CLOUDFLARE®

Guia de sobrevivência de provedores de SaaS

Desempenho, segurança e criptografia essenciais para aplicativos online

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

Sumário executivo

Espera-se que o mercado de SaaS cresça até 196% entre 2016 e 2020.[1] Conforme o mercado de SaaS continua a crescer e a se transformar em parte integrante da infraestrutura empresarial, a segurança e o desempenho permanecem as maiores preocupações dos provedores de SaaS e seus clientes. E, conforme esse crescimento prossegue, os provedores de SaaS enfrentam uma concorrência maior para oferecer aos clientes os aplicativos mais seguros com o melhor desempenho. Aplicativos com mau desempenho ou vulneráveis a ataques inevitavelmente prejudicam a receita, o envolvimento do usuário final, a reputação da marca e as taxas de abandono. Para um grupo importante de provedores de SaaS, a necessidade de criptografar domínios personalizados com a marca do cliente significa gerenciar manualmente o ciclo de vida d SSL, resultando em tempos de implementação longos e custos indiretos. Opcionalmente, a criação de uma solução interna automática e complexa desvia os recursos de engenharia do foco nas competências principais.

A solução de desempenho e segurança da Cloudflare para provedores de SaaS protege e acelera a experiência do provedor de SaaS, do cliente final e do visitante final. A CDN (content delivery network, rede de transmissão de conteúdo) global de 10 Tbps da Cloudflare, aliada ao Argo Smart Routing, ao balanceamento de carga e à otimização de desempenho, reduz a latência do visitante à metade. A proteção avançada contra DDoS da Cloudflare, combinada ao Rate Limiting e o firewall de aplicativo web (WAF, web application firewall), mitiga grandes ataques volumétricos e ataques complexos direcionados às camadas de rede, transporte e aplicativos. Além disso, os provedores de SaaS têm a opção de proteger a transferência de dados do cliente com uma solução de SSL de fácil implementação e totalmente gerenciada para domínios personalizados.

Impactos comerciais de latência e segurança inadequada

A latência e a segurança inadequada dos aplicativos SaaS em qualquer formato podem levar a baixos níveis de experiência do cliente, taxas de conversão e classificações nos sistemas de busca, além de perdas de receita e taxas de abandono maiores.

Impactos do desempenho e da disponibilidade na interação com aplicativos SaaS

Os clientes exigem experiências rápidas e alta disponibilidade ao interagirem com sites, aplicativos e APIs. Quando os recursos online estão latentes ou indisponíveis, a interação e as taxas de conversão dos aplicativos SaaS são afetadas negativamente de forma perceptível.

Por exemplo, o Google informou que um aumento na latência do site de meros 100 a 400 milissegundos tem impacto mensurável no comportamento do consumidor[1]. O Walmart sofreu um forte declínio na taxa de conversão quando o tempo de carregamento do site aumentou apenas alguns segundos[2] e, da mesma forma, a Amazon constatou que cada 100 milissegundos de redução na latência no site resultou em 1% de aumento na receita.[3]

Os problemas típicos no desempenho de aplicativos SaaS estão relacionados a fatores internos que prejudicam a infraestrutura de hospedagem compartilhada ou a configuração de aplicativos dos provedores de SaaS. Um desses fatores é a distância geográfica entre a localização dos visitantes e a do servidor de origem do aplicativo SaaS; estima-se que para cada 160 km de distância, há um acréscimo de 0,82 milissegundos na latência.[4] A distância, combinada com conteúdo estático não otimizado e pesado, resulta em latências ainda maiores para os visitantes.

No entanto, o desempenho não é determinado somente por servidores, redes e aplicativos; pode depender também de tráfego de pico ou sazonal, que pode sobrecarregar infraestruturas compartilhadas, tornando os aplicativos latentes ou completamente indisponíveis.

Carregamento lento e aplicativos SaaS indisponíveis podem afetar dramaticamente receitas, taxas de conversão, taxas de rejeição, classificações em sistemas de busca (SEO), reputação da marca, satisfação do cliente e contratos de nível de serviço (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/

O impacto de ataques direcionados a aplicativos SaaS

Seja um novo provedor de SaaS chegando ao mercado ou uma empresa estabelecida de software migrando um aplicativo de local para a nuvem, as implicações de segurança de um aplicativo sempre online devem ser consideradas.

