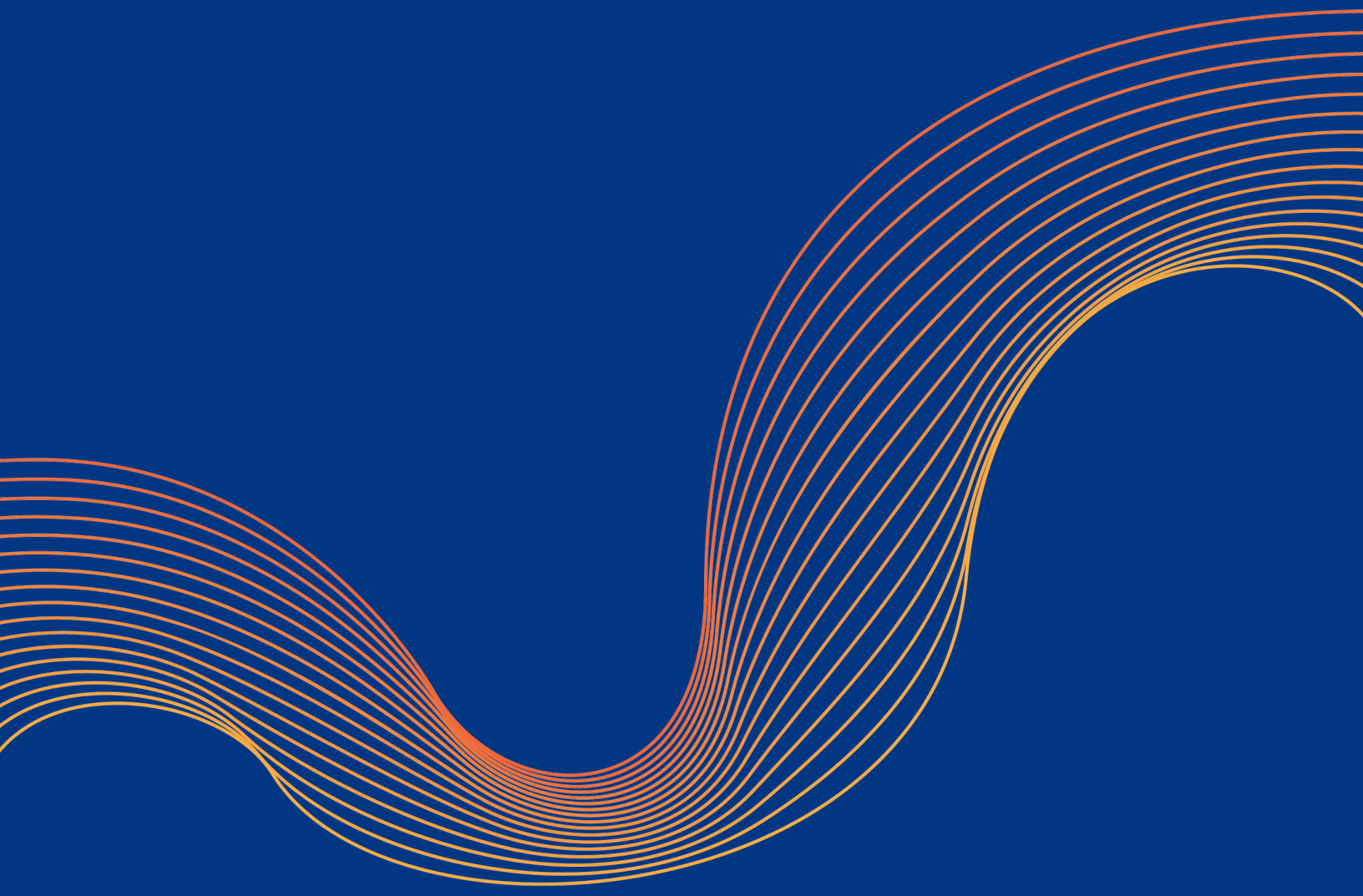
CLOUDFLARE

Seguridad de aplicaciones eficaz: protección integral, rápida y siempre activa



+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

ÍNDICE

INTRODUCCIÓN

Las amenazas a la seguridad de las aplicaciones siempre están acechando. En 2020, la base de datos nacional de vulnerabilidades (NVD) informó de un total de 18.000 vulnerabilidades, una cifra sin precedentes. Resulta alarmante que más de 10.000 de ellas fueran calificadas como críticas o de alta gravedad.

Al mismo tiempo, los atacantes siguen aprovechando vulnerabilidades conocidas. Una investigación conjunta de la Agencia de seguridad de infraestructura y ciberseguridad (CISA) de EE. UU., la Oficina federal de investigación (FBI), el Centro nacional de seguridad cibernética (NCSC) del Reino Unido y el Centro australiano de ciberseguridad (ACSC) reveló que una buena parte de las 30 principales vulnerabilidades que los ciberdelincuentes aprovecharon durante 2020 (y 2021) eran muy conocidas, y todas ellas tenían un parche disponible.

