de las aplicaciones de clientes mediante la apropiación de contenidos y cuentas, y mediante procedimientos de compra fraudulentos.



Aunque el coste en dólares causado por una DDoS, una filtración de datos o bots maliciosos puede variar en función del tamaño o del sector de la empresa, la gravedad del impacto empresarial está creciendo en todas las organizaciones.

Según un informe de IDC de 2015, el coste medio por tiempo de inactividad es de 100 000 $ por hora.[1]

Una filtración de datos puede consistir en una filtración de información de usuarios o en la extracción de datos confidenciales de clientes, tales como las tarjetas de crédito y contraseñas del almacén de datos de una aplicación. El coste global promedio por filtraciones de datos por registro perdido o robado fue de 141 $ en 2017, y el coste total promedio de una filtración de datos fue de 3,62 millones de dólares.[2] Debido al mayor escrutinio por parte de los gobiernos y los medios, las empresas se enfrentan a repercusiones más considerables, incluso por la más mínima filtración de datos, que no solo se puede traducir en sanciones económicas, sino también en la pérdida de la confianza del público.

Los bots maliciosos pueden apoderarse de la cuenta de un usuario, pero también pueden dirigir procedimientos fraudulentos de compra y apropiarse de contenidos. Un procedimiento fraudulento ejecutado por un bot que compre de forma repetitiva y automática productos con un inventario limitado puede dañar la marca de una tienda, desalentar a futuros compradores causando una disminución en las ventas e incluso perjudicar las relaciones con los proveedores. La apropiación de contenidos, en particular en las empresas impulsadas por la publicidad, puede reducir directamente los ingresos haciendo descender las clasificaciones SEO, disminuyendo el coste por cada mil impresiones (CPM) o causando la pérdida de anunciantes.

La ventaja

Para combatir tanto el aumento de la exposición como la intensificación de los impactos sobre el negocio, las empresas tienen que abordar los problemas tácticos específicos, pero también deben tener una ventaja frente a los actores maliciosos en un escenario de amenazas en constante evolución.

Tres variantes esenciales son **la dimensión, el rendimiento y la facilidad de uso**.

La dimensión importa

Cloudflare tiene a su favor el tamaño de la red y la variabilidad del tráfico para el análisis de datos. Al proteger más de 6 millones de sitios web de clientes, Cloudflare dispone de una valiosa perspectiva de las amenazas globales emergentes. Como resultado, las protecciones DDoS y el cortafuegos de aplicaciones web de Cloudflare defienden proactivamente a los clientes de los ataques que causan tiempos de inactividad y pérdidas de ingresos.

Diseñada para ser escalable, la red de Cloudflare ofrece velocidad y capacidad de adaptación. Con el fin de proporcionar todos sus servicios en más de 300 000 millones de solicitudes diarias, los servicios que se ejecutan en cada servidor de cada centro de datos, como los de DNS, cifrado y WAF, pueden procesar enormes cargas de tráfico con poca latencia y una alta fiabilidad.

A medida que crece el tamaño de los ataques DDoS, las dimensiones y la capacidad de adaptación de la red benefician a los clientes. La escala de Cloudflare a partir de sus más de 116 centros de datos, combinada con la red de difusión por proximidad (anycast), permite a Cloudflare resistir incluso los ataques distribuidos más grandes.

Aumento del rendimiento protegiendo al mismo tiempo las aplicaciones

Los clientes han tenido que elegir durante mucho tiempo entre seguridad y rendimiento. Las soluciones TLS y WAF a menudo degradaban el rendimiento de un sitio. Por ejemplo, TLS, un protocolo para cifrar conexiones, puede establecer hasta cuatro recorridos de ida y vuelta solamente para iniciar una única sesión segura. Esos recorridos adicionales pueden aumentar la latencia. Del mismo modo, un WAF causa también retrasos, ya que inspecciona cada solicitud en línea.

[1] IDC, DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified, Stephen Elliot, marzo de 2015

[2] Ponemon Institute, 2017 Cost of Data Breach Study, junio de 2017

Cloudflare elimina la necesidad de sacrificar el rendimiento por la seguridad. En lugar de disminuir el rendimiento, las funciones de seguridad de Cloudflare pueden aumentar el rendimiento de las aplicaciones gracias a los servicios de seguridad de baja latencia integrados con la aceleración del tráfico. La compatibilidad con TLS 1.3 y la reanudación de sesión global pueden reducir el número de recorridos de ida y vuelta, y HTTP/2, que permite descargas multiplexadas, acelera los tiempos de carga de página. Las aplicaciones pueden experimentar un rendimiento más rápido que si se ejecutan sin la protección de Cloudflare, ya que los servicios de seguridad de Cloudflare se integran con los servicios de aceleración de tráfico, tales como el almacenamiento en caché y el enrutamiento inteligente.