A superfície de ataques de aplicativos e serviços SaaS tornam-se mais amplas ao serem expostas à Internet pública e, em muitos casos, distribui cargas de trabalho entre infraestruturas compartilhadas. Entre os exemplos de vetores de ataque de provedores de SaaS estão portais de login, DNS e hospedagem compartilhada e vulnerabilidades de aplicativos complexos. É importante observar que muitos provedores de SaaS hospedam aplicativos de diversos clientes dentro de uma infraestrutura compartilhada. Quaisquer vazamentos de dados, incidentes de confiabilidade ou ataques contra essa infraestrutura compartilhada podem afetar negativamente outros clientes.

Ataques específicos direcionados aos vetores mencionados acima incluem ataques DDoS volumétricos e complexos, tentativas de login por força bruta, explorações de vulnerabilidades de aplicativos e a interceptação de dados não criptografados de clientes, todos direcionados a sites, aplicativos e APIs em uma grande variedade de dispositivos. O impacto comercial de sofrer um ataque bem sucedido varia desde interrupções nos serviços, degradação da marca e perda de clientes, até prejuízos maiores na receita e na despesa do controle de danos.

Em 2013, a Adobe foi infiltrada por hackers, que obtiveram acesso a informações de cartões de crédito, e outros dados pessoais, de 2,9 milhões de seus clientes.[5] O diretor de segurança da Adobe, Brad Arkin, reconhece os riscos das empresas online, comentando que os “ataques cibernéticos são uma das tristes realidades de fazer negócios atualmente”.

Em 16 de outubro de 2016, Airbnb, Amazon.com, Netflix, The New York Times, Paypal, Pinterest, Reddit, Tumblr, Twitter, Verizon, Visa, The Wall Street Journal, Yelp, Zillow e muitos outros, todos foram derrubados por um longo período, devido a um ataque do infame botnet Mirai. Os ataques diretos não foram direcionados aos aplicativos propriamente ditos, mas à Dyn, o provedor de serviços de DNS de todos esses sites e aplicativos. A Dyn conseguiu resolver o incidente 11 horas depois, normalizando os serviços de todos os sites afetados.[6]

Como escolher entre criptografia e domínios personalizados de marca

A adoção de criptografia SSL/TLS para organizações online tornou-se uma prática recomendada de segurança, e cada vez mais torna-se um requisito devido às pressões de grandes empresas de tecnologia que desejam construir uma Internet mais segura. Por exemplo, o navegador da Web Google Chrome começou a identificar visualmente os sites que não usam HTTPS como "Inseguros" para seus usuários, no fim de 2016.[7] Além disso, a Apple agora exige que todos os aplicativos do iOS tenham conexões HTTPS para poderem ser enviados à App Store.[8]

Nos primeiros anos do SSL, as organizações online tiveram que escolher entre tráfego criptografado por HTTPS ou a oferta de experiências ao visitante que atendessem às expectativas de desempenho. Até poucos anos atrás, o protocolo SSL causava aumentos na latência, ao mesmo tempo degradando o desempenho de sites e aplicativos. E mesmo se uma organização decidisse perder desempenho em nome da segurança, as dificuldades operacionais da implementação do SSL, naquela época, limitariam sua ampla adoção. Com as melhorias do SSL atual, como o desenvolvimento do HTTP/2 (sucessor do HTTP 1.1), a utilização de SSL para proteger tráfego por HTTPS atualmente excede o desempenho do HTTP não criptografado.

