CLOUDFLARE®

Guía de supervivencia para el proveedor SaaS

Elementos fundamentales de rendimiento, seguridad y cifrado para aplicaciones en línea

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

Resumen ejecutivo

Se prevé que el mercado de SaaS experimente un crecimiento del 196 % desde el año 2016 hasta el 2020.[1] A medida que el mercado de SaaS sigue creciendo y se convierte en un componente integral de la infraestructura de negocios, la seguridad y el rendimiento siguen siendo los factores fundamentales, tanto para los proveedores SaaS como para sus clientes. Al tiempo que este crecimiento continúa, los proveedores Saas se enfrentan a una mayor competencia en el servicio de las aplicaciones más seguras y eficaces. Las aplicaciones de bajo rendimiento y aquellas vulnerables a ataques experimentarán de forma inevitable un impacto negativo en los ingresos, la satisfacción del usuario final, la reputación de la marca y la pérdida de clientes. Para un subconjunto importante de proveedores SaaS, el requisito de cifrado de dominios mnemónicos de marca de cliente conlleva la gestión manual del ciclo de vida de un SSL, lo que implica tiempos de implementación largos y gastos adicionales. Por otro lado, la creación de una solución interna automatizada y compleja desvía los recursos de ingeniería de sus competencias básicas.

La solución de rendimiento y seguridad de Cloudflare para proveedores SaaS protege y acelera las experiencias del proveedor SaaS, el cliente final y el visitante final. La red de distribución de contenido (CDN) global de 10 TBPS de Cloudflare, en combinación con el enrutamiento inteligente de Argo y las optimizaciones de rendimiento reducen a la mitad o más la latencia del visitante. La protección frente a DDoS avanzada Cloudflare, junto con la funcionalidad Rate Limiting y el cortafuegos de aplicaciones web (WAF) mitigan tanto los grandes ataques volumétricos como los ataques complejos dirigidos a las capas de aplicación, redes y transporte. Además, los proveedores SaaS tienen la opción de asegurar la transferencia de datos de cliente con una solución SSL fácil de implementar y completamente gestionada para los dominios mnemónicos personalizados.

Impactos empresariales de latencia y seguridad deficiente

Toda seguridad deficiente y latencia de aplicaciones SaaS puede dar lugar a malas experiencias de cliente, tasas de conversión y posición en buscadores, además de un aumento de pérdida de clientes e ingresos.

Los impactos del rendimiento y la disponibilidad en la contratación de aplicaciones SaaS

Cuando los clientes contratan sitios web, aplicaciones y API, demandan experiencias rápidas y con alto grado de disponibilidad. Cuando los activos en línea son latentes o no están disponibles, la contratación de las aplicaciones SaaS y las tasas de conversión sufren un gran efecto negativo.

Por ejemplo, Google afirmó que el aumento de latencia de un sitio tan pequeño como entre 100 y 400 milisegundos conlleva un impacto medible en el comportamiento del consumidor [1],Walmart sufrió una gran disminución de la tasa de conversión cuando el tiempo de carga del sitio aumentó tan solo unos segundos[2] y, del mismo modo, Amazon descubrió que por cada reducción de latencia de 100 milisegundos en su sitio se lograba un aumento de ingresos del 1 %.[3]

Los típicos problemas de rendimiento de aplicaciones SaaS están relacionados con factores internos que actúan contra la configuración de la aplicación o la infraestructura de hosting compartido de un proveedor de SaaS. Uno de estos factores es la distancia geográfica entre los visitantes y las ubicaciones de los servidores de origen de la aplicación SaaS; se estima que por cada 160 kilómetros de distancia, se produce una latencia de 0,82 milisegundos.[4] La distancia junto con un contenido estático pesado y sin optimizar aumenta en mayor medida la latencia para los visitantes.

Sin embargo, el rendimiento no solo depende de los servidores, las redes y las aplicaciones; también del tráfico estacionario o los picos de tráfico que pueden sobrecargar la infraestructura compartida aumentando la latencia de las aplicaciones o inhabilitándolas.

La carga lenta y la inhabilitación de las aplicaciones SaaS pueden provocar un impacto dramático en los ingresos, las tasas de conversión, las tasas de rebote, el posicionamiento en buscadores (SEO), la reputación de la marca, la satisfacción del cliente y los acuerdos de nivel de servicio (SLA).

