CLOUDFLARE

WHITEPAPER

Maximize the power of TLS — while minimizing your overhead

Content

TLS overview

Why do we need TLS?

It has become increasingly critical to handle personal data over the Internet with care. In certain jurisdictions, data privacy is considered a fundamental human right, and more data protection regulations are being implemented worldwide. But beyond that, ensuring that Internet traffic is private and secure is just the right thing to do.

Transport Layer Security (TLS) is the communications backbone of privacy and data security. It allows users to browse the Internet privately, without exposing their credit card information or other personal and sensitive information. At Cloudflare, we believe in helping to build a better Internet, and that includes protecting the privacy of Internet users with protocols such as TLS.

What happens when we don’t get TLS right?

TLS certification validates that a website or application accomplishes three main components:

- **Encryption:** hides the data being transferred from third parties
- **Authentication:** ensures that parties exchanging data are who they claim to be
- **Integrity:** verifies that the data has not been forged or tampered with

When a TLS certificate expires, the gap in protection can have tangible consequences. For example:

- **Negative SEO impact:** Google and other search engines prioritize websites with TLS/SSL certificates (https://) higher in search results. This can make it harder to compete against HTTPS websites if you are only running HTTP.
- **Warnings deterring visitors:** Browsers warn users when they attempt to access a website that does not have a valid TLS certificate – many users will understandably be concerned about privacy risks if they see a browser warning, and may be dissuaded from visiting your website. Less traffic means fewer conversions and downstream impacts to brand awareness and revenue.
- **Breaches and fines:** Having expired TLS certificates also increases the risk of data breaches. Today, there are numerous regulations governing data privacy for different regions across the globe, and they usually either require or imply the need for encryption. If an organization suffers a data breach and did not have proper encryption in place at the time, they could be subject to fines or other regulatory repercussions.

All of these possible consequences demonstrate how essential TLS is for both your application performance and bottom line.

When TLS breaks, trust is often damaged with end-users, customers, partners, and other stakeholders. The good news is that the consequences are simple to avoid — this guide details how.

Did you know?

The Internet is moving more and more towards certificates with a lifecycle of 90 days, departing from the previous lifecycle of 398 days. That means you will have to renew your certificates about 3.5x more frequently than before! [1]

Top four TLS challenges today

1) Streamlining TLS management

At Cloudflare, when we talk to our customers about TLS certificate lifecycle management, they frequently tell us it is a manual and arduous process. Their organization's process of tracking renewals may be as tedious as documenting renewals in a frequently-updated spreadsheet. A lack of tooling and automation to address TLS certificate renewal can be frustrating for the security professional or team that has to renew certificates manually.

2) Ensuring compliance

As mentioned previously, encryption is a foundational component of keeping an application private and compliant. And as we in the IT world try to keep our applications secure, certificate issuance requirements become stricter. Cryptographic best practices such as recommended key lengths or hash algorithms constantly evolve as our knowledge of how to strengthen them evolves.

Many Zero Trust frameworks, such as NIST SP 800-207 (for the private sector) and NIST SP 800-53 (for the public sector), directly call out encryption as a vital component of a comprehensive Zero Trust strategy. And although most data privacy regulations do not directly call out encryption as a requirement, they do imply its necessity with phrases like “appropriate security measures.”

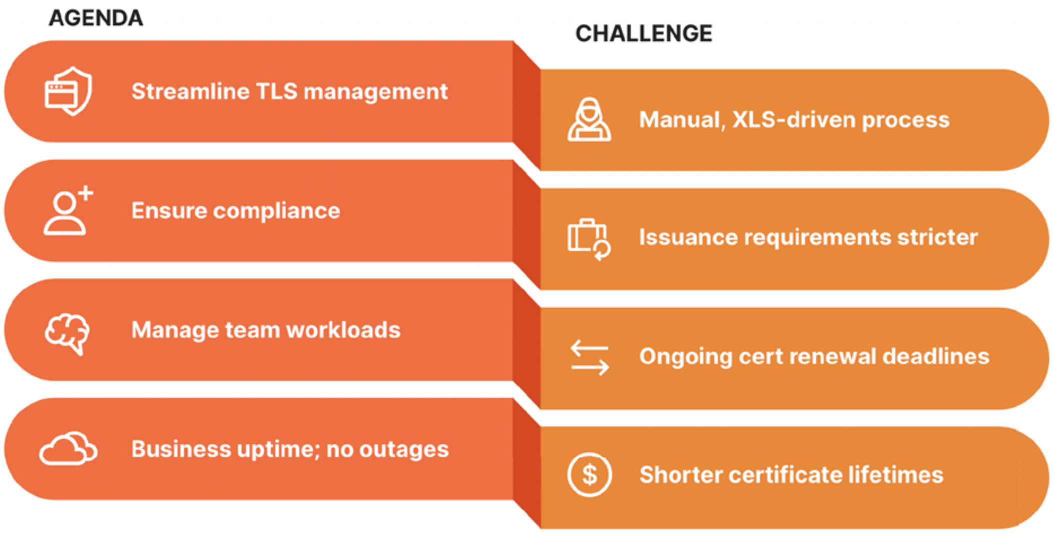
However, it can be difficult for teams to stay abreast of the most recent standards for keeping data secure and private.