El almacenamiento en caché ofrece contenido estático más cercano a los visitantes del sitio web. Eso no solo reduce la carga en los servidores de origen, sino que aumenta la velocidad de respuesta de la aplicación. El enrutamiento inteligente determina el camino más rápido desde Cloudflare hasta el origen, acelerando tanto el contenido dinámico como el estático.

Dimensión

Capacidad de adaptación desde cero

Fácil de usar

Interfaz de usuario intuitiva y API que agilizan la configuración y la administración

Velocidad

Seguridad de alto rendimiento integrada con la aceleración del tráfico

La facilidad de uso mejora el nivel de seguridad

La facilidad de uso de una aplicación de seguridad para los usuarios y administradores es algo más que una bonita interfaz; también contribuye a mejorar el nivel de seguridad de una empresa. Las investigaciones de Gartner sugieren que, hasta el 2020, el 99 % de las infracciones de cortafuegos serán causadas por errores de configuración del cortafuegos, no por defectos.[3]

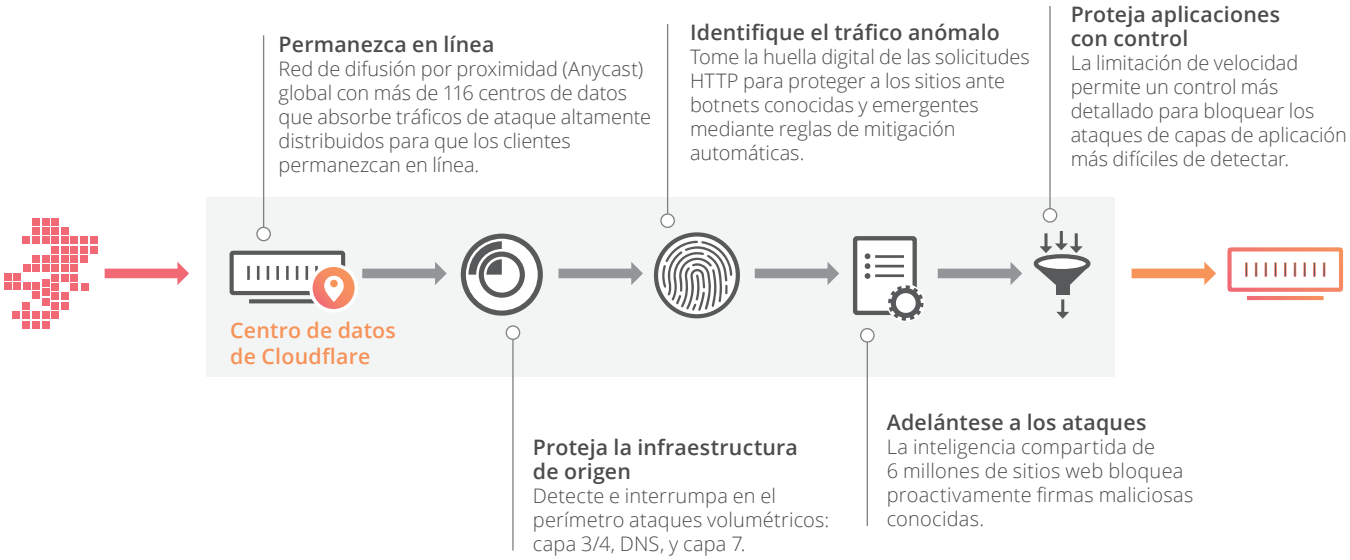
Una buena experiencia del usuario reduce los riesgos de seguridad producidos por una configuración deficiente y aumenta la agilidad en un escenario de amenazas en constante cambio. Cloudflare se puede configurar en menos de 5 minutos. Esta facilidad de uso permite a las empresas ampliar la gestión de políticas de seguridad a más empleados que pueden no ser expertos en seguridad, reducir el tiempo necesario para cambiar e implementar nuevas políticas y mejorar los ajustes oportunos del nivel de seguridad de aplicaciones complejas.

