CLOUDFLARE

DOCUMENTO TÉCNICO

Mayor eficiencia con menos gasto

Estrategias rentables de 7 empresas para garantizar la seguridad y el rendimiento de las aplicaciones.

Contenido

Resumen ejecutivo

La mayoría de las arquitecturas informáticas son demasiado complejas u obsoletas para garantizar la seguridad en todas las aplicaciones web de manera sistemática. Los equipos de seguridad se ven obligados a agrupar manualmente herramientas aisladas, con visibilidad limitada y controles imprecisos en entornos de nube, híbridos y locales, lo que ralentiza el negocio.

Toda esta complejidad ha generado una sobrecarga de trabajo para los equipos, vulnerabilidades cada vez mayores, ataques más potentes y un nivel insostenible de recursos solo para mantenerse a la vanguardia de los ataques pasados.

La protección de las aplicaciones web y las API contra bots maliciosos, ataques DDoS, inyección de código y otras vulnerabilidades es una tarea esencial para las organizaciones. Sin embargo, la implementación de una estrategia de seguridad sólida puede ser un desafío, principalmente cuando se tiene que lidiar con presupuestos reducidos y un crecimiento limitado de los equipos de trabajo.

Este documento revela casos reales de empresas que han conseguido mejorar la eficiencia y reducir los costos en su estrategia de seguridad de las aplicaciones. Estos casos de éxito ofrecerán a otras empresas información útil sobre el uso de las prácticas de seguridad de las aplicaciones para optimizar los gastos.

Cuando los equipos de seguridad e informática tienen que mejorar la eficiencia con menos recursos

Cuando las organizaciones se enfrentan a restricciones presupuestarias, ningún equipo es totalmente inmune. Ya sea por la incertidumbre económica general, la caída de las ventas, las reestructuraciones organizativas o por otras muchas razones, los equipos de seguridad e informática se ven obligados a menudo a mejorar la eficiencia operativa sin el esperado aumento del presupuesto, o peor aún, a hacerlo mientras recortan costos al mismo tiempo.

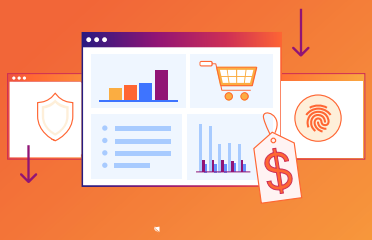
Sin embargo, la seguridad y el rendimiento de las aplicaciones no son áreas que menoscaben los resultados. En lo que se refiere a la seguridad, la protección de las aplicaciones es cada año más complicada. Los ataques son más voluminosos y complejos que nunca, y a medida que las organizaciones escalan, también lo hacen sus superficies de ataque. Por ejemplo, hubo un aumento del 15 % en el número de CVE divulgadas entre 2022 y 2023, y aunque en 2023 se divulgaron más de 5000 vulnerabilidades críticas, el tiempo promedio para actualizar una vulnerabilidad crítica de una aplicación web se mantiene en torno a los 35 días, un tiempo durante el cual la aplicación no está protegida.

En cuanto al rendimiento, los consumidores esperan que toda experiencia digital sea rápida, fiable y personalizada. Incluso una ralentización insignificante puede tener un impacto significativo en la interacción de los usuarios y los porcentajes de conversión, lo que podría dejar mal paradas a las empresas si no pueden cumplir las expectativas de sus clientes.

Cuando se enfrentan a la doble presión de las limitaciones presupuestarias y el aumento de las expectativas, los equipos de seguridad e informática tienen que encontrar formas de ofrecer más con menos. Este documento analiza las experiencias de empresas que han creado eficazmente estrategias de seguridad y rendimiento rentables, sin menoscabar los resultados.

Formas de reducir los costos en tu práctica de seguridad y rendimiento de las aplicaciones

En cuanto a la protección de las aplicaciones web y las API de las amenazas modernas, la mejor defensa no es solo la que ofrece servicios de seguridad por capas, sino la que permite a las organizaciones recortar gastos innecesarios. Para conseguirlo, las organizaciones pueden utilizar varias estrategias clave, tales como la consolidación de proveedores, la optimización de la gestión de certificados, la protección exclusiva frente a ataques que aumentan los costos de tráfico y la reducción de las tarifas de salida.



Reduce los costos con la consolidación de proveedores de soluciones de seguridad

Optimiza los costos laborales y de infraestructura con la gestión automatizada de certificados

Bloquea los ataques que aumentan los costos de tráfico

Elimina tarifas y costos inesperados como el ancho de banda, la nube y las tarifas de salida

Reduce los costos con la consolidación de proveedores de soluciones de seguridad

Un estudio reciente de Gartner revela que el 75 % de las empresas están contemplando la consolidación de proveedores en su estrategia de seguridad. La reducción del número de proveedores de los que dependen permite a las organizaciones optimizar los procesos de la cadena de suministro y lograr una mayor eficiencia, lo que se traduce en una reducción de los costos.