3) Managing team workloads

IT teams are already overburdened. Staying on top of certificate renewal deadlines can seem like a never-ending task. Keeping track of certificate renewal deadlines is becoming more time-consuming, especially as renewal periods are becoming shorter and shorter.

4) Keeping websites and apps in front of customers

Missed certificate renewal deadlines can lower your website's search engine rankings, or if users come to your site from another source, they may not continue on after seeing a browser security warning. Keeping up with certificate renewals is one important way to help ensure your organization's web applications stay in front of customers and users.


AGENDA
CHALLENGE
Streamline TLS management
Manual, XLS-driven process
Ensure compliance
Issuance requirements stricter
Manage team workloads
Ongoing cert renewal deadlines
Business uptime; no outages
Shorter certificate lifetimes

How Cloudflare solves key TLS challenges

In the following section, you'll learn some of the primary use cases for customers using Cloudflare to encrypt their data and traffic with TLS:

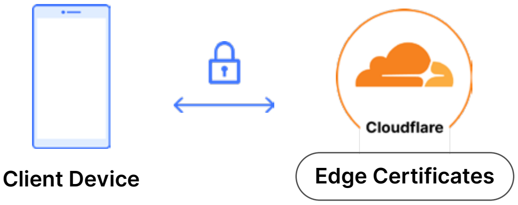
- Common use cases:
  - Securing edge connections
  - Securing origin connections with mutual TLS (mTLS)
- Emerging use cases for mTLS:
  - Authenticating clients and devices
  - Enhancing Zero Trust access
  - Protecting APIs
  - Protecting IoT traffic

These are likely some of the most common scenarios you will encounter in your own work with content delivery network (CDN) deployments, including Cloudflare deployments..

Securing edge connections

Securing connections between a web visitor / client device protects user privacy when browsing — and is therefore foundational to the Cloudflare mission.

As you're implementing this for visitors to your domains, consider these options for securing edge connections with Cloudflare TLS.



Reducing certificate management overhead using Cloudflare

Use basic TLS certs and have Cloudflare manage issuance and renewal
Cloudflare offers free certificates for millions and millions of domains across the Internet. This Universal SSL service is included for all domains that are onboarded behind the Cloudflare proxy, and serves as a "one size fits most" solution used by personal websites and Fortune 500 organizations alike.

This is an ideal free option for organizations looking to reduce management overhead. Our scalable infrastructure can handle more than 50 million certificates (as of May 2023), and we can serve TLS certificates from each one of our data centers, closer to your users — bringing down latency. Cloudflare also handles domain control validation and issues and renews the certificates on your behalf. Once your domains are onboarded to Cloudflare, Cloudflare automatically handles certificate validation, issuance, and renewal — with no additional action needed on your part.

Universal SSL from Cloudflare is ideal if you:

- Need a free option that reduces certificate lifecycle management overhead (especially if you have limited staff, budget, or time); and
- Do not have unique needs for custom certificates, or do not need to select which Certificate Authorities (CAs) to accept.

Customize your TLS deployment while reducing management overhead

Many organizations behind the Cloudflare proxy find that they love the certificate lifecycle management that Universal SSL offers. However, for those that need more customization due to organizational or regulatory requirements — but still want the benefit of reducing management overhead, Cloudflare offers Advanced Certificates Manager.

Advanced Certificates Manager is ideal if you:

- Have specific requirements for what hostnames need to be on the certificate;
- Prefer to reduce the validity period down from the default 90 days (for example, some organizations with higher security requirements may want their certificate to only be valid for 2-week cycles); and/or
- Need more flexibility on which CA you'd prefer to use. (See here for a current list of Cloudflare's CA partners.)

