CLOUDFLARE

Cloudflare Security Guide for Small and Medium Enterprises

Learn the steps, tools, and products available to transform your network and modernize your business's security.

Cloudflare Security Guide for Small and Medium Enterprises (SMEs)

Small businesses are increasingly becoming prime targets for cyberattacks due to their limited resources and expertise in how to keep their online business secure. In 2024, approximately 43% of cyberattacks were directed at small businesses. These attacks can have devastating consequences, with 60% of small businesses closing within six months following a cyberattack.

The financial impact is significant, as the average cost of a data breach for SMEs is estimated at $3.31 million. Despite these risks, many small businesses remain unprepared, with only 14% having a formal cybersecurity plan in place. This lack of comprehensive cybersecurity measures, combined with the increasing sophistication of cyber threats, underscores the urgent need for small businesses to invest in robust security solutions to protect operations and customer data.

How can Cloudflare help SMEs stay secure?

In today's digital landscape, small businesses are facing an increasing number of cyber threats ranging from disruptive DDoS attacks to sophisticated phishing, malware, and exploitation attempts. **Cloudflare offers a solution to this problem with a free plan that delivers security tools designed to protect websites, APIs, and internal systems.** For small businesses, this means access to tools like easy configuration DDoS protection, Web Application Firewall (WAF), bot protection, secure DNS, traffic filtering, caching, and more, all without needing a dedicated cybersecurity team or high upfront investment.

Cloudflare's free plan provides essential protections that can drastically reduce the risk of data breaches, downtime, and reputational damage. Even without deep technical knowledge, small business owners can configure basic protections in minutes and progressively layer on more advanced features as needed.

Cloudflare acts as a **front-line defense**, filtering malicious traffic before it ever reaches your servers. Whether you're running a WordPress site for your small accounting firm or e-commerce site, Cloudflare's free tools can shield you from the most common and damaging cyber threats, giving small businesses peace of mind and room to grow.

How do I use this guide?

In this guide intended for SMEs, we hope to demystify the work of website and internal team security and offer easy to follow steps to boost your cyber security efforts in your business. This guide includes a range of Cloudflare's security products with configuration recommendations to make the complex world of cyber security more accessible and understandable to a wider audience.

This guide was built by Cloudflare security experts to provide guidance to businesses that are beginning their journey with Cloudflare and looking to increase the security of their websites and internal teams. This guide is structured into sections:

- Website Security Checklist
- Internal Team Security Checklist (Zero Trust)
- Onboarding Your Website to Cloudflare
- Implementing Cloudflare Website Security products
- Implementing Cloudflare Internal Team Security (Zero Trust) products
- Example implementation timeline for Cloudflare

Who is the audience for this guide?

This guide is intended to help SME’s who may not have a dedicated cybersecurity staff but are looking for easy actionable steps to improve their security for their online business.

Are the products in this guide free for my SME?

Yes! All the tools and services mentioned in this security guide are available through Cloudflare’s free plan.

Checklist for Cloudflare Website Security

- ☐ Adding the site to Cloudflare
  - ☐ Add the site and all DNS records from the existing provider.
  - ☐ After migrating nameservers and verifying DNS is working as anticipated, then we'd recommend proxying. This will ensure that every request going to your website goes to Cloudflare first instead of going to your origin server. You must have your website's DNS records proxied for the security products below to be enabled.
- ☐ DNS records orange-clouded (proxied)
  - ☐ Ensures that every request going to your website goes to Cloudflare first instead of going to your origin server. You must have your DNS records proxied for the security products below to be enabled.
- ☐ Leverage Custom WAF Rules and Rate Limiting Rules
  - ☐ Custom rules allow you to control incoming traffic by filtering requests to a zone. You can perform actions like Block or Managed Challenge on incoming requests according to rules you define.
- ☐ Only allow Cloudflare IP addresses to access your origin server
  - ☐ All traffic to proxied DNS records passes through Cloudflare before reaching your origin server. This means that your origin server will stop receiving traffic from individual visitor IP addresses and instead receive traffic from Cloudflare IP addresses .
- ☐ Enable Bot Fight Mode
  - ☐ Identify traffic matching patterns of known bots, challenge or block bots, and protect static resources on your website.
- ☐ If under attack, enable "Under Attack Mode"
  - ☐ If the site is experiencing an attack after implementing the above steps, you can enable "Under Attack Mode" to force a challenge for all incoming requests / clients.
- ☐ Cache as much as you can with Cloudflare Cache Rules
  - ☐ Use Cache Rules to customize cache settings on Cloudflare. Cache Rules allows you to make adjustments to what is eligible to cache (store at Cloudflare's edge), how long it should be cached and where, as well as trigger specific interactions with Cloudflare's cache and other Rules products for matching requests.

Checklist for Cloudflare Internal Team Security (Zero Trust)

- ☐ Add your applications to Cloudflare Access
  - ☐ Authenticate users accessing your internal applications and SaaS apps.
- ☐ Connect your Identity Provider (IdP)
  - ☐ Configure login methods and enforce Multi-Factor Authentication (MFA).
- ☐ Create Granular Access Policies
  - ☐ Define who can access each application based on user, group, location, or device posture.
  - ☐ Apply Allow or Deny rules for precise security control.
- ☐ Deploy Cloudflare Tunnel
  - ☐ Securely connect internal resources to Cloudflare without exposing public IPs.
  - ☐ Establish outbound-only encrypted connections from your infrastructure to Cloudflare's global network.
- ☐ Set up HTTP filtering with Secure Web Gateway
  - ☐ Refer to our list of common HTTP policies for other policies you may want to create.
- ☐ Implement WARP for device security
- ☐ Set up Cloudflare Access Security Broker (CASB)
  - ☐ Integrate (up to 2 read-only APIs on the free plan) to monitor SaaS apps and cloud environments.
- ☐ Configure Data Loss Prevention (DLP)
  - ☐ Scan web traffic and SaaS applications for sensitive data like social security numbers, financial data, secret keys, or source code.
- ☐ Monitor and audit regularly
  - ☐ Adjust access and security policies based on user behavior and emerging threats.

Getting Started with Cloudflare Fundamentals

Cloudflare's global anycast network helps mitigate DDoS attacks and boosts website performance via our reverse proxy and content delivery network (CDN) respectively. Additionally, it provides visibility into traffic volume, uptime, and performance that you can use to further secure or improve the site as well. The intent of this document is to help sites enhance their security posture and mitigate ongoing disruption.

Onboarding your website to Cloudflare

If your website is not already using Cloudflare, you'll need to create an account and onboard the website to Cloudflare. To do this, ensure you have access to your domain registrar account (e.g., GoDaddy, Namecheap, or Google Domains). If your site is already on Cloudflare, you can skip this step.

Add a website to Cloudflare

1. Log in or create a Cloudflare account via the the Cloudflare dashboard
2. In the top navigation bar, click Add site.
3. Enter your website's apex domain (example.com) and then click Add Site. If Cloudflare is unable to identify your domain as a registered domain, make sure you are using an existing top-level domain (.com, .net, .biz, or others). Additionally, Cloudflare requires your apex domain to be one level below a valid TLD defined in the Public Suffix List (PSL)
4. For this guide, we recommend using **"Free plan". But if you are interested in our paid plans that provide additional products, please visit our plans.**
5. Review your DNS records.. When you add a new site to Cloudflare, Cloudflare automatically scans for common records and adds them to the DNS zone. The records show up under the respective zone DNS > Records page. Since this scan is not guaranteed to find all existing DNS records, you need to review your records, paying special attention to the following record types:
    a. Zone apex records (example.com)
    b. Subdomain records (www.example.com or blog.example.com)
    c. Email records
    d. If you activate your domain on Cloudflare *without* setting up the correct DNS records for your domain and subdomain, your visitors may experience DNS_PROBE_FINISHED_NXDOMAIN errors.
    e. If you find any missing records, manually add those records.
    f. Depending on your site setup, you may want to adjust the proxy status for certain A, AAAA, or CNAME records.
6. Click Continue.

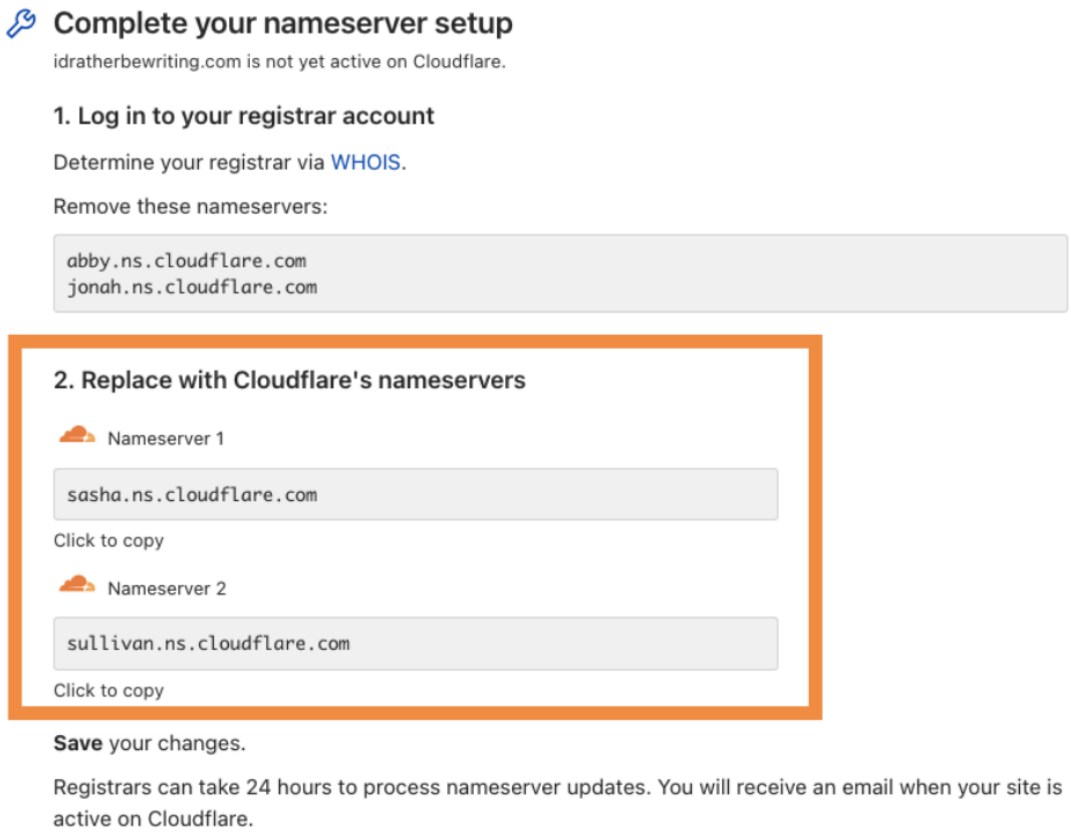
7. Go through the Quick Start Guide and when you have finished, click Finish.

