Zero Trust security | What is a Zero Trust network?

Zero Trust is a security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter.

Zero Trust Security

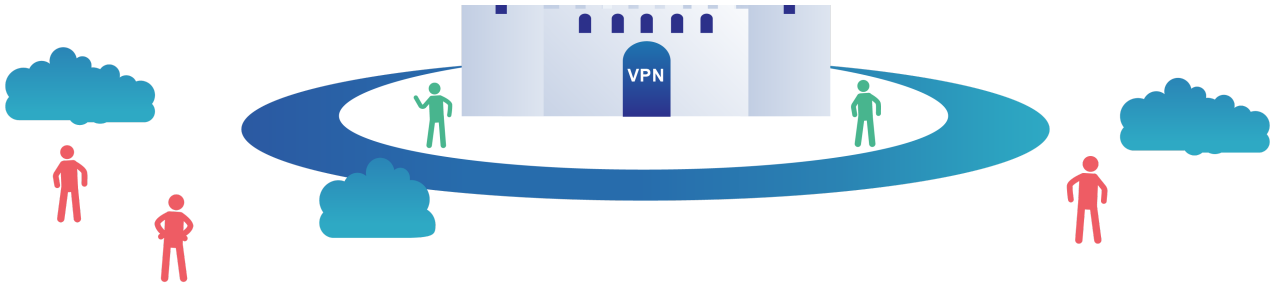
Copy article link

What is Zero Trust security?

Zero Trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. ZTNA is the main technology associated with Zero Trust architecture; but Zero Trust is a holistic approach to network security that incorporates several different principles and technologies.

More simply put: traditional IT network security trusts anyone and anything inside the network. A Zero Trust architecture trusts no one and nothing.

Traditional IT network security is based on the castle-and-moat concept. In castle-and-moat security, it is hard to obtain access from outside the network, but everyone inside the network is trusted by default. The problem with this approach is that once an attacker gains access to the network, they have free rein over everything inside.



This vulnerability in castle-and-moat security systems is exacerbated by the fact that companies no longer have their data in just one place. Today, information is often spread across cloud vendors, which makes it more difficult to have a single security control for an entire network.

Zero Trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network. This added layer of security has been shown to prevent data breaches. Studies have shown that the average cost of a single data breach is over $3 million. Considering that figure, it should come as no surprise that many organizations are now eager to adopt a Zero Trust security policy.

What are the main principles behind Zero Trust security?

Continuous monitoring and validation

The philosophy behind a Zero Trust network assumes that there are attackers both within and outside of the network, so no users or machines should be automatically trusted. Zero Trust verifies user identity and privileges as well as device identity and security. Logins and connections time out periodically once established, forcing users and devices to be continuously re-verified.

Least privilege

Another principle of zero trust security is least-privilege access. This means giving users only as much access as they need, like an army general giving soldiers information on a need-to-know basis. This minimizes each user's exposure to sensitive parts of the network.

Implementing least privilege involves careful managing of user permissions. VPNs are not well-suited for least-privilege approaches to authorization, as logging in to a VPN gives a user access to the whole connected network.

Device access control

In addition to controls on user access, Zero Trust also requires strict controls on device access. Zero Trust systems need to monitor how many different devices are trying to access their network, ensure that every device is authorized, and assess all devices to make sure they have not been compromised. This further minimizes the attack surface of the network.

Microsegmentation

Zero Trust networks also utilize microsegmentation. Microsegmentation is the practice of breaking up security perimeters into small zones to maintain separate access for separate parts of the network. For example, a network with files living in a single data center that utilizes microsegmentation may contain dozens of separate, secure zones. A person or program with access to one of those zones will not be able to access any of the other zones without separate authorization.

Preventing lateral movement

In network security, "lateral movement" is when an attacker moves within a network after gaining access to that network. Lateral movement can be difficult to detect even if the attacker's entry point is discovered, because the attacker will have gone on to compromise other parts of the network.

Zero Trust is designed to contain attackers so that they cannot move laterally. Because Zero Trust access is segmented and has to be re-established periodically, an attacker cannot move across to other microsegments within the network. Once the attacker's presence is detected, the compromised device or user account can be quarantined, cut off from further access. (In a castle-and-moat model, if lateral movement is possible for the attacker, quarantining the original compromised device or user has little to no effect, since the attacker will already have reached other parts of the network.)

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is also a core value of Zero Trust security. MFA means requiring more than one piece of evidence to authenticate a user; just entering a password is not enough to gain access. A commonly seen application of MFA is the 2-factor

authorization (2FA) used on online platforms like Facebook and Google. In addition to entering a password, users who enable 2FA for these services must also enter a code sent to another device, such as a mobile phone, thus providing two pieces of evidence that they are who they claim to be.

What is the history of Zero Trust security?

The term "Zero Trust" was coined by an analyst at Forrester Research Inc. in 2010 when the model for the concept was first presented. A few years later, Google announced that they had implemented Zero Trust security in their network, which led to a growing interest in adoption within the tech community. In 2019, Gartner, a global research and advisory firm, listed Zero Trust security access as a core component of secure access service edge (SASE) solutions.

What is Zero Trust Network Access (ZTNA)?

Zero Trust Network Access (ZTNA) is the main technology that enables organizations to implement Zero Trust security. Similar to a software-defined perimeter (SDP), ZTNA conceals most infrastructure and services, setting up one-to-one encrypted connections between devices and the resources they need. Learn more about how ZTNA works.

How to implement Zero Trust security

Zero Trust may sound complex, but adopting this security model can be relatively simple with the right technology partner. For instance, Cloudflare One is a SASE platform that combines networking services with a built-in Zero Trust approach to user and device access. With Cloudflare One, customers automatically implement Zero Trust protection around all their assets and data.

RELATED CONTENT

What is ZTNA?

Castle-and-Moat Security

What is SASE?

What is IAM?

Network Perimeter

What is SASE? | Secure access service edge

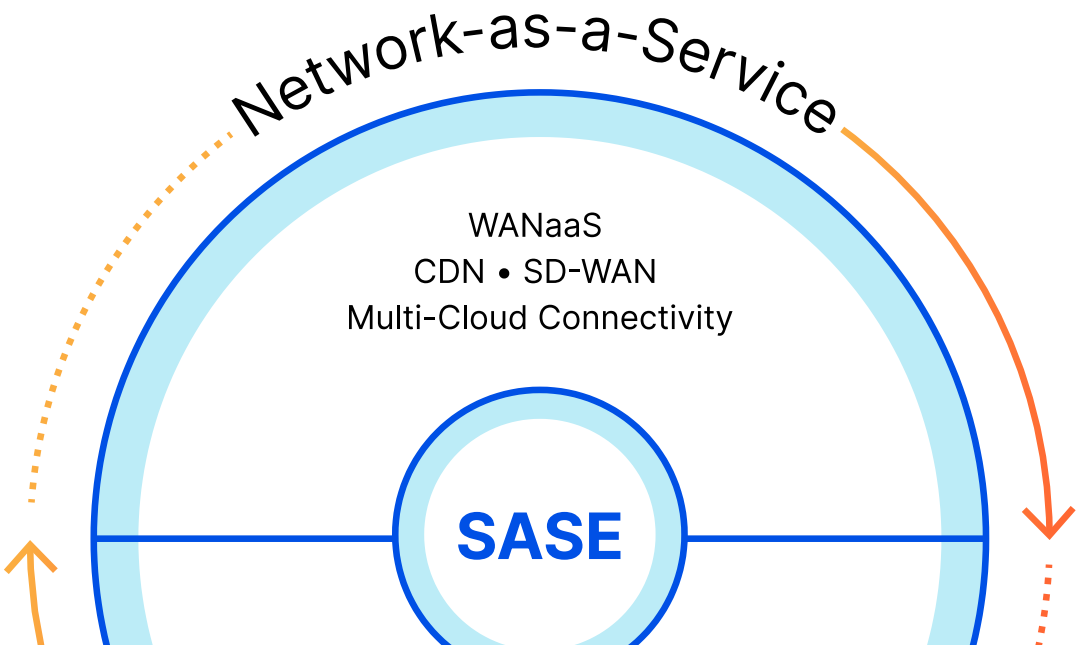
Secure access service edge, or SASE, is a cloud-based IT model that combines networking and security services.

Copy article link

What is SASE?

Secure access service edge, or SASE, is a cloud-based IT model that bundles software-defined networking with network security functions and delivers them from a single service provider. Gartner, a global research and advisory firm, coined the term "SASE" in 2019.

A SASE approach offers better control over and visibility into the users, traffic, and data accessing a corporate network — vital capabilities for modern, globally distributed organizations. Networks built with SASE are flexible and scalable, able to connect globally distributed employees and offices across any location and via any device.



What security capabilities does SASE include?

SASE combines software-defined wide area networking (SD-WAN) capabilities with a number of network security functions, all of which are delivered from a single cloud platform. In this way, SASE enables employees to authenticate and securely connect to internal resources from anywhere, and gives organizations better control over the traffic and data that enters and leaves their internal network.

SASE includes four core security components:

1. *Secure web gateways (SWG):* An SWG prevents cyber threats and data breaches by filtering unwanted content from web traffic, blocking unauthorized user behavior, and enforcing company security policies. SWGs can be deployed anywhere, making them ideal for securing remote workforces.

2. *Cloud access security broker (CASB):* A CASB performs several security functions for cloud-hosted services, including revealing shadow IT (unauthorized corporate systems), securing confidential data through access control and data loss prevention (DLP), and ensuring compliance with data privacy regulations.

3. *Zero trust network access (ZTNA):* ZTNA platforms lock down internal resources from public view and help defend against potential data breaches by requiring real-time verification of every user and device to every protected application.

4. *Firewall-as-a-Service (FWaaS):* FWaaS refers to firewalls delivered from the cloud as a service. FWaaS protects cloud-based platforms, infrastructure, and applications from cyber attacks. Unlike traditional firewalls, FWaaS is not a physical appliance, but a set of security capabilities that includes URL filtering, intrusion prevention, and uniform policy management across all network traffic.

Depending on the vendor and the needs of the enterprise, these core components may be bundled with additional security services, including web application and API protection

(WAAP), remote browser isolation, or Wi-Fi hotspot protection.

What are the advantages of a SASE framework?

SASE offers several benefits compared to a traditional, data center-based network security model:

- **Identity-based Zero Trust network access.** SASE leans heavily on a Zero Trust security model, which does not grant a user access to applications and data until their identity has been verified — even if they are already inside the perimeter of a private network. When establishing access policies, a SASE approach takes more than an entity's identity into account; it also considers factors like user location, time of day, enterprise security standards, compliance policies, and an ongoing evaluation of risk/trust.

- **Blocking attacks against network infrastructure.** The firewall and CASB components of SASE help prevent external attacks (like DDoS attacks and vulnerability exploits) from getting in and compromising internal resources. Both on-premise and cloud-based networks can be protected by a SASE approach.

- **Preventing malicious activity.** By filtering URLs, DNS queries, and other outgoing and incoming network traffic, SASE helps prevent malware-based attacks, data exfiltration, and other threats to corporate data.

- **Streamlined implementation and management.** SASE merges single-point security solutions into one cloud-based service, freeing enterprises to interact with fewer vendors and to spend less time, money, and internal resources configuring physical infrastructure.

- **Simplified policy management.** Instead of juggling multiple policies for separate solutions, SASE allows organizations to set, adjust, and enforce access policies across all locations, users, devices, and applications from a single portal.

- **Latency-optimized routing.** SASE helps cut down on latency by routing network traffic across a global edge network in which traffic is processed as close to the user as possible. Routing optimizations can help determine the fastest network path based on network congestion and other factors.

How does SASE compare to traditional

networking?

In a traditional network model, data and applications live in a core data center. In order to access those resources, users, branch offices, and applications connect to the data center from within a localized private network or a secondary network that typically connects to the primary one through a secure leased line or VPN.

This model has proved to be ill-equipped to handle the complexities introduced by cloud-based services like software-as-a-service (SaaS) and the rise of distributed workforces. It is no longer practical to reroute all traffic through a centralized data center if applications and data are hosted in the cloud.