Automatically issue TLS certificates for new hostnames

As organizations grow, it's very likely that they will need new hostnames and new web properties — such as new product lines or localized versions of their websites. When you use advanced certificates, you will always need to inform us which hostnames are on the certificate. But there may be times when you want to tell Cloudflare, "I want you to issue TLS certificates for every new hostname I put behind the Cloudflare proxy." In this scenario, automatically issuing TLS certificates for any new hostnames, with a service we call Total TLS, can be a more effective option for rapidly growing organizations.

With Total TLS, automatic issuance with each new hostname created means no security and privacy gaps for your newly created domains. It also allows you to forgo the management overhead associated with issuing new TLS certs on top of thinking about everything that is involved in onboarding new subdomains.

Cloudflare will issue a certificate for each one of your hostnames with per-hostname certificates, and you can also choose the issuing CA for all the certs. As you create more subdomains, Cloudflare will always issue a certificate on your behalf — and renew them when their validity periods are up. Like with other Cloudflare-managed certificate models, we will renew your certs on your behalf to your security specifications and in accordance with your preferred CA and validity periods.

Total TLS is ideal if you:

- Are managing websites/applications for a rapidly-growing organization;
- Will need TLS certificates for multiple web properties — such as hosting information on new product lines, services, or localized (translated) versions of your websites;
- Do not have the internal resources to manage the overhead associated with issuing TLS certs on top of onboarding new subdomains; and/or
- Want to ensure there are no security or privacy gaps for any newly created domains.

Automatically back up certificates

In addition to selecting the right solution for reducing certificate management, it is crucial to **ensure security redundancy for your TLS certificates**. An event like a key compromise or CA revocation could result in a need to immediately re-issue certificates — given that your current certificates will be compromised. For example, in 2021, one of the most popular CAs underwent a revocation, during which this CA revoked a few thousand certificates. Or, such as in the instance of the Heartbleed CVE in 2014, certificates could be compromised by a vulnerability or other security issue.

As soon as a CA revocation starts, organizations and individuals only have 24 hours to issue and deploy replacement certs before all of their certs are marked as revoked. At Cloudflare, we manage tens of millions of certs. If one of the CAs we support underwent a revocation or if their certs were compromised, we would have to re-issue tens of millions of certs at once. Even though Cloudflare's pipeline is able to handle that surge of demand, we still need to work with CAs to reissue certs, and on top of that, customers may need to upload domain control validation records to Cloudflare manually depending on how they manage their TLS certificates.

It is crucial to have a contingency plan for a disaster scenario like a revocation or a vulnerability. If a CA revocation does happen again, backup certs mean that you can instantly switch over to a valid cert, preventing the possibility of a gap in your TLS protection. This will mitigate any website downtime, ensure your websites will stay secure, and provide continuity for end users.

To implement this, we recommend **automatically backing up certificates with Cloudflare** (enabled by default), which are issued using a separate encryption key and a different CA than the primary certificate. This allows for quick rollover in the event of a key compromise or CA revocation. And like other Cloudflare-managed certificate scenarios, we will manage issuance and renewals for you.

Did you know?

About 91% of web traffic on Google originating from the United States is encrypted [2]. That percentage is higher for the other top 9 countries Google sees traffic from, including:

- United Kingdom - 93%
- Germany - 94%
- Brazil - 95%
- Mexico - 96%
- Japan - 96%
- Indonesia - 96%
- Netherlands - 96%
- India - 97%
- Belgium - 99%

Self-managing your certificates

Bring your own certificates

There are a number of reasons why organizations may want to use their own custom certificates issued by the CA of their choice. For example, if you want to use extended validation (EV) or organizational validation (OV), you can obtain a cert from the CA of your choice and upload the certificate and private key to Cloudflare. Our users who have a preferred CA or a pre-existing relationship with a CA not in our ecosystem prefer this option, as this deployment model allows you to obtain your certificate at the external CA and upload it to Cloudflare, where you will receive all the benefits of serving certificates at the edge.

Handle renewals while Cloudflare retains your private key

If you want to use custom certs, you can get a certificate from the CA of your choice, and ask Cloudflare to retain control of the private key. In this scenario, you'd only be responsible for the public certificate component. You can use a Certificate Signing Request (CSR) for certificate renewals, and handle the certificate renewal yourself and re-use the CSR for certificate renewals.