Update Nameservers

Once you have added a domain (also known as a zone) to Cloudflare, that domain will receive two assigned authoritative nameservers. Before your domain can begin using Cloudflare for DNS resolution, you need to add these nameservers at your registrar. Make sure DNSSEC is disabled at this point.

Get nameserver names

1. Log in to the Cloudflare dashboard and select your account and domain.
2. On **Overview**, locate the nameserver names in **2. Replace with Cloudflare's nameservers**.



3. Keep this window open while you perform the next step.

> Cloudflare automatically assigns nameservers to a domain and these assignments cannot be changed. For more details, refer to Nameserver assignments.

Update your registrar

1. Log in to the admin account for your domain registrar. If you do not know your provider, use ICANN WHOIS.
2. Remove your existing authoritative nameservers.
3. Add the nameservers provided by Cloudflare. If their names are not **copied exactly**, your DNS will not resolve correctly.

▶ **Provider-specific instructions**

> To avoid common issues, refer to our Nameserver replacement checklist.

Verify changes

Wait up to 24 hours while your registrar updates your nameservers.

When your domain is **Active**:

- You will receive an email from Cloudflare.
- Your domain will have a status of **Active** on the **Websites** page of your account.
- Online tools such as https://www.whatsmydns.net/ will show your Cloudflare-assigned nameservers (most of these tools use cached query results, so it may take longer for them to show the updated nameservers).
- CLI commands will show your Cloudflare-assigned nameservers

```
*Linux/Unix*
dig <DOMAIN_NAME> +trace @1.1.1.1
dig <DOMAIN_NAME> +trace @8.8.8.8

*Windows*
nslookup <DOMAIN_NAME> 1.1.1.1
nslookup <DOMAIN_NAME> 8.8.8.8
```

> If you see unexpected results, refer to our troubleshooting suggestions and check with your domain registrar.

4 Re-enable DNSSEC

When you updated your nameservers, you should have also disabled DNSSEC at your registrar.

You should now enable DNSSEC to protect from domain spoofing.

Save the information from the Verification TXT Record. If you lose the information, you can also access it by going to DNS > Records > Verification TXT Record.

2 Verify ownership for your domain

Once you add your domain to Cloudflare, add the **Verification TXT Record** at your authoritative DNS provider. Cloudflare will verify the TXT record and send a confirmation email. This can take up to a few hours.

▶ **Example verification record**

> If your authoritative DNS provider automatically appends DNS record `name` fields with your domain, make sure to only insert `cloudflare-verify` as the record name. Otherwise, it may result in an incorrect record name, such as `cloudflare-verify.example.com.example.com`.
>
> After creating the record, you can use this Dig Web Interface link to search (`dig`) for `cloudflare-verify.<YOUR DOMAIN>` and validate if it is working.

That record must remain in place for as long as your domain is active on the partial setup on Cloudflare.

3 Optional - Provision an SSL certificate

To provision a Universal SSL certificate through Cloudflare, follow these instructions.

If your domain is already live with a partial DNS setup — with Cloudflare or another DNS provider — you cannot use a TXT record for Domain Control Validation. That domain's TXT record needs to be reserved for forwarding traffic to Cloudflare.

4 Add DNS records

1. In Cloudflare, add an `A`, `AAAA`, or `CNAME` record.
2. At your authoritative DNS provider:
   a. Remove any existing `A`, `AAAA`, or `CNAME` records on the hostname you want to proxy to Cloudflare.
   b. Add a `CNAME` record for `{your-hostname}.cdn.cloudflare.net`.

      ▶ **Example CNAME record at authoritative DNS provider**

   c. Repeat this process for each subdomain proxied to Cloudflare.

You're **DONE.**

Now that your domain is protected by Cloudflare, let's ensure key security features are enabled so you can take full advantage of Cloudflare's protection.

DNS

Cloudflare provides fast and secure managed DNS as a built-in service on our network. Migrating your records to Cloudflare should be a straightforward process but there are a few
security measures to keep in mind. When you add a new site to Cloudflare, Cloudflare automatically scans for common records and adds them to the DNS zone. The records show up under the respective zone DNS > Records page.

To create a DNS record in the dashboard:

1. Log in to the Cloudflare dashboard and select an account and domain.
2. Go to DNS > Records.
3. Click Add record.
4. Choose a record Type.
5. Complete the required fields, which vary per record. Particularly important fields (for
some records) include:
    - Proxy status: For A, AAAA, and CNAME records, decide whether hostname

traffic is proxied through Cloudflare.

- TTL: Short for Time to Live, this field controls how long each record is valid and — as a result — how long it takes for record updates to reach your end users.
- Comment and Tag: Record attributes meant for your reference.

6. Click Save.

Set up Email Records

There are three reasons to set up email records for your domain:

- To make sure your domain can receive email.
- To make sure your domain can send and receive email.
- To prevent other email senders from spoofing your domain.

The exact values for your DNS mail records depend on your email provider. If you have issues, review the Troubleshooting and contact your email service provider to confirm your DNS records are correct.

Receive Email

If you only need to receive emails, Cloudflare offers Email Routing for free email forwarding to custom email addresses.

Send and receive email

To send and receive emails from your domain, you need an SMTP provider. Then, create two DNS records within Cloudflare, following the steps below:

1. Get the IP address and MX record details from your SMTP provider (vendor-specific guidelines).
2. Add an A or AAAA record for your mail subdomain that points to the IP address of your mail server. Below is an example:

Type	Name	IPv4 address	Proxy status
A	`mail`	`192.0.2.1`	DNS only

.

3. Add an MX record that points to that subdomain. Below is an example:

Type	Name	Mail server	TTL
MX	`@`	`mail.example.com`	Auto

Prevent Email Spoofing

There are several DNS mechanisms to prevent others from sending emails on behalf of your domain. These all work as TXT records that need to be added on your domain:

- Sender Policy Framework (SPF) ↗: List authorized IP addresses and domains that can send email on behalf of your domain.
- DomainKeys Identified Mail (DKIM) ↗: Ensure email authenticity by cryptographically signing emails.
- Domain-based Message Authentication Reporting and Conformance (DMARC): Receive aggregate reports about your email traffic and provide clear instructions for how email receivers should treat non-conforming emails.

Enabling the Proxy: 'Orange Cloud'

While your DNS records make your website or application available to visitors and other web services, the Proxy status of a DNS record defines how Cloudflare treats incoming DNS queries for that record. The records you can proxy through Cloudflare are records used for IP address resolution — meaning A, AAAA, or CNAME records.

Cloudflare recommends setting to proxied all A, AAAA, and CNAME records that are used for serving web traffic. For example, CNAME records being used to verify your domain for a third-party service should not be proxied. When you set a DNS record to Proxied (also known as orange-clouded), Cloudflare can:

- Protect your origin server from DDoS attacks.
- Optimize, cache, and protect all requests to your application.
- Apply your configurations for a variety of Cloudflare products.

Example:

DNS management for **example.com**:

Type	Name	Content	Proxy status	TTL
A	`blog`	`192.0.2.1`	Proxied	Auto
A	`shop`	`192.0.2.2`	DNS only	Auto

In the example DNS table above, there are two DNS records. The record with the name `blog` has proxy on, while the record named `shop` has the proxy off (that is, **DNS only**).

This means that:

- A DNS query to the proxied record `blog.example.com` will be answered with a Cloudflare anycast IP address instead of `192.0.2.1`. This ensures that HTTP/HTTPS requests for this name will be sent to Cloudflare's network and can be proxied, which allows the benefits listed above.
- A DNS query to the DNS-only record `shop.example.com` will be answered with the actual origin IP address, `192.0.2.2`. In addition to exposing your origin IP address and not benefitting from several features, Cloudflare cannot provide HTTP/HTTPS analytics on those requests (only DNS analytics). For further context, refer to How Cloudflare works.

DNS-only records (grey cloud)

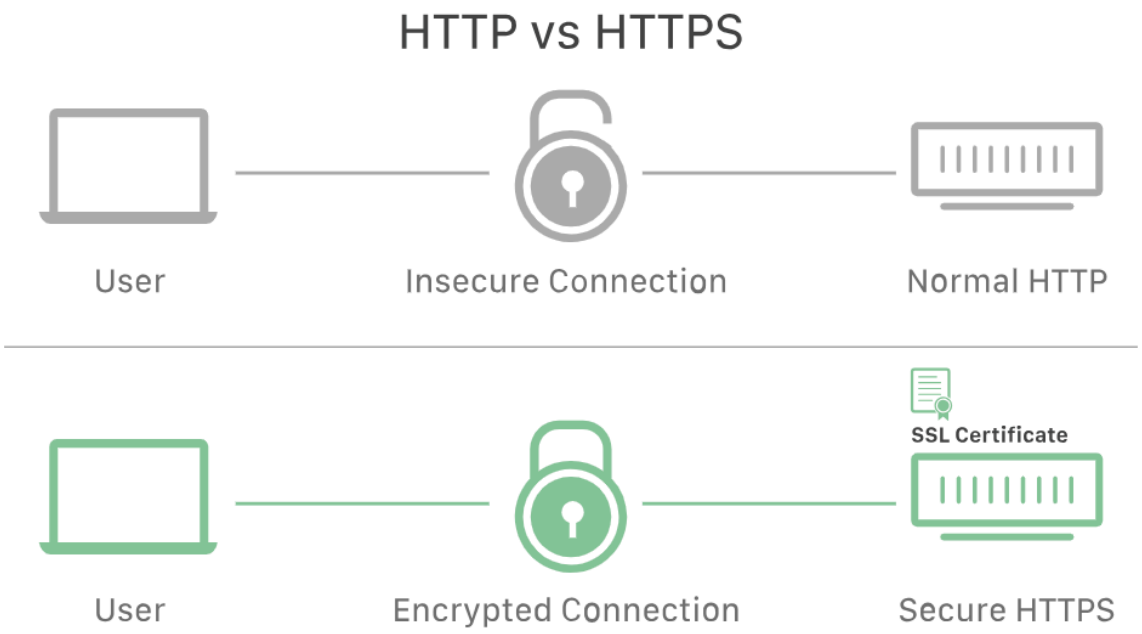
When an A, AAAA, or CNAME record is **DNS-only** — also known as being gray-clouded — DNS queries for these will resolve to the record's origin IP address, as described in the example.