Cloudflare aplica estas ventajas para proteger a los clientes ante tres desafíos principales: Ataques DDoS que pueden degradar el rendimiento y la disponibilidad de sus aplicaciones, el compromiso de los datos de los clientes por ataques multivector y los bots maliciosos que abusan de su sitio web.

Proteja sus aplicaciones ante DDoS

Un ataque DDoS envía grandes volúmenes de tráfico en un intento de hacer caer un sitio o servicio. Al sobrecargar los servidores de origen, este tráfico malicioso hace que la aplicación de destino se ralentice o deje de estar disponible para los usuarios finales. Cloudflare ofrece una defensa de varias capas.

[3] Gartner, Inc., One Brand of Firewall Is a Best Practice for Most Enterprises, Adam Hils y Rajpreet Kaur, 5 de junio de 2017



Red de difusión por proximidad (Anycast) global

La red de difusión por proximidad (Anycast) de más de 116 centros de datos aumenta el área expuesta a través de la cual Cloudflare puede dispersar los ataques DDoS. Con Anycast, varias máquinas comparten la misma dirección IP. Cuando se envíe una solicitud a una dirección IP de Anycast, los enrutadores lo dirigirán a la máquina más cercana de la red. Eso mitiga los ataques altamente distribuidos por redes de bots, ya que nuestros centros de datos absorben una parte del tráfico DDoS, y este no se concentra en un único punto.

Mitigaciones inteligentes y automatizadas en el perímetro

Como Cloudflare tiene visibilidad de sus 6 millones de sitios web, el servicio de protección DDoS puede desarrollar heurísticas en función de los ataques a un sitio para proteger a muchos otros.

Las mitigaciones automatizadas mediante la toma de huellas digitales de los flujos de red y el tráfico de ataques HTTP identifican y frenan proactivamente el tráfico de ataque antes de que perjudique los sitios de los clientes.

Al interrumpir esos ataques de alto volumen en el perímetro de la red, los servidores de origen de los clientes permanecen protegidos y en línea.

Pila integrada de protecciones DNS, de red y de capa 7

Debido a que cada servidor perimetral tiene una pila integrada de servicios de seguridad, tales como DNS, cortafuegos, limitación de velocidad y WAF, Cloudflare puede proporcionar no solo protección distribuida, sino también una defensa en capas contra diferentes tipos de ataques DDoS, en particular DDoS de capa de aplicación, red y DNS.

El servicio DNS distribuido de Cloudflare puede resistir ataques dirigidos contra servidores de nombres de dominio. Los ataques de red, tales como los de capa 3 y 4, no solo se bloquean automáticamente, sino que pueden ser configurados por los clientes para bloquear fuentes perniciosas por IP, país de origen o ASN a través de un cortafuegos de IP. La configuración de seguridad puede aprovechar la visibilidad que tiene Cloudflare de la reputación de cualquier dirección IP en sus 6 millones de sitios web para bloquear de forma proactiva el tráfico perjudicial que se detecta.

> Nos encanta la tranquilidad que nos da saber que podemos configurar Cloudflare, olvidarnos de él y tener la seguridad de que no nos veremos afectados por ningún tipo de ataque DDoS malicioso.

BUYCRAFT

LEE MCNEIL
Director de tecnología

Mitigaciones configurables en función de la velocidad
Aunque las soluciones DDoS de Cloudflare protegen automáticamente a los clientes ante ataques volumétricos de red y de aplicaciones, algunos clientes necesitan controles configurables para protegerse contra el tráfico de bajo volumen y aun así malicioso.

La capacidad de personalizar los umbrales de velocidad de solicitudes, la URI de destino y los atributos de solicitud, tales como el método y el código de respuesta, dan a los clientes la flexibilidad necesaria para configurar su protección en función de su perfil de tráfico y aplicaciones.

Reducción de los riesgos de filtración de datos mediante una defensa en capas

Los atacantes suelen utilizar varios vectores de ataque cuando intentan comprometer los datos de los clientes. Para protegerse, las empresas necesitan una defensa en capas.