Chrono24, plataforma digital líder en relojes de lujo, redujo su dependencia de varios proveedores tras consolidarse con Cloudflare.

Antes del cambio, Chrono24 utilizaba una solución CDN de EdgeCast y soluciones de mitigación de DDoS y WAF de varios proveedores. La combinación de soluciones no funcionaba bien, lo que provocaba una latencia significativa, un rendimiento deficiente de la seguridad y gastos innecesarios en proveedores.

Tras la consolidación con las soluciones de Cloudflare, como la CDN, el WAF y la mitigación de DDoS, Chrono24 experimentó una reducción del 67 % en los costos de seguridad y rendimiento de su sitio web.

"Nuestra base de costos es mucho menor ahora que hemos consolidado el rendimiento y la seguridad en un único proveedor", afirma Sven Ferber, director de Tecnología. "Calculo que gastamos aproximadamente un tercio de lo que gastábamos antes".

La consolidación de proveedores puede ser una estrategia muy eficaz para que las empresas optimicen sus gastos de compra y gestión. A continuación, te planteamos tres preguntas rápidas que puedes utilizar cuando pienses en consolidar proveedores:

1. ¿Ofrece tu proveedor protección contra amenazas y un mayor rendimiento de las aplicaciones?
2. ¿Puedes gestionar tus aplicaciones y API desde una sola consola?
3. ¿Pueden los equipos de tu organización utilizar el mismo proveedor para una mayor eficiencia presupuestaria?

Estos consejos de consolidación que hemos mencionado permiten a las organizaciones reducir costos, simplificar la gestión de la cadena de suministro y reforzar las relaciones con proveedores clave.

chrono24

Conclusiones

El **75 %** de las empresas está contemplando la consolidación de proveedores

Chrono24 experimentó una reducción del **67 %** en los costos de seguridad e informáticos de su sitio web tras su consolidación con Cloudflare

La reducción del número de proveedores y la consolidación de los servicios permiten a las empresas **reducir los costos** y simplificar la gestión de la cadena de suministro

Optimiza los costos laborales y de infraestructura con la gestión automatizada de certificados

La implementación de configuraciones de seguridad en varios dominios y regiones geográficas puede ser un proceso costoso y largo para los equipos informáticos. Además, los costos ocultos pueden ser una dificultad adicional para las organizaciones a las que dan soporte, especialmente a las que se enfrentan a restricciones presupuestarias.

A menudo, esos costos ocultos se esconden en la gestión de certificados. Los certificados SSL/TLS conforman la identidad digital de una red. En promedio, la presencia web de una empresa puede requerir cientos o miles de certificados. Sin embargo, la gestión de estos certificados puede resultar costosa, ya que hay que sumar los gastos de mano de obra e infraestructura, e incluso la pérdida de ingresos que puede suponer una interrupción inesperada de los certificados.

SHOPYY, una plataforma de comercio electrónico, utiliza los servicios de Cloudflare para automatizar la gestión de certificados SSL, incluida la creación de claves privadas, protección, validación de dominios, emisión, renovación y reexpedición.

Inicialmente, SHOPYY utilizaba una herramienta gratuita de gestión de certificados que les proporcionaba certificados poco fiables y periodos de validez cortos. Como resultado, SHOPYY tuvo que contratar más empleados para supervisar la gestión de certificados y el proceso de renovación.

Con Cloudflare SSL for SaaS, SHOPYY confía el proceso de gestión de certificados a Cloudflare y solo necesita un empleado interno para mantener todo el proceso.

"El uso de los productos de Cloudflare ha reducido un 60 % los costos operativos y de mantenimiento", afirmó el fundador y director técnico, Yuanming Chen.

Las prácticas ineficaces de gestión de certificados también pueden afectar los ingresos debido a los certificados caducados. LendingTree, un mercado de préstamos en línea, utiliza los certificados TLS de Cloudflare para ahorrar dinero y evitar interrupciones.

"Tenemos miles de propiedades diferentes. A esa escala, era cuestión de tiempo que se nos pasara renovar un certificado", afirma John Turner, responsable de seguridad de las aplicaciones. "Con los certificados TLS de Cloudflare, que se renuevan automáticamente, ahorramos alrededor de 50 000 dólares al año, tanto en costos administrativos como en la pérdida de ingresos por interrupciones debidas a certificados caducados".

La incorporación de un sistema eficaz de gestión de certificados también puede ayudar a reasignar los recursos de forma adecuada. Fundada en Alemania, mogenius, una plataforma automatizada que implementa aplicaciones en la nube, automatiza sus prácticas de gestión de certificados con Cloudflare, lo que permite a la empresa dedicar más tiempo a desarrollar su actividad principal.