El riesgo de seguridad de estas vulnerabilidades conocidas persiste posiblemente por la dificultad de las empresas para aplicar parches en su software. Y lo que es peor, incluso cuando las empresas intentan instalar un parche para corregir una vulnerabilidad antes de que sea tarde, la aplicación del parche puede tardar una media de 16 días, lo que deja las aplicaciones expuestas a ataques.

Lamentablemente, las vulnerabilidades nativas no son la única preocupación de seguridad para los propietarios de aplicaciones. Las API conllevan sus propios riesgos y los datos de la red de Cloudflare muestran que más del 50 % de las solicitudes están relacionadas con las API. Además, los bots representan el 40 % del tráfico de Internet, por lo que la protección contra ataques de bots es indispensable. Por último, el código de terceros, del que dependen muchos sitios para funcionar, expone las aplicaciones a ataques a la cadena de suministro.

Los productos y soluciones disponibles para proteger una aplicación de todos los ataques posibles, podría fragmentar y dificultar la seguridad de las aplicaciones muy rápidamente. La implementación de una estrategia de seguridad de aplicaciones integral puede ayudar. Un enfoque eficaz de seguridad de las aplicaciones debe contemplar una estrategia de protección frente a riesgos integral, rápida y siempre activa.

El panorama de los problemas de seguridad de las aplicaciones

Los problemas de seguridad más acuciantes para los propietarios de aplicaciones son los siguientes:

Vulnerabilidades de las aplicaciones

Las vulnerabilidades de las aplicaciones son increíblemente comunes. Un reciente informe de seguridad de software llevado a cabo por Veracode concluyó que el 83 % de las aplicaciones tenían al menos un fallo de seguridad, incluso más de uno. Además, más del 20 % de las aplicaciones del estudio tenían al menos un fallo grave.

Ataques a la API

Las aplicaciones dependen cada vez más de las interfaces de programación de aplicaciones (API) para funcionar. Gartner pronosticó hace poco que "para 2022, los abusos de las API pasarían de ser un vector de ataque poco frecuente a ser el más común, lo que se traduciría en fugas de datos en las aplicaciones web empresariales."[1]

[1]Gartner pronosticó que "para 2022, los abusos de las API pasarían de ser un vector de ataque poco frecuente a ser el más común, lo que se traduciría en fugas de datos en las aplicaciones web empresariales". Fuente: Gartner "API Security: What You Need to Do to Protect Your APIs", Mark O'Neill, Dioniso Zumerle, Jeremy D'Hoinne, 1 de marzo de 2021, (se requiere suscripción a Gartner).

Ataques de bots

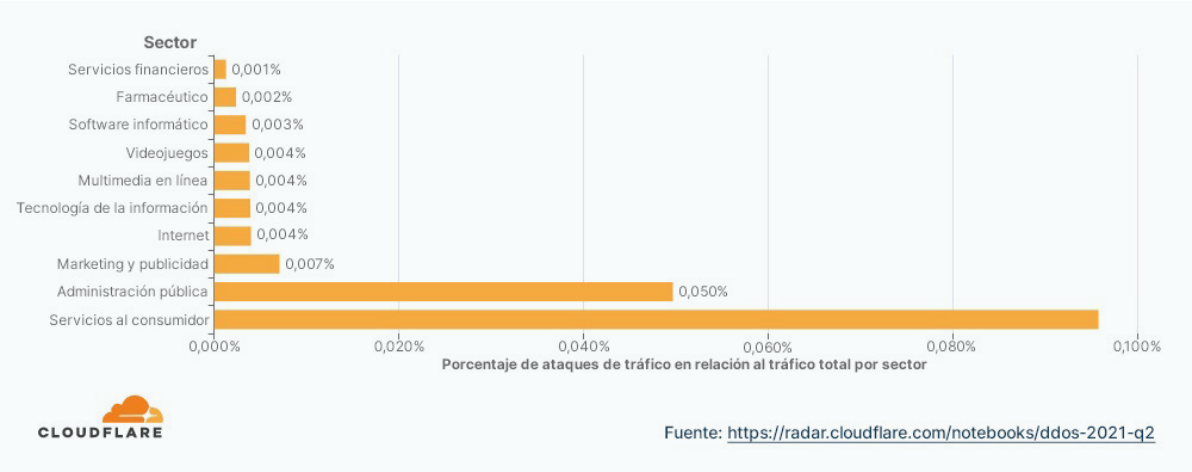
Los ataques de bots son muy frecuentes. Los atacantes suelen utilizar redes de dispositivos infectados, llamadas botnets, para llevar a cabo una serie de acciones malintencionadas. Un ejemplo es el relleno de credenciales, en el que los bots intentan "rellenar" cientos o miles de credenciales robadas en páginas de inicio de sesión con la esperanza de obtener acceso a cuentas. Los bots también se utilizan para llevar a cabo ataques de apropiación de contenidos, que consisten en descargar y duplicar el contenido de un sitio para robar una parte de los beneficios de optimización de los motores de búsqueda (SEO).