In addition to potentially exposing your origin IP addresses to bad actors and DDoS attacks, leaving your records as **DNS-only** means that **Cloudflare cannot** optimize, cache, and protect requests to your application or provide analytics on those requests.

Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer) is a security technology that establishes an encrypted connection between a web server and a visitor's browser. It ensures that all data transmitted between them remains private and secure. Modern SSL is implemented via TLS (Transport Layer Security), but the term "SSL" is still widely used. When a website uses SSL, you'll see:

- **https://** in the URL instead of **http://**
- A **padlock icon** in the browser address bar



SSL is important because it encrypts data between a user's browser and your website, protecting sensitive information from hackers. It also verifies your site's identity, builds user trust with the padlock icon and "https," improves search rankings, and helps meet security compliance requirements. Without SSL, your site may trigger browser warnings and lose credibility.

For your site, you have access to free SSL certificates to ensure all data going from the user to your site is secure. To enable:

1. In the Cloudflare dashboard, go to your domain.
2. Click **"SSL/TLS"** in the left-hand menu.
3. Under the **Overview** tab, confirm that the **certificate status is "Active"**.
    - This means the Universal SSL certificate is live and protecting your site.
4. Choose an SSL mode (we recommend full or full strict)

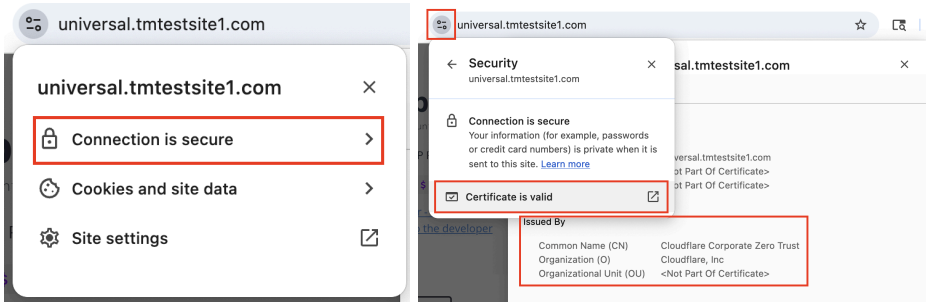
- Go to **SSL/TLS > Overview**, and select the most appropriate mode:
  - **Off** – No encryption (not recommended)
  - **Flexible** – Encrypts from browser to Cloudflare only (not secure for sensitive sites)
  - **Full** – Encrypts both ways (needs SSL on your origin server)
  - **Full (Strict)** – Encrypts both ways with a valid SSL cert on your origin (most secure)

5. Enable “Always use HTTPS” This ensures all HTTP traffic is redirected to HTTPS automatically.
   - Go to **SSL/TLS > Edge Certificates**
   - Scroll down to **Always Use HTTPS** and toggle it **ON**

To Test:

- Open browser tab to a proxied record, in this example universal.tmtestsite1.com is proxied and shows and orange cloud. This host is using a Cloudflare Universal Cert

- In Chrome, click the View Site Information icon to the left of the domain and you should see “Connection is secure”. Click there then click “Certificate is valid”. You should see a certificate issued by Cloudflare



Common Attack Surface Area

Now that your site is secured with Cloudflare's DNS protection and SSL encryption, the next step is to review common types of attacks targeting websites and how you can defend against them.

Websites / Web Traffic (HTTP/HTTPS)

Websites, being the front-door for most businesses, are often a common target as their outage/defacement is very public and disruptive. Below are some characteristics and recommendations for mitigating these attacks with Cloudflare.

Characteristics

- Types of Attacks
    - Usually a type of Layer 7 attack.
        - Cloudflare DDoS Protection Coverage - Developer Docs
- Often High Volume
        - Volume often measured in requests per second (rps).
    - Origin Unavailability / High Origin Response Times (likely due to the origin being saturated on CPU, Network, etc)
- Increase in Origin Errors (500s, 502s)

- Web DDoS Attack
    - Origin unavailability: User access issues and inaccessible web services.
- Web Fuzzing Attack
- Exploits: Cross-Site Scripting (XSS), Remote Code Execution (RCE), SQL Injection (SQLi)

Recommendations

- Cloudflare's free WAF Managed Rules
    - All customers have access to the Cloudflare Free Managed Ruleset, which provides mitigations against high and wide-impacting vulnerabilities. This is automatically enabled on all free plans.
- WAF Rules:
    - Challenge traffic outside of your region
    - Generic Rate Limiting Rules
    - Anti-Fuzzing Rate-Limiting Rules

Internet Infrastructure (IP Addresses, Domains)

In addition to websites that are often intentionally made public, attackers will scan for common DNS records such as vpn.mysite.com or remote.mysite.com to uncover critical infrastructure that's un-proxied or exposing important IPs. Exposing these IPs may allow them to attack around Cloudflare.

Characteristics

- Types of Attacks
    - Usually a type of Layer 3 / Layer 4 attack.
        - Cloudflare DDoS Protection Coverage - Developer Docs
    - DNS-specific attacks are considered L7.
        - Random hostnames, query floods, etc
        - Cloudflare DDoS Protection Coverage - Developer Docs
- Often High Bandwidth and/or High Packet Rate
        - Bandwidth is often measured in bits per second (bps).
        - Packet rate is often measured in packets per second (pps).
    - Internet/Network Unavailability / High Internet/Network Response Times (likely due to the internet or appliances being saturated on network or CPU)
    - Cascading Infrastructure Failures (Web, VPN, Firewall, ISP Saturation)

Recommendations

- Proxying with Cloudflare
    - When proxying traffic with Cloudflare, we are able to return Cloudflare IPs as the entry point for the traffic which obscures your real infrastructure. Cloudflare has means for proxying L4, and L7. We can also onboard ASNs, or Public IP spaces
- DNS Obscurity
    - Instead of `vpn.` or `remote.` you could migrate DNS names to a random string or something unique to your organization to hide your Firewall's VPN.
        - This could mitigate attackers efforts or increase the difficulty for them to uncover real IP addresses.

Application Attack Surface Area

Website built on WordPress

Characteristics

- Brute-forcing administrator paths such as `/wp-admin/*`.
    - Account Compromise
    - Vulnerable Admin Plugins
- Often High Volume
    - Origin Unavailability / High Origin Response Times (likely due to the origin being saturated on CPU, Network, etc)
- Increase in Origin Errors (500s, 502s)

Recommendations

- Cloudflare's free WAF Managed Rules
- WAF Rules:
    - Challenge traffic outside of your region
    - Generic Rate Limiting Rules
    - Anti-Fuzzing Rate-Limiting Rules
- Cloudflare Access SSO
    - With Cloudflare Access, you can apply a policy requiring an Email PIN or Identity Provider (Azure Entra, Google Workspace) authentication before traffic can be forwarded to the origin. This is very effective at mitigating

login spam to WordPress sites. Under the Cloudflare free plan, you have access to 50 free seats. More on this is in our Zero trust section of the security guide.

Best practices for your website

The following are “Phases” or things to try to address/deploy after first onboarding DNS and proxying with Cloudflare. Before diving into these phases, there are these sections below around investigating traffic and considerations. Not all configurations are applicable to all customers.

Phase	Relevant Configurations	Configuration Work	Recommended for
Phase 1	Managed Rules Bot Fight Mode Challenge traffic on County level	Low	All Sites
Phase 2	Generic Rate-Limiting Rules	Medium	Prominent Sites

Traffic Pattern Considerations

When configuring rules in Cloudflare be sure to also consider the traffic patterns you normally see and the amount of requests users make when visiting the site. You can gain insights into this in “Security > Analytics” and look for traffic from the origin for a given IP.

Rule Creation Considerations

Following reviewing Traffic Pattern Considerations above, and keeping the following in mind as well:

- All the rules and thresholds in screenshots in this document are examples and should not be directly copied.
- Only use the challenge actions with browser facing pages / traffic. Otherwise, automated systems interacting with APIs on your site may be disrupted.
- When first testing a rule, we would recommend using the challenge action at first so that legitimate users are still able to connect after completing the check. Then after verifying a low challenge solve rate (CSR) in the analytics view, you could more confidently move it to a blocking action.

Prevent non-Cloudflare IPs to Origin

Phase 1 Change - (Cloudflare Developer Docs)

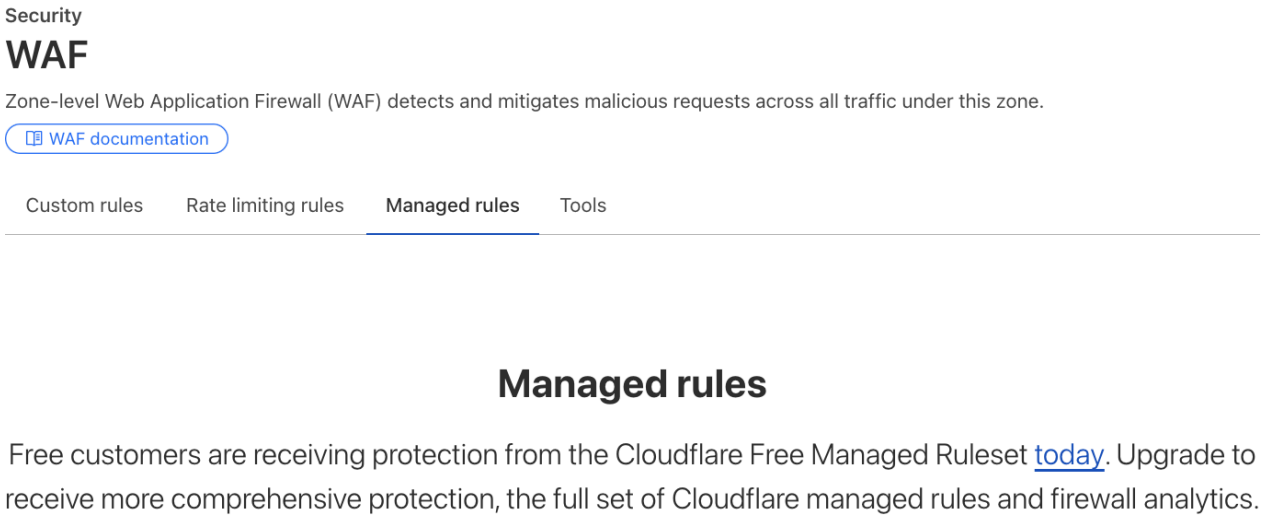
Another important step to ensuring your Cloudflare environment remains the front door for all web traffic and potential attacks after onboarding to the proxy, is to configure your firewall to limit access to the website unless the traffic is originating from Cloudflare IPs. Without this, crawlers scanning the internet may discover your server's, the origin server's, IP address and be able to bypass Cloudflare.