By contrast, SASE places network controls on the cloud edge — not the corporate data center. Instead of layering cloud services that require separate configuration and management, SASE streamlines network and security services to create a secure network edge. Implementing identity-based, Zero Trust access policies on the edge network allows enterprises to expand their network perimeter to any remote user, branch office, device, or application.

How organizations can implement SASE

Many organizations take a piecemeal approach to SASE implementation. In fact, some may have already adopted certain SASE elements without knowing it. Key steps organizations can take towards fully adopting a SASE model include:

1. Securing remote workforces
2. Placing branch offices behind a cloud perimeter
3. Moving DDoS protection to the edge
4. Migrating self-hosted applications to the cloud
5. Replacing security appliances with unified, cloud-native policy enforcement

These steps are broken down further in the white paper "Getting started with SASE," available for download here.

How Cloudflare enables SASE

Cloudflare is uniquely architected to deliver a platform of integrated network and security

Cloudflare is uniquely architected to deliver a platform of integrated network and security services across data centers in over 250 globally distributed cities, eliminating the need for enterprises to purchase and manage a complex collection of point solutions.

Cloudflare One is a SASE platform that securely connects remote users, offices, and data centers to each other and the resources that they need. To get started with Cloudflare One, see the Cloudflare One product page. Or, learn more about ZTNA, a crucial technology behind SASE.

RELATED CONTENT

Zero Trust Security

Secure Web Gateway

What is IAM?

Access Control

Software Defined Perimeter

What is identity and access management (IAM)?

Identity and access management (IAM) systems verify user identities and control user privileges.

What is IAM?

Copy article link

What is identity and access management (IAM)?

Identity and access management (IAM or IdAM for short) is a way to tell who a user is and what they are allowed to do. IAM is like the bouncer at the door of a nightclub with a list of who is allowed in, who isn't allowed in, and who is able to access the VIP area. IAM is also called identity management (IdM).

In more technical terms, IAM is a means of managing a given set of users' digital identities, and the privileges associated with each identity. It is an umbrella term that covers a number of different products that all do this same basic function. Within an organization, IAM may be a single product, or it may be a combination of processes, software products, cloud services, and hardware that give administrators visibility and control over the organizational data that individual users can access.

What is identity in the context of computing?

A person's entire identity cannot be uploaded and stored in a computer, so "identity" in a computing context means a certain set of properties that can be conveniently measured and recorded digitally. Think of an ID card or a passport: not every fact about a person is recorded in an ID card, but it contains enough personal characteristics that a person's identity can quickly be matched to the ID card.

To verify identity, a computer system will assess a user for characteristics that are specific to them. If they match, the user's identity is confirmed. These characteristics are also known as "authentication factors," because they help authenticate that a user is who they say they are.

The three most widely used authentication factors are:

- Something the user knows

- Something the user has
- Something the user is

Something the user knows: This factor is a piece of knowledge that only one user should have, like a username and password combination.

Imagine that John wants to check his work email from home. To do so, he will first have to log in to his email account by establishing his identity, because if somebody who wasn't John accessed John's email, then company data would be compromised.

John logs in by entering his email, *john@company.com*, and the password that only he knows – for example, *"5jt*2)f12?y"*. Presumably, no one else besides John knows this password, so the email system recognizes John and lets him access his email account. If someone else tried to impersonate John by entering their email address as *"john@company.com,"* they wouldn't be successful without knowing to type *"5jt*2)f12?y"* as the password.

Something the user has: This factor refers to possession of a physical token that is issued to authorized users. The most basic example of this authentication factor is the use of a

physical house key to enter one's home. The assumption is that only someone who owns, rents, or otherwise is allowed into the house will have a key.

In a computing context, the physical object could be a key fob, a USB device, or even a smartphone. Suppose that John's organization wanted to be extra sure that all users really were who they said they were by checking two authentication factors instead of one. Now, instead of just entering his secret password – the something the user knows factor – John has to show the email system that he possesses an object that no one else has. John is the only person in the world who possesses his personal smartphone, so the email system texts him a one-time code, and John types in the code to demonstrate his possession of the phone.

Something the user is: This refers to a physical property of one's body. A common example of this authentication factor in action is Face ID, the feature offered by many modern smartphones. Fingerprint scanning is another example. Less common methods used by some high-security organizations include retina scans and blood tests.

Imagine John's organization decides to tighten security even more by making users verify three factors instead of two (this is rare). Now John has to enter his password, verify possession of his smartphone, and scan his fingerprint before the email system confirms that he really is John.

To summarize: In the real world, one's identity is a complex mix of personal characteristics, history, location, and other factors. In the digital world, a user's identity is made up of some or all of the three authentication factors, stored digitally in an identity database. To prevent

impostors from impersonating real users, computer systems will check a user's identity against the identity database.

What is access management?

"Access" refers to what data a user can see and what actions they can perform once they log in. Once John logs into his email, he can see all the emails he has sent and received. However, he should not be able to see the emails sent and received by Tracy, his coworker.

In other words, just because a user's identity is verified, that doesn't mean they should be able to access whatever they want within a system or a network. For instance, a low-level employee within a company should be able to access their corporate email account, but they should not be able to access payroll records or confidential HR information.

Access management is the process of controlling and tracking access. Each user within a system will have different privileges within that system based on their individual needs. An accountant does indeed need to access and edit payroll records, so once they verify their identity, they should be able to view and update those records as well as access their email account.

Why is IAM so important for cloud computing?

In cloud computing, data is stored remotely and accessed over the Internet. Because users can connect to the Internet from almost any location and any device, most cloud services are device- and location-agnostic. Users no longer need to be in the office or on a company-owned device to access the cloud. And in fact, remote workforces are becoming more common.

As a result, identity becomes the most important point of controlling access, not the network perimeter.* The user's identity, not their device or location, determines what cloud data they can access and whether they can have any access at all.

To understand why identity is so important, here's an illustration. Suppose a cyber criminal wants to access sensitive files in a company's corporate data center. In the days before cloud computing was widely adopted, the cyber criminal would have to get past the corporate firewall protecting the internal network or physically access the server by breaking into the building or bribing an internal employee. The criminal's main goal would be to get past the network perimeter.

However, with cloud computing, sensitive files are stored in a remote cloud server. Because

However, with cloud computing, sensitive files are stored in a remote cloud server. Because employees of the company need to access the files, they do so by logging in via browser or an app. If a cyber criminal wants to access the files, now all they need is employee login credentials (like a username and password) and an Internet connection; the criminal doesn't need to get past a network perimeter.

IAM helps prevent identity-based attacks and data breaches that come from privilege escalations (when an unauthorized user has too much access). Thus, IAM systems are essential for cloud computing, and for managing remote teams.

**Network perimeter refers to the edges of an internal network; it is a virtual boundary that separates the secure managed internal network from the unsecured, uncontrolled Internet. All computers in an office, plus connected devices like office printers, are within this perimeter, but a remote server in a data center across the world are not.*

Where does IAM fit in a cloud deployment stack/cloud architecture?

IAM often is a cloud service that users have to pass through to get to the rest of an organization's cloud infrastructure. It can also be deployed on an organization's premises on an internal network. Finally, some public cloud vendors may bundle IAM with their other services.

Businesses using a multicloud or hybrid cloud architecture may instead use a separate vendor for IAM. Decoupling IAM from their other public or private cloud services offers them more flexibility: they can still maintain their identity and access their database if they switch cloud vendors.

What is an identity provider (IdP)?

An identity provider (IdP) is a product or service that helps manage identity. An IdP often handles the actual login process. Single sign-on (SSO) providers fit into this category. IdPs can be part of an IAM framework, but typically they don't help with managing user access.

What is Identity-as-a-Service (IDaaS)?

Identity-as-a-Service (IDaaS) is a cloud service that verifies identity. It is a SaaS offering from a cloud vendor, a way of partially outsourcing identity management. In some cases,

IDaaS and IdP are essentially interchangeable – but in other cases, the IDaaS vendor offers additional capabilities on top of identity verification and management. Depending on the capabilities offered by the IDaaS vendor, IDaaS can be a part of an IAM framework, or it can be the whole IAM system.

How does Cloudflare assist with IAM and the cloud?

Cloudflare Access is an IAM product that monitors user access to any domain, application, or path hosted on Cloudflare. It integrates with SSO providers and allows administrators to alter and customize user permissions. Cloudflare Access helps enforce security policies for both on-premises internal employees and remote workers.

Cloudflare can be deployed in front of any cloud infrastructure setup, allowing greater flexibility to companies with a multicloud or a hybrid cloud deployment that includes an IAM provider.

RELATED CONTENT

Access Control

What is SASE?

Zero Trust Security

Identity Provider (IdP)

Secure Web Gateway

About Zero Trust

VPN Resources

Glossary

Learning Center Navigation

What is SAML? | How SAML authentication works

SAML is the technical standard used by SSO providers to communicate that a user is authenticated.

Authentication

Copy article link

What is SAML?

Security Assertion Markup Language, or SAML, is a standardized way to tell external applications and services that a user is who they say they are. SAML makes single sign-on (SSO) technology possible by providing a way to authenticate a user once and then communicate that authentication to multiple applications. The most current version of SAML is SAML 2.0.

Think of SAML authentication as being like an identification card: a short, standardized way to show who someone is. Instead of, say, conducting a series of DNA tests to confirm someone's identity, it is possible to just glance at their ID card.

In computing and networking, one of the major challenges is getting systems and devices built by different vendors for different purposes to work together. This is called "interoperability": the ability for different machines to interact with each other, despite their differing technical specifications. SAML is an interoperable standard — it is a widely accepted way to communicate a user's identity to cloud service providers.

What is single sign-on (SSO)?

Single sign-on (SSO) is a way for users to be authenticated for multiple applications and services at once. With SSO, a user signs in at a single login screen and can then use a number of apps. Users do not need to confirm their identity with every single service they use.

For this to take place, the SSO system must communicate with every external app to tell them that the user is signed in — which is where SAML comes into play.

How does SAML work?

A typical SSO authentication process involves these three parties:

- Principal (also known as the "subject")
- Identity provider
- Service provider

Principal/subject: This is almost always a human user who is trying to access a cloud-hosted application.

Identity provider: An identity provider (IdP) is a cloud software service that stores and confirms user identity, typically through a login process. Essentially, an IdP's role is to say, "I know this person, and here is what they are allowed to do." An SSO system may in fact be separate from the IdP, but in those cases the SSO essentially acts as a representative for the IdP, so for all intents and purposes they are the same in a SAML workflow.

Service provider: This is the cloud-hosted application or service the user wants to use. Common examples include cloud email platforms such as Gmail and Microsoft Office 365, cloud storage services such as Google Drive and AWS S3, and communications apps such as Slack and Skype. Ordinarily a user would just log in to these services directly, but when SSO is used, the user logs into the SSO instead, and SAML is used to give them access instead of a direct login.

This is what a typical flow might look like: The principal makes a request of the service provider. The service provider then requests authentication from the identity provider. The identity provider sends a **SAML** assertion to the service provider, and the service provider can then send a response to the principal.

If the principal (the user) was not already logged in, the identity provider may prompt them to log in before sending a SAML assertion.

What is a SAML assertion?

A SAML assertion is the message that tells a service provider that a user is signed in. SAML assertions contain all the information necessary for a service provider to confirm user

assertions contain all the information necessary for a service provider to confirm user identity, including the source of the assertion, the time it was issued, and the conditions that make the assertion valid.

Think of a SAML assertion as being like the contents of a reference for a job candidate: the person providing the reference says when and for how long they worked with the candidate, what their role was, and their opinion on the candidate. Based on this reference, a company can make a decision about hiring the candidate, just as a SaaS application or cloud service can allow or deny user access based on a SAML assertion.

What is SAML 2.0?

SAML 2.0 is the modern version of SAML, and it has been in use since 2005. SAML 2.0 combined several versions of SAML that had previously been in use. Many systems support earlier versions, such as SAML 1.1, for backwards compatibility, but SAML 2.0 is the modern standard.