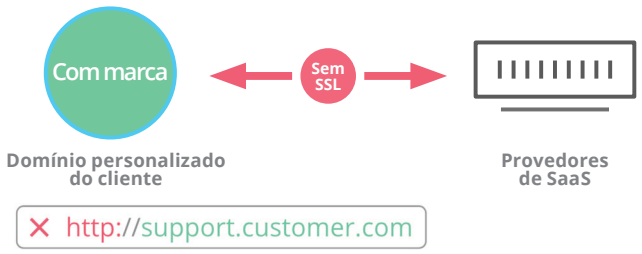
Da mesma forma que as organizações do passado tinham que optar entre criptografia ou desempenho, um subgrupo importante de provedores de SaaS atualmente precisa optar entre criptografar o tráfego de seus clientes e permitir que seus clientes tragam seus próprios domínios personalizados de marca. Ambos são cruciais para os benefícios combinados da representação adequada das marcas, segurança, classificações nos sistemas de busca e o melhor desempenho possível.

[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/

Esse subgrupo de provedores de SaaS oferece a seus clientes a possibilidade de criar recursos públicos online, como páginas de destino, sites, portais de atendimento e assim por diante. Normalmente o provedor de SaaS hospeda esses recursos recém criados em um subdomínio de seus domínios principais. Por exemplo, o URL de um recurso criado pelo cliente de um provedor de SaaS pode ser **empresacliente.provedorsaas.com**, em vez de **empresacliente.com** ou **atendimento.empresacliente.com**. Trata-se de um desafio para os clientes, porque sem um domínio personalizado há uma perda no reconhecimento da marca, nas classificações de SEO e na confiança do visitante.

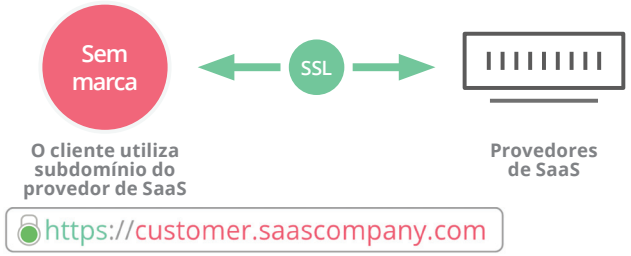
Os provedores de SaaS e seus clientes resolveram seus desafios de marca em domínios, associando com CNAME o URL empresacliente.com ou atendimento.empresacliente.com ao empresacliente.provedorsaas.com. Dessa forma, o cliente pode usar seu próprio domínio personalizado. No entanto, o provedor de SaaS perde a capacidade de ativar SSL com facilidade, e enfrenta o desafio de gerenciar todo um processo de vida útil do SSL. Gerenciar manualmente o processo de vida útil do SSL ou tentar criar uma solução interna para os clientes finais resultará em sérios comprometimentos de tempo, trabalho manual e custos.

Há três situações em que o provedor de SaaS pode se encontrar ao enfrentar os desafios descritos acima.



DOMÍNIO NÃO CRIPTOGRAFADO MAS PERSONALIZADO

Os domínios personalizados sem SSL não contam com os benefícios da transferência de dados com SSL e protegida, deixando-as vulneráveis ao acesso não autorizado e à modificação ou injeção de conteúdo, antes de chegarem aos visitantes.



