CLOUDFLARE®

A SaaS Provider Survival Guide

Performance, Security, and Encryption Essentials for Online Applications

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

Executive Summary

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 SaaS provider, SaaS customer, and web visitor experiences. Cloudflare's 10 Tbps global content delivery network (CDN), combined with Argo smart routing, load balancing, and performance optimizations, reduces visitor latency by up to 2x. Cloudflare's advanced DDoS protection, combined with Rate Limiting and Web Application Firewall (WAF), mitigate both large volumetric and complex attacks which target network, transport, and application layers. In addition, SaaS providers have the option of securing the transfer of customer data with an easy-to-implement and fully managed SSL solution for custom vanity domains.

Impacts of SaaS Application Attack and Lack of Encryption

Customers demand fast and highly-available experiences when engaging with websites, applications, and APIs. When online assets are latent or unavailable, SaaS application engagement and conversion rates are negatively and noticeably impacted.

For example, Google reported that increased site latency as small as 100 - 400 milliseconds has a measurable impact on consumer behavior[1], Walmart found a sharp decrease in conversion rate as site load time increased by just a few seconds[2], and likewise, Amazon found that every 100 milliseconds of decreased latency on their site resulted in a 1% increase in revenue.[3]

SaaS application performance issues can result from a variety of factors, including capabilities of the hosting platform, design of the application, and connectivity to visitors on the Internet. One such factor is the geographic distance between visitors and SaaS application origin server locations; it's estimated that for every 100 miles of distance, there is an added 0.82 milliseconds of latency.[4] Distance combined with heavy, unoptimized static content results in even further latency for visitors.

However, performance is not only determined by servers, networks, and applications; it may also depend on spiky or seasonal traffic which can overload shared infrastructure, making applications latent or completely unavailable. Slow loading and unavailable SaaS applications can have a dramatic impact on revenues, conversion rates, bounce rates, search engine (SEO) rankings, brand reputation, customer satisfaction, and service level agreements (SLA).

Targeted SaaS Application Attacks

Whether it's a new SaaS provider entering the market or established software company migrating a once-local application into the cloud, the security implications for an always-online application must be taken into consideration.

The attack surface for SaaS applications and services becomes more vast as they're exposed to the public internet and, in many cases, span workloads across shared infrastructures or providers. Example attack vectors for SaaS providers include login portals, shared DNS and hosting, and complex application vulnerabilities. It's important to note that many SaaS providers host multiple client applications within a shared infrastructure; any data leaks, reliability incidents, or attacks against that shared infrastructure could negatively affect other customers.

Specific attacks which target the vectors mentioned above include volumetric DDoS attacks, complex brute force login attempts and application vulnerability exploits, as well as the interception of unencrypted customer data. The business impact of enduring a successful attack ranges from services disruptions, brand degradation, and customer churn, to major losses in revenue and the expense of damage control.

In 2013, Hackers infiltrated Adobe, gaining access to credit card information and other personal data from 2.9 million of its customers.[5] Adobe's Chief Security Officer, Brad Arkin, acknowledge the risks of online businesses, citing "Cyberattacks are one of the unfortunate realities of doing business today,".

On October 16th 2016, Airbnb, Amazon.com, Netflix, The New York Times, Paypal, Pinterest, Reddit, Tumblr, Twitter, Verizon, Visa, The Wall Street Journal, Yelp, Zillow and many others all went down for an extended period of time, due to an attack from the infamous Mirai botnet. Direct targets did not include the applications themselves but Dyn, the DNS service provider shared amongst these websites and applications. Dyn managed to resolve the incident after 11 hours, bringing the services of impacted websites back to normal.[6]

Choosing between Encryption and Custom Vanity Domains

The adoption of SSL/TLS encryption for online organizations has become a security best practice, and is increasingly becoming a requirement due to pressures by large technology companies aspiring to build a safer Internet. For example, the Google Chrome web browser began visibly labeling websites not using HTTPS as "Not Secure" for their users at the end of 2016.[7] In parallel, Mozilla's FireFox web browser began issuing even graver warnings to users who attempt to submit information info forms not protected by HTTPS.[8] While Apple now requires that all iOS applications use HTTPS connections before submitting them to their app store.[9]