Is SAML authentication the same thing as user authorization?

SAML is a technology for user authentication, not user authorization, and this is a key distinction. User authorization is a separate area of identity and access management.

Authentication refers to a user's identity: who they are and whether their identity has been confirmed by a login process.

Authorization refers to a user's privileges or permissions: specifically, what actions they are allowed to perform within a company's systems.

Think about the difference between authentication and authorization like this: Imagine Alice attends a music festival. At the entrance to the festival, she presents her ticket and an additional form of identification to prove that she has the right to possess the ticket. On doing this, she is allowed to enter the festival. She has been authenticated.

However, just because Alice is within the festival does not mean she can go anywhere and do anything she wants. She can watch the festival acts, but she cannot go on stage and perform, nor can she go backstage and interact with the performers — because she is not authorized to do so. If she had purchased backstage passes, or if she was a performer in addition to being an attendee, she would have a greater amount of authorization.

Access management technologies handle user authorization. Access management platforms

use several different authorization standards (one of which is OAuth), but not SAML.

Cloudflare Access is one example of an access management solution. Cloudflare Access enables companies to manage user access to internal resources and data without the use of a virtual private network (VPN). It integrates easily with SSO providers to offer both user authorization and user authentication.

Learn more about SSO.

RELATED CONTENT

Access Control

What is IAM?

DNS Filtering

URL Filtering

What is a CASB?

What is SSO? | How single sign-on works

Single sign-on (SSO) is an important cloud security technology that reduces all user application logins to one login for greater security and convenience.

Authentication

Copy article link

What is single sign-on (SSO)?

Single sign-on (SSO) is a technology which combines several different application login screens into one. With SSO, a user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications. SSO is often used in a business context, when user applications are assigned and managed by an internal IT team. Remote workers who use SaaS applications also benefit from using SSO.

Imagine if customers who had already been admitted to a bar were asked to show their identification card to prove their age each time they attempted to purchase additional alcoholic beverages. Some customers would quickly become frustrated with the continual checks and might even attempt to circumvent these measures by sneaking in their own beverages.

However, most establishments will only check a customer's identification once, and then serve the customer several drinks over the course of an evening. This is somewhat like an SSO system: instead of establishing their identity over and over, a user establishes their identity once and can then access several different services.

SSO is an important aspect of many identity and access management (IAM) or access control solutions. User identity verification is crucial for knowing which permissions each user should have. Cloudflare Access is one example of an access control solution that integrates with SSO solutions for managing users' identities.

What are the advantages of SSO?

What are the advantages of SSO?

In addition to being much simpler and more convenient for users, SSO is widely considered to be more secure. This may seem counterintuitive: how can signing in once with one password, instead of multiple times with multiple passwords, be more secure? Proponents of SSO cite the following reasons:

1. **Stronger passwords:** Since users only have to use one password, SSO makes it easier for them to create, remember, and use stronger passwords.* In practice, this is typically the case: most users do use stronger passwords with SSO.

   **What makes a password "strong"? A strong password is not easily guessed and is random enough that a brute force attack is not likely to succeed. w7:g"5h$G@ is a fairly strong password; password123 is not.*

2. **No repeated passwords:** When users have to remember passwords for several different apps and services, a condition known as "password fatigue" is likely to set in: users will re-use passwords across services. Using the same password across several services is a huge security risk because it means that all services are only as secure as the service with the weakest password protection: if that service's password database is

   compromised, attackers can use the password to hack all of the user's other services as well. SSO eliminates this scenario by reducing all logins down to one login.

3. **Better password policy enforcement:** With one place for password entry, SSO provides a way for IT teams to easily enforce password security rules. For example, some companies require users to reset their passwords periodically. With SSO, password resets are easier to implement: instead of constant password resets across a number of different apps and services, users only have one password to reset. (While the value of regular password resets has been called into question, some IT teams still consider them an important part of their security strategy.)

4. **Multi-factor authentication:** Multi-factor authentication, or MFA, refers to the use of more than one identity factor to authenticate a user (see What is MFA?). For example, in addition to entering a username and password, a user might have to connect a USB device or enter a code that appears on their smartphone. Possession of this physical object is a second "factor" that establishes the user is who they say they are. MFA is much more secure than relying on a password alone. SSO makes it possible to activate MFA at a single point instead of having to activate it for three, four, or several dozen apps, which may not be feasible.

5. **Single point for enforcing password re-entry:** Administrators can enforce re-entering credentials after a certain amount of time to make sure that the same user is still active on the signed-in device. With SSO, they have a central place from which to do this for all

internal apps, instead of having to enforce it across multiple different apps, which some apps may not support.

6. **Internal credential management instead of external storage:** Usually, user passwords are stored remotely in an unmanaged fashion by applications and services that may or may not follow best security practices. With SSO, however, they are stored internally in an environment that an IT team has more control over.

7. **Less time wasted on password recovery:** In addition to the above security benefits, SSO also cuts down on wasted time for internal teams. IT has to spend less time on helping users recover or reset their passwords for dozens of apps, and users spend less time signing into various apps to perform their jobs. This has the potential to increase business productivity.

How does an SSO login work?

Whenever a user signs in to an SSO service, the service creates an authentication token that remembers that the user is verified. An authentication token is a piece of digital information

stored either in the user's browser or within the SSO service's servers, like a temporary ID card issued to the user. Any app the user accesses will check with the SSO service. The SSO service passes the user's authentication token to the app and the user is allowed in. If, however, the user has not yet signed in, they will be prompted to do so through the SSO service.

An SSO service does not necessarily remember who a user is, since it does not store user identities. Most SSO services work by checking user credentials against a separate identity management service.

Think of SSO as a go-between that can confirm whether a user's login credentials match with their identity in the database, without managing the database themselves — somewhat like when a librarian looks up a book on someone else's behalf based on the title of the book. The librarian does not have the entire library card catalog memorized, but they can access it easily.

How do SSO authentication tokens work?

The ability to pass an authentication token to external apps and services is crucial in the SSO process. This is what enables identity verification to take place separately from other cloud services, making SSO possible.

Think of an exclusive event that only a few people are allowed into. One way to indicate that

Think of an exclusive event that only a few people are allowed into. One way to indicate that the guards at the entrance to the event have checked and approved a guest is to stamp each guest's hand. Event staff can check the stamps of every guest to make sure they are allowed to be there. However, not just any stamp will do; event staff will know the exact shape and color of the stamp used by the guards at the entrance.

Just as each stamp has to look the same, authentication tokens have their own communication standards to ensure that they are correct and legitimate. The main authentication token standard is called SAML (Security Assertion Markup Language). Similar to how webpages are written in HTML (Hypertext Markup Language), authentication tokens are written in SAML.

How does SSO fit into an access management strategy?

SSO is only one aspect of managing user access. It must be combined with access control, permission control, activity logs, and other measures for tracking and controlling user behavior within an organization's internal systems. SSO is a crucial element of access management, however. If a system does not know who a user is, there is no way to allow or restrict that user's actions.

Does Cloudflare integrate with SSO solutions?

Cloudflare Access controls and secures user access to applications and websites; it can act as a replacement for most VPNs. Cloudflare Access integrates with SSO providers in order to identify users and enforce their assigned access permissions. Cloudflare Access is part of the Cloudflare for Teams product suite.

RELATED CONTENT

Access Control

What is IAM?

Software Defined Perimeter

Role-Based Access Control (RBAC)

What is a CASB?

Sales

Enterprise Sales

Become a Partner
Contact Sales:
6797 6901

About Access Management

About Zero Trust

VPN Resources

Glossary

Learning Center Navigation

 Privacy Policy Terms of Use Disclosure Cookie Preferences Trademark

What is a CASB? | Cloud access security brokers

A cloud access security broker (CASB) offers a number of services to protect companies that use cloud computing from data breaches and cyber attacks.

Access Glossary

Copy article link

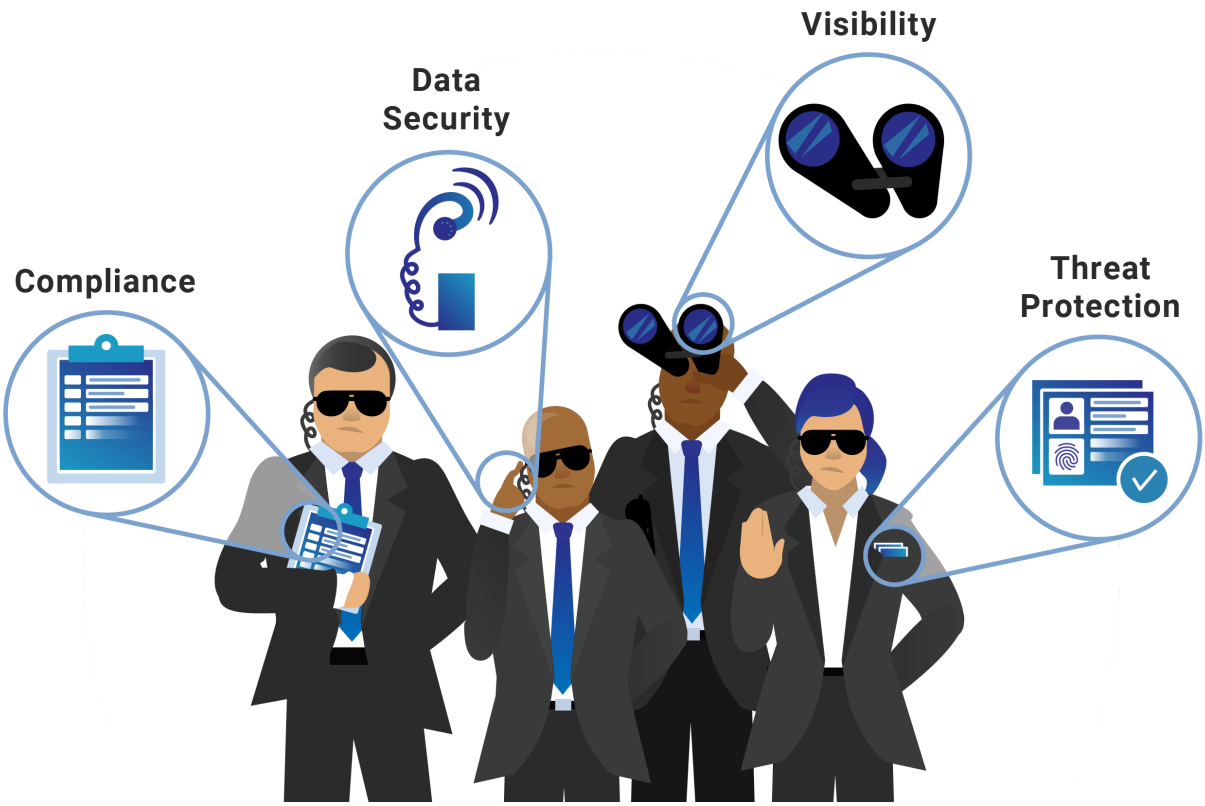
What is a cloud access security broker (CASB)?

A cloud access security broker, or CASB, is a company that helps protect other companies' cloud-hosted services. CASBs help keep corporate Software-as-a-Service (SaaS) applications, along with Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) services, safe from cyber attacks and data leaks. Typically, CASBs offer their services as cloud-hosted software, although some CASBs also offer on-premise software or on-premise hardware appliances.

A number of different security technologies fall under the CASB umbrella, and a CASB will typically offer these technologies together in one bundled package. These technologies include shadow IT discovery, access control, and data loss prevention (DLP), among several others.

Think of a CASB as being like a physical security firm that offers a number of services (surveillance, foot patrol, identity verification, etc.) to keep a facility safe, rather than a single security guard. Similarly, CASBs offer a variety of services rather than one, simplifying the process of cloud data protection.

What are the main areas in which CASBs provide security?



Gartner, an influential industry analyst firm, defines four "pillars" for cloud access security brokers:

1. **Visibility:** CASBs help discover "shadow IT": systems and processes, especially cloud services, that are not officially documented and that may introduce unknown security risks.