DOMÍNIO CRIPTOGRAFADO MAS NÃO PERSONALIZADO

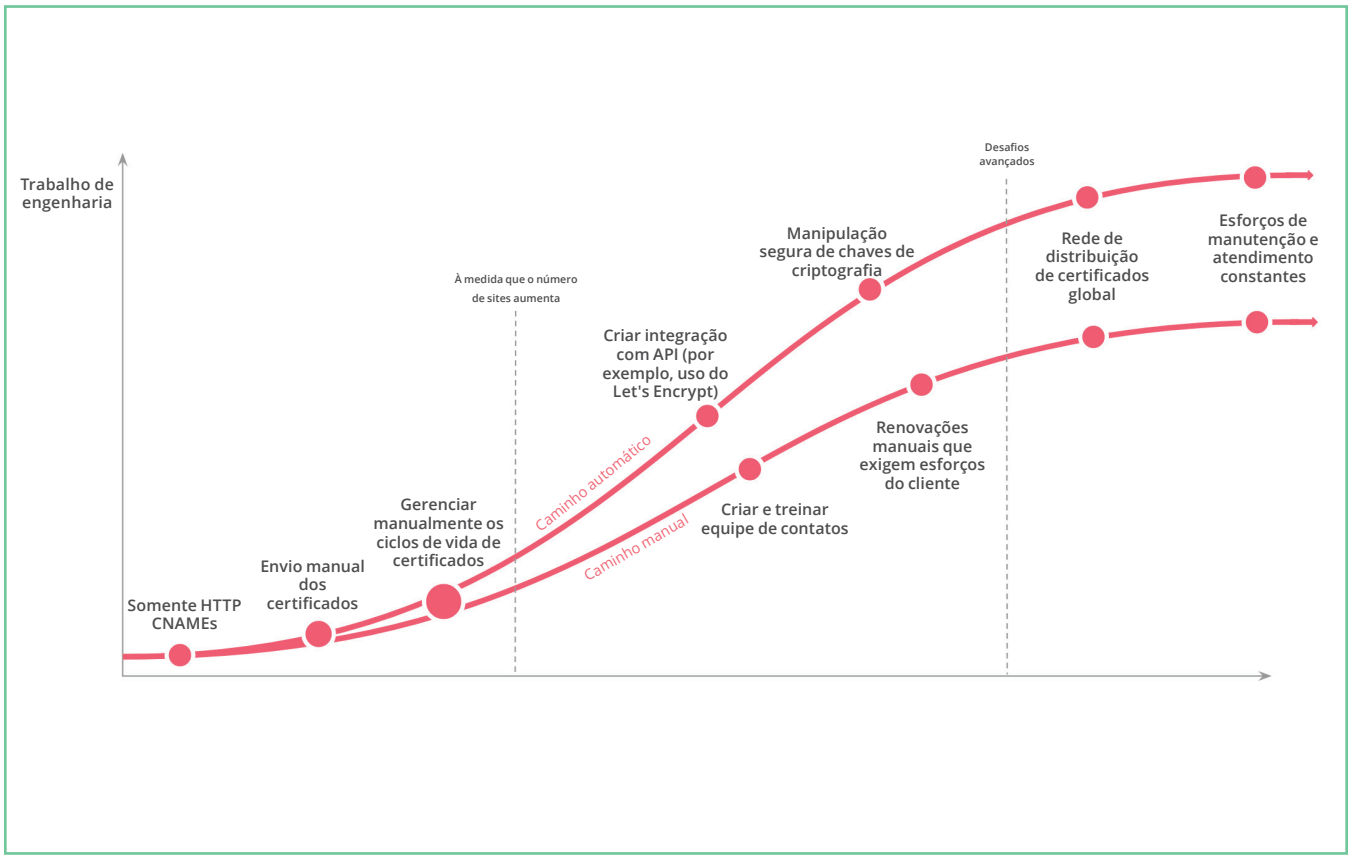
Domínios com SSL por meio de um provedor de SaaS não contam com os domínios personalizados, resultado em degradação da marca e classificações de SEO mais baixas.

O DIFÍCIL MÉTODO DA SOLUÇÃO INTERNA

Os provedores de SaaS que quiserem domínios personalizados e criptografados poderão gerenciar os ciclos de vida do SSL manualmente, resultando em tempos de implementação mais longos e custos indiretos.

É importante observar que os desafios técnicos que os provedores de SaaS enfrentam ao criarem suas próprias soluções de gerenciamento de SSL para domínios personalizados. O gráfico abaixo descreve um roteiro típico definidos por provedores de SaaS que tentaram criar soluções internas automáticas para SSL.

Há dois caminhos que podem ser utilizados na criação de uma solução interna e nenhum deles é ideal. O primeiro caminho (acima) automatiza o processo de SSL mas exibe esforços consideráveis de engenharia e implica em desafios complexos; e o segundo exige esforços manuais adequados tanto do provedor de SaaS como do cliente final.



Cloudflare para segurança, desempenho e disponibilidade de aplicativos SaaS

A Cloudflare melhora a experiência do usuário final nos sites, aplicativos e APIs do provedor de SaaS ao reduzir a latência e otimizar o desempenho da transmissão do conteúdo, enquanto estende esses benefícios aos ativos de Internet do cliente final.

