SaaS Application Performance, Security, and Encryption Essentials

The SaaS market is expected to grow by 196% from 2016 to 2020.[1] As the SaaS market continues to swell and become an integral component of business infrastructure, security and performance remains top-of-mind for both SaaS providers and their customers. As this growth continues, SaaS providers will face increased competition in delivering the most secure and performant applications to customers. Underperforming applications and those vulnerable to attack will inevitably experience a negative impact on revenue, end-user engagement, brand reputation, and customer churn. Beyond availability, SaaS customers expect that the applications they purchase are protected by SSL encryption and served from their own custom domain—rather than that of their provider. But doing so requires either significant investment (and ongoing maintenance) in automating the certificate lifecycle, or implementation of costly manual procedures that place a burden on customers to acquire, renew, and securely upload private keys and certificates.

Cloudflare's performance and security solution for SaaS providers protects and accelerates end customer experiences. Cloudflare's globally load balanced content delivery network (CDN), combined with Argo smart routing, load balancing, and performance optimizations, can reduce visitor latency by 2x or more. Cloudflare's 35 Tbps DDoS protection, combined with rate limiting and a web application firewall (WAF), mitigates both large volumetric attacks and complex attacks targeting layers 3, 4 and 7 of the OSI model. In addition, Cloudflare removes the burden of SSL lifecycle management for SaaS providers, facilitates serving their applications from the end-customers custom or vanity domain, and significantly improves performance over in-house solutions due to terminating SSL as physically close to web visitors as possible.

Secure Customer Data

Secure customer data across all custom "vanity" domains, with one-click setup in minutes and fully managed SSL/TLS

Improve Application Performance

Decrease application loading times by 2x or more for certain configurations with Cloudflare's Argo smart routing, load balancing, and content delivery network (CDN)

Availability at a Global Scale

Cloudflare's network of 200+ cities across 90+ countries, including 17 cities in mainland China ensures continuous enterprise-grade global availability even under stress

API Compatible

Extend all of the performance and security benefits of Cloudflare to SaaS application APIs

[1] https://motherboard.vice.com/en_us/article/google-chrome-shaming-http-unencrypted-websites-january

Zendesk Key Results

10x
improvement in
global response time

6x
improvement in targeted
content delivery time
by utilizing Cloudflare's
cookie-based key caching

> Cloudflare's solution just works. Their team accomplished all our requirements and customizations propagated near instantly. And, as an added bonus, their pricing is predictable and flat, regardless of how much our bandwidth usage grows.

AMANDA KLEHA
GM of Online Business Unit

zendesk

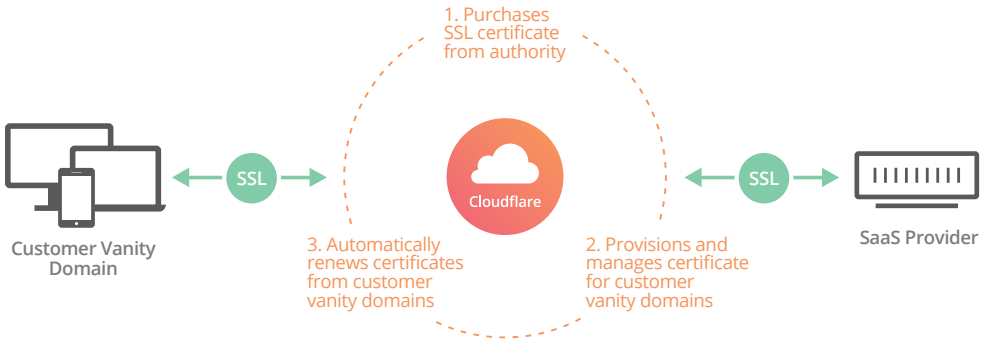
Ready to protect and accelerate your SaaS application?

Contact our Enterprise sales team:
1 (888) 99 FLARE
Enterprise@cloudflare.com
www.cloudflare.com/saas

EASY SSL FOR CUSTOMER VANITY DOMAINS

Cloudflare's SSL for SaaS offering allows SaaS providers to easily extend the security and performance benefits of Cloudflare's network to customers' custom or "vanity" hostnames. Enabling SSL brings additional trust to website and application visitors, improves customer SEO, and unlocks the modern HTTP/2 protocol, resulting in even greater speed improvements.

With a single API call, Cloudflare will provision individual SSL certificates for custom hostnames and be ready to serve traffic over HTTPS within just a few minutes. No action is required on the SaaS provider's customers' behalf, other than initially pointing their domain or subdomain in via CNAME. In addition, Cloudflare automatically handles certificate management and renewals—without any need to contact or involve the SaaS provider's customers.



COMPREHENSIVE SAAS SECURITY

Cloudflare's comprehensive security solution protects SaaS provider websites, applications, and APIs, while extending the benefits to end-customer Internet assets and their visitors. Cloudflare's 35 Tbps global Anycast network is 15x bigger than the largest DDoS attack ever recorded, offering protection against attacks targeting layers 3, 4, and 7 of the OSI model. Cloudflare absorbs traffic spikes and volumetric attacks, ensuring that unique customer assets, as well as neighboring customer assets served from a shared infrastructure, remain performant and available at all times. When combined with Rate Limiting and Web Application Firewall (WAF), Cloudflare's security solution mitigates complex attacks targeting the application layer, protecting against distributed denial-of-service, brute-force login, and API endpoint abuse.

FASTER SAAS EXPERIENCES

Cloudflare improves the end-user experience of SaaS provider websites, applications, and APIs by reducing latency and optimizing the performance of content delivery, while extending these benefits to end customer Internet assets. At the core of Cloudflare's solution is a global content delivery network (CDN) spanning 200+ cities in 90+ countries, including 17 cities in mainland China, bringing content closer to visitors of every region; additional CDN optimizations include auto-minification of HTML, CSS, and JavaScript, and Gzip compression, which save over 20% on the size of files and resources. Real-time network intelligence found in Argo's smart routing finds the fastest paths available, routing around congestion and maintaining open, secure connections to eliminate latency imposed by connection-setup. For additional availability with reductions in latency, Cloudflare Load Balancing distributes traffic across multiple servers, routing it to the closest geographic region, while rapidly avoiding failures.