2. **Data security:** CASBs prevent confidential data from leaving company-controlled systems, and help protect the integrity of that data. Relevant technologies for this area include access control and data loss prevention (DLP).

3. **Threat protection:** CASBs block external threats and attacks, in addition to stopping data leaks. Anti-malware detection, sandboxing, packet inspection, URL filtering, and browser isolation can all help block cyber attacks.

4. **Compliance:** Because the cloud is so spread out and is not under a company's control, it can be difficult for companies operating in the cloud to meet strict regulatory requirements like SOC 2, HIPAA, or the GDPR. Within certain industries and regions, companies that do not comply are at risk for penalties and fines. By implementing strong security controls, CASBs help companies that store data and run business processes in the cloud achieve regulatory compliance.

What security capabilities do CASBs offer?

Most CASBs will offer some or all of the following security technologies:

- Identity verification: Ensures a user is who they claim to be by checking several identity factors, such as a password or possession of a physical token

- Access control: Controls what users can see and do within company-controlled applications

- Shadow IT discovery: Identifies the systems and services internal employees are using for

business purposes without proper authorization

- Data loss prevention (DLP): Stops data leaks and prevents data from leaving company-owned platforms
- URL filtering: Blocks websites used by attackers for phishing or malware attacks
- Packet inspection: Inspects data entering or exiting the network for malicious activity
- Sandboxing: Runs programs and code in an isolated environment to determine whether or not it is malicious
- Browser isolation: Runs users' browsers on a remote server instead of on the users' devices, protecting the devices from potentially malicious code that can run in the browser
- Anti-malware detection: Identifies malicious software

This list is not exhaustive, as CASBs can offer a number of other security products in addition to those listed above. Some of these technologies are included in other types of security products as well. For instance, many firewalls offer packet inspection, and many endpoint security products offer anti-malware. CASBs, however, package these technologies specifically for cloud computing.

To provide a full complement of CASB services, many major CASBs have at some point acquired a product or company that they bundle with their other previously existing products. They may also partner with external companies to offer additional services.

Why do organizations use CASBs?

In cloud computing, data is stored remotely and accessed over the Internet. As a result, companies using the cloud have limited control over where data is stored and how users access it. Users can access cloud data and applications on any Internet-connected device and from any network, not just the internal company-managed network. For instance, a user could log into a company-managed SaaS app from an unsecured network on their personal device, which typically would not be possible for applications that run on on-premise computers and servers (unless remote desktop is used).

Using the cloud also makes it harder to ensure that data stays private and secure, just as it is harder to prevent strangers from eavesdropping when conversing in a public place instead of in a private room.

To fully protect data in the cloud, organizations typically use security services that are cloud

To fully protect data in the cloud, organizations typically use security services that are cloud-based as well. Sometimes, they obtain these services from different vendors: using one platform for DLP, one for identity, one for anti-malware, and so on. But this approach to cloud security also creates challenges: several contracts have to be negotiated separately, security policies have to be configured numerous times, implementing and managing multiple platforms creates complexity for IT, etc.

CASBs are one solution to these challenges. Purchasing these security measures from one cloud security broker instead of several different vendors means:

1. All the technologies involved work well together.

2. Simplified management of cloud security tools; IT teams can work with one vendor, instead of a half-dozen vendors. Additionally, many CASBs enable their customers to manage all cloud security services from a single dashboard.

What are the challenges of using a CASB?

Scalability: CASBs have to manage a lot of data and multiple cloud platforms and applications. Companies should ensure their CASB vendor is able to scale up with them as they grow.

Mitigation: Not all CASBs offer the ability to stop security threats once they are identified. Depending on the situation, a CASB without mitigation capabilities may be of limited use to a company.

Integration: Companies must ensure their CASB will integrate with all their systems and infrastructure. Without complete integration, the CASB will not have full visibility into unauthorized IT and potential security threats.

Data privacy: Does the CASB vendor keep data private, or are they just one more external party touching sensitive data? If the CASB moves their customers' data to the cloud, how secure and private is it? These are especially important questions for organizations that operate under strict data privacy regulations.

Who needs a CASB?

Most enterprises that rely partially or wholly on the cloud can benefit from working with a CASB vendor. Businesses that are struggling to contain the growth of shadow IT — a major concern for many businesses today — can especially benefit from CASB services.

How do CASBs integrate with SASE?

Secure access service edge, or SASE, is a cloud-based network infrastructure model that consolidates networking and security services into a single service provider, making it simpler for companies to secure and manage network access across all connected devices. In the same way that CASBs bundle a variety of security services, SASE bundles SD-WANs (among other network capabilities) with CASBs, secure web gateways (SWG), zero trust network access (ZTNA), firewall-as-a-service (FWaaS), and other network security functions. SASE solutions are built on top of a single global network.

Does Cloudflare have a CASB offering?

Cloudflare for Teams bundles a number of Cloudflare products to help keep company data secure. Cloudflare Access offers identity-based access control to control access to internally-managed applications that traditionally required a VPN. Cloudflare Gateway

protects client devices from malware, blocks malicious websites, and filters content. Cloudflare Gateway also includes browser isolation technology to protect against malicious in-browser JavaScript.

Cloudflare for Teams helps keep both cloud services and the companies that use them secure. Learn more about Cloudflare for Teams, or explore other access control technologies.

RELATED CONTENT

Zero Trust Security

Access Control

What is IAM?

Data Loss Prevention (DLP)

URL Filtering

Sales

Enterprise Sales

Become a Partner

Contact Sales:

6797 6901

About Access Management

About Zero Trust

VPN Resources

Glossary

Learning Center Navigation

 Privacy Policy Terms of Use Disclosure Cookie Preferences Trademark

What is data loss prevention (DLP)?

Data loss prevention (DLP) ensures that business-critical or sensitive data does not leave an organization's network and is not damaged or erased.

Access Glossary

Copy article link

What is data loss prevention (DLP)?

Data loss prevention (DLP) is a strategy for detecting and preventing data exfiltration or data destruction. Many DLP solutions analyze network traffic and internal endpoint devices to identify the leakage or loss of confidential information. Organizations use DLP to protect their confidential business information and personally identifiable information (PII), which helps them stay compliant with industry and data privacy regulations.

What is data exfiltration?

Data exfiltration is when data moves without company authorization. This is also known as data *extrusion*. The primary goal of DLP is to prevent data exfiltration.

Data exfiltration can occur in a number of different ways:

- Confidential data can leave the network via email or instant messaging
- A user can copy data onto an external hard drive without authorization to do so
- An employee could upload data to a public cloud that is outside of the company's control
- An external attacker can gain unauthorized access and steal data

To prevent data exfiltration, DLP tracks data moving within the network, on employee

devices, and when stored on corporate infrastructure. It can then send an alert, change permissions for the data, or in some cases block the data when it is in danger of leaving the corporate network.

What kinds of threats does data loss prevention help stop?

Insider threats: Anyone with access to corporate systems is considered an insider. This can include employees, ex-employees, contractors, and vendors. Insiders with access to sensitive data can leak, destroy, or steal that data. DLP can help stop the unauthorized forwarding, copying, or destruction of sensitive data by tracking sensitive information within the network.

External attacks: Data exfiltration is often the ultimate goal of a phishing or malware-based attack. External attacks can also result in permanent data loss or destruction, as in a ransomware attack when internal data becomes encrypted and inaccessible. DLP can help prevent malicious attackers from successfully obtaining or encrypting internal data.

Accidental data exposure: Insiders often inadvertently expose data — for instance, an employee may forward an email containing sensitive information to an outsider without realizing it. Similar to how DLP can stop insider attacks, it can detect and prevent this accidental data exposure by tracking sensitive information within the network.

How does DLP detect sensitive data?

DLP solutions may use a number of techniques to detect sensitive data. Some of these techniques include:

- **Data fingerprinting:** This process creates a unique digital "fingerprint" that can identify a specific file, just as individual fingerprints identify individual people. Any copy of the file will have the same fingerprint. DLP software will scan outgoing data for fingerprints to see if any fingerprints match those of confidential files.

- **Keyword matching:** DLP software looks for certain words or phrases in user messages and blocks messages that contain those words and phrases. If a company wants to keep their quarterly financial report confidential prior to their earnings call, a DLP system can be configured to block outgoing emails containing the phrase "quarterly financial report" or specific phrases that are known to appear in the report.

- **Pattern matching:** This technique classifies text by the likelihood that it fits into a

Pattern matching: This technique classifies text by the likelihood that it fits into a category of protected data. Suppose an HTTP response going out from a company database contains a 16-digit number. The DLP system classifies this string of text as being extremely likely to be a credit card number, which is protected personal information.

- **File matching:** A hash of a file moving within or leaving the network is compared to the hashes of protected files. (A *hash* is a unique string of characters that can identify a file; hashes are created via hashing algorithms, which have the same output every time when given the same input.)

- **Exact data matching:** This checks data against exact data sets that contain specific information that should remain within organizational control.

How can role-based access control (RBAC) help with data loss prevention?

Role-based access control (RBAC) gives users permission to perform actions based on their role within the organization. For example, an accountant in an organization that uses RBAC should be able to access corporate tax data; an engineer would not be able to.

Some RBAC solutions can allow access to data while restricting what is done with that data. For instance, Cloudflare One can stop users from saving data locally by restricting file downloads. This prevents data from moving or being copied without an organization's permission.

How does Cloudflare One prevent data loss?

Cloudflare One is a network-as-a-service solution that offers a number of data loss prevention capabilities. By logging DNS and HTTP requests, scanning outgoing data, and controlling user permissions across all applications via RBAC, enterprises can use Cloudflare One to stop data from leaving controlled environments. Cloudflare One also offers additional capabilities to prevent data loss: learn more about Cloudflare's DLP solution.

RELATED CONTENT

What is IAM?

Access Control

Zero Trust Security

What is a CASB?

Software Defined Perimeter

Sales

Enterprise Sales

Become a Partner
Contact Sales:
6797 6901

About Access Management

About Zero Trust

VPN Resources

Glossary

Learning Center Navigation

What is a VPN?

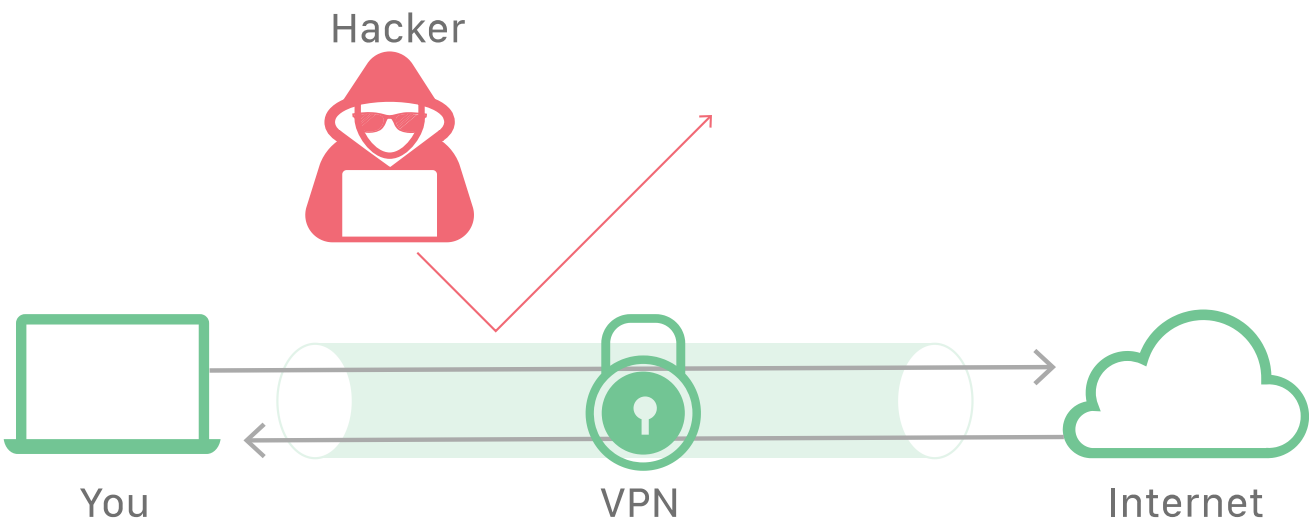
A virtual private network (VPN) lets a user remotely access a private network for purposes of privacy and security.