Uma presença disponível globalmente

No coração da solução da Cloudflare há uma rede de distribuição de conteúdo (CDN, content distribution network) global de anycast de 117+5 centrais de dados espalhadas entre 57 países, levando conteúdo de aplicativos SaaS até mais próximo dos visitantes de todas a regiões. A Cloudflare mantém também mais de 38% dos domínios de DNS gerenciados, mantendo uma das maiores redes de DNS autenticado do mundo. Com uma média de poucos milissegundos de velocidade de consulta, a Cloudflare conta com o desempenho global mais veloz de qualquer provedor de DNS gerenciado.

Disponibilidade de aplicativos em grande escala

Expandindo a partir da infraestrutura de DNS com alta disponibilidade e a rede Anycast™ glocal da Cloudflare, o Balanceador de Carga da Cloudflare reduz a latência fazendo o balanceamento de carga entre diversos servidores e roteando o tráfego até à região geográfica mais próxima. O Balanceador de Carga inclui verificações de integridade com failover rápido, para rotear os visitantes rapidamente afastando-os de falhas. Além disso, o balanceamento de carga pode ser usado entre diversos provedores ou na infraestrutura local, para mitigar o impacto das interrupções causadas por um único provedor ou servidor, enquanto evita o aprisionamento tecnológico de nuvem.

Experiências mais rápidas para os visitantes

A CDN da Cloudflare é criada com otimizações avançadas, inclusive minificação automática de HTML, CSS e JavaScript e compressão Gzip, que economizam mais de 20% do tamanho dos arquivos e recursos. Além disso, otimizações proprietárias de imagens e conteúdo móvel melhoram ainda mais o desempenho do seu aplicativos SaaS.

Enquanto a Cloudflare fornece 10% do tráfego mundial de Internet, analisa, em tempo real, a integridade e a confiabilidade reais dos caminhos da rede. O algoritmo de roteamento inteligente do Argo da Cloudflare utiliza essas informações coletadas para direcionar o tráfego através dos caminhos mais rápidos disponíveis e mantém conexões abertas e seguras para eliminar a latência imposta pela configuração de conexão. O roteamento inteligente do Argo reduz a latência da Internet em mais 35%, em média, e os erros de conexão em até 27%.

> "Qualidade do atendimento maximizada e tempo de resposta do atendimento minimizado da Cloudflare para a Crisp. É a comoditização da dispendiosa infraestrutura de rede para as massas. Não podemos ficar sem ela."

crisp™

Valérian Saliou
Diretor de tecnologia da Crisp

Proteção de aplicativos SaaS e dos dados de clientes

A solução de segurança na nuvem da Cloudflare protege sites, aplicativos e APIs dos provedores de SaaS, enquanto estende os benefícios aos ativos de Internet dos clientes finais.

A rede Anycast global de mais de 117 centrais de dados da Cloudflare, com mais de 10 Tbps de taxa de transferência, é 10 vezes maior do que o maior ataque de DDoS já registrado, oferecendo proteção contra ataques que visam as camadas 3, 4 e 7 do modelo OSI. Combinada com Rate Limiting e firewall de aplicativo web (WAF), a solução de segurança da Cloudflare mitiga também ataques complexos direcionados à camada de aplicativos. E com Cloudflare SSL para SaaS, provedores de SaaS e clientes finais podem confiar que a comunicação criptografada vai proteger contra a interceptação de dados e a injeção de conteúdo malicioso, mantendo o uso dos domínios personalizados.

Proteção e segurança de dados sigilosos dos clientes

À medida que os aplicativos SaaS armazenam cada vez mais dados privados e comercialmente sigilosos, é de grande importância garantir a proteção contra tentativas de login por força bruta, vazamentos de dados e ataques de interceptação.

A proteção contra esses tipos de ataques pode ser conseguida por meio do firewall de aplicativo web (WAF) da Cloudflare, que mitiga ataques complexos direcionados à camada de aplicativos. O WAF da Cloudflare inclui, por padrão, a proteção contra as 10 principais vulnerabilidades do OWASP, assim como as vulnerabilidades específicas de aplicativos direcionadas a integrações e linguagens comuns, tais como: PHP, Magento, WordPress, Drupal, Atlassian e outros. O WAF da Cloudflare permite que os provedores de SaaS criem conjuntos de regras personalizados instantâneos para proteger contra vetores de ataque e vulnerabilidades recém descobertos, propagando as regras por toda a rede da Cloudflare em menos de 30 segundos.