Ataques a la cadena de suministro

En los ataques a la cadena de suministro, los atacantes encuentran un punto de entrada a través de una fuente externa, como el software de vendedores de confianza, dependencias de sitios web de terceros o proveedores. En 2015, un grupo llamado Magecart llevó a cabo una serie de ataques de este tipo, como el robo de información de pago de sitios web de comercio electrónico infectando dependencias de terceros en el sitio con código malicioso. Los navegadores de los usuarios finales cargan la página que contiene las dependencias infectadas, lo que permite a los atacantes robar información de su página web y venderla. La consecuencia en este caso es que trabajar con terceros, ya sean vendedores o incluso dependencias del sitio web, puede aumentar en gran medida la superficie de ataque.

Ataques DDoS

En los ataques DDoS, los atacantes utilizan la entrada de tráfico basura en un intento de interrumpir una aplicación. Por desgracia, los ataques DDoS cambian constantemente de tamaño, vectores utilizados, etc. Además, no muestran una tendencia al descenso. Los datos de la red de Cloudflare descubrieron que una de cada 200 solicitudes HTTP destinadas a organizaciones con sede en Estados Unidos durante el segundo trimestre de 2021 formaba parte de un ataque DDoS.



Ataques en ruta

Las aplicaciones también pueden ser víctimas de ataques en ruta, en los que un atacante intercepta la comunicación entre dos partes (como un navegador y un servidor) con fines malintencionados. El atacante puede hacerse pasar por una de las partes y cambiar su comunicación o recabar información confidencial. Los ataques en ruta pueden adoptar muchas formas y se dirigen, por ejemplo, a los servidores del sistema de nombres de dominio (DNS) y los servidores de correo electrónico, entre otros. En los ataques DNS en ruta, un atacante intercepta el proceso de búsqueda de DNS y envía a los usuarios a un sitio web diferente, normalmente malicioso. Del mismo modo, en el secuestro de correo electrónico, un atacante intercepta la conexión entre un servidor de correo electrónico y la web, lo que le permite leer e interferir en las comunicaciones por correo electrónico.

Prácticas recomendadas para proteger las aplicaciones web

La protección contra estos tipos de ataques debería formar parte de la estrategia de seguridad de las aplicaciones de toda organización. Sin embargo, la forma en que las organizaciones se protegen también es importante. Una estrategia de seguridad de aplicaciones sofisticada debería contemplar:

- **Una red perimetral en la nube:** la protección local contra las amenazas a las aplicaciones web solía ser la norma, pero este enfoque es difícil de escalar. Si una aplicación está protegida con un WAF basado en hardware, por ejemplo, la única forma de ampliar la protección es adquirir más hardware. Aumentar la protección de una aplicación con hardware puede requerir mucho tiempo durante el que la aplicación queda expuesta. Las soluciones basadas en la nube no tienen este problema ya que, al tener más capacidad disponible de forma permanente, la ampliación de los servicios de protección es ilimitada.

  Más allá de las limitaciones de capacidad, la compra y el mantenimiento de la protección en un entorno local conllevan un coste elevado. El hardware puede quedar obsoleto con relativa rapidez, por lo que los costes de reparación o sustitución pueden aumentar. Además, la contratación de personal formado para gestionar el hardware también contribuye al incremento total del coste de propiedad. Por el contrario, el uso de una solución en la nube lo reduce significativamente.

  Otra ventaja de las soluciones en la nube es que se pueden actualizar de forma automática, fácil y con frecuencia. Esto es especialmente útil para soluciones como los firewalls de aplicaciones web (WAF), cuyas reglas, mecanismos de mitigación y software subyacente se pueden actualizar rápidamente cuando se suministran en la nube. En cambio, los proveedores locales pueden actualizar las soluciones de forma remota, pero el proceso es más complejo y generalmente ocurre con menos frecuencia.

  Las redes perimetrales en la nube aportan mayores ventajas. Una red perimetral en la nube es un grupo de servidores repartidos geográficamente que ejecutan los mismos servicios. La protección desde el perímetro permite a las organizaciones aprovechar las ventajas de escalabilidad de la nube al tiempo que ofrece otras ventajas de rendimiento en comparación con los modelos centralizados.