Remote Access

Copy article link

What is a VPN?

A virtual private network (VPN) is an internet security service that allows users to access the Internet as though they were connected to a private network. This encrypts Internet communications as well as providing a strong degree of anonymity. Some of the most common reasons people use VPNs are to protect against snooping on public WiFi, to circumvent Internet censorship, or to connect to a business's internal network for the purpose of remote work.



How does a VPN work?

Ordinarily, most Internet traffic is unencrypted and very public. When a user creates an Internet connection, such as visiting a website in a browser, the user's device will connect to their Internet Service Provider (ISP), and then the ISP will connect to the Internet to find the appropriate web server to communicate with to fetch the request website.

Information about the user is exposed in every step of the website request. Since the user's IP address is exposed throughout the process, the ISP and any other intermediary can keep logs of the user's browsing habits. Additionally, the data flowing between the user's device and the web server is unencrypted; this creates opportunities for malicious actors to spy on the data or perpetrate attacks on the user, such as a on-path attack.

Conversely, a user connecting to the Internet using a VPN service has a higher level of security and privacy. A VPN connection involves the following 4 steps:

1. The VPN client* connects to the ISP using an encrypted connection.
2. The ISP connects the VPN client to the VPN server, maintaining the encrypted connection.
3. The VPN server decrypts the data from the user's device and then connects to the Internet to access the web server in an unencrypted communication.
4. The VPN server creates an encrypted connection with the client, known as a 'VPN tunnel'.

The VPN tunnel between the VPN client and VPN server passes through the ISP, but since all the data is encrypted, the ISP cannot see the user's activity. The VPN server's communications with the Internet are unencrypted, but the web servers will only log the IP address of the VPN server, which gives them no information about the user.

*The VPN client is the VPN software installed on the user's device.

Is a VPN only for people with something to hide?

As with other Internet privacy services, VPNs are sometimes categorized as tools for illegal or subversive activity. The truth is that there are a number of valid and legitimate reasons to use a VPN. Here are a few of the most common:

- **Protection over public WiFi** - Users who go on public WiFi networks without a VPN are putting themselves at risk. Their Internet traffic is unencrypted, and other users on the

putting themselves at risk. Their internet traffic is unencrypted, and other users on the same network can monitor their activity using easily accessible tools. This is a common way for attackers to steal login credentials and other sensitive information. If a user is connected through a VPN, a snooping attacker will only be able to see encrypted data, which won't reveal any sensitive information.

- **Remote work** - Many businesses allow their employees to work remotely using a VPN. This can allow the remote employee to have access to the company's internal network, as well as provide encryption to protect the business from attackers or spying.

- **Freedom from censorship in oppressive states** - In some parts of the world, expressing or even reading views that are critical of the government is forbidden. Many of these states also provide their citizens with a suppressed version of the Internet that blocks significant amounts of domains. People accessing the Internet in these states can use a VPN to access content that their state wants blocked, as well as speak freely online, since VPN encryption protects their activity from state surveillance.

- **Location anonymity** - Some web services will restrict or filter content based on the location of the user. A VPN can be used to anonymize a user's location and get around these restrictions.

- **The right to online privacy** - ISPs have been known to sell the private data of their uses. Similarly, some websites will sell information about their visitors. The privacy offered by VPN services enable consumers to opt out of having their data harvested.

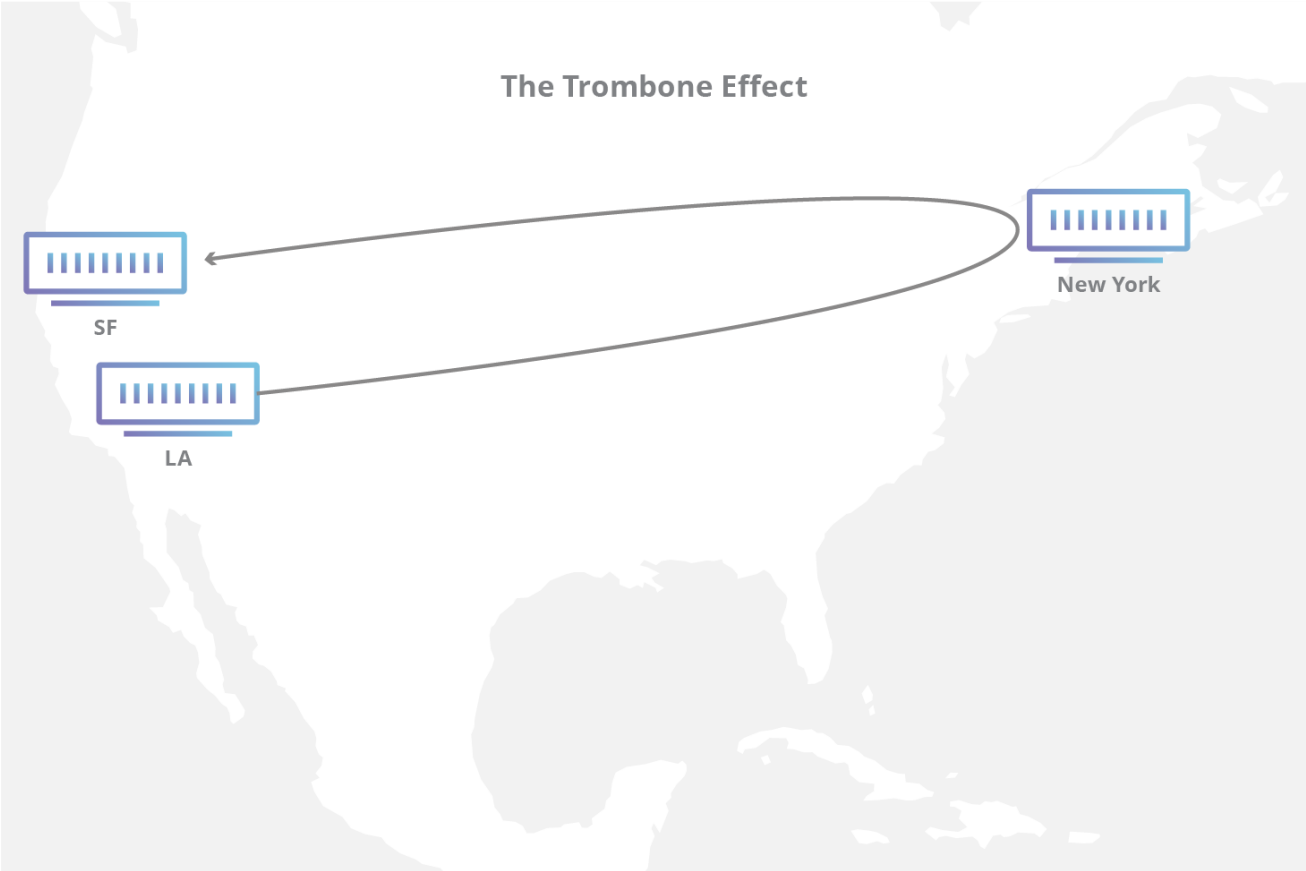
What are the downsides of a VPN?

A VPN service doesn't guarantee an increased level of security; users can only feel secure with a VPN if they trust the VPN provider. A dishonest VPN provider could sell their users' information or leave them open to attacks. It's also worth noting that most VPN services come at a recurring monthly cost. Some VPN users may also experience issues with performance.

How does a VPN affect performance?

Some users will experience performance degradation from a VPN, and this depends largely on which VPN service they are using. Not all VPNs are created equal, and if a VPN service does not have the server capacity to handle the load created by their users, those users will experience a slowdown in their Internet connection. Additionally, if a VPN is located a great distance from both the user and the web server they are trying to access, the resulting travel time can create latency. For example, if a user in San Francisco is accessing a web site

time can create latency. For example, if a user in San Francisco is accessing a web site whose servers are also in San Francisco, but that user's VPN service is located in Tokyo, the user's request will have to travel halfway around the world and back before connecting to a server just a few miles away. This is sometimes called the trombone effect.



RELATED CONTENT

RELATED CONTENT

Access Control

What is IAM?

DNS Filtering

URL Filtering

Zero Trust Security

Sales

Enterprise Sales

Become a Partner
Contact Sales:
6797 6901

About Access Management

About Zero Trust

VPN Resources

Glossary

Learning Center Navigation

Cloudflare for Teams documentation

Cloudflare for Teams replaces legacy security perimeters with our global edge, making the Internet faster and safer for teams around the world.

Zero Trust access for all of your applications.

- Authenticate users on our global edge network
- Onboard third-party users seamlessly
- Log every event and request

A Secure Web Gateway to protect users and devices.

- Enforce your company's Acceptable Use Policy (AUP)
- Block risky sites with custom blocklists and built-in threat intel
- Enhance visibility and protection into SaaS applications

A fast and reliable solution for remote browsing.

- Execute all browser code in the cloud
- Mitigate the impact of attacks
- Seamless, lightning-fast end user experience

Edit on GitHub · Updated 1 day ago

Cloudflare WARP client

The Cloudflare WARP client allows individuals and organizations to have a faster, more secure, and more private experience online. The WARP client has several modes, to better suit different connection needs. To learn more about WARP and the several modes, refer to WARP modes.

For more information on how to use WARP to enhance your Teams experience, refer to the Cloudflare for Teams documentation.

Welcome

Welcome to the Cloudflare Browser Isolation documentation!

How Browser Isolation works

Browser Isolation works by intercepting normal browsing traffic and serving a web-native remote client to the user's browser instead of the normal HTML/CSS/Javascript content.

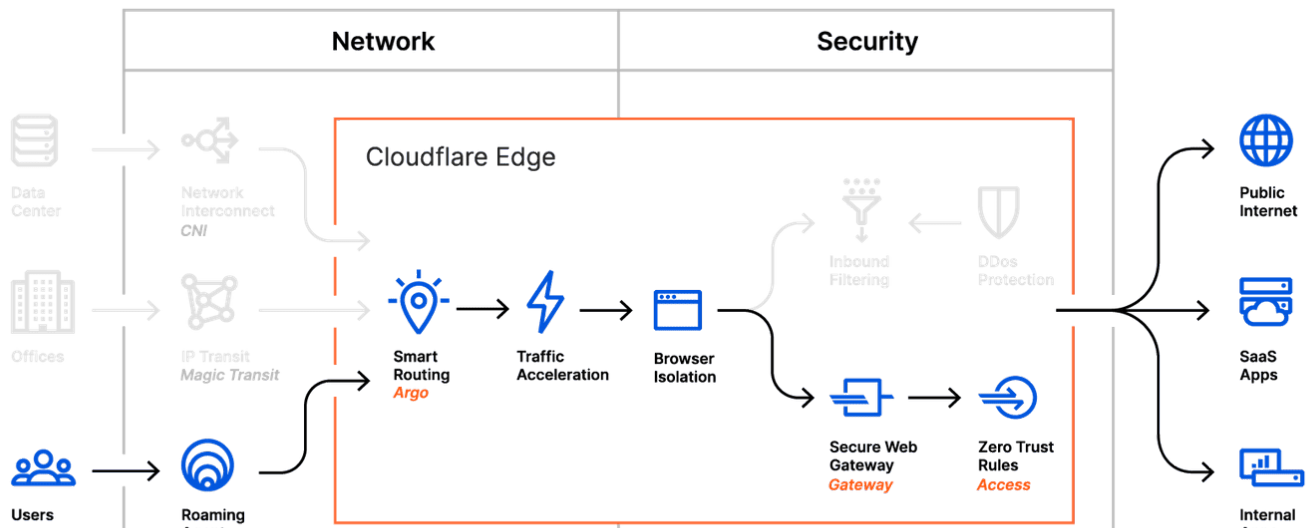
This web-based remoting client connects to a containerized headless browser hosted in a nearby Cloudflare data center. The remote browser is responsible for downloading and executing all foreign webpage code (HTML, CSS, Javascript etc), and serves network vector drawing commands over the network to your local browser.