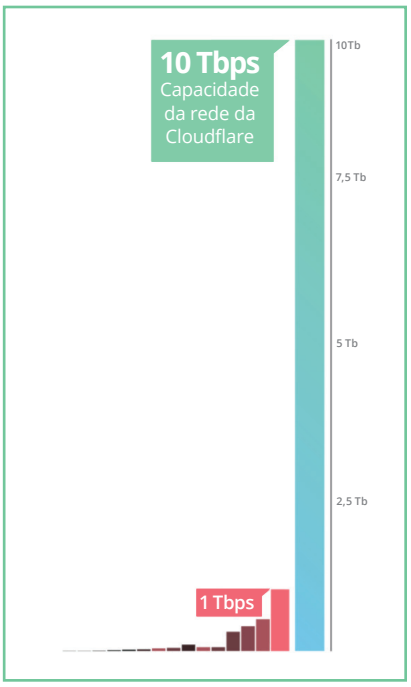
Trabalhando em conjunto com a proteção contra DDoS da Cloudflare, a Rate Limiting alcança um controle altamente detalhado para bloquear visitantes com taxas de solicitação suspeitas. A Rate Limiting está equipada para mitigar tentativas de login por força bruta, que buscam o acesso a áreas não autorizadas de um aplicativo ou site. A Rate Limiting restringe o número de solicitações feitas a partir de um IP específico a um ponto de extremidade, por um período determinado.

> "A solução da Cloudflare funciona sem contratempos. A equipe deles propagou todos os nossos requisitos e personalizações quase instantaneamente."
>
> zendesk | **Amanda Kleha**
> Gerente geral da unidade de negócios da Zendesk Online

O Cloudflare SSL para SaaS oferece a maneira mais eficiente de automatizar o gerenciamento de certificados SSL/TLS para domínios personalizados com CNAME, garantindo a proteção contra a ataques de interceptação ou o acesso não autorizado aos dados, devido a conexões não criptografadas.

Garantia de disponibilidade com bloqueio de tráfego malicioso

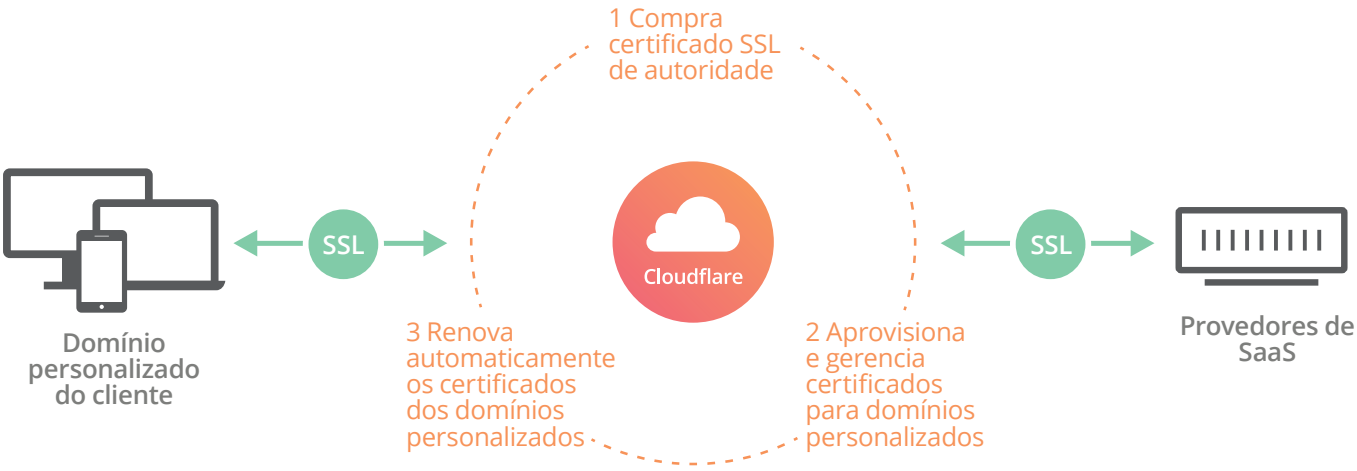
Embora o roubo ou a perda de dados sigilosos do cliente possam ser desastrosos, ser vítima de um ataque bem-sucedido que visa a interrupção do serviço também pode ser destrutivo. O backbone da Cloudflare é sua rede de distribuição de conteúdo (CDN) de mais de 117 centrais de dados, localizadas em 57 países. A taxa de transferência total da rede da Cloudflare excede os 10 Tbps, que é aproximadamente 10 vezes o tamanho do maior ataque de DDoS já registrado. Qualquer ataque volumétrico de DDoS direcionado às camadas 3, 4 e 7, é absorvido e distribuído homogeneamente por toda a rede da Cloudflare, impedindo quedas e garantindo a maior disponibilidade para clientes de SaaS. A solução Rate Limiting da Cloudflare funciona em conjunto com a proteção contra DDoS, permitindo o controle altamente detalhado para bloquear visitantes com solicitações suspeitas. Se um IP específico exceder limites predefinidos, poderá ser bloqueado e impedido de fazer outras solicitações a uma extremidade específica, por um período predeterminado.