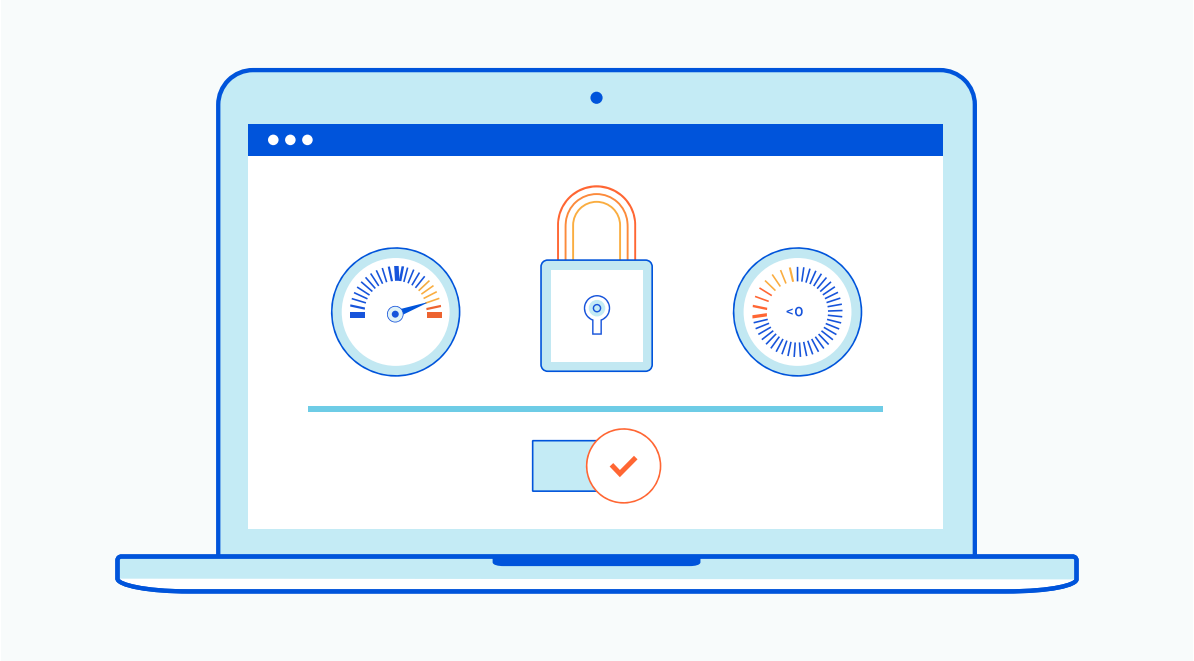
  En una red perimetral en la nube, la protección tiene lugar lo más cerca posible del usuario final. En cambio, en un modelo centralizado, la protección ocurre en un centro de datos consolidado, mucho más alejado de los usuarios finales que están repartidos por todo el mundo. Para garantizar la seguridad, todo el tráfico de los usuarios debe retornar al centro de datos centralizado, donde se despliegan los dispositivos de seguridad, independientemente de la ubicación del usuario final. Si los centros de datos están ubicados en el estado de California, el tráfico tendrá que viajar allí primero antes de retornar a un usuario final en Nueva York, por ejemplo.

- **Un sistema unificado:** tratar de aplicar una protección consistente a través de varias herramientas aumenta el margen de error, de ahí que sea mejor utilizar un sistema único y unificado para defenderse de los ataques en lugar de combinar varias herramientas.

  Cuando los equipos de trabajo utilizan herramientas que no están vinculadas entre sí, a menudo tienen diferentes personas que gestionan diferentes productos de seguridad. Este enfoque puede impedir que la información importante se comparta de un modo más amplio, creando silos de seguridad y falta de información. Por otra parte, todas las herramientas necesitan su propia configuración y gestión, lo que supone una carga para los equipos de trabajo y añade una complejidad innecesaria.

  Además, contar con demasiadas herramientas puede dificultar el análisis de todas las alertas. Cada herramienta tiene su propio conjunto de reglas y lógica para el envío de alertas, y tener varias herramientas dificulta la determinación de qué alertas son realmente importantes.

  Por otro lado, el uso de un sistema unificado permite a los equipos interactuar con menos herramientas y alertas centralizadas, por lo que entender lo que necesita atención es mucho más fácil. Las herramientas integradas también suelen hacer referencia a políticas coherentes, lo que facilita la aplicación de políticas a nivel global. Los propietarios de aplicaciones pueden establecer reglas de prevención de pérdida de datos (DLP), por ejemplo, solo una vez y hacer que su WAF, API y otras herramientas aplicables las ejecuten de forma automática.