Free WAF Managed Rules

Phase 1 Change - (Cloudflare Developer Docs)

This ruleset is automatically deployed on any new Cloudflare zone and is specially designed to reduce false positives to a minimum across a very broad range of traffic types. Customers will be able to disable the ruleset, if necessary, or configure the traffic filter or individual rules. As of today, the ruleset contains the following rules:

- Log4J rules matching payloads in the URI and HTTP headers;
- Shellshock rules;
- Rules matching very common WordPress exploits;

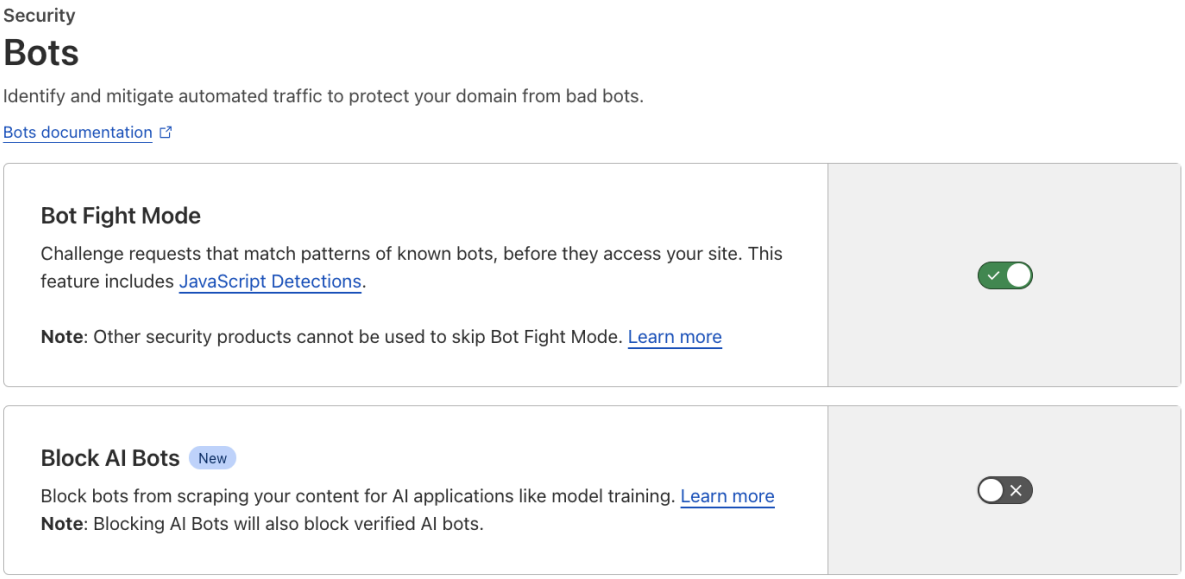


Bot Fight Mode

Phase 1 Change - (Cloudflare Developer Docs)

Cloudflare's Bot Fight Mode is a security feature built on the WAF that is designed to detect, manage, and mitigate bot traffic on websites and applications. Using similar threat intelligence to distinguish between good and bad bots. This protects the website from abuse, scraping, credential stuffing, DDoS attacks, and more.

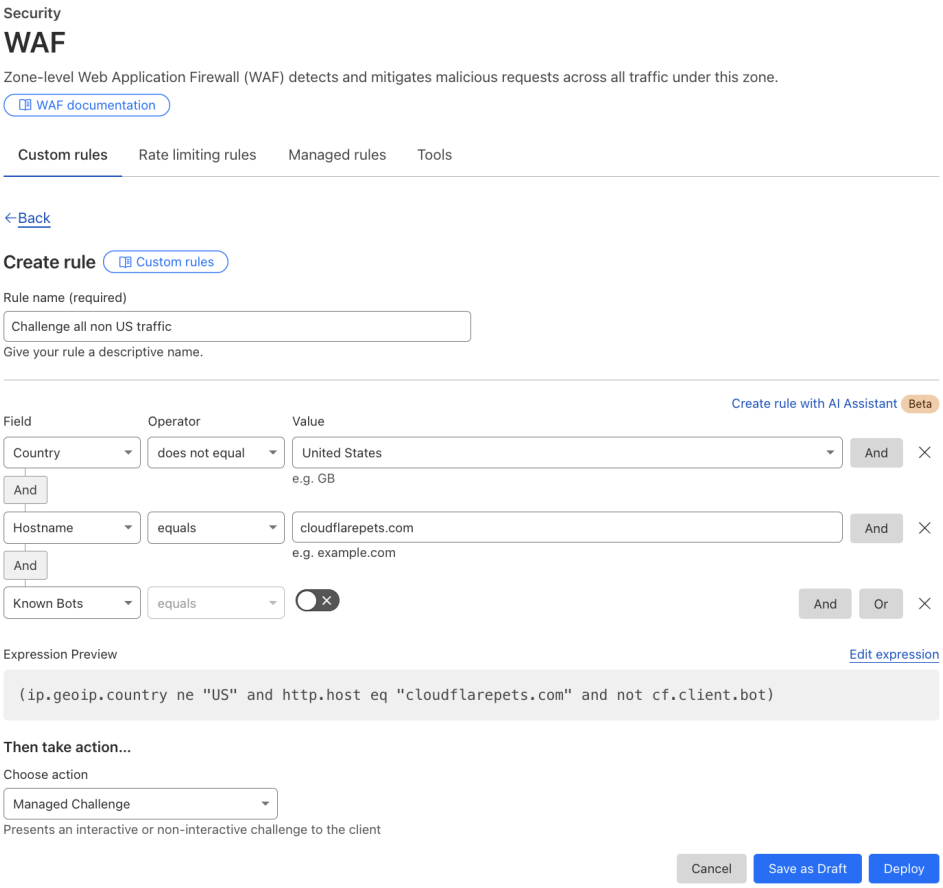
1. Go to the "Security > Bots" section, and click "Configure Bot Fight Mode".



Challenge traffic on a Country IP level

Phase 1 Rule - (Cloudflare Developer Docs)

It is also very easy to quickly set up a challenge for traffic outside of the country that you expect to receive visitors. For example, if you are a US based business and typically only have visitors from the US visiting the site, you can challenge all traffic outside of the US. This allows us to slow incoming attacks and validate the browsers before letting the users through. Under the free plan, you have access to 5 custom firewall rules.



Generic Rate-Limiting Rules

Phase 1 Rule - (Cloudflare Developer Docs)

Cloudflare's Automatic DDoS Mitigation reduces very large volume attacks, but using rate-limiting you can control at a more granular level, the number of requests that an IP can make over a defined period. This can include a variety of attempts that contain brute force logins, smaller scale volume attacks, and scraping. Actions used to thwart these actors' efforts are blocking or issuing challenges. Under the free plan, you have access to 1 rate limiting rule.

Example 1

The following rule performs rate limiting on incoming requests from the US addressed at the login page, except for one allowed IP address.

Expression:

```
(http.request.uri.path eq "/login" and ip.geoip.country eq "US" and ip.src ne 192.0.0.1)
```

Rule characteristics:

- *Data center ID* (included by default when creating the rule in the dashboard)
- *IP Address*

Example 2

The following rule performs rate limiting on incoming requests with a given base URI path, incrementing on the IP address and the provided API key.

Expression:

```
(http.request.uri.path contains "/product" and http.request.method eq "POST")
```

Rule characteristics:

- *Data center ID* (included by default when creating the rule in the dashboard)
- *IP Address*
- *HTTP Header* > `x-api-key`

Example 3

The following rule performs rate limiting on requests targeting multiple URI paths in two hosts, excluding known bots. The request rate is based on IP address and `User-Agent` values.

Expression:

```
(http.request.uri.path eq "/store" or http.request.uri.path eq "/prices") and (http.host eq "mystore1.com" or http.host eq "mystore2.com") and not cf.client.bot
```

Rule characteristics:

- *Data center ID* (included by default when creating the rule in the dashboard)
- *IP Address*
- *HTTP Header* > `user-agent`

Cloudflare Zero Trust

Zero Trust is a cybersecurity model built on the principle of “never trust, always verify.” Every user and device must prove their identity before accessing any company resource, no matter where they’re located. **For SMEs, adopting Zero Trust is critical to reduce risk, limit damage from breaches, and maintain business continuity. Even if attackers get hold of stolen credentials, Zero Trust can block access without re-verification, protecting sensitive data and your company’s reputation.**

Cloudflare’s free plan offers robust Zero Trust tools for up to 50 users, with 24-hour log retention. It's part of Cloudflare One, a comprehensive platform to secure your apps, users, and networks, at no cost.

How to get started with Cloudflare Zero Trust

Access

Authenticate users accessing your applications, seamlessly onboard third-party users, and log every event and request.

Cloudflare Tunnel

Securely connect your resources to Cloudflare without exposing a public IP by using Cloudflare Tunnel, which establishes outbound-only connections from your infrastructure to Cloudflare's global network.

WARP

Protect corporate devices by privately sending traffic from those devices to Cloudflare's global network, build device posture rules, and enforce security policies anywhere.