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

El impacto de los ataques dirigidos a una aplicación SaaS

Ya se trate de un nuevo proveedor SaaS que se introduce en el mercado o una empresa de software establecida migrando una aplicación de local a la nube, es necesario tener en cuenta las implicaciones de seguridad para una aplicación siempre en línea.

La superficie de ataque para aplicaciones y servicios SaaS se hace más amplia, ya que están expuestos a la internet pública y, en muchos casos, las cargas de trabajo se extienden a través de infraestructuras compartidas. Entre los ejemplos de vectores de ataque para proveedores SaaS se incluyen los portales de inicio de sesión, los hosting y DNS compartidos, y las vulnerabilidades de aplicaciones complejas. Es importante señalar que muchos proveedores SaaS alojan múltiples aplicaciones de clientes dentro de una infraestructura compartida; cualquier fuga de datos, incidentes de fiabilidad, o ataques contra la infraestructura compartida podrían afectar negativamente a otros clientes.

Loa ataques específicos dirigidos a los vectores mencionados anteriormente incluyen ataques DDoS volumétricos y complejos, intentos de inicio de sesión por fuerza bruta, explotación de vulnerabilidades de aplicaciones y la interceptación de datos de clientes sin cifrar, todo ello dirigido a sitios web, aplicaciones y API a través de una variedad de dispositivos. El impacto empresarial de sufrir un ataque con éxito varía desde las interrupciones de servicio, la degradación de la marca y la pérdida de clientes hasta las grandes pérdidas de ingresos y el gasto por el control de daños.

En 2013, unos hackers se infiltraron en Adobe, obteniendo acceso a información de tarjetas de crédito y otros datos personales de 2,9 millones de sus clientes.[5] El responsable de seguridad de Adobe, Brad Arkin, conoce los riesgos de los negocios en línea y afirma que “Los ciberataques son una de las realidades más fatídicas de los negocios hoy en día”.

El 16 de octubre de 2016, Airbnb, Amazon.com, Netflix, The New York Times, Paypal, Pinterest, Reddit, Tumblr, Twitter, Verizon, Visa, The Wall Street Journal, Yelp, Zillow y otras muchas empresas sufrieron una caída durante un período prolongado debido a un ataque de la infame red de robots Mirai. Los blancos directos no incluyeron a las propias aplicaciones, sino a Dyn, el proveedor de servicios DNS compartido entre estos sitios web y aplicaciones. Dyn logró resolver el incidente al cabo de 11 horas, recuperando el funcionamiento normal de los servicios de todos los sitios web afectados.[6]

Elección entre el cifrado y los dominios mnemónicos personalizados

La adopción del cifrado SSL/TLS para organizaciones en línea se ha convertido en una buena práctica de seguridad y se está convirtiendo en un requisito debido a las presiones de grandes empresas de tecnología que pretenden crear un Internet más seguro. Por ejemplo, el navegador web Google Chrome empezó a etiquetar de forma visible los sitios web que no usan HTTPS como “No seguros” para sus usuarios a finales del 2016.[7] Además, actualmente Apple requiere ahora que todas las aplicaciones iOS tengan conexiones HTTPS antes de enviarlas a su tienda de aplicaciones.[8]

En los comienzos del SSL, las organizaciones en línea tenían que elegir entre el cifrado de tráfico sobre HTTPS u ofrecer experiencias que cumplieran las expectativas de rendimiento de los visitantes. Hasta hace unos años, el protocolo SSL suponía un aumento de la latencia, al tiempo que degradaba el rendimiento de los sitios web y las aplicaciones. Además, incluso si una organización tomaba la decisión de renunciar a prestaciones de mejora de seguridad, las dificultades operativas de implementar el SSL en aquel momento limitaban su extensa adopción. Con las actuales mejoras del SSL, como el desarrollo del HTTP/2 (sucesor del HTTP 1.1), la utilización de SSL para proteger el tráfico sobre HTTPS hoy en día supera el rendimiento del HTTP sin cifrar.

Del mismo modo que las organizaciones del pasado tenían que elegir entre cifrado o rendimiento, un subconjunto importante de proveedores SaaS actuales tienen que elegir entre el cifrado del tráfico de sus clientes y permitir que esos clientes usen su propio dominio mnemónico de marca, siendo ambos cruciales para los beneficios combinados de la óptima representación de la marca, la seguridad, la posición en buscadores y el mejor rendimiento posible.