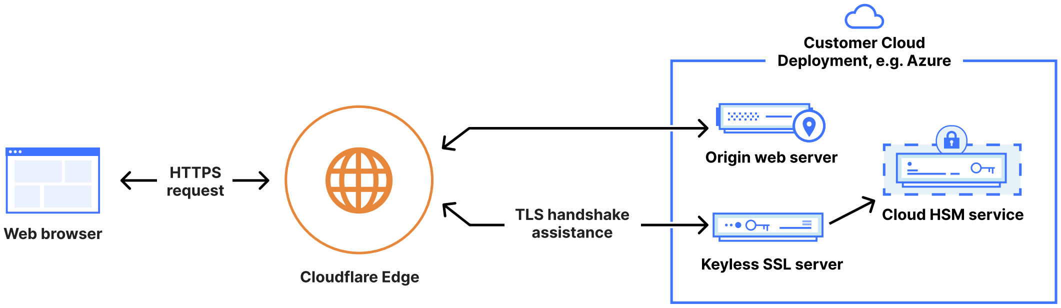
Handling renewals and allowing Cloudflare to retain your private key can be useful for organizations requiring a hands-on approach to cert management or that have specific issuance requirements for certificates. In both of these instances, you would have full responsibility for staying on top of renewals; however, we will email cert renewal reminders to help you stay on top of your deadlines.

Security teams will need to renew certs independently and re-upload them to Cloudflare once they are renewed. When you change out your certificates, we recommend that you stage out your transition on our staging network. Staging can help security teams find any issues before deploying in production. After you deploy your certificate to production, Cloudflare provides the ability to easily roll back your cert. Even though we don't manage the renewal pipeline in this scenario, we give you tools to ensure you can manage this safely and reliably.

Retain custody of your private keys on a hardware security model (HSM)

Many organizations in highly regulated industries such as government, those handling healthcare records, and financial services, cannot share their private keys outside of their organization. With keyless SSL, these organizations are still able to use TLS and leverage the cloud while keeping their private keys secure on their own hardware security modules (HSMs). Some customers have a requirement to store their keys in an HSM — including cloud HSMs — and likely have keys already stored in these servers. If this applies to your organization, you can still retain use of Cloudflare security, performance, and reliability services while retaining on-premise custody of your private keys.

With keyless configurations, you can retain your private key in your own infrastructure, while having Cloudflare serve the public certificate and allowing for TLS termination by using a session key. To do this, you will need to run a Cloudflare keyless SSL daemon on your own infrastructure, which you can read about in our product documentation.



Overall considerations for your TLS security posture

We recommend that organizations only allow connections from traffic that supports TLS 1.3 — the newest, fastest, and more secure version of the TLS protocol. With Cloudflare, you can set TLS 1.3 as the minimum TLS setting.

NIST SP 800-52 (Guidelines for the Selection, Configuration, and Use of Transport Layer Security Implementations) will require TLS 1.3 by January 1st, 2024. PCI DSS version 4.0 compliance requires payment card processors to use TLS 1.2 or 1.3.

Clients can support a wide range of cipher suites, some of which have been found to be insecure over the years. We recommend that you restrict legacy cipher suites and only allow connections from clients that support more secure cipher suites, for example those that use perfect forward secrecy (PFS), or authenticated encryption. Choosing this option offers your organization the most optimal security and performance, limiting connections to only those clients with the most modern, secure devices and browsers.

Just like personally identifiable information (PII), cryptographic keys are often subject to regulations. Some components of this include keeping keys in a certain geographical location. The EU and GDPR requirements are the most common examples of this, but private key regulations continue to proliferate worldwide.

The Cloudflare Data Localization Suite makes it simple to store data and keys in a specific geography. Using a tool like Data Localization Suite will not only ensure your keys are stored securely, but will also guarantee they do not leave the region that they are required by law to remain in. As more and more regions add GDPR-like rules (and truly, it appears that more countries and regions are using GDPR as a model for data privacy laws), the need for geographically-based storage requirements will increase as well.

Geo Key Manager allows you to restrict the location of your private keys to only data centers in allowed regions, and can also create exclusions with rule-based geo-restrictions. For example, your settings could permit storing keys in the EU and US but exclude France.

This functionality can be used for storing private keys along with other data affected by privacy laws.

Did you know?

Over 50% of web servers still support TLS 1.0 and TLS 1.1, despite both versions of the protocol being officially deprecated by the IETF in 2021. [3].