Secure Web Gateway

Inspect and filter DNS, network, HTTP, and egress traffic to enforce your company's Acceptable Use Policy (UAP), block risky sites with custom blocklists and threat intelligence, and enhance visibility and protection across SaaS applications.

Cloudflare Access Security Broker (CASB) Up to 2 read-only API integrations for the free plan

Protect users and sensitive data at rest in SaaS applications and cloud environments, scan for misconfigurations, and detect insider threats as well as unsanctioned application usage to prevent data leaks and compliance violations.

Data Loss Prevention (DLP) Limited predefined profiles for the free plan

Scan your web traffic and SaaS applications for the presence of sensitive data such as social security numbers, financial information, secret keys, and source code.

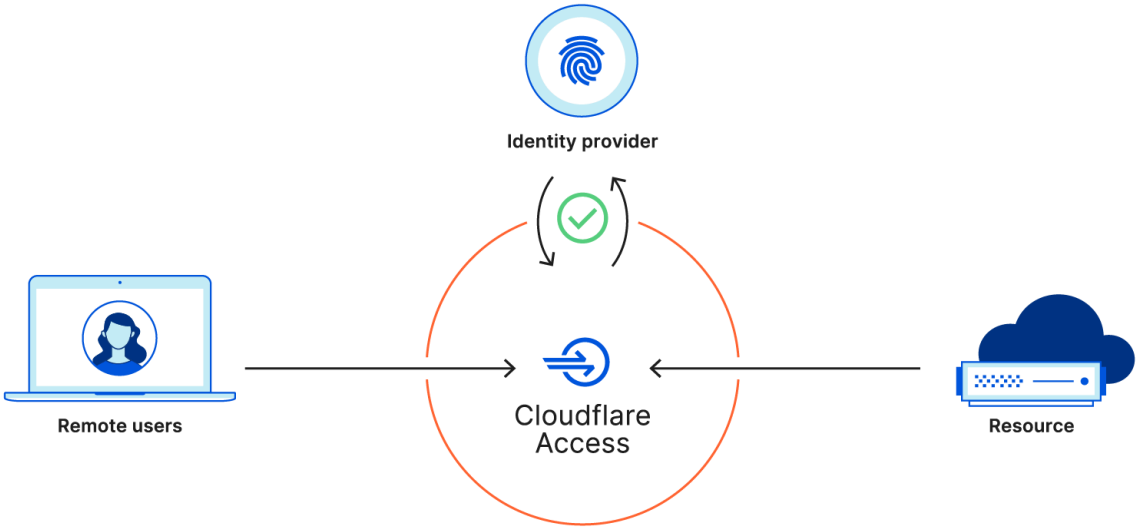
Onboard to Cloudflare Zero Trust

Once you are on the onboarding page, you will be asked to create a team name, unique, internal identifier for your organization. This team name will be used to enroll users, the team name is typically the organization's name. **After this, you will be asked to select a subscription plan and enter in your payment details, this step is still required for the Free plan and you will not be charged.**

Cloudflare Access

Cloudflare Access is a security tool that provides secure, zero-trust access to internal applications by verifying each user's identity before granting access. Unlike traditional VPNs, it only allows authorized users to connect to specific resources, making remote work safer and simpler.

For small and medium businesses, Cloudflare Access offers enterprise-level security without the complexity or cost of managing VPNs. It supports remote work by securely connecting employees from anywhere, improves control by setting precise access rules, and helps prevent unauthorized access. It's easy to set up, cost-effective, and scales with your business as it grows. **The free plan's support for up to 50 users makes it an accessible and scalable solution for small and growing businesses to adopt robust Zero Trust security practices.**



How to set up Cloudflare Access

This can be found in the Cloudflare Dashboard under Zero Trust. Access policy consists of an **Action** as well as rules which determine the scope of the action. To build a rule, you need to choose a **Rule type**, **Selector**, and a **Value** for the selector.

Actions let you grant or deny permission to a certain user or user group. You can set only one action per policy. The Allow action allows users that meet certain criteria to reach an application behind Access. You can add a Require rule in the same policy action to enforce additional checks. Finally, if the policy contains an Exclude rule, users meeting that definition are prevented from reaching the application.

Action	Rule type	Selector	Value
Allow	Include	Country	`Portugal`
	Require	Emails Ending In	`@team.com`
	Exclude	Email	`user-1@team.com`, `user-2@team.com`

The Block action prevents users from reaching an application behind Access.

Action	Rule type	Selector	Value
Block	Include	Everyone	`Everyone`
	Exclude	Email	`user-1@team.com`

The Bypass action disables any Access enforcement for traffic that meets the defined rule criteria. Bypass is typically used to enable applications that require specific endpoints to be public. **Cloudflare does not recommend using Bypass to grant direct permanent access to your internal applications.**

Action	Rule type	Selector	Value

Bypass	Include	Everyone	`Everyone`

Rules work like logical operators. They help you define which categories of users your policy will affect. All Access policies must contain an Include rule. This is what defines the initial pool of eligible users who can access an application.

- The Include rule is similar to an OR logical operator. In case more than one Include rule is specified, users need to meet only one of the criteria.
- The Exclude rule works like a NOT logical operator. A user meeting any Exclusion criteria will not be allowed access to the application.
- The Require rule works like an AND logical operator. A user must meet all specified Require rules to be allowed access.

For Selectors, when you add a rule to your policy, you will be asked to specify the criteria/attributes you want users to meet. These attributes are available for all Access application types, including SaaS, self-hosted, and non-HTTP applications.

Selector	Description	Checked at login	Checked continuously[1]
Emails	`you@company.com`	✅	❌
Emails ending in	`@company.com`	✅	❌
External Evaluation	Allows or denies access based on custom logic in an external API.	✅	❌
IP ranges	`192.168.100.1/24` (supports IPv4/IPv6 addresses and CIDR ranges)	✅	✅

Access policies define the users who can log in to your Access applications. You can create, edit, or delete policies at any time and reuse policies across multiple applications.

To create a reusable Access policy:

1. In Zero Trust go to **Access** > **Policies**.
2. Select **Add a policy**.
3. Enter a **Policy name**.
4. Choose an **Action** for the policy.
5. Choose a **Session duration** for the policy.
6. Configure as many **Rules** as needed.
7. (Optional) Configure additional settings for users who match this policy:
    - Isolate application.
    - Purpose justificaton
    - Temporary authentication
8. Select **Save**.

With Zero Trust policies, you can require that users log into certain applications with specific types of multifactor authentication (MFA) methods. **For example, you can create rules that only allow users to reach a given application if they authenticate with a physical hard key.** This feature is only available if you are using the following identity providers:

-
- Okta
- Microsoft Entra ID (formerly Azure AD)
- OpenID Connect (OIDC)
- SAML

To enforce an MFA requirement to an application:

- In Zero Trust , go to Access > Applications.
- Find the application for which you want to enforce MFA and select Configure. Alternatively, create a new application.
- Go to Policies.
- If your application already has a policy containing an identity requirement, find it and select Configure.
- Add the following rule to the policy:

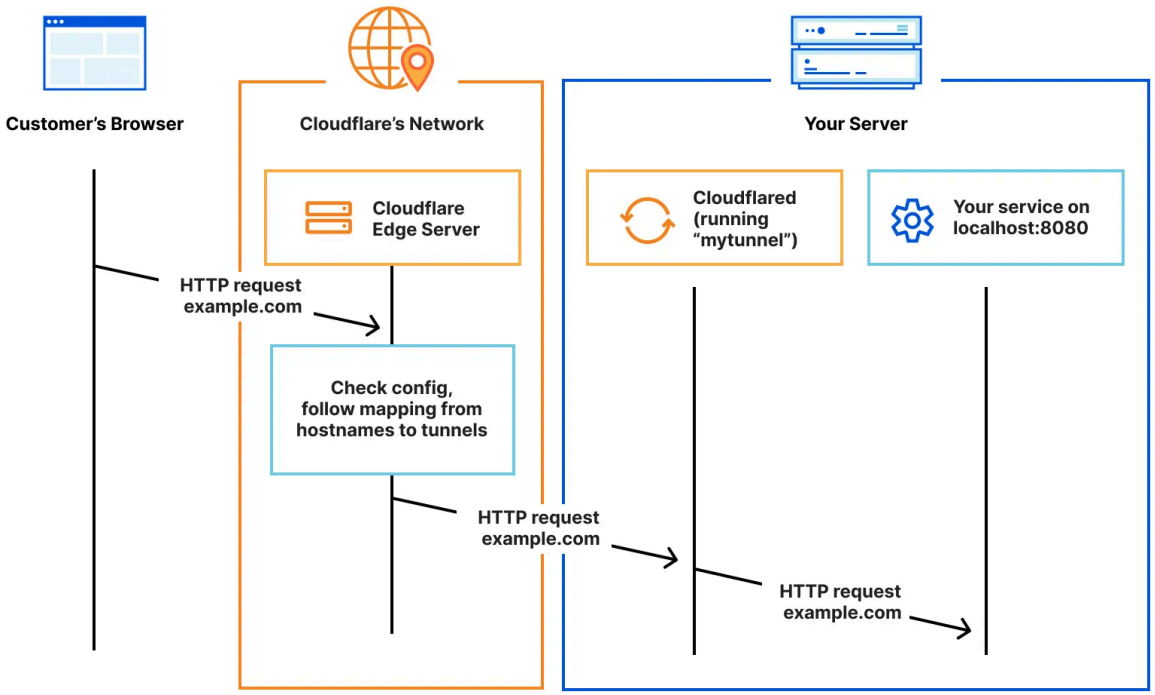
Rule type	Selector	Value
Require	Authentication method	`mfa - multiple-factor authentication`

- Save the policy.

Cloudflare Tunnel

Cloudflare Tunnel provides you with a secure way to connect your resources to Cloudflare without a publicly routable IP address. With Tunnel, you do not send traffic to an external IP, instead, a lightweight daemon in your infrastructure (cloudflared) creates outbound-only connections to Cloudflare's global network.

Cloudflare Tunnel can connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare. This way, your origins can serve traffic through Cloudflare without being vulnerable to attacks that bypass Cloudflare. It helps ensure Zero Trust policies by creating outbound-only encrypted connections from your internal resources to Cloudflare's global network. This means your servers do not expose public IP addresses, preventing direct-external access.