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

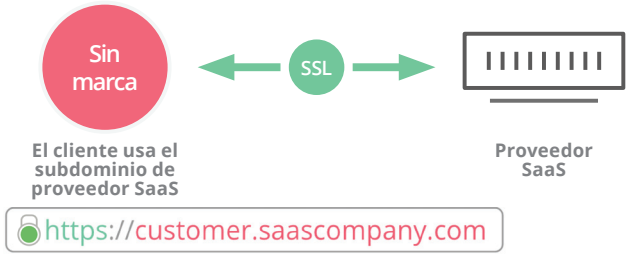
Este subconjunto de proveedores SaaS normalmente ofrece a sus clientes la posibilidad de crear activos en línea de cara al público, tales como páginas de destino, sitios web y portales de apoyo, entre otros. El proveedor SaaS normalmente aloja estos activos de cliente recién creados en un subdominio de su dominio principal, por ejemplo, la URL para un activo creado por un cliente de proveedor SaaS puede ser **rmpresacliente.proveedorsaas.com**, en lugar de una URL mnemónica como **empresacliente.com** o **asistencia.empresacliente.com**. Esto supone un desafío para los clientes porque sin un dominio mnemónico de marca, se produce una pérdida del reconocimiento de la marca, el posicionamiento de SEO y la confianza del visitante.

Los proveedores SaaS y sus clientes han superado los retos del dominio de marca mediante la inclusión del nombre de la empresa de la URL empresacliente.com o servicio.empresacliente.com en empresacliente.saasprovider.com. De este modo, el cliente puede usar su propio dominio mnemónico de marca; sin embargo, el proveedor SaaS pierde la capacidad de habilitar el SSL de forma sencilla y le resultará difícil gestionar un proceso de ciclo de vida de SSL completo. La gestión manual del proceso de ciclo de vida del SSL o intentar crear una solución interna para los clientes finales conllevará una gran pérdida de tiempo, esfuerzos manuales y coste añadido.

Existen tres escenarios en los que se pueden encontrar los proveedores SaaS al hacer frente a los desafíos mencionados:

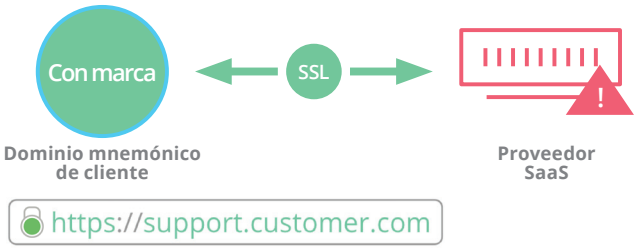
DOMINIO MNEMÓNICO DE MARCA PERO SIN CIFRAR

Los dominios mnemónicos personalizados sin SSL carecen de las ventajas del rendimiento de SSL y la transferencia segura de datos, haciéndolos vulnerables al espionaje y la modificación o inserción de contenido antes de llegar a los visitantes.



DOMINIO SIN MARCA PERO CIFRADO

Los dominios con el SSL activado a través de un proveedor SaaS carecen de un dominio mnemónico personalizado, lo que provoca la degradación de la marca y afecta negativamente al posicionamiento de SEO.