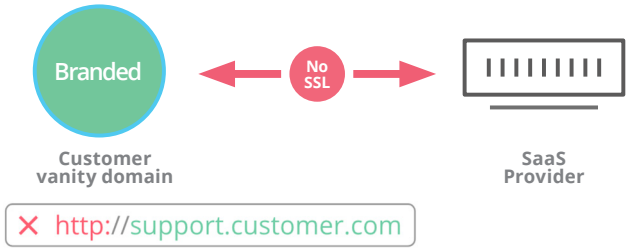
In the infancy of SSL, online organizations had to choose between encrypting traffic over HTTPS or offering visitor experiences which meet performance expectations. Up until a few years ago, the SSL protocol would cause increases in latency, while degrading website and application performance. And, even if an organization made the decision to forfeit performance for improved security, the operational difficulties of implementing SSL at that time limited its broad adoption. With modern SSL improvements, such as the development of HTTP/2 (the successor of HTTP 1.1), utilizing SSL to secure traffic over HTTPS today exceeds the performance of unencrypted HTTP.

In the same way that organizations of the past had to choose between encryption or performance, an important subset of SaaS providers today have to choose between encryption their customer's traffic and allowing those customers to bring their own branded vanity domain. Both of which are crucial for the combined benefits of proper brand representation, security, search engine rankings, and the best available performance.

This subset of SaaS provider typically offers their customers the ability to create public-facing online assets, such as landing pages, websites, support portals, and so forth. The SaaS provider typically hosts these newly created customer assets on a subdomain of their primary domain; for example, the URL for an asset created by a SaaS provider's customer may read **customercompany.saasprovider.com**, rather than a branded vanity URL such as **customercompany.com** or **support.customercompany.com**. This is a challenge for customers, because without a branded vanity domain, there is a loss in brand recognition, SEO rankings, and visitor trust.

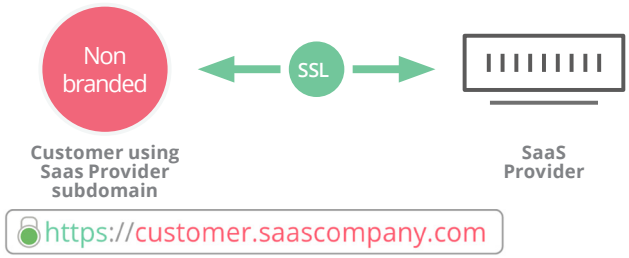
SaaS providers and their customers have overcome domain branding challenges by CNAME'ing the **customercompany.com** or **support.customercompany.com** URL to **customercompany.saasprovider.com.** In doing so, the customer is able to use their own branded vanity domain; however, the SaaS provider loses the ability to easily enable SSL and will find it challenging to manage an entire SSL lifecycle process. Manually managing the SSL lifecycle process or trying to build an in-house solution for end customers will result in serious time commitments, manual efforts, and cost.

There are three scenarios in which SaaS provider can find themselves in, when addressing the challenges stated above:



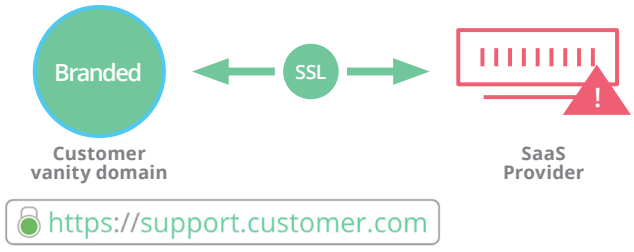
UNENCRYPTED BUT BRANDED VANITY DOMAIN

Custom vanity domains without SSL lack performance benefits of SSL and secure data transfer, making them vulnerable to snooping and content being modified or injected before reaching visitors.



ENCRYPTED BUT UNBRANDED DOMAIN

Domains which have SSL enabled through a SaaS provider lack a custom vanity domain, resulting in brand degradation and lower SEO rankings.