Securing origin connections

Best practices for securing origin connections
The best practice for securing origin connections is to require Cloudflare to connect to your origin using HTTPS, while simultaneously using mutual TLS (mTLS) – also known as two-way TLS.

When Cloudflare connects to your origin through an HTTPS connection, we check that the origin serves a server certificate on its side. We verify that the certificate:

- Is valid and unexpired;
- Contains the common name of the target hostname (has the right hostnames on it); and
- Is either publicly trusted or you have listed the CA into our trust store to tell us we can trust it.

This helps protect the Cloudflare proxy when we connect to your origin in the same way you know you can trust our network when your client connects to Cloudflare.

When your organization allows Cloudflare to connect to your origin, other clients around the world can theoretically also connect to your origin. To mitigate potential security issues, the best practice here is to restrict that connection and only allow traffic originating from — or proxying through — Cloudflare.

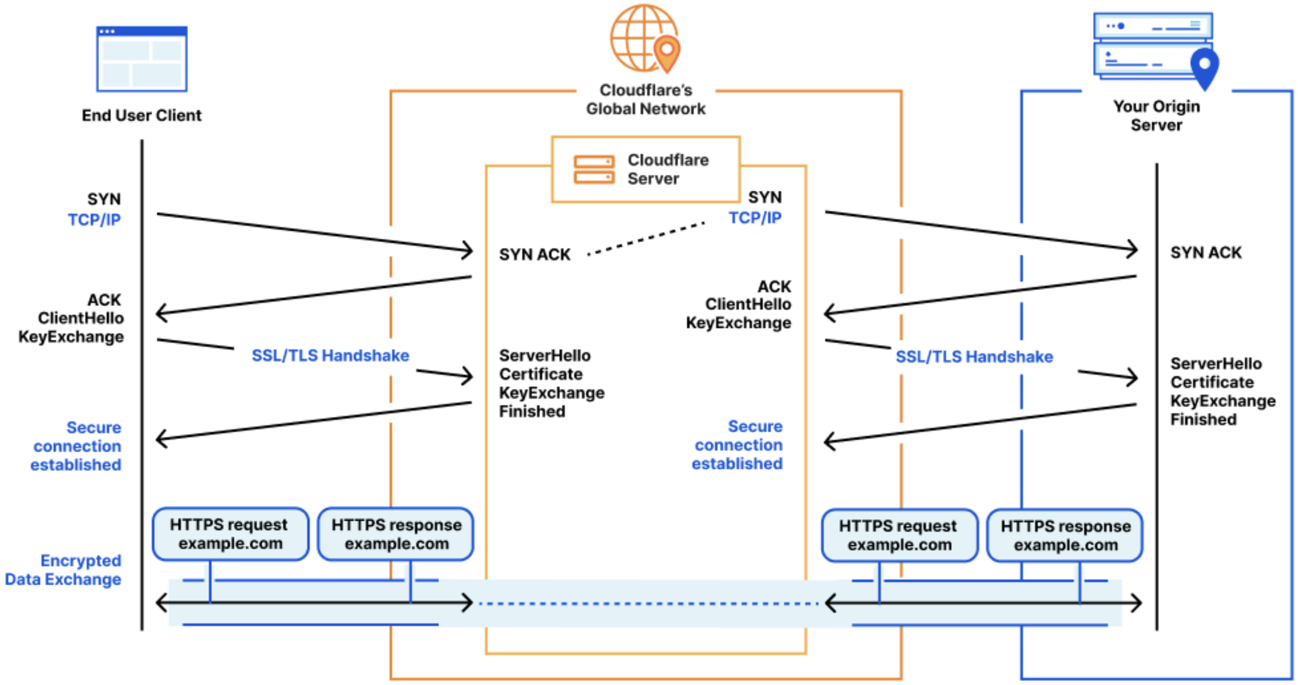
Unauthorized connections can consume valuable CPU, so it's best to not even process those unwanted requests.

Securing your origin with mTLS can similarly help with your overall denial-of-service (DoS) mitigation strategy. With mTLS, Cloudflare will always serve a client certificate on a request. And on the origin side, you can validate that client certificate to guarantee that the traffic is coming from a trusted source — Cloudflare.

If you see that the client certificate matches Cloudflare, you can allow that request to pass through. If the client certificate is invalid, you can drop the request, thereby preventing attacks from unknown, untrusted third parties.

With mTLS, security teams can ensure that traffic is coming from Cloudflare and not from a third party server. To set this up, configure Authenticated Origin Pulls on your whole domain or on a specific hostname. Use a Cloudflare managed certificate or upload your own client certificate, as outlined in previous sections.