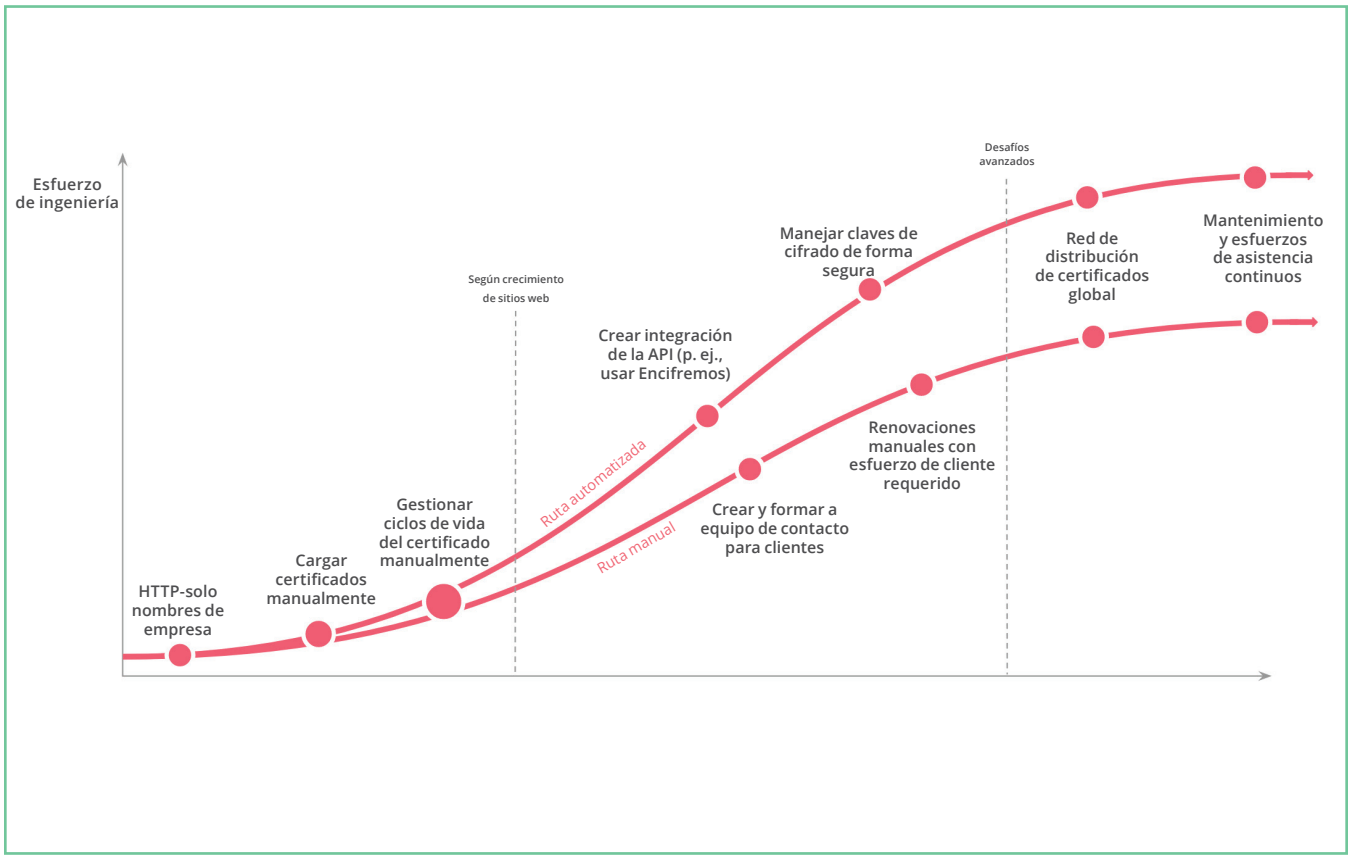


LA DIFICULTAD DEL ENFOQUE INTERNO

Los proveedores SaaS que quieren dominios mnemónicos de marca cifrados pueden gestionar los ciclos de vida de SSL manualmente, lo que resulta en largos tiempos de implementación, y gastos adicionales, o la creación de una compleja solución interna automatizada.

Es importante tener en cuenta las dificultades técnicas a las que se enfrentan los proveedores SaaS con la creación de su propia solución a fin de gestionar SSL para dominios de cliente. En el siguiente gráfico se muestra una hoja de ruta típica descrita por proveedores SaaS, que han intentado crear soluciones internas de SSL.

En la creación de una solución interna pueden tomarse dos rutas, aunque ninguna de las dos son idóneas. La primera ruta (superior) automatiza el proceso de SSL pero requiere grandes esfuerzos de ingeniería y conlleva desafíos complejos, y la segunda requiere esfuerzos manuales adecuados por parte de ambos; el proveedor SaaS y el cliente final.



Cloudflare como solución de mejora de disponibilidad, rendimiento y seguridad de aplicaciones SaaS

Cloudflare mejora la experiencia del usuario final de los sitios web, las aplicaciones y las API de los proveedores SaaS reduciendo la latencia y optimizando el rendimiento de entrega de contenido, al tiempo que amplía estos beneficios a los activos de Internet de los clientes finales.