"Gestionar internamente todo lo que Cloudflare hace por nosotros nos llevaría al menos un 20 % de nuestro tiempo", afirma Jan Lepsky, cofundador y director de producción. "**Con Cloudflare, podemos centrarnos en optimizar el desarrollo en la nube y los canales de implementación para nuestros clientes".**

Delegar la gestión de certificados es crucial para las empresas que buscan evitar costos ocultos y garantizar operaciones empresariales eficientes. Las prácticas ineficaces, manuales o actualización de certificados implican elevados gastos de mano de obra e infraestructura, pérdida de ingresos debido a la interrupción de certificados caducados y una asignación de recursos poco rentable.

La implementación de la gestión de certificados con funciones como SSL for SaaS o certificaciones TLS permite a las empresas ahorrar costos significativos y mejorar sus resultados.

SHOPYY

lendingtree

mogenius®

Conclusiones

Cloudflare SSL for SaaS permitió a SHOPYY reducir un 60 % los costos operativos y de mantenimiento

El TLS de Cloudflare ayuda a LendingTree a ahorrar 50 000 dólares al año en costos administrativos y pérdida de ingresos

Cloudflare permite a mogenius automatizar sus prácticas de gestión de certificados, lo que le ha permitido aumentar un 20 % el tiempo que dedica a su actividad principal

Bloquea los ataques que aumentan los costos de tráfico

A medida que crece el uso de las API, también lo hace la superficie de ataque. Los bots maliciosos, los ataques DDoS y otras amenazas pueden poner en peligro las aplicaciones y las API. Los directivos y los responsables técnicos son los únicos que conocen la importancia del impacto que esos ataques pueden tener en su actividad.

Según una estimación, se ha descubierto que la falta de seguridad de las API cuesta a las empresas hasta 75 000 millones de dólares al año.

Estos ataques (de relleno de credenciales y DDoS) no solo pueden interrumpir el servicio para los usuarios legítimos, sino obligar a las organizaciones a cubrir el costo asociado al aumento de tráfico causado por el ataque de tráfico.

LendingTree gastaba grandes cantidades de dinero con su proveedor de soluciones de seguridad anterior que le cobraba tarifas de congestión durante los ataques DDoS. Este modelo no solo generaba elevadas cuotas por uso adicional, sino que acababa bloqueando el tráfico legítimo.

"Cada vez que lanzábamos un nuevo anuncio de televisión o una nueva campaña en las redes sociales, las solicitudes se disparaban por encima del límite arbitrario que nuestro proveedor nos hacía especificar, lo que significaba que el proveedor interpretaba el pico como un ataque DDoS y bloqueaba el tráfico legítimo", recuerda John Turner, responsable de seguridad de aplicaciones. "**No solo perdíamos esos clientes potenciales, sino también el dinero que gastábamos en llevarlos a nuestro sitio, y nuestro proveedor nos facturaba la 'protección DDoS'".**

Para resolver estas ineficiencias, LendingTree recurrió a las funciones de gestión de bots y limitación de velocidad de Cloudflare. **En 48 horas, un ataque a un punto final concreto de la API se redujo un 70 %, y en menos de cinco meses, LendingTree logró un ahorro de 250 000 dólares tras eliminar el abuso del punto final de la API.**

Cuando Flutter Entertainment, un holding de videojuegos en línea, se dio cuenta de que casi el 70-90 % de su tráfico era malicioso, necesitaba una solución para filtrar y bloquear los bots maliciosos. Tras implementar el servicio de gestión de bots de Cloudflare, **Flutter redujo un 90 % su tráfico malicioso y logró un ahorro de más de 2 millones de libras al año.**

Mediante la gestión de bots y la protección DDoS, las organizaciones pueden evitar los ataques y el abuso de las API, y reducir los gastos relacionados con los ataques. En el proceso de evaluación de proveedores de soluciones de seguridad, las organizaciones deben contemplar proveedores que:

- Utilicen el aprendizaje automático para establecer límites de velocidad basados en los datos de tráfico observados
- Trasciendan los límites de velocidad basados en la geografía y la ubicación IP, porque los ataques modernos pueden sortear fácilmente los límites de IP
- Garanticen que los desarrolladores dirigen todo el tráfico de las aplicaciones web y las API públicas a través de un WAF y una puerta de enlace de API
- Integren herramientas DDoS, WAF y puertas de enlace de API para ofrecer una protección por capas contra amenazas
- Reduzcan la latencia garantizando la protección en el lugar donde la empresa sirve su tráfico
- Ofrezcan una mitigación DDoS ilimitada para evitar el pago de tarifas por uso excesivo

La implementación de una estrategia de proveedor/seguridad adecuada puede suponer un ahorro de miles, si no millones, de dólares al año.