Since HTML, CSS and Javascript content is not served to the user's browser, it is protected from malicious websites that attempt to exploit web-based vulnerabilities.

The web-based remoting client is downloaded, installed and updated on-the-fly without requiring the user to make any changes to their browser.

Our network automatically provisions, scales and upgrades browsers for users. The first time a user connects, we assign them a remote browser, and when all active tabs are closed the remote browser is automatically destroyed after 15 minutes of inactivity.

Remote browsing is invisible to the user who continues to use their browser normally without changing their preferred browser and habits. Every open tab and window is automatically isolated.



While the Browser Isolation technology does not require any additional software to be installed on a device, it does require a method to reroute Internet traffic through Cloudflare's network. This is achieved by leveraging Cloudflare WARP, a VPN-like desktop agent that securely tunnels your Internet traffic through a nearby Cloudflare data center.

Get started

Browser Isolation is integrated into Cloudflare for Teams HTTP Policies.

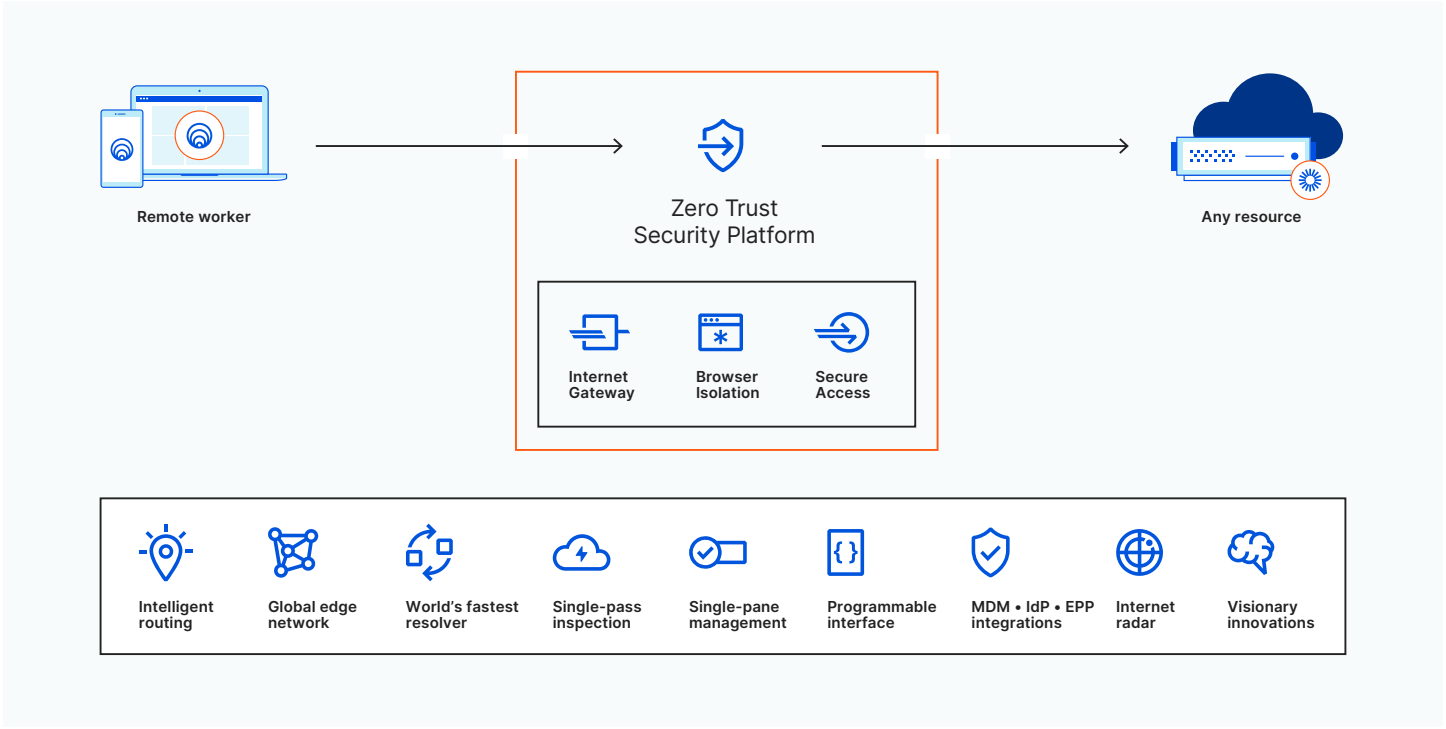
In order to use Browser Isolation with administrative controls you will need your own Cloudflare for Teams account with the Browser Isolation add-on subscription. Follow this guide to get started.

Securing remote worker connectivity for the long haul with Cloudflare

When COVID-19 forced an overnight transition to remote work, businesses scrambled to keep employees connected. Some solutions were strategic, but others were tactical bandaids — like doubling down on slow and unreliable VPNs, split-tunneling Internet traffic, and applying hasty remote access hacks. Now the cracks in this approach are showing, as familiar challenges with visibility, security and complexity persist.

Fixing remote work security flaws shouldn't take months or weeks. With Cloudflare's Zero Trust security platform, administrators can address over 20 pressing workforce security and connectivity use cases in just 30 minutes.

The solution: Cloudflare for Teams



Cloudflare's Zero Trust security platform increases visibility, eliminates complexity, and reduces risks as remote workers connect to applications and the Internet. It runs on the world's fastest edge network to deploy faster and perform better than other providers.

Three ways a Zero Trust platform can enhance remote worker security

Reduce risks

Reliance on VPNs has created failover risk and has left holes in corporate infrastructure for attackers to exploit. Once an attacker gains access, they can move laterally across multiple resources to steal data. Despite best efforts to block and tackle threats, endpoints still get compromised by undiscovered malware.

Zero Trust security platforms reduce remote work risks by enforcing identity and context-based authentication on every request to your corporate apps, leaving little room for lateral movement. Browser Isolation isolates endpoints from browsing activity, mitigating known and unknown threats.

Increase visibility

It was straightforward to maintain activity logs when users were in the office, but maintaining an audit trail is much more difficult when employees are geographically distributed and working from new devices. Logging capabilities within SaaS applications are often inconsistent, and VPN logs can be difficult to parse.

Zero Trust platforms restore visibility by intercepting and logging requests from all remote devices — even unmanaged devices. Administrators can monitor remote worker activity in internally-hosted and SaaS apps, with an audit trail to investigate incidents. Logs are centralized in one dashboard, and automatically sent to the SIEM of choice.

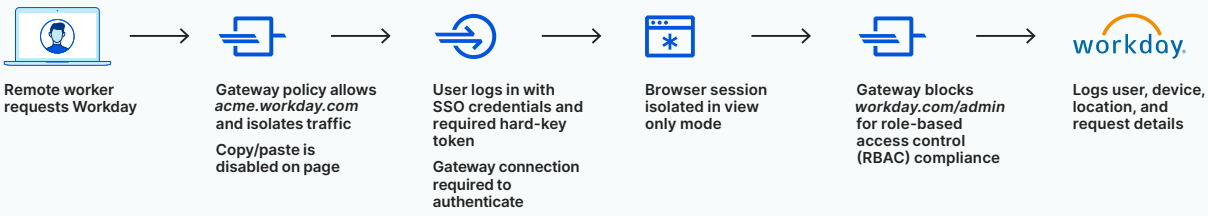
Eliminate complexity

Band-aid solutions implemented to connect remote workers are proving to be too fragile for the long run. Administrators are left to manage traffic filtering policies across multiple incompatible tools, and users are frustrated by the sluggish performance.

Zero Trust platforms simplify how users connect, and streamline how administrators work. With reduced reliance on legacy VPNs, administrators can apply standard security controls to all traffic - regardless of how that connection starts or where in the network stack it lives. And policies can all be managed from one dashboard.

Zero Trust security in action

Use case: prevent data loss in SaaS applications



In a single-pass architecture, remote worker traffic is inspected, isolated, logged, and secured from Internet threats; and performance never suffers, as users connect to data centers just one short hop nearby.

6 critical remote work problems solved

Use Case	How
Connect remote workers to corporate apps	Between devices and apps, route traffic (DNS, HTTP(S), RDP/SSH) through Cloudflare's network for better performance and reliability than your VPN
Adopt Zero Trust security for app access	Enforce application access policies based on identity, device posture and context (geo) instead of network location (IP)
Adopt Zero Trust security for internet browsing	Isolate browser activity from protected devices to stop malware and phishing from compromising endpoints
Protect data from unauthorized access and uploads	Exert finer-grained control over user and device access rights; prevent file uploads/downloads, copy/paste
Protect devices from malicious content within a site	Any known or unknown malicious content runs remotely in safe containers across our network, isolating it from reaching the device's local browser
Protect users from phishing sites	Native and third-party threat intel blocks phishers before they strike

Key Results

80%↓

less time spent resolving IT tickets and security posture for remote workers

30 min

to achieve the first two steps to Zero Trust security

91%↓

decrease in attack surface by placing Cloudflare in front of application access and Internet browsing

Next steps

Watch the demo

Try Teams, free for up to 50 users

Request a live demo with a Cloudflare expert

Cloudflare Access

Prevent lateral movement and reduce VPN reliance. Free for up to 50 users.

Works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules that limit access to corporate applications, private IP spaces and hostnames. Connects users faster and more safely than a VPN.

Watch a demo (7 minutes)

Get started Contact sales

Services

Granular application access control without lateral movement. Users can seamlessly access the resources they need and are blocked from those they do not.

Enforce consistent role-based access controls across all SaaS and self-hosted applications -- cloud, hybrid, or on-premises.

Accelerate remote access and reduce reliance on VPN with ZTNA delivered on Cloudflare's globally distributed, DDoS-resistant edge network.

Protect any app

- Cloudflare is both identity and application agnostic, allowing you to protect any application, SaaS, cloud, or on-premises with your preferred identity provider.
- Apply strong, consistent authentication methods to even legacy applications with IP firewall and Zero Trust rules.

Enforce device-aware access policies

- Before you grant access, evaluate device posture signals including presence of Gateway client, serial number, and mTLS certificate, ensuring that only safe, known devices can connect to your resources.
- Integrate device posture from Endpoint Protection Platform (EPP) providers including Crowdstrike, Carbon Black, Sentinel One, and Tanium.

Learn more >

"Access is easier to manage than VPNs and other remote acc
our IT teams. They can focus on internal projects instead of s

Alexandre Papadopoulos
Director of Cyber Security

Enable identity federation across multiple identity providers

- Integrate all of your corporate identity providers (Okta, Azure AD, and more) for safer migrations, acquisitions and third-party user access.
- Enable one-time-pins for temporary access.
- Incorporate social identity sources like LinkedIn and GitHub.

Connect users flexibly, with or without a client

- Facilitate web app and SSH connections with no client software or end user configuration required.
- For non-web applications, RDP connections, and private routing, utilize one comprehensive client across Internet and application access use cases

---

Visibility meets simplicity

- Access allows you to log any request made in your protected applications - not just login and log out.

- Aggregate activity logs in Cloudflare, or export them to your cloud log storage or SIEM provider.

"We launched quickly in April 2020 to bring remote learning t coronavirus pandemic. Cloudflare Access made it fast and sir and developers into our production sites and we set it up in lit

John Roberts
Technology Director

Sign up free for up to 50 users

Sign Up Free

Contact Sales

How it works

Yesterday's approach to securing applications

Put applications behind on-premise hardware, and then force users through a VPN to secure their traffic. As more of the world shifts to mobile and applications move to the cloud, this model breaks.

Cloudflare for Teams

Instead of a VPN, users connect to corporate resources through a client or a web browser. As requests are routed and accelerated through Cloudflare's edge, they are evaluated against Zero Trust rules incorporating signals from your identity providers, devices, and other context. Where RDP software, SMB file viewers, and other thick client programs used to require a VPN for private network connectivity, teams can now privately route any TCP traffic through Cloudflare's network where it's accelerated, verified, and filtered in a single pass, facilitating improved performance and security.