Cloudflare Tunnel is helpful for SMEs because it:

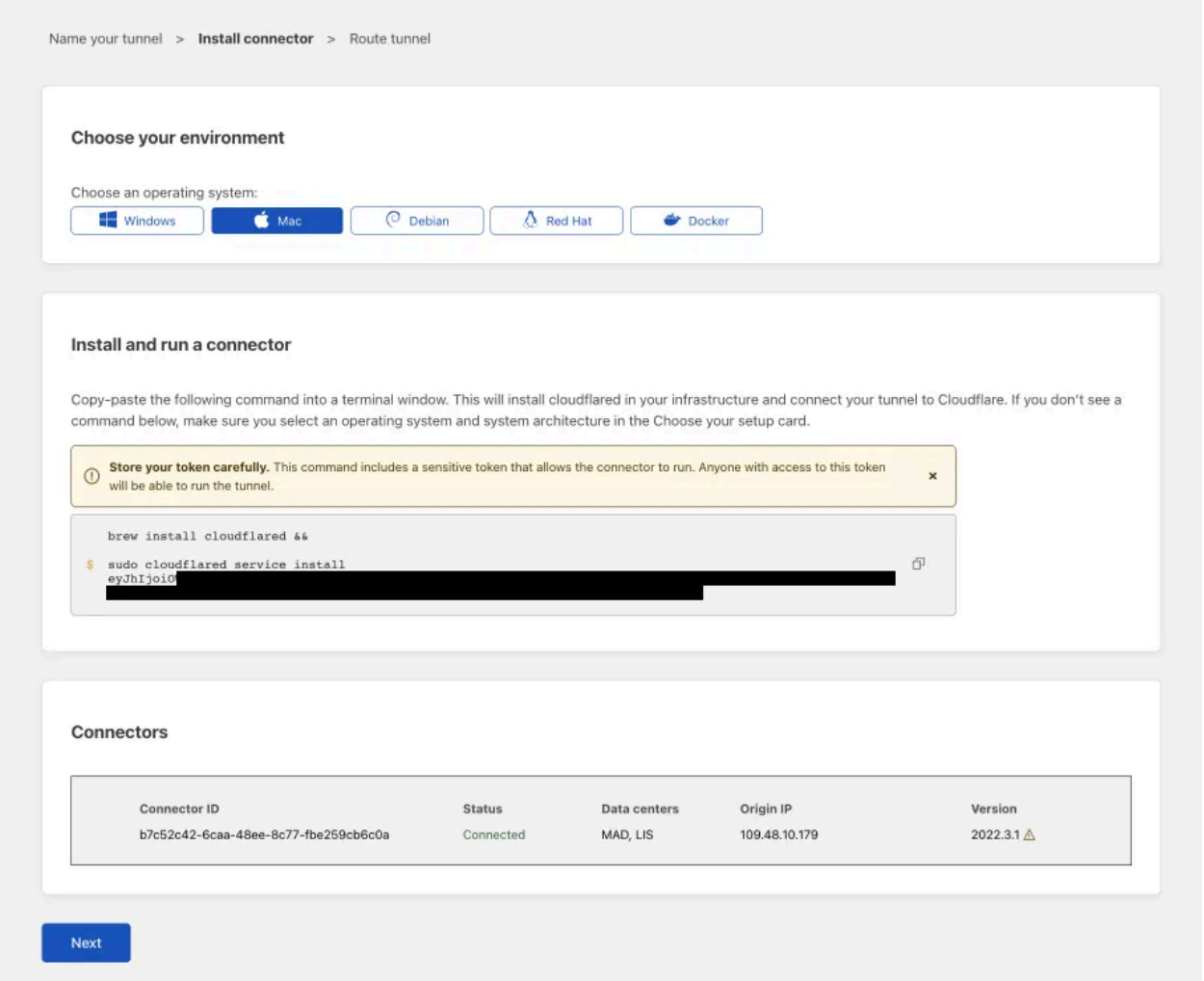
- **Eliminates Public IPs:** Reduces the attack surface by making internal resources unreachable from the public internet unless accessed through Cloudflare.
- **Enhances Security:** Prevents direct attacks on your origin servers by obscuring their IP addresses.

- **Simplifies Access Control:** When used with Cloudflare Access, it allows granular access policies for internal applications without the complexity of traditional VPNs. Only authenticated and authorized users/devices can reach resources.
- **Scales Easily:** Can adapt to growing numbers of applications and users without needing major network re-architecting.

How to set up Cloudflare Tunnel

1. Log in to Zero Trust and go to **Networks** > **Tunnels**.
2. Select **Create a tunnel**.
3. Choose **Cloudflared** for the connector type and select **Next**.
4. Enter a name for your tunnel. We suggest choosing a name that reflects the type of resources you want to connect through this tunnel (for example, `enterprise-VPC-01`).
5. Select **Save tunnel**.
6. Next, you will need to install `cloudflared` and run it. To do so, check that the environment under **Choose an environment** reflects the operating system on your machine, then copy the command in the box below and paste it into a terminal window. Run the command.

7. Once the command has finished running, your connector will appear in Zero Trust.



8. Select **Next**.

Before you connect an application through your tunnel, you must: Add a website to Cloudflare & Change your domain nameservers to Cloudflare. This can be found in the beginning of the guide. Follow these steps to connect an application through your tunnel.

1. In the **Public Hostnames** tab, select **Add a public hostname**.
2. Enter a subdomain and select a **Domain** from the dropdown menu. Specify any subdomain or path information.
3. Specify a service, for example `https://localhost:8000`.
4. Under **Additional application settings**, specify any parameters you would like to add to your tunnel configuration.
5. Select **Save hostname**.

The application is now publicly available on the Internet. To allow or block specific users, create an Access application. Follow these steps to connect a private network through your tunnel.

1. In the **Private Networks** tab, add the IP or CIDR of your service.
2. Select **Save tunnel**.

To configure Zero Trust policies and connect as a user, refer to Connect private networks.

Cloudflare WARP

Cloudflare WARP client allows you to protect corporate devices by securely and privately sending traffic from those devices to Cloudflare's global network. The WARP client also makes it possible to apply advanced Zero Trust policies that check for a device's health before it connects to corporate applications.

Cloudflare WARP is great for small businesses because it provides secure, encrypted internet connections that protect sensitive data (especially on public Wi-Fi) while improving performance through Cloudflare's fast global network. It's easy to set up and manage without needing a dedicated IT team, making it ideal for businesses with limited resources. Plus, it's cost-effective, with a free version available, and can be combined with Cloudflare's advanced security tools for better access control and monitoring. WARP also supports reliable, secure connectivity for remote workers, helping small businesses maintain productivity and data safety without complicated or expensive infrastructure.

How to enable Cloudflare WARP

1. Firstly, configure a One-time PIN or connect a third party identity provider in Zero Trust. This can be done in the Cloudflare Dashboard:
    a. In Zero Trust , go to **Settings** > **Authentication**.
    b. Under **Login methods**, select **Add new**.
    c. Select **One-time PIN**.
2. Next define device enrollment permissions. This defines which users in your organization should be able to connect devices to your organization's Zero Trust setup. As you create your rule, you will be asked to select which login method you would like users to authenticate with.
    a. In Zero Trust go to **Settings** > **WARP Client**.
    b. In **Device enrollment permissions**, select **Manage**.
    c. In the **Rules** tab, configure one or more Access policies to define who can join their device. For example, you could allow all users with a company email address:

Rule type	Selector	Value
Include	Emails ending in	`@company.com`

3. Install the Cloudflare root certificate on your devices. Advanced security features such as HTTPS traffic inspection, Data Loss Prevention, anti-virus scanning, Access for Infrastructure, and Browser Isolation require users to install and trust a root certificate on their device. To generate a new Cloudflare root certificate for your Zero Trust organization in the Cloudflare Dashboard:
    a. In Zero Trust , go to **Settings** > **Resources**.
    b. In **Certificates**, select **Manage**.
    c. Select **Generate certificate**.
    d. Choose a duration of time before the certificate expires. Cloudflare recommends expiration after five years. Alternatively, choose *Custom* and enter a custom amount in days.
    e. Select **Generate certificate**.

The certificate will appear in your list of certificates as **Inactive**. To download a generated certificate, select it, then choose **Download .pem** and/or **Download .crt**. To deploy your certificate and turn it on for inspection, you need to activate the certificate.

To activate your root certificate:

1. In Zero Trust , go to **Settings** > **Resources**.
2. In **Certificates**, select **Manage**.
3. Select the certificate you want to activate.
4. Select **Activate**.

The status of the certificate will change to **Pending** while it deploys. Once the status of your certificate is **Available**, you can install it on your user's devices either with WARP or manually.

Once you deploy and install your certificate, you can turn it on for use in inspection:

1. In Zero Trust, go to **Settings** > **Resources**.
2. In **Certificates**, select **Manage**.
3. Select the certificate you want to turn on.
4. In **Basic information**, select **Confirm and turn on certificate**.

You can set multiple certificates to **Available**, but you can only turn on one certificate for use in inspection at a time. Setting a certificate as **In-Use** will set any other in-use certificates as **Available** only and prevent them from being used for inspection until turned on again.

4. **Download and deploy the WARP client to your devices**. Choose one of the different ways to deploy the WARP client, depending on what works best for your organization.

5**. Log in to your organization's Cloudflare Zero Trust instance from your devices**.

On your device, go to the Settings section in the WARP client and insert your organization's team name.