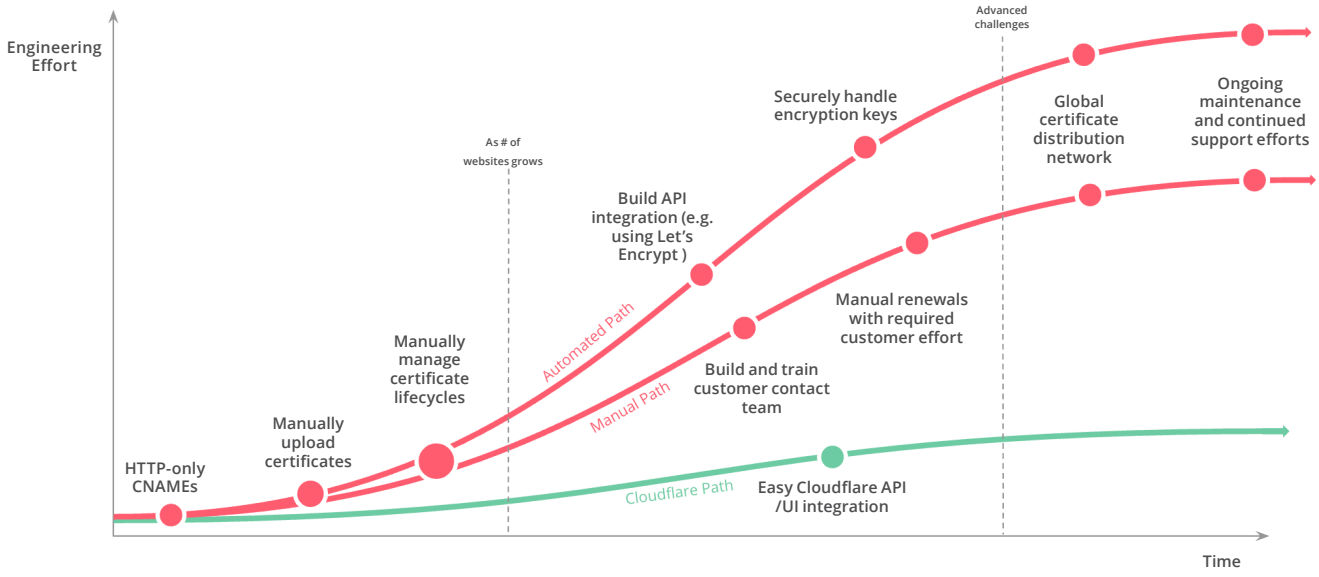


CHALLENGING IN-HOUSE APPROACH

SaaS providers who want encrypted branded vanity domains can either manually manage SSL lifecycles, resulting in long deployment times and overhead costs, or build a complex automated in-house solution.

It's important to note the technical challenges SaaS providers face when building their own solution to manage SSL for customer domains. The graphic below depicts a typical roadmap outlined by SaaS providers, who've attempted to build automated in-house SSL solutions.

There are two paths which can be taken in building an in-house solution, neither of which are ideal. The first (upper) path automates the SSL process but requires significant engineering efforts and comes with complex challenges; and the second (lower path), which requires adequate manual efforts by both the SaaS provider and end customer. In both cases, performance will suffer unless the certificates can be deployed on a large scale global distribution network and continued maintenance will always be required.



Cloudflare for SaaS Application Performance and Availability

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 through to end customer Internet assets.

A Globally Available Presence

At the core of Cloudflare's solution is a global Anycast content delivery network (CDN) of 115+ data centers spread across 57 countries, bringing SaaS application content closer to visitors in every region. Cloudflare also powers over 38% of managed DNS domains, running one of the largest authoritative DNS networks in the world. With an average of a few milliseconds query speed, Cloudflare has the fastest global performance of any managed DNS provider.[10]

Application Availability at Scale

Expanding on Cloudflare's highly available DNS infrastructure and global Anycast network, Cloudflare Load Balancing reduces latency by load balancing traffic across multiple servers and routing traffic to the closest geographic region. Load Balancing includes health checks with fast failover, to rapidly route visitors away from failures. In addition, Load Balancing can be used across multiple cloud providers or on-premise infrastructure to mitigate the impact of disruptions caused by a single provider or server, while avoiding cloud vendor lock-in.

Faster Visitor Experiences

Cloudflare's CDN is build with advanced optimizations, including auto-minification of HTML, CSS, and JavaScript, and Gzip compression, which save over 20% on the size of files and resources. In addition, proprietary image and mobile optimizations take the performance of your SaaS application even further.

While Cloudflare delivers over 10% of the world's Internet traffic, it's analyzing, in real-time, the true health and reliability of network paths. Cloudflare's Argo smart routing algorithm uses this collected information to route traffic across the fastest paths available, while maintaining open, secure connections to eliminate latency imposed by connection-setup. Argo smart routing reduces Internet latency on average by an additional 35%, and connection errors by 27%.