Cloudflare Access and SASE

Zero Trust application access is an important part of the Secure Access Service Edge (SASE) network security model. Learn how Cloudflare Access integrates seamlessly with the other security and connectivity tools in Cloudflare's SASE solution, Cloudflare One.

Learn more >

Resources

Datasheet: Cloudflare Access

Summarizes key features and benefits of Cloudflare's Zero Trust Network Access service.

Download datasheet >

Considering VPN replacement? Compare 3 remote access approaches

Yes, you really can replace your VPN with Zero Trust Network Access. Download this technical whitepaper to compare alternative remote access approaches and find the best option for your organization.

Download whitepaper >

Solution Brief: Remote work security over the long haul

Learn how Cloudflare's Zero Trust solution works together to provide secure, optimized connectivity for remote workforces.

Download solution brief >

The Zero Trust Guide to Developer Access

Zero Trust Network Access can empower your technical teams to work faster, while strengthening the security of your build environment.

Download whitepaper >

Zero Trust for SaaS Apps

Cloudflare's Zero Trust platform enables your organization with visibility into and policy controls over SaaS applications. Learn how Cloudflare helps you discover shadow IT, apply Zero Trust access policies, and data protection controls for SaaS apps.

Download solution brief >

Secure access to your corporate applications without a VPN.

Get started Contact us

Helping organizations worldwide progress towards Zero Trust

View case studies >

Sales

Enterprise Sales

Become a Partner
Contact Sales:
6797 6901

Getting Started

Community

Developers

Support

Company

 Privacy Policy Terms of Use Disclosure Cookie Preferences Trademark

Zero Trust Network Access with Private Routing

Prevent lateral movement and reduce VPN reliance

Trusting network-based controls (like VPNs and IP location restriction) for application access can increase your attack surface, limit visibility, and frustrate end users. Cloudflare's Zero Trust Network Access works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules that limit access to corporate applications, private IP spaces and hostnames. Powered by Cloudflare's vast and performant Anycast network, it makes user connections faster than a VPN.

Since deploying Zero Trust Network Access internally, Cloudflare has seen the following benefits:

- 91% reduction in attack surface[1]
- 2x cost savings from reduced IT efforts
- 80% reduced time spent servicing VPN related tickets
- 70% reduction in ticket volume
- 300+ annual hours of unlocked productivity during new employee onboarding

What you can do with Access

Protect any application

Cloudflare is both identity and application agnostic, allowing you to protect any application, SaaS, cloud, or on-premises with your preferred identity provider.

Connect users flexibly, with or without a client

Facilitate web app and SSH connections with no client software or end user configuration required. For non-web applications, RDP connections, and private routing, utilize one comprehensive client across Internet and application access use cases.

Enable identity federation across multiple identity providers

Integrate all of your corporate identity providers (Okta, Azure AD, and more) for safer migrations, acquisitions and third-party user access. Enable one-time-pins for temporary access, or incorporate social identity sources like LinkedIn and GitHub.

Restrict lateral movement between corporate resources

Apply strong, consistent authentication methods to even legacy applications with IP firewall and Zero Trust rules.

Enforce device-aware access

Before you grant access to a resource, evaluate device posture including presence of Gateway client, serial number, and mTLS certificate, ensuring only safe, known devices can connect to your resources. Integrate device posture from Endpoint Protection Platform (EPP) providers including Crowdstrike, Carbon Black, Sentinel One, and Tanium.

Log user activity across any app

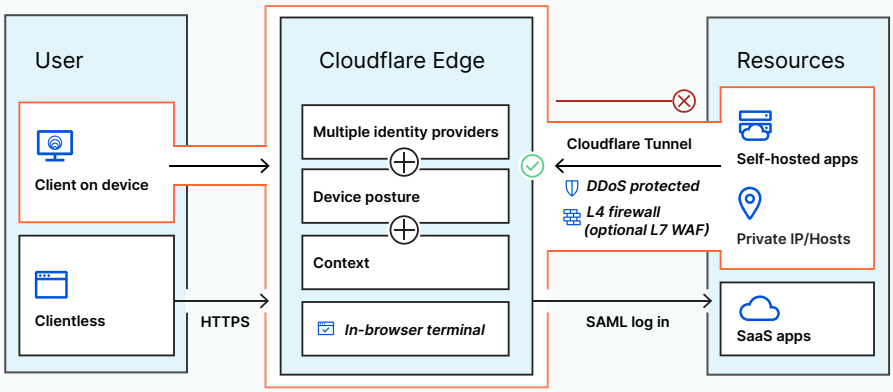
Log any request made in your protected applications - not just login and log out. Aggregate activity logs in Cloudflare, or export them to your SIEM provider.

[1]When Zero Trust Network Access is combined with Internet Browsing

The Cloudflare Difference

- **Unbeatable performance** routes requests faster with optimized, intelligence-driven routing across Cloudflare's Anycast network. On average, web apps are accessed 30% faster and TCP connections see a 17% decrease in round trip time. Our intelligence is based on analyzing network data from 25M HTTP requests/second and 39K new TCP connections/second.
- **Simpler management** combines Zero Trust Network Access, Secure Web Gateway, Remote Browser Isolation and more into one control plane with an admin experience built from the ground up, not acquired and stitched together from multiple vendors.
- **Single-pass inspection** verifies, filters, isolates and inspects traffic speedily and consistently across the globe, because every Cloudflare service is deployed on every data center in our 200+ locations worldwide.

How it works



Instead of a VPN, users connect to corporate resources through a client or a web browser. As requests are routed and accelerated through Cloudflare's edge, they are evaluated against Zero Trust rules incorporating signals from your identity providers, devices, and other context. Where RDP software, SMB file viewers, and other thick client programs used to require a VPN for private network connectivity, teams can now privately route any TCP traffic through Cloudflare's network where it's accelerated, verified, and filtered in a single pass, facilitating improved performance and security.

"Cloudflare Access saved us from having to develop our own Identity and Access Management (IAM) system. We don't have to build user permission functions into the apps that Access protects. We went all in; everyone in the company has a seat."

Jim Tyrell
Head of Infrastructure, Canva

"At delivery Hero, we always strive to deliver an amazing experience to our customers. Cloudflare Access helps us do the same for our internal teams: offering them a secure working environment, and removing the need for a VPN to access all of our applications across the globe."

William Carminato
Senior Director, Engineering, Delivery Hero

CLOUDFLARE

Identity and access management (IAM) integrations

Active Directory · okta · Google Workspace · PingIdentity · CITRIX · Centrify · onelogin · SAML OIDC

Endpoint protection platform (EPP) integrations

CROWDSTRIKE · vmware Carbon Black · SentinelOne · TANIUM

Key Features

Consistent policy	
Custom application, private network, and Internet access policies	**Unlimited**
Authentication via enterprise and social IdPs	✓
Device posture using third-party integrations and Cloudflare	✓
CSV-based bulk import for corporate device serial number lists	✓

Increase visibility	
Activity log retention	**6 months**
Identity-based country, state, and device detail views	✓
Push logs to cloud storage or SIEMs	✓

Secure connectivity	
Client-based encrypted connections to the Internet (WARP client)	**Win, Mac, iOS, Android**
Clientless secure access to self-hosted and SaaS applications	✓
Private connections for self-hosted applications, IPs, and hostnames (Cloudflare Tunnel)	✓

Simple interoperability	
Endpoint and mobility management integrations	✓
Split-tunneling for local or VPN connectivity	✓
Client self-enrollment for unmanaged devices	✓
Customizable app launcher	✓
Authentication supports multiple identity providers concurrently	✓
Generic and custom connectors to support SAML and OIDC	✓
Token-based authentication for automated services	✓
Certificate-based auth for IoT and other mTLS use cases	✓

No performance sacrifices	
Uptime SLA	**100%**
Fastest, global edge network (200+ PoPs)	✓
Fastest, global policy updates (<500ms)	✓
Fastest, intelligent IP routing (<100ms)	✓
Fastest, secure remote browser (2x speed of others)	**Add on**

Interested in learning more? Visit cloudflare.com/teams/access to start an account, free for up to 50 users.

The Zero Trust guide to developer access

Unburden technical teams with safer, faster access to critical tools and infrastructure

Engineers need privileged access to infrastructure to keep your business moving, and they don't like to be slowed down. ZTNAs allow privileged technical users to access your critical infrastructure from anywhere, without the performance tradeoffs of corporate VPNs. Learn how Zero Trust security can empower your technical teams to work faster, while strengthening the security of your build environment.

In a recent Forrester study commissioned by Cloudflare, 83% of security decision makers plan to focus on enabling faster and safer developer access this year.[1]

3 ways to accelerate technical teams with Zero Trust access

Protect build environments

Connect developers to applications without exposing them to the public Internet. Utilize secure tunnelling software to create a private tunnel to Cloudflare's network, and use our policy engine to enforce multifactor authentication policies.

Reduce VPN reliance

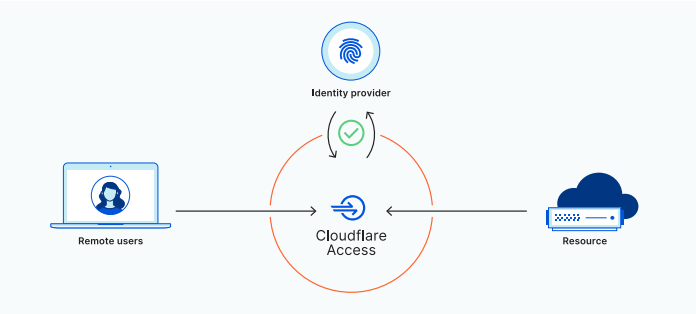
Connecting to infrastructure over a VPN tunnel can add latency, especially for globally distributed teams. Users experience lightning fast performance when they connect to your tools through one of Cloudflare's data centers in 200+ locations around the world.

Log everything

Log any request made in your protected applications — not just entrances and exits. Aggregate activity logs in Cloudflare, or export them to your SIEM provider for analysis.

How it works

Cloudflare's global edge network is in 200+ locations around the world; always close to your users and to the applications they need. With Cloudflare Access in front of your infrastructure, VPN tunnels and backhauling are no longer needed. Developers get fast, reliable performance, wherever they are.



What you can protect with Cloudflare Access

SSH Connections

Secure Shell (SSH) protocol allows users to connect to infrastructure to perform activities like remote command execution. Cloudflare Access can secure connections over Secure Shell (SSH). When users attempt to reach resources from command lines, Access launches a browser window prompting them to login with their identity provider.

Web and SaaS Applications

Use Cloudflare Access to protect internally-managed applications like Jira, WordPress, GitLab, so users can login to access them without a VPN. Cloudflare Access evaluates requests to your application and determines whether visitors are authorized based on policies you define.

Remote Desktops

The Remote Desktop Protocol (RDP) allows users to connect to a desktop from a different machine. Cloudflare Access lets end users authenticate with their single sign-on (SSO) provider and connect to shared files over RDP without being on a VPN.

Other Protocols

You can use Cloudflare Access to add authentication to Secure Messaging Block (SMB) fileshares or applications that use arbitrary TCP.

Interested in learning more?
Visit cloudflare.com/teams/access

1. Forrester Opportunity Snapshot: Zero Trust, October 2020

"Discord is where the world builds relationships. Cloudflare helps us deliver on that mission, connecting our internal engineering team to the tools they need. With Cloudflare, we can rest easy knowing every request to our critical apps is evaluated for identity and context — a true Zero Trust approach"

Mark Smith
Director of Infrastructure at Discord

DISCORD

"OneTrust relies on Cloudflare to maintain our network perimeter, so we can focus on delivering technology that helps our customers be more trusted. With Cloudflare, we can easily build context-aware Zero Trust policies for secure access to our developer tools. Employees can connect to the tools they need so simply teams don't even know Cloudflare is powering the backend. It just works."