CLOUDFLARE

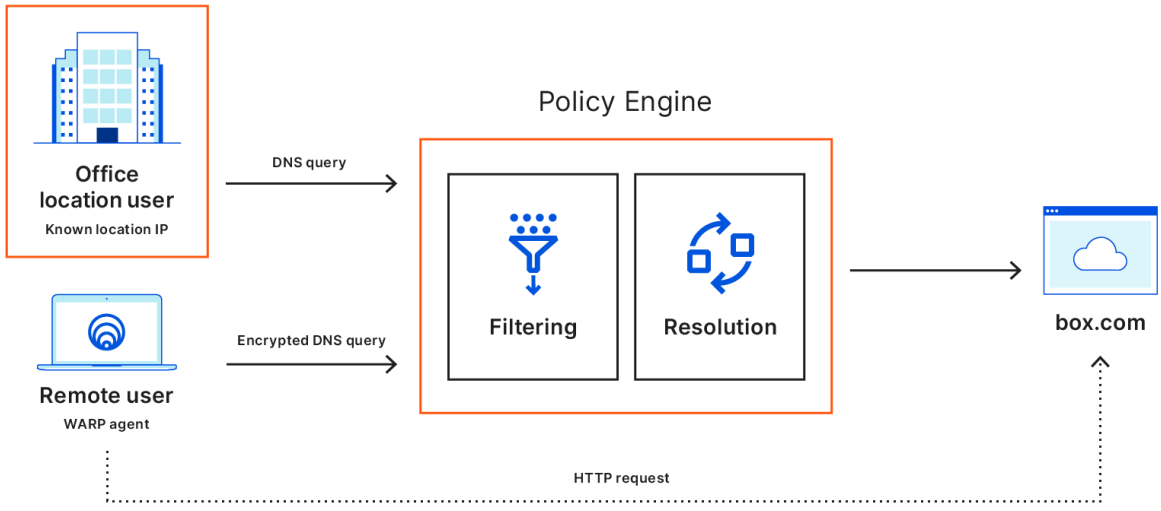
Secure Web Gateway (HTTP filter)

A Secure Web Gateway (SWG) is a critical cybersecurity tool that protects company data by filtering web traffic and enforcing security policies between employees and the Internet. Like a water filter removing contaminants, an SWG blocks harmful content such as malware, phishing sites, or unauthorized applications, before it reaches your business.

For SMEs, which often lack dedicated security teams or complex IT infrastructure, SWGs are especially vital. Cyberattacks increasingly target smaller businesses because they're seen as easier to breach. A single incident can cause major disruption, financial loss, and reputational damage.

SWGs help prevent this by providing:

- **URL filtering** to block malicious or inappropriate websites
- **Anti-malware protection** to detect and stop threats in real time
- **Application control** to monitor and manage what tools employees can use



They also give SMEs visibility into outbound traffic and allow them to set policies that prevent sensitive data from leaving the network—especially when combined with Cloudflare Zero Trust. This adds a crucial layer of defense without the complexity or cost of traditional enterprise solutions.

By deploying a Secure Web Gateway, small businesses can reduce their attack surface, ensure business continuity, and protect customer trust, all while gaining enterprise-grade protection that fits their size and budget.

This can be done through inspecting DNS, Network, HTTP, and Egress traffic:

- **DNS policies** inspect DNS queries. You can block domains and IP addresses from resolving on your devices. For more information on DNS filtering, refer to our Learning Center article.
- **Network policies** inspect individual TCP/UDP/GRE packets. You can block access to specific ports on your origin server, including non-HTTP resources.
- **HTTP policies** inspect HTTP requests. You can block specific URLs from loading, not just the domain itself. For more information on URL filtering, refer to our Learning Center article.
- **Egress policies** inspect traffic to assign egress IP addresses unique to your organization.
- **Resolver policies** inspect DNS queries to enable resolution by custom authoritative nameservers.

Recommended policies depend on the type of traffic you're trying to filter, For example:

- To block websites, create an HTTP policy.
- To block non-HTTP traffic such as SSH and RDP, create a network policy.
- To block malware and other security threats, create both DNS and HTTP policies.
- To assign static IP addresses to your organization's egress traffic, create an egress policy.

How to set up Cloudflare Secure Web Gateway

To filter DNS requests from an individual device such as a laptop or phone:

1. Install WARP client on your device.
2. In the WARP client Settings, log in to your organization's Zero Trust instance.

To filter DNS requests from a location such as an office or data center. You will need to add the location to Zero Trust Settings. To add a DNS location to Gateway:

1. In Zero Trust, go to **Gateway** > **DNS Locations**.
2. Select **Add a location**.
3. Choose a name for your DNS location.
4. Choose at least one DNS endpoint to resolve your organization's DNS queries.
5. (Optional) Toggle the following settings:

    - **Enable EDNS client subnet** sends a user's IP geolocation to authoritative DNS nameservers. EDNS Client Subnet (ECS) helps reduce latency by routing the user to the closest origin server. Cloudflare enables EDNS in a privacy preserving way by not sending the user's exact IP address but rather the first `/24` range of the larger range that contains their IP address. This `/24` range will share the same geographic location as the user's exact IP address.
    - **Set as Default DNS Location** sets this location as the default DoH endpoint for DNS queries.
6. Select **Continue**.
7. (Optional) Turn on source IP filtering for your configured endpoints, then add any source IPv4/IPv6 addresses to validate.
    - Endpoint authentication is required for standard IPv4 addresses and optional for dedicated IPv4 addresses.
    - **DoH endpoint filtering & authentication** lets you restrict DNS resolution to only valid identities or user tokens in addition to IPv4/IPv6 addresses.
8. Select **Continue**.
9. Review the settings for your DNS location, then choose **Done**.
10. Change the DNS resolvers on your router, browser, or OS by following the setup instructions in the UI.
11. Select **Go to DNS Location**. Your location will appear in your list of locations.

To create a new DNS policy:

1. In Zero Trust, go to **Gateway** > **Firewall policies**.
2. In the **DNS** tab, select **Add a policy**.
3. Name the policy.
4. Under **Traffic**, build a logical expression that defines the traffic you want to allow or block.
5. Choose an **Action** to take when traffic matches the logical expression. For example, we recommend adding a policy to block all security categories:

Selector	Operator	Value	Action
Security Categories	in	*All security risks*	Block

6. Select **Create policy**.

Refer to our list of common DNS policies for other policies you may want to create.

Network Filtering:

1. To install a WARP client on your device.
2. In the WARP client Settings, log in to your organization's Zero Trust instance.
3. Enable the Gateway proxy for TCP. This is done in your Zero Trust settings, go to Network, then to Firewall, and turn on Proxy. Then select TCP.
4. Optionally, you can enable the UDP proxy to inspect all port 443 UDP traffic.

To verify your device is connected to Zero Trust:

1. In Zero Trust, go to **Settings** > **Network**.
2. Under **Gateway logging**, enable activity logging for all Network logs.
3. On your WARP-enabled device, open a browser and visit any website.
4. Determine the **Source IP** for your device:
    1. Open the WARP client settings.
    2. Go to **Preferences** > **General**.
    3. Note the **Public IP**.
5. In Zero Trust, go to **Logs** > **Gateway** > **Network**. Before building Network policies, make sure you see Network logs from the Source IP assigned to your device.

To create a new network policy:

1. In Zero Trust, go to **Gateway** > **Firewall policies**.
2. In the **Network** tab, select **Add a policy**.
3. Name the policy.
4. Under **Traffic**, build a logical expression that defines the traffic you want to allow or block.
5. Choose an **Action** to take when traffic matches the logical expression. For example, you can use a list of device serial numbers to ensure users can only access an application if they connect with the WARP client from a company device:

Selector	Operator	Value	Logic	Action
SNI Domain	is	`internalapp.com`	And	Block
Passed Device Posture Checks	not in	*Device serial numbers*		

6. Select **Create policy**.

Refer to our list of common network policies for policies you may want to create.

HTTP Filtering:

For HTTP filtering, a Cloudflare root certificate will need to be installed before the WARP Client. Instructions on how to do so can be found here.

1. Install the WARP client on your device.
2. In the WARP client Settings, log in to your organization's Zero Trust instance.
3. Enable the Gateway proxy for TCP. Optionally, you can enable the UDP proxy to inspect all port 443 UDP traffic.
4. To inspect HTTPS traffic, enable TLS decryption.
5. (Optional) To scan file uploads and downloads for malware, enable anti-virus scanning.

To verify your device is connected to Zero Trust:

1. In Zero Trust , go to **Settings** > **Network**.
2. Under **Gateway logging**, enable activity logging for all HTTP logs.
3. On your device, open a browser and go to any website.
4. In Zero Trust, go to **Logs** > **Gateway** > **HTTP**.
5. Make sure HTTP requests from your device appear.

To create a new HTTP policy:

1. In Zero Trust, go to **Gateway** > **Firewall policies**.
2. In the **HTTP** tab, select **Add a policy**.
3. Name the policy.
4. Under **Traffic**, build a logical expression that defines the traffic you want to allow or block.
5. Choose an **Action** to take when traffic matches the logical expression. For example, if you have configured TLS decryption, some applications that use embedded certificates may not support HTTP inspection, such as some Google products. You can create a policy to bypass inspection for these applications:

Selector	Operator	Value	Action
Application	in	*Do Not Inspect*	Do Not Inspect

6. Cloudflare also recommends adding a policy to block known threats such as Command & Control, Botnet and Malware based on Cloudflare's threat intelligence:

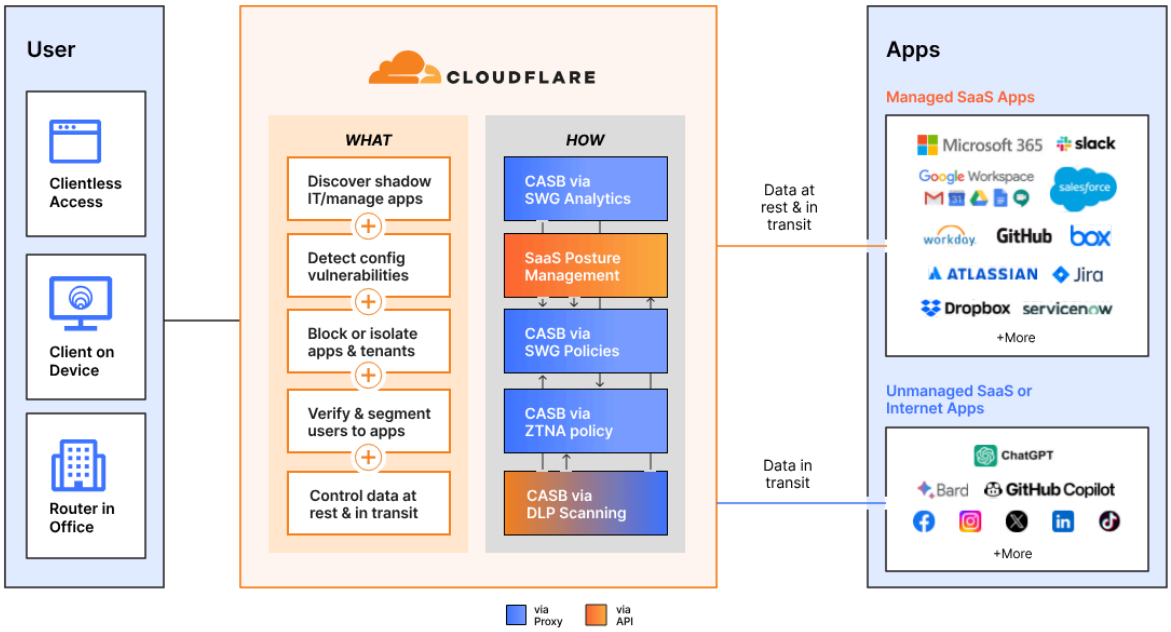
Selector	Operator	Value	Action
Security Categories	in	*All security risks*	Block

7. Select **Create policy**.

Refer to our list of common HTTP policies for other policies you may want to create.