ATAQUES	SOLUCIONES CLOUDFLARE
1. Inyectan cargas maliciosas a través de formularios y las API	**Bloqueo de las vulnerabilidades OWASP y de los ataques de nivel de aplicación que atraviesan el WAF**
2. Espían datos confidenciales sin cifrar introducidos por los clientes	**Cifrado mediante SSL/TLS que bloquea la intromisión**
3. Se abren paso por fuerza bruta en las páginas de inicio de sesión	**Protección de inicio de sesión mediante la limitación de la velocidad**
4. Los atacantes intentan falsificar respuestas DNS para interceptar las credenciales de los clientes	**DNS y DNSSEC con capacidad de adaptación que evitan respuestas falsificadas**

Reducción de las suplantaciones mediante un DNS seguro

El envenenamiento de caché o las «suplantaciones» engañan a los visitantes de un sitio para que introduzcan datos confidenciales, como, por ejemplo, números de tarjetas de crédito, en un sitio bajo ataque. Este tipo de ataque se produce cuando un atacante envenena la caché de un servidor de nombres DNS con registros incorrectos. Ese servidor de nombres devolverá los registros DNS falsos hasta que caduque la entrada de caché. Se redirige a los visitantes al sitio de un atacante en lugar de al sitio correcto, lo que permite al actor malicioso robar datos confidenciales.

DNSSEC verifica los registros DNS utilizando firmas criptográficas. Al comprobar la firma asociada a un registro, las resoluciones de DNS pueden verificar que la información solicitada proviene de su servidor de nombres autoritativo y no de un atacante de tipo «man in the middle».

Reducción de las suplantaciones mediante el cifrado

Los atacantes pueden interceptar o «espiar» las sesiones del cliente para robar datos confidenciales de clientes, incluyendo credenciales tales como contraseñas o números de tarjetas de crédito. En el caso de un ataque de tipo «man in the middle», el navegador piensa que está hablando con el servidor en un canal cifrado, y el servidor piensa que está hablando con el navegador, pero ambos están hablando con el atacante que está situado en el medio. Todo el tráfico pasa a través de este «man in the middle», quien puede leer y modificar cualquiera de los datos.

La rapidez del cifrado y la terminación, la sencilla administración de los certificados y la compatibilidad con los últimos estándares de seguridad permiten a los clientes proteger la transmisión de los datos de los usuarios.

Bloqueo de cargas maliciosas mediante un WAF escalable y actualizado automáticamente

Los atacantes aprovechan las vulnerabilidades de las aplicaciones enviando cargas maliciosas que pueden extraer datos confidenciales de la base de datos y del navegador del usuario, o inyectando malware capaz de comprometer sistemas específicos.

Un cortafuegos de aplicaciones web (WAF) analiza el tráfico web en busca de tráfico sospechoso; después puede filtrar automáticamente las solicitudes ilegítimas en función de los conjuntos de reglas que se le pida que aplique. Examina las solicitudes HTTP GET y POST y aplica un conjunto de reglas, como el conjunto de reglas básicas de ModSecurity que cubre las vulnerabilidades del OWASP Top 10, para determinar qué tráfico bloquear, comprobar o dejar pasar. Puede bloquear el spam de comentarios, los ataques de scripts entre sitios y los ataques de inyección SQL.

El WAF de Cloudflare actualiza las reglas en función de las amenazas detectadas en 6 millones de clientes, y puede proteger a estos sin perjudicar el rendimiento de las aplicaciones gracias a su inspección de baja latencia y a la integración con la aceleración del tráfico.

Reducción de las apropiaciones de cuentas mediante la protección de inicio de sesión

Los atacantes pueden cometer «ataques por diccionario» automatizando inicios de sesión con credenciales volcadas para abrirse paso por «fuerza bruta» a través de una página protegida de inicio de sesión. Cloudflare permite a los usuarios personalizar las reglas de limitación de velocidad para identificar y bloquear en el perímetro esos ataques tan difíciles de detectar.

Protección mediante la supervisión y la puntuación

Las aplicaciones de terceros de Cloudflare ofrecen una capa adicional de protección proactiva mediante la supervisión de sitios web en busca de vulnerabilidades, la puntuación del desarrollo de seguridad de las empresas y la integración en su proceso de desarrollo.