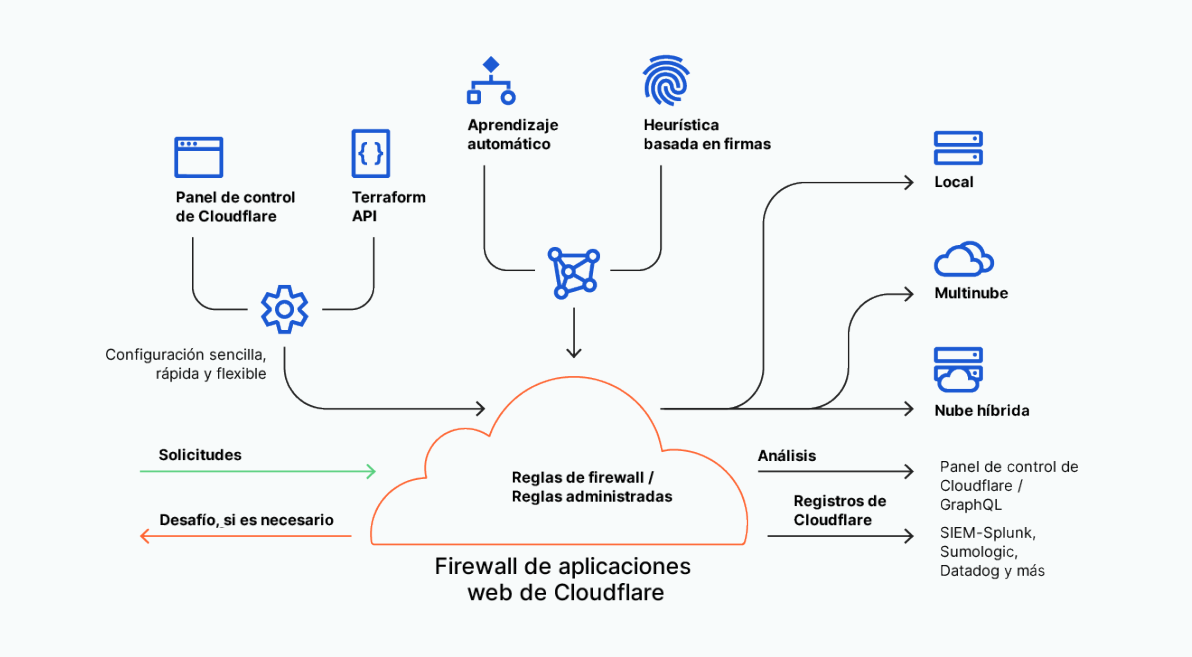


Estrategias concretas para prevenir ataques

La gran variedad de tipos de riesgos de seguridad a los que se enfrentan las aplicaciones hace necesario contemplar varios tipos de protección. A continuación, describimos algunas de las estrategias para prevenir ataques que los propietarios de aplicaciones pueden utilizar:

Vulnerabilidades de las aplicaciones

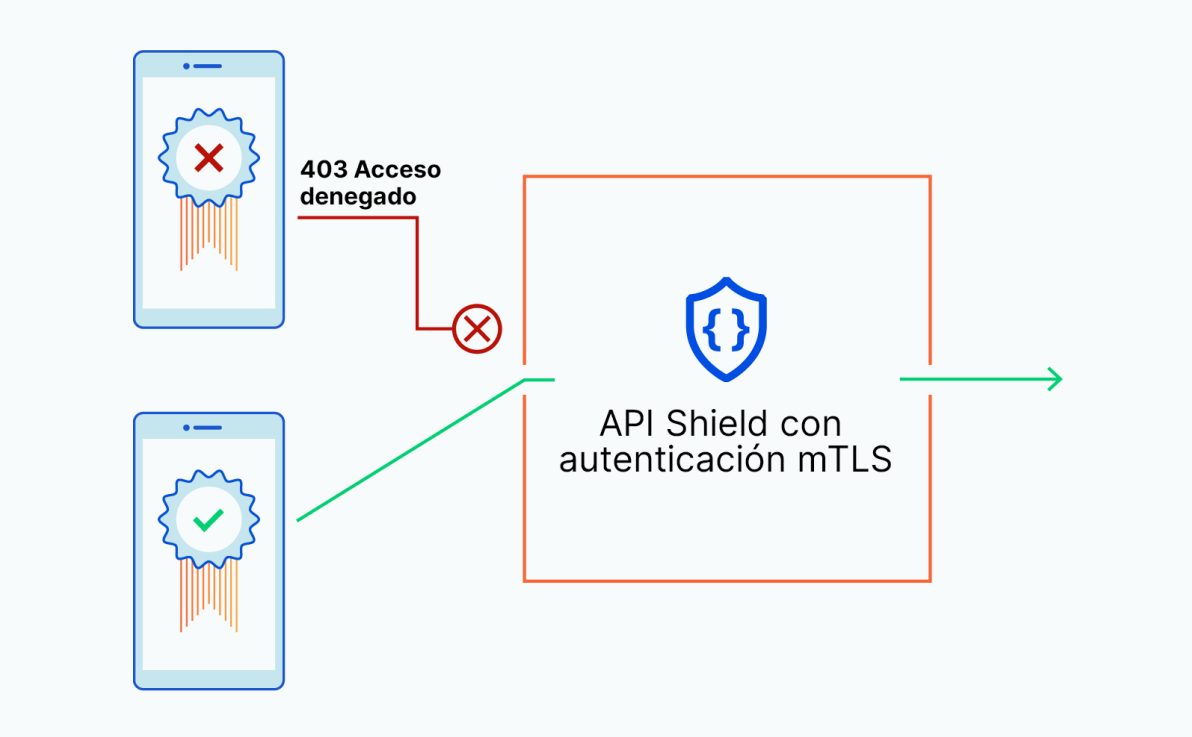
Firewall de aplicaciones web: un WAF es una de las formas más eficaces de evitar que los atacantes exploten las vulnerabilidades de las aplicaciones. Los WAF utilizan un conjunto de reglas de seguridad sobre técnicas de ataque conocidas para filtrar el tráfico malicioso y prevenir ataques. Los WAF con reglas preestablecidas y opciones de personalización que despliegan los cambios de reglas rápidamente son los más eficaces. El motivo es que estas características mitigan dos de los mayores problemas de muchos WAF: los falsos positivos y la lentitud en el despliegue de los cambios en las reglas. Los falsos positivos se producen cuando las reglas del WAF bloquean involuntariamente el tráfico web legítimo. Algunos WAF requieren complejos procedimientos de creación de reglas, lo que dificulta el mantenimiento de listas precisas y actualizadas y el desbloqueo del tráfico legítimo. Por ello, los WAF que ofrecen conjuntos de reglas OWASP además de conjuntos de reglas administradas y personalizadas, reducen la frecuencia de los falsos positivos. Sin embargo, si se tarda demasiado en desplegar estas nuevas reglas, las aplicaciones quedarán expuestas a ataques.