Presencia disponible a nivel mundial

El epicentro de la solución de Cloudflare es la entrega de contenido (CDN) global mediante Anycast (difusión por proximidad) de más de 117 centros de datos a lo largo de 57 países, lo que aproxima el contenido de aplicaciones SaaS a los visitantes en cada región. Cloudflare también acciona más del 38 % de dominios DNS gestionados, administrando una de las mayores redes DNS autorizadas del mundo. Con un promedio de velocidad de pedido de pocos milisegundos, Cloudflare ofrece el rendimiento global más rápido de cualquier proveedor DNS gestionado.

Disponibilidad de aplicaciones a escala

A la infraestructura de DNS de alta disponibilidad y la red global mundial de Anycast™, se suma el Load Balancer de Cloudflare, que reduce la latencia mediante el equilibrio de carga de tráfico entre varios servidores y el enrutamiento de tráfico a la región geográfica más cercana. El Load Balancer incluye comprobaciones de estado con rápido Failover, para redirigir rápidamente a los visitantes y apartarlos de los errores. Además, el Load Balancer puede se puede utilizar en varios proveedores de nube o en la infraestructura local para mitigar el impacto de las interrupciones causadas por un único proveedor o servidor, al tiempo que evita el blocamiento del proveedor de nube.

Experiencias más rápidas para el visitante

La CDN de Cloudflare se ha desarrollado mediante optimizaciones avanzadas, que incluyen la minificación automática de HTML, CSS y JavaScript y la compresión de Gzip, lo que ahorra más de 20 % en el tamaño de archivos y recursos. Además, la imagen propia y las optimizaciones móviles llevan el rendimiento de la aplicación SaaS a otro nivel.

Mientras que Cloudflare entrega más del 10 % del tráfico de Internet internacional, analiza en tiempo real el estado y la fiabilidad auténticos de las rutas de red. El algoritmo de enrutamiento inteligente de Argo de Cloudflare usa esta información recopilada para dirigir tráfico a través de las rutas más rápidas disponibles, al tiempo que mantiene conexiones abiertas y seguras para eliminar la latencia proveniente de la configuración de conexión. El enrutamiento inteligente de Argo reduce la latencia de Internet en un promedio del 35 %, y los errores de conexión en un 27 %.

> "Para Crisp, la calidad del servicio maximizado y el tiempo de respuesta del servicio minimizado de Cloudflare representa una indiferenciación de la costosa infraestructura de red para las masas. No podemos vivir sin ello".
>
> crisp™ | **Valérian Saliou**
> Directora de tecnología de Crisp.

Protección de datos de cliente y aplicaciones SaaS

La solución de seguridad basada en la nube de Cloudflare protege los sitios web, las aplicaciones y las API de los proveedores SaaS, al tiempo que extiende sus beneficios a los activos de Internet del cliente final.

La red de difusión global de la red de Anycast de más de 117 centros de datos con 10 Tbps de rendimiento de Cloudflare es 10 veces superior al mayor ataque DDoS jamás registrado, lo que ofrece protección frente ataques dirigidos a las capas 3, 4 y 7 del modelo OSI. En combinación con la funcionalidad Rate Limiting y el cortafuegos de aplicaciones web (WAF), la solución de seguridad de Cloudflare también mitiga ataques complejos dirigidos a la capa de la aplicación. Y con el SSL para SaaS de Cloudflare, los proveedores SaaS y los clientes finales cuentan con comunicaciones cifradas para la protección frente a la intercepción de datos y la inyección de contenido malicioso, sin dejar de utilizar dominios mnemónicos personalizados.

Protección de datos sensibles de cliente

Puesto que las aplicaciones SaaS contienen cada vez más datos sensibles a nivel comercial y privado, es fundamental asegurar la protección frente los intentos de inicio de sesión por fuerza bruta, las fugas de datos y los ataques de intermediario.

La protección frente a estos tipos de ataques se puede lograr en primer lugar mediante el cortafuegos de aplicaciones web de Cloudflare (WAF), que mitiga los ataques complejos dirigidos a la capa de la aplicación. El WAF de Cloudflare incluye la protección contra las 10 principales vulnerabilidades OWASP de forma predeterminada, así como las vulnerabilidades de específicas de aplicaciones dirigidas a integraciones y lenguajes comunes, tales como: PHP, Magento, WordPress, Drupal y Atlassian entre otros. El WAF de Cloudflare permite que los proveedores SaaS creen conjuntos de reglas personalizadas sobre la marcha para la protección frente a vulnerabilidades y vectores de ataque recién descubiertos, al tiempo que propaga reglas a través de la red de Cloudflare's en menos de 30 segundos.