Enabling Secure SSL/TLS Connections

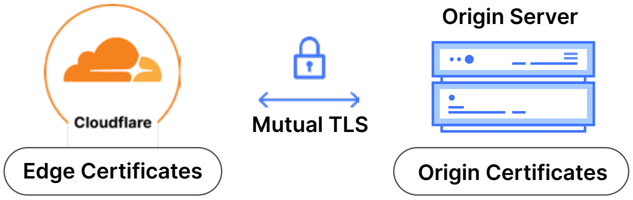


Emerging TLS use cases

Authenticating clients and devices

In traditional one-way TLS, devices will check a server's certificate to ensure that it is safe to connect. mTLS, on the other hand, is a two-way connection that protects both the client and the server, as both have to present a valid certificate to prove that they are who they say they are.

mTLS is an essential tool for ensuring that only authorized clients and devices are making requests to your application. Some examples of how Cloudflare customers use it are discussed in more detail below.



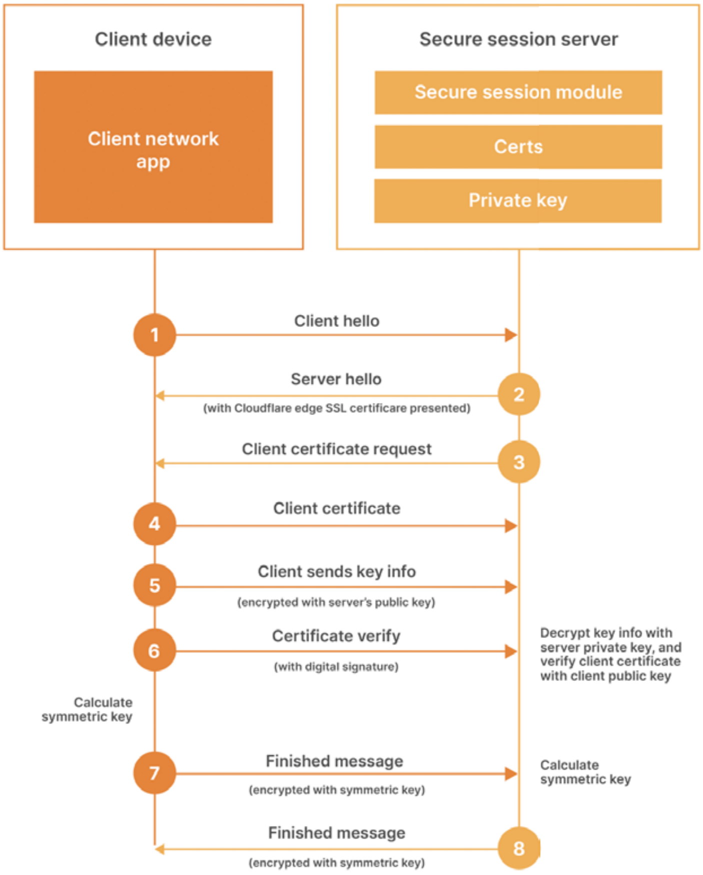
Enhancing Zero Trust access

When you hear Zero Trust, you may call to mind concepts such as denying by default: denying every connection and access request except for those you very explicitly allow. Consider mTLS as another Zero Trust security layer that can be incredibly powerful to ensure that only desired connections are permitted.

mTLS is a similar form of authentication: devices will present a client certificate as an extra layer of security, and the origin can validate the client certificate in order to allow that connection to proceed. If a request is sent that contains an incorrect client certificate, the origin notes that the cert is invalid, and organizations can configure their security settings to automatically block those requests from going through. This can be complementary to other layers of security like identity and access management.

In a corporate network, it's not uncommon for organizations to specify sensitive internal resources that employees should be able to access only from a corporate device, and not from personal devices. mTLS is a powerful tool for this use case: approved work devices can be granted client certificates by the security team, and organizations can also create policies to block access from devices lacking valid certificates.

Client-authentificated TLS handshake



Protecting APIs

Managing and securing APIs is top of mind at Cloudflare. In fact, the majority of the dynamic traffic we see on our global network is API-related. With more large enterprises using APIs for business-critical operations, security leaders and teams are becoming increasingly responsible for API security.