> "Cloudflare maximized service quality and minimized service response time for Crisp. It's a commoditization of expensive network infrastructure for the masses. We can't live without it."
>
> crisp™ | **Valérian Saliou**
> CTO of Crisp

Modern SaaS Application Security and Encryption

Cloudflare's cloud-based security solution protects SaaS provider websites, applications, and APIs, while extending the benefits through to end customer Internet assets.

Cloudflare's 10 Tbps global Anycast network is 10x bigger than the largest DDoS attack ever recorded, offering protection from attacks targeting layers 3, 4, and 7 of the OSI model. When combined with Rate Limiting and Web Application Firewall (WAF), Cloudflare's security solution also mitigates complex attacks targeting the application layer. 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. And with Cloudflare SSL for SaaS, SaaS providers and end customers can expect encrypted communications to protect against data interception and injection of malicious content, while continuing to use custom vanity domains.

Protecting and Securing Sensitive Customer Data

As SaaS applications increasingly hold more private and commercially-sensitive data, it's critical to ensure protection against brute force login attempts, data leaks, and man-in-the-middle attacks.

Protection from these types of attacks can be achieved first through Cloudflare's web application firewall (WAF), which mitigates complex attacks targeting the application layer. Cloudflare's WAF includes protection against the OWASP top 10 vulnerabilities by default, as well as application-specific vulnerabilities targeting common integrations and languages, such as: PHP, Magento, WordPress, Drupal, Atlassian, and more. Cloudflare's WAF allows SaaS providers to create custom rulesets on-the-fly to protect against newly discovered attack vectors and vulnerabilities, while propagating rules across Cloudflare's network in less than 30 seconds.

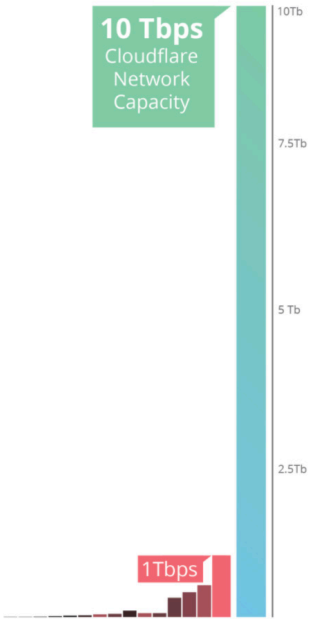
Working in conjunction with Cloudflare's DDoS Protection, Rate Limiting achieves a fine-grained control to block visitors with suspicious request rates. Rate Limiting is equipped to mitigate brute force logins attempts, which seek to access unauthorized areas of an application or website; rate Limiting restricts the number of requests made from a specific IP address, to a particular endpoint, for an specified amount of time.

> "Cloudflare's solution just works. Their team accomplished all our requirements and customizations propagated near instantly."
>
> zendesk | **Amanda Kleha GM**
> Zendesk Online Business Unit

Cloudflare SSL for SaaS offers the most efficient way to automate the management of SSL / TLS certificates for custom CNAME'd vanity domains. ensuring protection against data interception through man-in-the-middle attacks, or snooping on traffic, due to unencrypted connections.