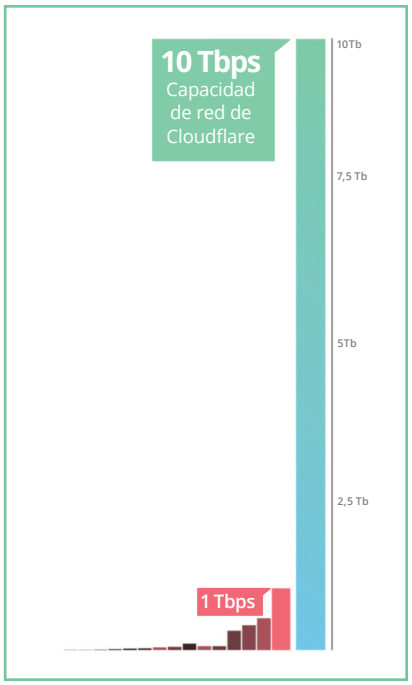
Trabajando en conjunto con la protección frente a DDoS de Cloudflare, el Rate Limiting ejerce un estricto control que bloquea a visitantes con tasas de solicitud sospechosa. Rate Limiting está equipado para reducir intentos de inicios de sesión de fuerza bruta, que pretenden acceder a áreas no autorizadas de una aplicación o sitio web; Rate Limiting restringe el número de solicitudes realizadas desde una dirección IP específica, a un extremo particular, durante un período de tiempo determinado.

> "La solución Cloudflare funciona a la perfección. Su equipo logró satisfacer todas nuestras necesidades y personalizaciones de forma casi inmediata".
>
> zendesk | **Amanda Kleha, directora general**
> Unidad de negocio en línea de Zendesk

El SSL para SaaS de Cloudflare ofrece la manera más eficaz para automatizar la gestión de los certificados SSL/TLS para dominios mnemónicos de nombre de empresa personalizados, asegurando la protección frente a la intercepción de datos a través de ataques de intermediario, o el espionaje de tráfico debido a conexiones sin cifrar.

Asegurar la disponibilidad mediante el bloqueo de tráfico malicioso

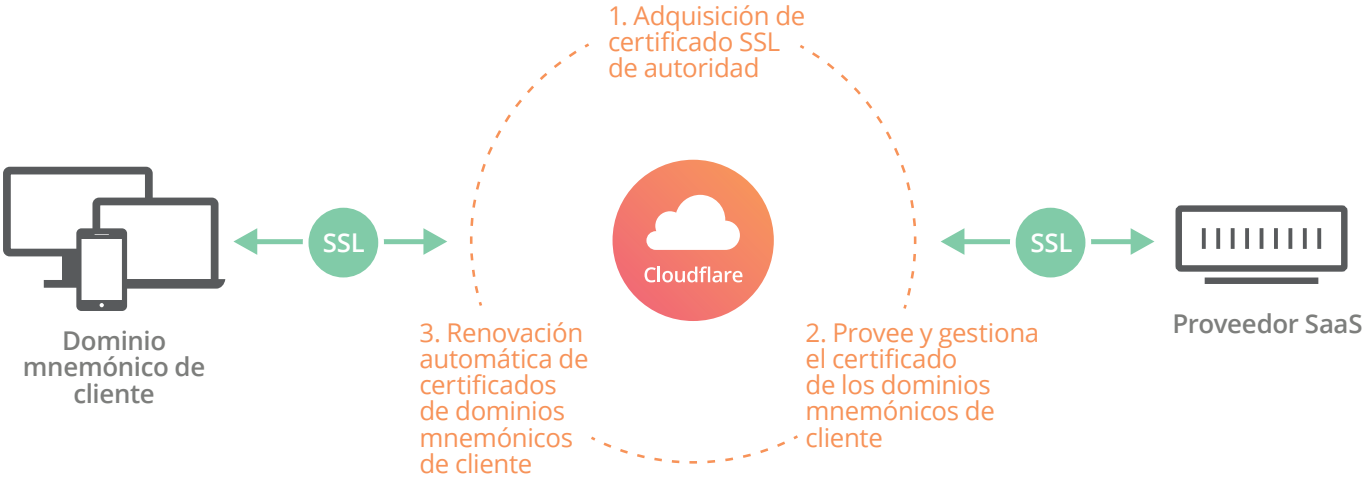
Si bien el robo o la pérdida de datos de cliente sensibles puede ser desastroso, ser la víctima de un ataque exitoso que intenta interrumpir la disponibilidad del servicio puede ser igual de destructivo. El pilar del Cloudflare es su red de entrega de contenido (CDN) global con más de 117 centros de datos a lo largo de 57 países. El rendimiento de la red completa de Cloudflare supera los 10 Tbps, que es aproximadamente 10 veces el tamaño del ataque DDoS más grande jamás registrado. Cualquier intento de ataque DDoS volumétrico dirigido a las capas 3, 4 y 7, se absorbe y distribuye uniformemente a través de la red de Cloudflare, evitando la inactividad y garantizando la máxima disponibilidad para los clientes de SaaS. La solución Rate Limiting Cloudflare trabaja en conjunto con la protección frente a DDoS, lo que permite un control exhaustivo para bloquear a visitantes con solicitudes sospechosas. Cuando una dirección IP específica supera los umbrales definidos, pueden bloquearse haciendo peticiones adicionales a un extremo específico, durante un período de tiempo asignado.



