# Cloudflare & DigiCert Make SSL a 1-Click Experience

Cloudflare is determined to help build a better internet. Launched in 2010 at TechCrunch Disrupt as an easy way to protect websites from attacks, Cloudflare has evolved into an internet performance and security company that protects websites, APIs, applications, and pretty much anything connected to the internet, all while accelerating and improving performance.

Utilizing 150+ data centers in 74 countries around the world, Cloudflare protects internet applications against DDoS attacks, web application vulnerabilities and traffic from malicious bots, and in addition Cloudflare accelerates internet applications, improves mobile experiences and ensures availability. Cloudflare makes more than 8.5 million internet properties faster and safer, and serves more web traffic than Twitter, Amazon, Apple, Instagram, Bing, and Wikipedia combined.

CLOUDFLARE®

cloudflare.com
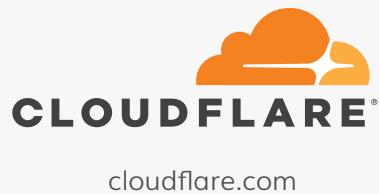
Industry: Technology

Region: Global

Customer Since: 2010

DigiCert Solutions:
REST API
Mass Issuance Certificate Platform
Certificate Issuance Speed

Challenge

Customers have shifted from seeing SSL as nice to have, to a non-negotiable part of running a business. Demand has been driven by industry changes, like Google Chrome visibly labeling websites as "Not Secure" if they don't use HTTPS. Unfortunately, there wasn't a fast and easy way for SaaS providers to deploy certificates by the millions for their customers.

Traditionally, websites purchased and installed certificates on their own, often requiring extra effort to make them function with CDNs and other service providers. Delivering secure connections was a prerequisite for the modern web, but getting there one site at a time wasn't fast enough.

Patrick and his team saw the opportunity to give all customers—and their customers' end users—SSL certificates for all their Cloudflare-protected domains. This would require a CA partner who could handle high-volume deployment and deliver the fastest issuance speeds.

digicert®

> "SSL for SaaS was a big opportunity and a big undertaking. We needed a CA partner that could handle issuing millions of certificates—quickly and reliably."

Patrick R. Donahue, Security Engineering Product Lead, Cloudflare

Solution

Working with DigiCert, Cloudflare made issuing and managing SSL certificates simple and fast. The result was SSL for SaaS—a solution which allows a SaaS provider's customers to use SSL with their custom vanity domain and receive all the other security and performance benefits of Cloudflare's network.
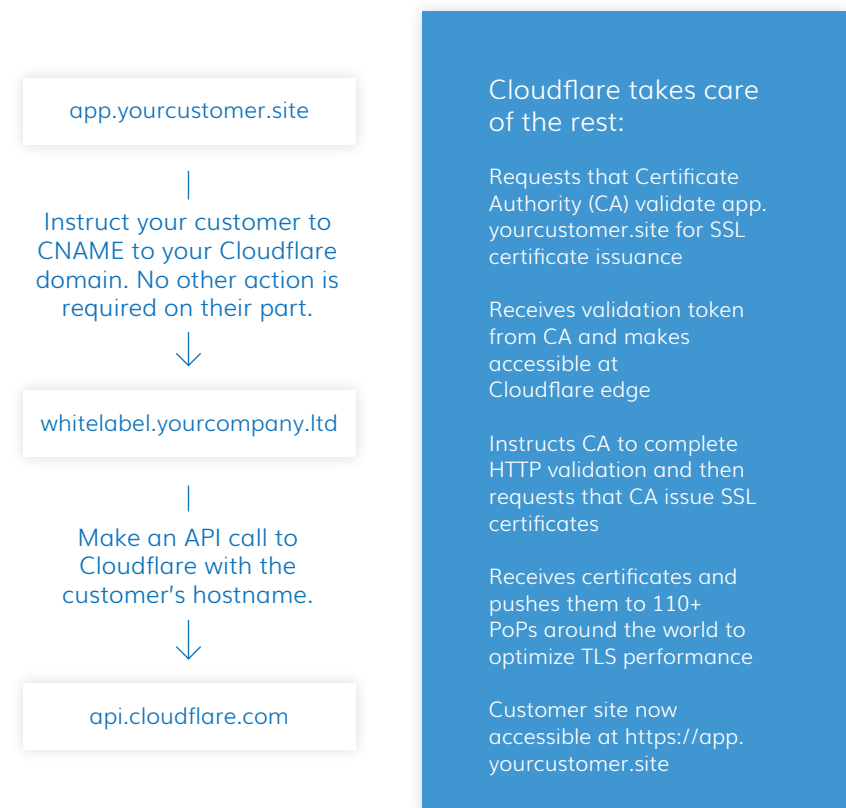
Before SSL for SaaS, there was no automated solution for SaaS companies to manage the SSL lifecycle for their customers. Providers were forced to build their own costly integration, or put in place manual processes which required their customers to obtain, upload, and renew SSL certificates.