Solução de SSL para provedores de SaaS

O SSL para SaaS oferece aos provedores de SaaS a possibilidade de ampliar os benefícios de segurança e desempenho da rede da Cloudflare aos clientes finais que trouxerem seus próprios domínios personalizados. O SSL da Cloudflare para soluções de SaaS permitem que os clientes continuem usando CNAME em seus domínios

personalizados para o subdomínio de um provedor de SaaS, oferecendo os benefícios de um URL de marca, enquanto a Cloudflare possibilita e gerencia todo o ciclo de vida de SSL para os provedores de SaaS e seus clientes. A habilitação do SSL nos domínios dos clientes traz mais confiança aos visitantes, melhora a SEO do cliente e libera o moderno protocolo HTTP/2, o que aumenta ainda mais a velocidade.



Experiências de marca para os visitantes

Os clientes de provedores de SaaS que têm a opção de trazer seus próprios domínios personalizados de marca podem continuar fazendo isso, desfrutando do benefício adicional de um certificado SSL totalmente gerenciado. Os domínios personalizados com CNAME oferecem ao clientes de SaaS melhor visibilidade de marca e classificações de SEO, assegurando ainda o sentimento de confiança dos visitantes do site ou do aplicativo.

Ativos dos clientes seguros e eficientes

SSL para SaaS permite e facilita a possibilidade de adicionar certificados SSL/TLS dedicados a domínio personalizado com CNAME. A transferência de dados por HTTPS garante o transporte seguro de dados sigilosos de clientes, protegendo contra ataques de interceptação e acesso não autorizado à rede. Com SSL ativado, o protocolo HTTP/2 para velocidades ainda maiores torna-se disponível.

Gerenciamento automático e ciclo de vida e implementações rápidas de SSL

A Cloudflare gerencia todo o ciclo de vida de SSL dos domínios personalizados dos clientes com CNAME de um provedor de SaaS, desde a emissão e a proteção e chaves privadas até a validação, emissão, renovação e reemissão de domínios. A responsabilidade do manuseio do ciclo de vida do SSL é removida tanto do provedor de SaaS como do cliente final. Durante o processo de emissão do SSL, a Cloudflare transmite novas solicitações de certificados e coloca o HTTPS online em apenas alguns minutos.

> "Como engenheiro, eu não poderia estar mais satisfeito em trabalhar com a Cloudflare."
>
> UDACITY | **Paul Bauer**
> Engenheiro de plataformas na Udacity

Conclusões

Inscreva-se na Cloudflare para melhorar o desempenho e a segurança do seu aplicativos SaaS e implementar SSL com facilidade para URLs personalizadas com CNAME. A configuração é fácil e normalmente entra em funcionamento em menos de cinco minutos. Consulte os planos, desde o Gratuito até o Corporativo, em www.cloudflare.com/br/plans/ e conheça mais sobre o Cloudflare para provedores de SaaS em www.cloudflare.com/br/saas/.

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