Cloudflare Access Security Broker

Cloudflare Access Security Broker (CASB) is a cloud based security tool that helps small businesses see and control how their cloud apps and services are used. It protects against risks like unauthorized access, data leaks, and breaking compliance rules. CASB finds “shadow IT” , cloud tools being used without permission, that can cause security problems. It also stops sensitive data from leaving your company’s control and protects that data from threats. CASBs block outside attacks and help businesses follow important security rules when using the cloud.



For SMEs, CASB is important because it applies Zero Trust principles, meaning it never assumes access is safe and always checks users and devices. It controls who can access sensitive data, monitors activity, and encrypts data in the cloud. This is especially helpful for small businesses using cloud services that may not have big IT teams to handle complicated security setups.

How to get setup with Cloudflare CASB

Before you can integrate a SaaS application or cloud environment with CASB, your account with that integration must meet certain requirements. Refer to the SaaS application or cloud environment's integration guide to learn more about the prerequisites and permissions.

How to add an integration:

1. In Zero Trust, go to **CASB > Integrations.**
2. Select Connect an integration or Add integration.
3. Browse the available integrations and select the application you would like to add.
4. Follow the step-by-step integration instructions in the UI.
5. To run your first scan, select Save integration.

After the first scan, CASB will automatically scan your SaaS application or cloud environment on a frequent basis to keep up with any changes. Scan intervals will vary due to each application having their own set of requirements, but the frequency is typically between every 1 hour and every 24 hours. More information on CASB can be found here.

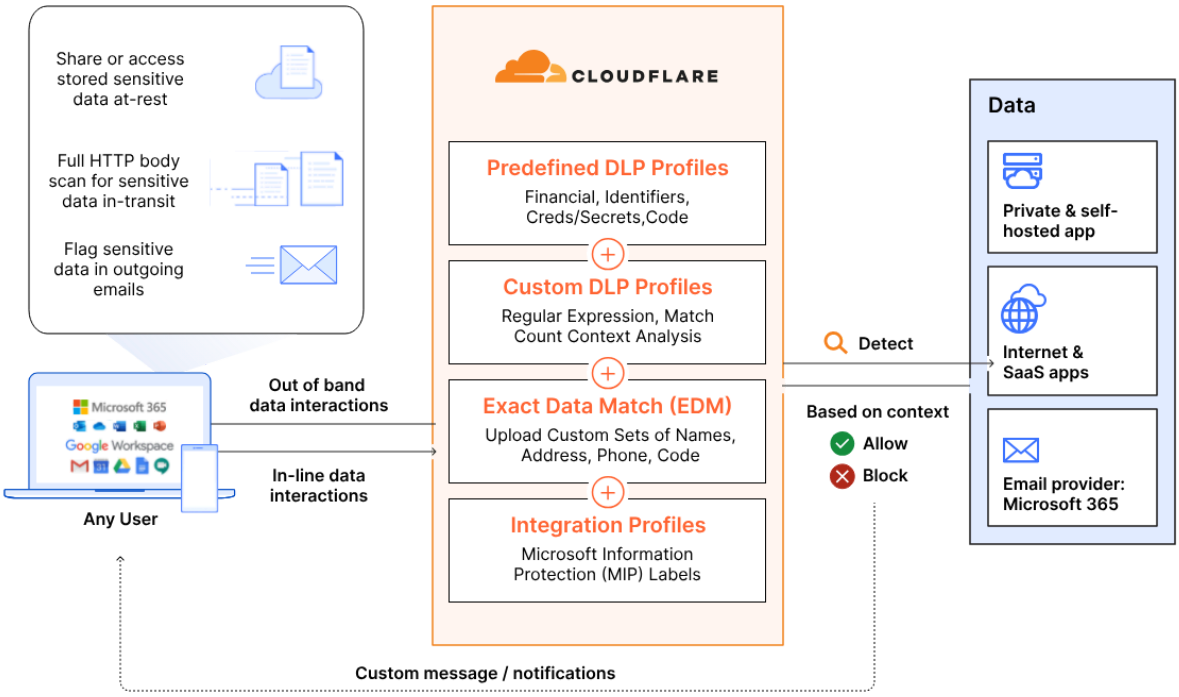
Once CASB detects at least one finding, you can view and manage your findings. Findings are security issues detected within SaaS and cloud applications that involve users, data at rest, and other configuration settings. Cloudflare CASB labels each finding with one of the following severity levels:

Severity level	Urgency
Critical	Suggests the finding is something your team should act on today.
High	Suggests the finding is something your team should act on this week.
Medium	Suggests the finding should be reviewed sometime this month.
Low	Suggests the finding is informational or part of a scheduled review process.

Data Loss Prevention (DLP)

After setting up the core elements of your Zero Trust architecture, your network will begin generating large amounts of data about internal activity. At this stage, it's important to implement Data Loss Prevention (DLP) and logging. DLP involves a set of tools and processes designed to protect sensitive information within your business and detect any attempts at data leakage. The first step is to identify where your sensitive data resides, then apply Zero Trust controls to prevent unauthorized access and data exfiltration.

Cloudflare's DLP solution scans your web traffic and SaaS applications for sensitive data such as social security numbers, financial details, secret keys, and source code. It integrates with Cloudflare's Secure Web Gateway to inspect HTTP requests, including uploaded or downloaded files, chat messages, forms, and other web content. Additionally, Cloudflare DLP works alongside Cloudflare CASB to detect sensitive information stored in your cloud applications.



Set up of Cloudflare Data Loss Prevention (DLP)

Firstly, DLP profiles need to be defined.

1. In Zero Trust, go to **DLP** > **DLP profiles**.
2. Choose a predefined profile and select **Configure**.
3. Enable one or more **Detection entries** according to your preferences. The DLP Profile matches using the OR logical operator — if multiple entries are enabled, your data needs to match only one of the entries.
4. Select **Save profile**.

You can also configure your own custom DLP profiles, with instructions found here.

Secondly, sensitive data needs to be defined.

If your organization is most concerned about general data patterns that fit existing classifications such as personal identifiable information (PII), protected health information (PHI), financial information, or source code, Cloudflare has default predefined profiles.

However, if this doesn't fit the needs of your organization, then you can build a complex profile that matches data to both an existing library and a custom string detection or database. For example:

Selector	Operator	Value	Logic	Action
DLP Profile	in	*Credentials and Secrets*	Or	Block
DLP Profile	in	*AWS Key Dataset*		

To start applying data loss prevention, create policies targeting sensitive data types and high-risk destinations, both inside and outside your organization. After analyzing data flow from these known sources, you can focus on more specific datasets from broader sources. It's also important to allow trusted internal locations where sensitive data is intentionally shared. We've developed examples, in addition to the one above, on our developer documents.

Example implementation timeline for Cloudflare

Every Cloudflare path is unique but there are a common set of steps that most projects follow. This is a recommended timeline for your business to get started with Cloudflare.

Timeline	Goal	Relevant Products
Phase 1	☐ Protect applications from Layer 7 attacks (DDoS, Injection, Bots, etc.)	Cloudflare Website Security tools (section 1 of this guide)
	☐ Deploy global DNS filtering	Cloudflare Gateway
	☐ Identify misconfigurations and publicly shared data in SaaS tools	Cloudflare CASB
Phase 2	☐ Establish corporate identity	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
	☐ Enforce MFA for all application	**Identity providers:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin, Duo (outside of Cloudflare products) **Application Reverse Proxies:** Cloudflare Access
	☐ Enforce HTTPS and DNSSEC	Cloudflare Website Security tools (section 1 of this guide)
	☐ Block or isolate threats behind SSL	**TLS Decryption:** Cloudflare Gateway
	☐ Zero Trust policy enforcement for publicly addressable applications	**Zero Trust Reverse Proxies:** Cloudflare Access
	☐ Close all inbound ports open to the Internet for application delivery	Cloudflare Access
Phase 3	☐ Inventory all corporate applications	**Secure Web Gateway and CASB with Shadow IT discovery:** Cloudflare Gateway

	🔲 Zero Trust policy enforcement for SaaS applications	**Zero Trust Network Access (ZTNA):** Cloudflare Access **CASB:** Cloudflare CASB
	🔲 Segment user network access	Cloudflare Zero Trust (Access and Gateway)
	🔲 Zero Trust Network Access for critical privately addressable applications	Cloudflare Access
	🔲 Define what data is sensitive and where it exists	DataDog, Splunk, SolarWinds (outside of Cloudflare products)
	🔲 Send out hardware-based authentication tokens	**Hard Keys:** Yubico (outside of Cloudflare products)
	🔲 Stay up to date on known threat actors	Cloudflare Radar, CISA, OWASP
Phase 4	🔲 Enforce hardware token-based MFA	**Hard Keys:** Yubico (outside of Cloudflare products)
	🔲 Zero Trust policy enforcement and network access for *all* applications	Cloudflare Access
	🔲 Establish a process to log and review employee activity on sensitive applications	**Secure Web Gateway (SWG):** Cloudflare Gateway **Security Incident and Event Monitoring (SIEM):** DataDog, Splunk, SolarWinds (outside of Cloudflare products)
	🔲 Stop sensitive data from leaving your applications (e.g. PII, credit cards, SSNs)	Cloudflare Gateway