Flutter™

Conclusiones

Se ha descubierto que la falta de seguridad de las API cuesta a las empresas **hasta 75 000 millones de dólares al año**

La implementación de las herramientas de seguridad de aplicaciones adecuadas puede suponer un **ahorro de miles o millones de dólares al año**

Con la protección DDoS, LendingTree vio cómo un ataque a una API concreta se reducía en un 70 % en 48 horas, y ahorró 250 000 dólares en menos de cinco meses gracias a la detección de ataques

La gestión de bots de Cloudflare ayudó a Flutter a reducir un 90 % su tráfico malicioso y a ahorrar más de 2 millones de libras al año

Elimina tarifas y costos inesperados como el ancho de banda, la nube y las tarifas de salida

Muchos servicios de seguridad dependen de la nube, y muchos proveedores de nube cobran a las empresas por el almacenamiento y la informática. Además, a menudo exigen a las empresas que paguen tarifas de salida de datos, que son gastos asociados a la transferencia de datos desde el almacenamiento.

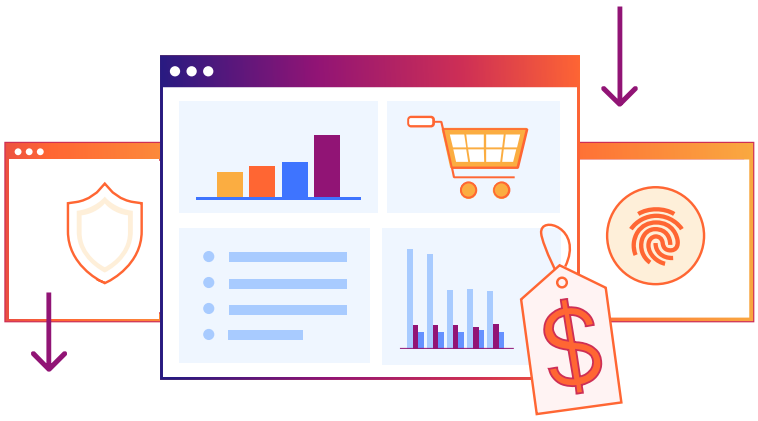
Las tarifas de salida se calculan en función de numerosos factores, como el nivel del cliente, el tipo de suscripción y el volumen de datos transferidos. Por estas razones, estas tarifas suelen ser difíciles de prever, lo que puede pasar factura a las organizaciones cuando se empiezan a añadir. De hecho, IDC estima que las tarifas de salida representan al menos el 6 % de los costos de almacenamiento en la nube.

Teniendo esto en cuenta, PagesJaunes, un directorio digital europeo y servicio de búsqueda local, decidió implementar la CDN de Cloudflare para ayudar a reducir las tarifas de ancho de banda y mejorar su gestión de caché y DNS.

"Rápidamente nos dimos cuenta de que el tráfico que absorbía la CDN de Cloudflare sobrecargaba menos nuestra infraestructura, mejorando así su resistencia", explica Loïc Troquet, responsable de Arquitectura, Rendimiento y Seguridad. "**La infraestructura de Solocal ya no necesitaba gestionar el 70 % del ancho de banda".**

Además, el ahorro de ancho de banda se traduce en ahorro de costos. Tras implementar los servicios de CDN, DNS, WAF y mitigación de DDoS de Cloudflare, la herramienta de aprendizaje y estudio en línea **Quizlet ahorró más de 10 TB de ancho de banda total cada día y redujo la factura de salida de la red de Google Cloud Services en más de un 50 %.**

La adopción de estrategias y prácticas de seguridad de las aplicaciones puede eliminar las tarifas de salida imprevistas.



PagesJaunes

Quizlet

Conclusiones

La adopción de estrategias de seguridad de las aplicaciones, como la elección del proveedor de CDN adecuado, puede eliminar las tarifas de salida inesperadas

Con la CDN de Cloudflare, PagesJaunes redujo un 70 % su ancho de banda

Quizlet utilizó los servicios de Cloudflare **para ahorrar más de 10 TB de ancho de banda total al día** y redujo la factura de salida de la red de Google Cloud Services en más de un 50 %, lo que se tradujo en un ahorro de miles de dólares al mes

Optimiza la seguridad de las aplicaciones y reduce costos con Cloudflare

Con Cloudflare, las organizaciones pueden incorporar estrategias de seguridad para las aplicaciones con el fin de aumentar la eficacia y optimizar los gastos. La cartera integrada de soluciones de seguridad de aplicaciones de Cloudflare reúne la mejor protección DDoS ilimitada de su clase, un firewall de aplicaciones web que detiene los ataques más avanzados, seguridad proactiva de API, gestión de bots respaldada por la información sobre amenazas y detección avanzada de ataques del lado del cliente.

¿Te interesa?

Contacta a Cloudflare hoy mismo

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/

BDES-5972.31MAYO2024