Ensuring Availability by Blocking Malicious Traffic

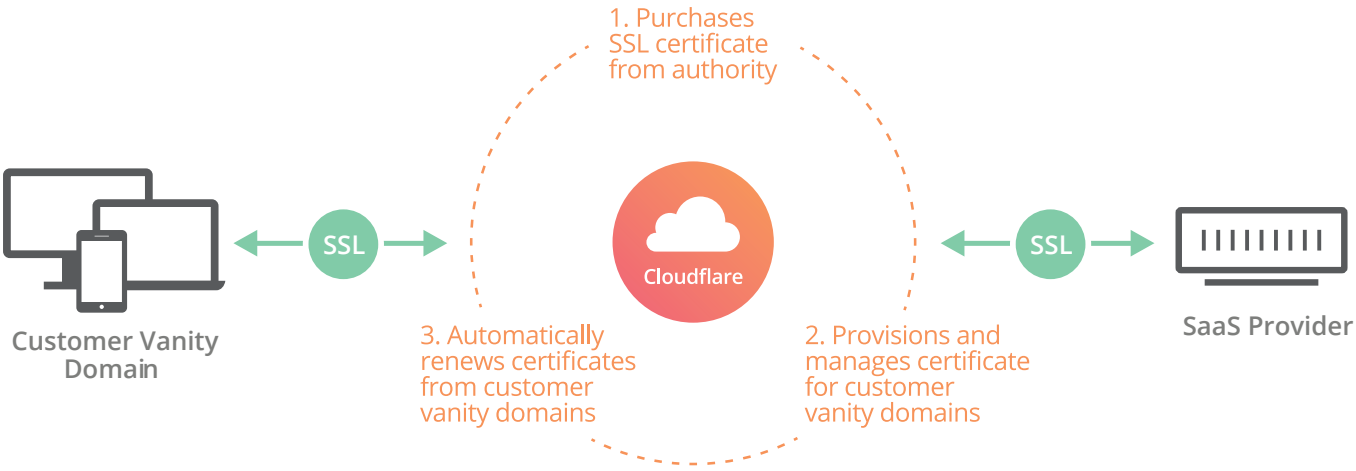
While theft or loss of sensitive customer data can be disastrous, being the victim of a successful attack which attempt to interrupt service availability can be just as destructive. Cloudflare's backbone is its global content delivery network (CDN) of 115+ data centers across 57 countries. Cloudflare's total network throughput exceeds 10 Tbps, which is roughly 10x the size of the largest DDoS attack ever recorded. Any attempted volumetric DDoS attack targeting layers 3, 4, and 7, is absorbed and evenly distributed across Cloudflare's network, preventing downtime and ensuring the highest availability for SaaS customers. Cloudflare's Rate Limiting solution works in conjunction with DDoS protection, allowing for fine-grained control to block visitors with suspicious requests. When a specific IP exceeds defined thresholds, they can be blocked from making further requests to a specific endpoint, for an allotted period of time.



An Automated SSL Solution for SaaS Providers

SSL for SaaS offers SaaS providers the ability to extend the security and performance benefits of Cloudflare's network to end customers bringing their own custom vanity domains. Cloudflare's SSL for SaaS solution allows

customers to continue CNAME'ing their vanity domains to a SaaS providers subdomain, offering the benefits of a branded URL, while Cloudflare enables and manages the entire SSL lifecycle for SaaS providers and their customers. Enabling SSL on customer domains offers additional trust to visitors, improves SEO search rankings, and unlocks the modern HTTP/2 protocol, resulting in even greater speed improvements.



Branded Visitor Experiences

SaaS providers who offer their customers the option of bringing their own branded domain can continue to do so, while enjoying the added benefit of a fully managed SSL certificate. Custom domains offer SaaS customers better brand visibility and SEO rankings, while ensuring an ever greater sense of trust in website or application visitors.

Secure and Performant Customer Assets

SSL for SaaS allows for the seamless ability to add dedicated SSL/TLS certificates to comer vanity domains. Transferring data over HTTPS ensures the secure transport of sensitive customer data, protecting against man-in-the-middle attacks and network snooping. With SSL enabled, the HTTP/2 protocol for even greater speed improvements becomes available for use.

Automated Lifecycle Management and Rapid SSL Deployments

Cloudflare manages the entire SSL lifecycle for a SaaS provider's customer vanity domain, from private key creation / protection through domain validation, issuance, renewal, and reissuance. The burden of handling the SSL lifecycle is removed for both the SaaS provider and end customer. During the SSL issuance process, Cloudflare transmits new certificate requests and brings HTTPS online within minutes.

"I couldn't be happier as an engineer to work with Cloudflare."

UDACITY | **Paul Bauer**
Platform Engineer at Udacity

Takeaways

Sign up with Cloudflare to improve the performance and security of your SaaS application, while easily deploying SSL for end customer vanity domains. The set up is easy and usually takes less than 5 minutes to get up and running. Check out the plans, ranging from Free to Enterprise at www.cloudflare.com/plans/ and learn more about Cloudflare for SaaS providers at www.cloudflare.com/saas/.

[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] https://www.techwalla.com/articles/network-latency-milliseconds-per-mile
[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://motherboard.vice.com/en_us/article/google-chrome-shaming-http-unencrypted-websites-january
[8] https://blog.mozilla.org/security/2017/01/20/communicating-the-dangers-of-non-secure-http/
[9] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[10] https://www.dnsperf.com/

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