On top of Cloudflare API Gateway capabilities, mTLS also fits into an API security strategy for organizations pivoting to a positive security model, or the "deny by default" security posture we discussed earlier. Again, this means blocking all connections except the ones we want to allow — for example, from trusted business partners or trusted developers, and only allowing those authorized users and devices to make API calls. Here as in other use cases, mTLS can again be used as an authentication and identification tool to only allow hosts that present the right certificate to actually make those API calls.

This mTLS use case is particularly popular with financial services and financial technology companies, but many organizations have API endpoints that should only be accessed securely with a valid client certificate. mTLS makes it possible to validate — for example — that an API making a write request to your database is coming from an approved source. As the need for API security expands, mTLS plays an important role in the positive security model.

Protecting IoT traffic

Headless devices, like IoT devices, present a novel use case for mTLS. Despite the lack of a GUI on these devices, it is still possible for organizations to identify and authenticate them. In the same way that work laptops in a corporate network have client certificates installed, you can also install client certificates onto devices like camera systems, coffee makers, smart locks, office card readers, and more.

When these devices make requests to a server, the server should be able to validate which device the request came from, as well as check if the device is authorized to make the request. Organizations can block any other requests from unauthorized devices. So if someone is trying to hack into your application, they can't make a request to the web server unless they are using an authenticated and identified IoT device. Additional security measures outside the scope of mTLS, like bot mitigation, can help identify if abusive traffic is stemming from a compromised but authenticated device.

Securing serverless development

Increasingly, many of our customers use our serverless compute platform — Cloudflare Workers — to develop their own applications. And serverless computing comes with its own unique security demands.

Ensure your developers are sending data to a trusted source
When building on Workers, you will often direct individual Cloudflare Service Workers (workers that handle HTTP traffic) to make outbound requests to databases, services, cloud providers, and more. You may run multiple services on Workers and will need to be able to identify specific Workers so that you know whether they're authorized to make a specific request to a particular resource.

By using mTLS to require the Worker to identify the server, and requiring the server to identify which Worker a request is coming from, you can better protect your origin servers from data breaches and other attacks.

Further securing the connection between a server and a Worker with mTLS prevents an unauthorized Worker from receiving sensitive information. With mTLS, developers can be sure that they are sending data to a trusted, known source.

Allowing a Worker and an origin to verify each other's identity decreases the likelihood of attacks between the two. mTLS can prevent attacks such as credential stuffing, on-path attacks, spoofing, phishing, and more.

As previously mentioned, mTLS adheres to principles of Zero Trust — neither the Worker nor your server are considered "trustworthy" until they can each verify their identity.

Gain more granular access controls over authentication
With multiple Workers services that are each writing to the same database, you may want to be able to distinguish them. What if, at some point, you need to take the "write" power away from the Worker? Or, what if only Workers "A" and "B" should be allowed to make write requests, and Worker "C" should only make read requests? Cloudflare offers two options:

- You can leverage our Zero Trust Network Access (ZTNA) service, Cloudflare Access, and set up token-based authentication by using a pre-shared key and configuring your Worker to allow or deny access based on the pre-shared key, presented in the header.

- Alternatively, if you don't want to expose your client's identity or require the two services to speak over HTTP, you can use mTLS authentication for Workers. mTLS support on Workers is an easy way to manage authentication and identity for developers building on Workers.

Both methods allow you to lock down authentication on a per-Worker or even per-request level, for more granularity when it comes to authentication and identification.

Customer stories

DHL

DHL, one of the largest shipping and logistics companies in the world, uses Cloudflare to encrypt all customer communications to maintain compliance with data privacy laws. “We have zero tolerance for security breaches,” says Vice President of Digital and Business Process Optimization Jan De Groot. “We protect customer data and make sure all communications with our clients are secure.”

With Cloudflare TLS, DHL Parcel can extend strong encryption to its consumer and business-to-business customer communications, regardless of which web browser they use.

Even as attacks rise, DHL Parcel can simplify compliance requirements for customer-facing applications who need to comply with the EU’s General Data Protection Requirements (GDPR) as well as Germany’s even more stringent data protection laws.

“Cloudflare helps DHL Parcel protect our customer data and client communications, simplifying compliance with data privacy regulations like GDPR,” says de Groot.

Challenge: Ensuring strong security and compliance

“We have zero tolerance for security breaches ... We protect customer data and make sure all communications with our clients are secure.”