Una solución SSL automatizada para proveedores SaaS

El SSL para SaaS ofrece a los proveedores SaaS la capacidad de ampliar los beneficios de seguridad y rendimiento de la red de Cloudflare a los clientes finales con sus propios dominios mnemónicos personalizados. La solución SLL para SaaS de Cloudflare permite que los clientes sigan incorporando el nombre de la empresa de sus dominios

mnemónicos en el subdominio de los proveedores SaaS, ofreciendo las ventajas de una URL de marca, al tiempo que Cloudflare activa y gestiona el ciclo de vida de SSL completo para los proveedores SaaS y sus clientes. La activación de SSL en los dominios de los clientes aporta fiabilidad adicional a los visitantes, mejora el posicionamiento de SEO y desbloquea el moderno protocolo HTTP/2, lo que mejora notablemente la velocidad.



Experiencias de marca para el visitante

Los clientes de los proveedores SaaS que tienen la opción de usar su propio dominio mnemónico personalizado de marca pueden seguir haciéndolo, al tiempo que disfrutan de la ventaja añadida de un certificado SSL totalmente gestionado. Los dominios mnemónicos personalizados con el nombre de la empresa ofrecen a los clientes de SaaS una mejor visibilidad de la marca y posicionamiento de SEO, asegurando una mayor sensación de confianza en los visitantes de la aplicación o el sitio web.

Activos de clientes eficaces y seguros

El SSL para SaaS ofrece la posibilidad de añadir certificados SSL/TLS a los dominios mnemónicos personalizados con el nombre de la empresa. La transferencia de datos sobre HTTPS garantiza el transporte seguro de datos sensibles de clientes, la protección frente a ataques de intermediario y el espionaje de red. Con el SSL habilitado, se puede utilizar el protocolo HTTP/2 con incluso más mejoras de velocidad.

Gestión de ciclo de vida automatizado e implementaciones rápidas de SSL

Cloudflare gestiona el ciclo de vida completo de dominios mnemónicos personalizados con el nombre de la empresa de un proveedor SaaS, desde emisión y la protección de claves hasta la validación, emisión, renovación y reemisión del dominio. Tanto el proveedor de SaaS y el cliente final como el cliente final se evitan la carga de gestionar el ciclo de vida del SSL. Durante el proceso de emisión de SSL, Cloudflare transmite nuevas solicitudes de certificado y pone el HTTPS en línea en cuestión de minutos.

"Como ingeniero, no podría estar más contento de trabajar con Cloudflare".

UDACITY

Paul Bauer
Ingeniero de plataforma en Udacity

Conclusiones

La contratación de Cloudflare mejorará el rendimiento y la seguridad de su aplicación SaaS, al tiempo que implementa de forma sencilla el SSL para las URL mnemónicas con el nombre de la empresa para el cliente final. La configuración es sencilla y normalmente no se necesitan más de 5 minutos para ponerla en marcha. Consulte los planes, que varían desde el gratuito al Enterprise en www.cloudflare.com/es/plans/ y obtenga más información sobre Cloudflare para proveedores SaaS en www.cloudflare.com/es/saas/.

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

© 2017 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.