Prevención de la pérdida de datos (DLP): es una estrategia para prevenir la exfiltración de datos (o la salida no autorizada de datos de una organización). Las herramientas y soluciones de DLP supervisan la actividad de las aplicaciones y las API para identificar posibles fugas y detenerlas antes de que se produzcan. Las herramientas de DLP inspeccionan el tráfico saliente y lo comparan con tipos de datos conocidos para determinar si se trata de una fuga de datos que se deba bloquear. Por ejemplo, una herramienta de DLP puede identificar una cadena de caracteres como un nombre de usuario. Basándose en las reglas que la organización ha establecido, la herramienta de DLP puede marcar, detener o permitir que la actividad continúe. Algunas herramientas de DLP se integran con los controles de acceso basados en roles (RBAC), que dictan qué nivel de acceso tienen los tipos de usuarios, para asegurar aún más la forma en que se mueven los datos dentro de una organización o aplicación.

Riesgos de seguridad de la API

Validación de esquemas y modelos de seguridad positivos: los esquemas de las API son contratos que describen el comportamiento esperado para quienes interactúan con una API. Los esquemas establecen las reglas básicas de lo que los usuarios pueden hacer al trabajar con las API. OpenAPI (o Swagger) es el formato de esquema más común. Los esquemas son modelos eficaces para imponer la seguridad positiva de la API. Un modelo de seguridad positiva valida las solicitudes de acuerdo con el esquema, permitiendo solo las solicitudes que se ajustan al mismo, evitando así el abuso y posibles ataques. Un modelo de seguridad positiva es más estricto que un modelo de seguridad negativa, que permite por defecto todas las solicitudes excepto las que se le ha ordenado bloquear.



Autenticación y autorización: la autenticación (o la garantía de que las solicitudes de la API son legítimas) y la autorización (la confirmación del nivel de acceso que tiene un punto de conexión o un cliente) son también aspectos importantes de la seguridad de la API. Hay muchas formas de autenticar y autorizar las solicitudes de la API. La seguridad de la capa de transporte mutua (mTLS), por ejemplo, es un proceso en el que tanto un cliente como un servidor tienen certificados de autenticación que utilizan para verificar la identidad del otro.

Descubrimiento de la API: las API "en la sombra" son aquellas que un equipo de seguridad puede desconocer. Dado que no son supervisadas, las API en la sombra pueden ocasionar fugas de datos o puede que no se adhieran a las normas de cumplimiento. Las herramientas de descubrimiento de API supervisan los puntos de conexión para descubrir las API en la sombra y así mejorar la gestión de las mismas.

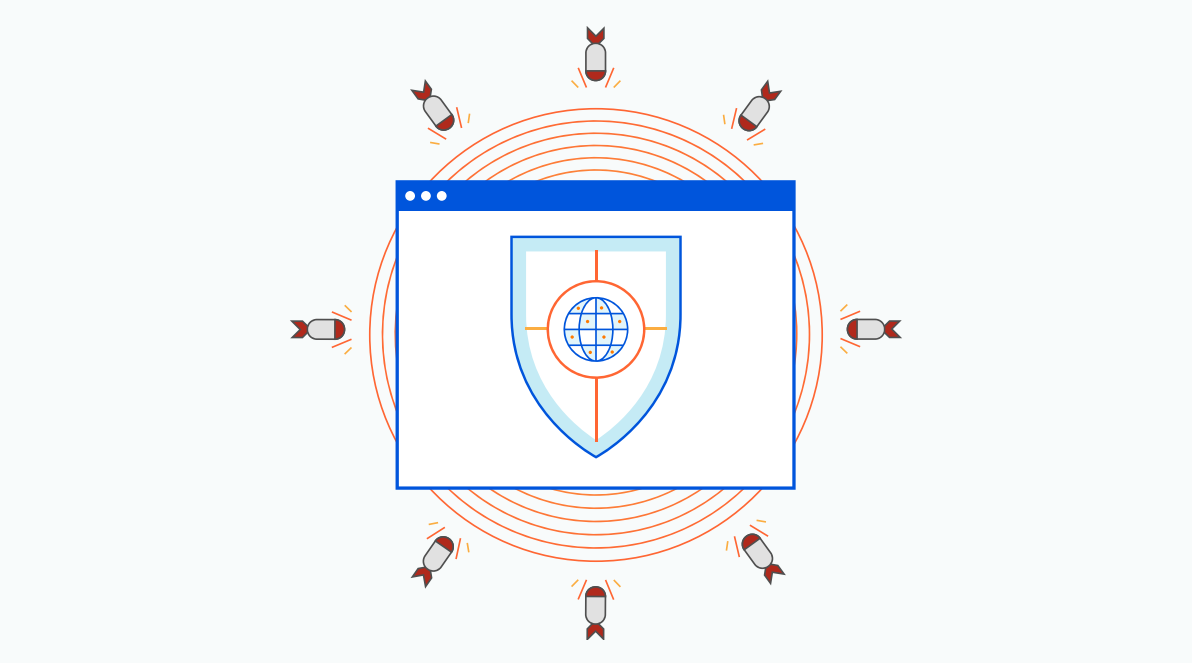
DLP: la exfiltración de datos también puede ocurrir con las API, no solo con las aplicaciones convencionales. Las herramientas de DLP se pueden utilizar para supervisar el tráfico saliente de las API y detectar y bloquear cualquier dato potencialmente confidencial en las respuestas de las API.