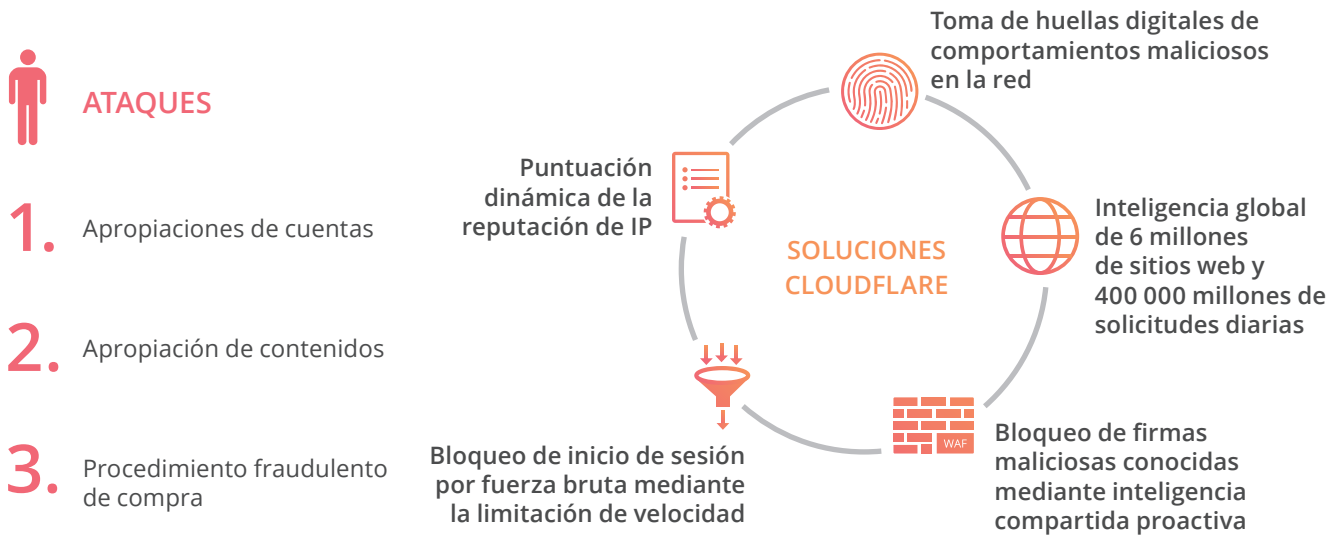
> Las características de seguridad de Cloudflare liberan a nuestros desarrolladores de preocupaciones por mantener el sitio en línea y les permiten centrarse en otras mejoras del sitio.

Gazeta Esportiva | DAVID VERZOLLA
Director de tecnología

Prevención de bots abusivos

Hay tres tipos de bots abusivos que están aumentando su frecuencia, su sofisticación y el impacto en los clientes. Por ese motivo, una solución de prevención de bots necesita otros elementos para abordar los diferentes perfiles de ataque potenciales.

Los ataques más comunes son las apropiaciones de cuentas y contenidos y los procedimientos fraudulentos de compra. Todos ellos pueden usar distintos estilos de «bot», y es posible detectar y mitigar cada uno de ellos con diferentes planteamientos.



Detección y mitigación en función de la velocidad

Algunos bots están automatizados y necesitan atacar el sitio a una velocidad alta para poder lograr su objetivo, así que la automatización en función de la velocidad puede detectar y mitigar esos ataques. Por ejemplo, los inicios de sesión por fuerza bruta tienen una proporción superior de inicios de sesión fallidos desde una única dirección IP que un usuario normal. Los umbrales en función de la velocidad pueden detectar esos tipos de intento de apropiación de cuentas. De igual modo, las apropiaciones de contenido que llegan a páginas que ya no se pueden encontrar (errores 404) generarán estas en una proporción superior a la de un usuario normal.

Bloqueo en función de firmas maliciosas conocidas

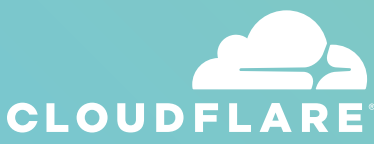
Con 6 millones de sitios web protegidos en Cloudflare, las firmas maliciosas que se detectan en un sitio son bloqueadas en todos los demás.

Conclusión

Para mantenerse protegido y «siempre en línea» en un escenario de amenazas en constante cambio, las empresas necesitan rendimiento, seguridad inteligente a escala y defensas en capas para protegerse contra las denegaciones de servicio, el robo de datos y los bots maliciosos.

Siempre habrá humanos en la ecuación, así que la facilidad de uso para implementar, configurar y ajustar las políticas de seguridad influye en el nivel general de seguridad, ya que reduce los errores en la introducción de datos y permite que los empleados reaccionen a los cambios evitando riesgos o complicaciones innecesarias.

La seguridad en la nube de Cloudflare protege ante la sofisticación cada vez mayor de los ataques DDoS, los intentos por parte de actores maliciosos de comprometer los datos y los bots maliciosos.



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com