> "One thing that gave us a lot of comfort in partnering with DigiCert was the fact that they had stress tested their systems to issue a billion certificates. It gave us confidence that, were we to hit that number, DigiCert's infrastructure could keep up."

Patrick R. Donahue, Security Engineering Product Lead, Cloudflare

Customers were required to make DNS changes, generate private keys and CSRs, send them to a CA for signing, upload the certificates, securely provide the key material, and repeat this process every time the certificate was up for renewal. This was highly disruptive to customers and end users, and resulted in low HTTPS adoption rates.

Now, customers need only make the DNS change. Cloudflare takes care of the rest by automating validation, issuance, and renewal using DigiCert APIs. Sending a single API call or making a few clicks in the Cloudflare dashboard, customers can issue and deploy a certificate worldwide in around 60 seconds. By the time the SaaS application is provisioned, Cloudflare has an SSL certificate ready at the edge.

app.yourcustomer.site

|

Instruct your customer to CNAME to your Cloudflare domain. No other action is required on their part.

↓

whitelabel.yourcompany.ltd

|

Make an API call to Cloudflare with the customer's hostname.

↓

api.cloudflare.com

Cloudflare takes care of the rest:

Requests that Certificate Authority (CA) validate app.yourcustomer.site for SSL certificate issuance

Receives validation token from CA and makes accessible at Cloudflare edge

Instructs CA to complete HTTP validation and then requests that CA issue SSL certificates

Receives certificates and pushes them to 110+ PoPs around the world to optimize TLS performance

Customer site now accessible at https://app.yourcustomer.site

The ability to scale up to millions—even billions—of certificates was one of the many reasons Cloudflare chose to partner with DigiCert. Patrick explained, "One thing that gave us a lot of comfort in partnering with DigiCert was the fact that they had stress tested their systems to issue a billion certificates. It gave us confidence that, if we were to hit that number, DigiCert's infrastructure could keep up."

Results

Using the DigiCert RESTful API, Cloudflare recently helped multiple large-enterprise customers issue hundreds of thousands of certificates to end users in just a few days. Doing this manually would have taken weeks of engineering time and been prone to human error. That's the value of SSL for SaaS—securing the internet a few clicks at a time.

"SaaS customers expect their site to be online and secured with HTTPS immediately after they complete the signup process. With DigiCert, we're able to issue most certificates and distribute them around the world 60 seconds after receiving the custom hostname from the SaaS provider."

Patrick R. Donahue, Security Engineering Product Lead, Cloudflare

For more information, contact an IoT expert 1.801.770.1736 or email iot@digicert.com.

Scaled to issue tens of millions of SSL certificates for SaaS providers

Helped customers drive HTTPS adoption to 100% by simplifying SSL issuance to a 1-step process

Cut issuance times from minutes or even hours to seconds (more than 90% of certificates are issued and deployed in under 60 seconds)