Bots maliciosos

La gestión del tráfico de bots requiere detectar y bloquear los bots malos sin bloquear los buenos. Estos últimos, como los rastreadores de motores de búsqueda, son necesarios para entender las métricas clave del negocio. Los bots malos, por el contrario, pueden causar problemas en una aplicación, tales como relleno de credenciales, spam de contenido y otros tipos de ataques. Una solución de gestión de bots analizará el tráfico para detectar la actividad de los bots y determinar si es buena o mala, y en consecuencia bloquear o autorizar el tráfico. Una gestión eficaz de bots requiere métodos de detección sofisticados, la capacidad de comprender las tendencias del tráfico de bots a lo largo del tiempo con análisis y la flexibilidad para utilizar esos datos para personalizar las reglas de bloqueo de bots.

Ataques DDoS

Defenderse eficazmente de los ataques DDoS conlleva optimizar el tiempo de mitigación y no comprometer el rendimiento en pro de la seguridad. Una forma de reducir el tiempo de mitigación es utilizar la protección DDoS siempre activa, en lugar de la protección bajo demanda. A diferencia de esta última, la mitigación siempre activa no espera a que el tráfico alcance un umbral determinado para que la protección se ponga en marcha, por lo que todo el tráfico se filtra y la mitigación se agiliza. La mitigación de DDoS desde el perímetro permite a los propietarios de aplicaciones beneficiarse del rendimiento y la seguridad. A diferencia de la protección centralizada, que tiene lugar en una ubicación predefinida independientemente de dónde se origine el ataque, la mitigación de DDoS se produce lo más cerca posible del origen del ataque, mejorando así el rendimiento.



Vulnerabilidades de terceros

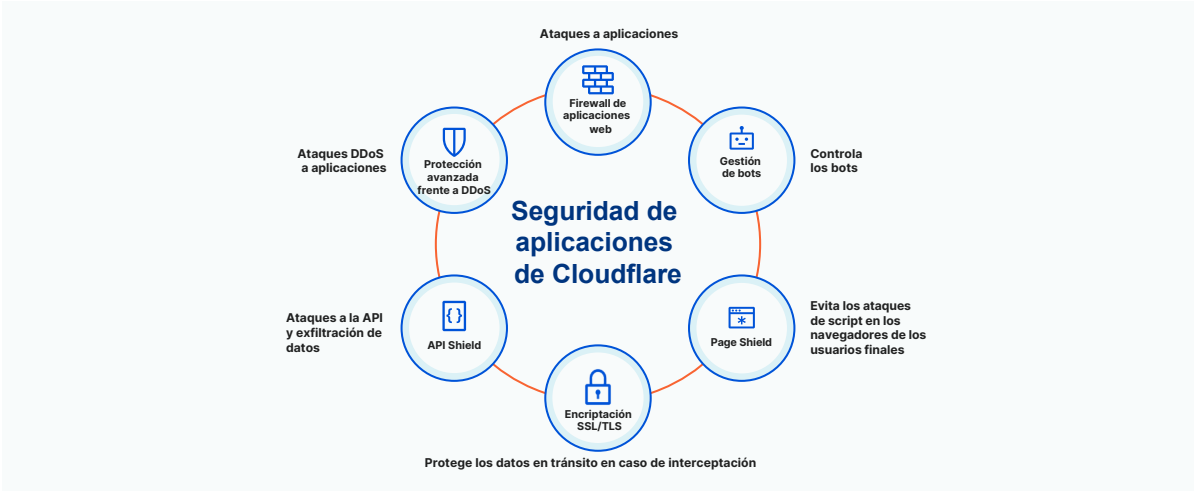
Soluciones de seguridad del lado del cliente: muchos sitios dependen de terceros que no suelen supervisar estas dependencias, por lo que pueden quedar expuestos a ataques a la cadena de suministro. En la seguridad del lado del cliente la actividad se protege en el lado del usuario, normalmente en su navegador. La seguridad del lado del cliente protege contra los ataques a la cadena de suministro supervisando los cambios en las dependencias de terceros y analizando la naturaleza de los cambios de código. Por ejemplo, la tecnología de la política de seguridad de contenidos (CSP) utiliza una lista de recursos aprobados y bloquea la ejecución de cualquiera que no esté en la lista. Sin embargo, un defecto de la tecnología CSP es que no es dinámica. Si un recurso de la lista permitida se ve comprometido y pasa a ser malicioso, la CSP no sabrá cómo bloquearlo. Afortunadamente, algunas ofertas de seguridad del lado del cliente se basan en las ventajas de la CSP. Algunas herramientas son capaces de rastrear nuevas dependencias de JavaScript y alertar a los propietarios de sitios para que las analicen. Del mismo modo, algunas soluciones pueden detectar URL maliciosas conocidas que sirven JavaScript en un sitio o alertar a los propietarios del sitio para que investiguen la naturaleza de los cambios de script detectados.