Results with Cloudflare:

- With Cloudflare TLS, DHL Parcel can extend strong encryption to its consumer and business-to-business customer communications, regardless of which web browser they use.
- From malicious browser plug-ins to the latest application and network threats, Cloudflare helps DHL Parcel protect its business and customers against data breaches and business disruption.
- Even as attacks rise, DHL Parcel can simplify compliance requirements for customer-facing applications that need to comply with the EU’s General Data Protection Requirements (GDPR) as well as Germany’s even more stringent data protection laws.

“Cloudflare helps DHL Parcel protect our customer data and client communications, simplifying compliance with data privacy regulations like GDPR.”

Jan De Groot,

Vice President of Digital and Business Process Optimization

Read full case study >

SHOPYY

SHOPPY, an e-commerce platform, turns to Cloudflare for the SSL for SaaS feature, which automates the management of SSL certificates - from private key creation, protection, domain validation, issuance, and renewal to re-issuance. Initially, SHOPPY used a free certificate management tool, resulting in unreliable certificates and short validity periods. The free tool also required extensive time and labor, requiring SHOPPY to hire additional employees to oversee the certification management process.

With Cloudflare SSL for SaaS, SHOPPY entrusts all of their certificate management to Cloudflare, requiring only one employee to maintain the entire process. "The use of Cloudflare products has cut our staffing costs by 60% in operation and maintenance alone," said founder and CTO Yuanming Chen. "Efficiency and cost-effectiveness are values that Cloudflare has brought to us as a customer, and allows us to provide the same great service to our own customers."

Challenge: Upgrade from a homegrown platform to a mature cloud offering — that includes reliable full-service certificate hosting

Results with Cloudflare:

- After turning to Cloudflare SSL for SaaS, which automates management of SSL certificates, SHOPYY is now able to fully entrust certificate management to Cloudflare without having to worry about any part of the SSL certificate lifecycle.
- Cloudflare manages the entire process, from private key creation and protection to domain validation, issuance, renewal and re-issuance.
- As a result, SHOPYY only needs one employee now to maintain the entire Operations and Maintenance structure, reducing staffing costs by approximately 60%.

SHOPYY

The use of Cloudflare products has cut our staffing costs by 60% in operation and maintenance alone ... Efficiency and cost-effectiveness are values that Cloudflare has brought to us as a customer, and allows us to provide the same great service to our own customers."

Yuanming Chen,

Founder and CTO

Read full case study >

OneTrust

OneTrust is a popular privacy and compliance service. Over 7,500 businesses worldwide utilize OneTrust's SaaS solutions to manage privacy, security, and governance to comply with regulations such as the CCPA, GDPR, LGPD, PDPA, and ISO27001. OneTrust uses Cloudflare products on approximately 33 top-level domains and about 16,000 subdomains, and the company just exceeded 2 petabytes of traffic a month served through the Cloudflare. Thanks to Cloudflare SSL for SaaS, all OneTrust customers have the option of deploying a vanity domain.

The company also uses Cloudflare to protect their own domains. Colin Henderson, Head of Information Security at OneTrust says, "Advanced Certificates Manager has simplified the way we manage certificates across our many domains, while still allowing us to meet our strict security requirements. The ability to manage cipher suites, as well as auto-renewal within our parameters, creates for an available and secure environment."

Challenge: Deploy efficient, scalable, and cost-effective performance & security solutions to support tremendous growth

Results with Cloudflare:

- OneTrust uses Cloudflare products on approximately 33 top-level domains and about 16,000 subdomains, and the company exceeded 2 petabytes of traffic a month served through the Cloudflare CDN. Thanks to Cloudflare SSL for SaaS, all OneTrust customers have the option of deploying a vanity domain.
- The company also uses Cloudflare to protect their own domains. The ability to manage cipher suites, as well as auto-renewal within their parameters, creates for an available and secure environment.

onetrust

Advanced Certificates Manager has simplified the way we manage certificates across our many domains, while still allowing us to meet our strict security requirements."

Colin Henderson

Head of Information Security

Read full case study >

Cloudflare's SSL/TLS offerings

Cloudflare offers free and enterprise-grade SSL/TLS certificate management and issuance, providing privacy for your end users and your data, and broad customization options:

- Universal SSL - Free SSL/TLS certificates, with Cloudflare-managed issuance and renewal
- Advanced Certificates Manager - Automatic certificate issuance and renewal with robust customization options
- SSL for SaaS - Enables SaaS providers to issue and renew certificates on their customers' behalf

To explore how our SSL/TLS offerings can meet your security goals

Request a demo

or contact us! +1 (888) 99 FLARE

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