Ataques en ruta

El cifrado es la clave para defenderse de los ataques en ruta. La adopción del cifrado de la capa de sockets seguro (SSL) / seguridad de la capa de transporte (TLS) es uno de los mejores métodos para proteger el tráfico HTTP. TLS encripta los datos, autentifica las partes que los intercambian y valida que no han sido manipulados. Este proceso protege los intercambios entre los servicios web y los usuarios finales, impidiendo ataques en ruta. Sin embargo, algunos atacantes pueden eludir los protocolos SSL / TLS, y ahí es donde entra en juego la seguridad de transporte estricta HTTP (HSTS). HSTS bloquea cualquier conexión no segura de los atacantes, impidiendo nuevos ataques en ruta.

Cómo proteger tu aplicación de amenazas externas con Cloudflare

La protección contra amenazas externas a las aplicaciones es posible con Cloudflare. La red perimetral de Cloudflare abarca más de 200 ciudades en más de 100 países y protege a millones de propiedades de Internet de ataques DDoS, vulnerabilidades de aplicaciones, bots maliciosos, abuso de API y mucho más. Todos nuestros servicios de seguridad se ejecutan en todos los servidores de nuestra red y aprenden de la misma información global sobre amenazas.



La oferta de seguridad de aplicaciones de Cloudflare incluye:

- **Vulnerabilidades de las aplicaciones**
  - **WAF:** el WAF de Cloudflare ofrece un conjunto de reglas por capas, un conjunto de reglas administrado que se actualiza de forma periódica en respuesta a los últimos ataques, un conjunto de reglas básico basado en las 10 principales vulnerabilidades de OWASP y reglas personalizadas que los clientes pueden configurar e implementar en segundos. Nuestro WAF funciona con el mismo motor de reglas basado en Rust que nuestras soluciones de gestión de bots y API Shield, lo que garantiza una protección coherente.
- **Riesgos de la API**
  - **API Shield:** Cloudflare API Shield protege las API utilizando una validación basada en el certificado del cliente y en el esquema. API Shield utiliza mTLS para verificar los dispositivos / clientes que intentan acceder a una API, analiza el tráfico saliente para DLP y mucho más.
    - **DLP:** Cloudflare también ofrece la funcionalidad DLP para que las API bloqueen las respuestas que contengan datos confidenciales como claves de API o información de tarjetas de crédito. La funcionalidad DLP de Cloudflare no solo protege a las API, sino también a las aplicaciones y los dispositivos, por ejemplo.
- **Vulnerabilidades de terceros: ataques a la cadena de suministro del navegador**
  - **Page Shield:** Script Monitor, una parte de Cloudflare Page Shield, registra las dependencias de JavaScript de un sitio a lo largo del tiempo y alerta a las organizaciones para que analicen los cambios o las nuevas dependencias según vayan apareciendo.
- **Ataques de bots**
  - **Gestión de bots:** nuestra solución de gestión de bots utiliza el aprendizaje automático, el análisis del comportamiento y los datos globales para bloquear los bots malos. Puedes usar Bot Analytics para comprender los patrones de tráfico y ajustar el acceso con reglas personalizadas y listas de permisos.
- **Ataques DDoS**
  - **DDoS:** con una red de 90 Tbps que bloquea una media de 87.000 millones de amenazas al día, la mitigación de DDoS de Cloudflare protege contra los mayores ataques desde el perímetro.
- **Cifrado**
  - **SSL / TLS gratuito de Cloudflare:** con nuestro SSL / TLS gratuito, puedes cifrar el tráfico web para proteger tu aplicación. Cloudflare SSL también es compatible con el protocolo HSTS para asegurar una mayor protección.

Si deseas más información, visita https://www.cloudflare.com/security/.

© 2021 Cloudflare Inc. Todos los derechos reservados. El logotipo de Cloudflare es una marca comercial de Cloudflare. Todos los demás nombres de empresas y productos pueden ser marcas comerciales de las respectivas empresas a las que están asociados.