Blake Brannon
CTO of OneTrust

OneTrust

Cloudflare Gateway

Zero Trust security for Internet browsing — no backhauling required. Free for up to 50 users. Scalable to 100,000s of users.

Cloudflare's secure web gateway keeps your data safe from malware, ransomware, phishing, command & control, Shadow IT, and other Internet risks over all ports and protocols. Log every user interaction with rich details.

Get Started Free | Contact Sales

Services

Block phishing and malware before they strike, and contain compromised devices before they cause breaches.

Point traffic to Cloudflare from corporate devices, with client support for Windows, Mac, iOS and Android.

Traffic inspection with a policy builder that offers advanced control to filter how data flows.

Block threats on the Internet, known and unknown

- Block access to known bad, risky, or unwanted destinations at the DNS or HTTP level with our massive corpus of threat intelligence.
- Security, content and application-based categories make building policies and auditing security or compliance incidents easy.
- Not sure whether to allow or block something? Just add Browser Isolation to keep all risks faraway from your endpoints with one click.

Control the flow of data in and out of your organization.

- Gain the benefits of data loss prevention (DLP) without the complexity with file type controls that can stop users from uploading files like documents and spreadsheets to unsanctioned apps and sites like social media.
- Prevent malicious downloads with AV scanning and by blocking users from downloading active types of files like executables and libraries.

> "Algolia is growing pretty fast. We needed a way to have visib slowing things down for our employees. Gateway gave us a si

Adam Surak
Director of Infrastructure & Security

Faster Internet access

- Existing firewall or secure web gateway solutions haul user requests to centralized scrubbing centers for inspections, slowing down user access.
- Cloudflare's edge network operates in 250 locations around the world, which means it's always close to your users and the resources on the Internet they need.
- It uses Anycast with a 100% uptime SLA, which means you never have to configure where user-initiated traffic is routed or worry about outages.

SaaS application control

- Cloudflare's logging capabilities allow you to discover unsanctioned use of SaaS applications, and easily build a policy to block access to such applications.
- Integrate users and role-based groups from your identity provider into Cloudflare to limit access to specific subdomains and functions of SaaS applications.

Near real-time monitoring of traffic across your organization.

- Cloudflare's logs provide visibility into your Internet and web traffic — across all users, devices, and locations.
- In under five minutes, you can push logs directly into your SIEM or cloud storage platform of choice.

Sign up free for up to 50 users

Sign Up Free

Contact Sales

How it works

Legacy approach

Teams need to connect to the Internet to do their work. Legacy approaches attempted to force that traffic, which is mostly encrypted, through appliances that could not scale with complex and costly implementations to mitigate hardware failure or software upgrade downtime.

Cloudflare for Teams

Cloudflare replaces always outdated boxes with one global network. And in one platform, we unite once-distinct point products including Secure Web Gateway (SWG), DNS Security, and Remote Browser Isolation (RBI) with Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) use cases.

Cloudflare Gateway and SASE

A secure web gateway is an important component of the Secure Access Service Edge (SASE) network security model. Learn how Cloudflare Gateway integrates seamlessly with the other security and connectivity tools in Cloudflare's SASE solution, Cloudflare One.

Learn more >

Resources

Datasheet: Cloudflare Gateway

Summarizes key features and benefits of Cloudflare's Secure Web Gateway service.

Download datasheet >

Solution Brief: Remote work security over the long haul

Learn how Cloudflare's Zero Trust solution works together to provide secure, optimized connectivity for remote workforces.

Download solution brief >

Zero Trust for SaaS Apps

Cloudflare's Zero Trust platform enables your organization with visibility into and policy controls over SaaS applications. Learn how Cloudflare helps you discover shadow IT, apply Zero Trust access policies,

and data protection controls for SaaS apps.

Download solution brief >

Helping organizations worldwide progress towards Zero Trust

View case studies >

Protect employees from threats on the Internet with Cloudflare Gateway.

Get started Contact us

Sales

Enterprise Sales

Become a Partner

Contact Sales:
6797 6901

Getting Started

Community

Developers

Support

Company

 Privacy Policy Terms of Use Disclosure Cookie Preferences Trademark

Cloudflare Gateway

Keep users and data safe from threats on the Internet - no backhauling required

How do you stop sensitive data from leaving your organization? Traditional approaches to securing employee Internet traffic have relied on network appliances that backhaul traffic from branch offices to a centralized corporate security boundary. Learn how Cloudflare Gateway utilizes Cloudflare's powerful global network to inspect and secure every connection from every device to every destination on the Internet without sacrificing performance.

Features

Block known and unknown threats on the Internet

Block access to potentially risky sites at the domain or URL level with our massive corpus of threat intelligence, which includes 100+ categories of pre-built lists to help you easily block access to malicious or risky sites.

Control the flow of data in and out of your organization

Implement data loss prevention (DLP) with file type controls that can stop users from uploading files to sites. Prevent malicious downloads by blocking users from downloading specific types of files.

SaaS application control

Discover unapproved use of SaaS applications and use Gateway's policy engine to block access to non-approved apps.

Integrate user identities and roles into Cloudflare Gateway to limit access to specific subdomains and functions of enterprise SaaS applications.

Monitor traffic across your network

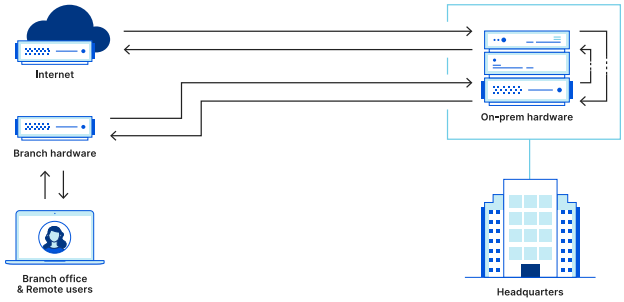
Gateway's logs provide visibility into your Internet and web traffic — across all users, devices, and locations.

You can export Gateway's logs into your SIEM or cloud storage platform of choice.

How it works

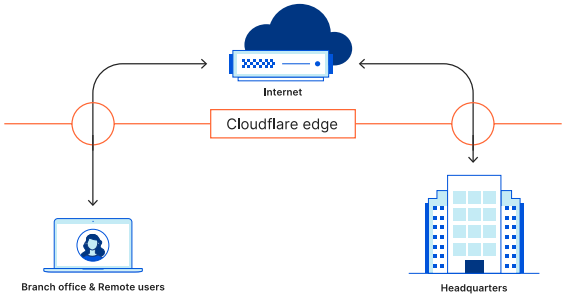
Legacy approach

Teams need to connect to the Internet to do their work. Legacy approaches attempted to force that Internet traffic through hardware that could not scale and only slowed down users.



With Cloudflare Gateway

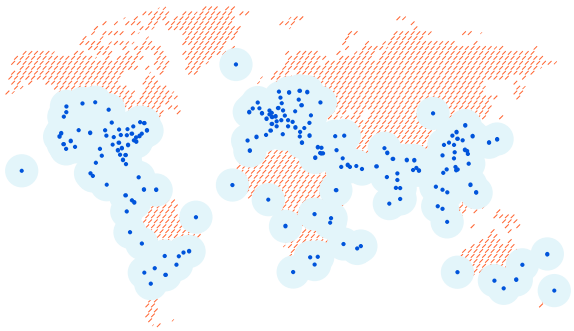
Cloudflare Gateway replaces outdated boxes with Cloudflare's global network. Instead of backhauling traffic, users connect to one of Cloudflare's data centers in 200 cities around the world, where Cloudflare applies security policies and filtering.



The Cloudflare Difference

Only Cloudflare has the scale and experience to handle security and protection for every request.

- Threat intelligence from protecting more than 25 million web properties
- Security powered by 1.1.1.1, the world's fastest DNS resolver
- Network presence in more than 200 cities in more than 100 countries



"Algolia is growing pretty fast. We needed a way to have visibility across our corporate network without slowing things down for our employees. Gateway gave us a simple way to do that."

Adam Surak
Director of Infrastructure & Security

algolia

CLOUDFLARE

Gateway Features

Reduce risk	
Recursive DNS Filters	✓
DNSSEC Validation	✓
Layer 4 Firewall Filters	✓
Layer 7 Proxy Filters	✓
Antivirus Inspection	✓
CASB-lite	✓
Remote Browser Isolation	**Add on (natively-integrated)**

Increase visibility	
Activity log retention	**30 days**
Application groups for ShadowIT visibility	✓
Identity-based country, state, and device detail views	✓
Push logs to cloud storage or SIEMs	✓

Consistent policy	
13 security categories including phishing and malware via machine learning and intelligence feeds	✓
Malware Domain Generation Algorithm (DGA) protection	✓
Newly Seen/ Newly Registered Domains	✓
DNS Tunneling protection	✓
Content categories (100+) for acceptable use policies	✓
Custom block, allow, or decryption bypass lists	✓
Identity provider integration for ID and group-based rules	✓
Granular HTTP and URL rules	✓
File type controls	✓
Device posture using third-party integrations and Cloudflare	✓
CSV-based bulk import for lists	✓

Secure connectivity	
Client-based encrypted connections to the Internet (WARP client)	**Win, Mac, iOS, Android**
Private connections for self-hosted applications to Cloudflare (Argo Tunnel)	✓
Network-level security for physical locations	**50**
Editable IP network locations	✓

Simple interoperability	
DNS over HTTPS mode	✓
DNS over TLS mode	✓
Management dashboard	✓
Export logs to cloud storage or SIEM providers	✓
Endpoint and mobility management integrations	✓
Split-tunneling for local or VPN connectivity	✓
Client self-enrollment for unmanaged devices	✓
Hybrid deployment	✓

No performance sacrifices	
Uptime SLA	**100%**
Fastest, global edge network (200+ PoPs)	✓
Fastest, global policy updates (<5 seconds)	✓
Fastest, intelligent IP routing (<100ms)	✓
Fastest, private DNS resolver (7-31ms)	✓
Fastest, secure remote browser (2x speed of others)	**Add on**

Ready to learn more? Visit cloudflare.com/teams-gateway to try Gateway today.

Security, Performance, and Reliability - all in one package

Application Services

Overview

Core Features

Secure users, devices, and networks with Zero Trust browsing and application access. All of our pricing plans start with the same base set of security controls designed to bring the power of Cloudflare's global edge network.

- Zero Trust Network Access
- Secure Web Gateway
- Private Routing to IP/Hosts
- HTTP/S Inspection and Filters
- Network Firewall as a Service
- DNS Resolution and Filters
- Cloud Access Security Broker

Free Plan

Essential security controls to keep employees and apps protected online. Best for teams under 50 users, or proof-of-concept test runs.

$0 per user

Maximum of 50 users

Get started

USAGE

- All core features
- Up to 50 users
- Up to 3 network locations
- Up to 24 hours of activity logging

SUPPORT

- Community forums available for tips and troubleshooting

Standard Plan

Protects access to anything on your network and the Internet. Best for teams over 50 users that do not require enterprise support services.

$7 per user

Billed month-to-month

Get started

*Add Browser Isolation for an additional $10 per user

USAGE

USAGE

- All core features
- No user limit
- Up to 20 network locations
- Up to 30 days of activity logging

SUPPORT

- Email and chat
- 4 hour median initial response time for urgent issues
- 100% Uptime SLA

ADDITIONAL FEATURES

- Auth for automated services

Enterprise Plan

Best for organizations that want security transformation backed by maximum support, visibility, connectivity and interoperability.

$14 per user

Tier-based custom quotes available

Talk to an expert

*Add Browser Isolation based on a custom quote per user

USAGE

- All core features
- No user limit
- Up to 250 network locations
- Up to 6 months of DNS activity logging

SUPPORT

- Priority phone, email, and chat
- 1 hour median initial response time for urgent issues
- 100% Uptime SLA
- Specialist onboarding for Teams

ADDITIONAL FEATURES

- Auth for automated services
- Logpush to SIEM/cloud storage
- Cert-based auth for IoT
- Editable IP network locations

Compare all features

ADD-ON

Zero Trust Browser Isolation

Faster than any legacy remote browser. Natively integrated in the Cloudflare for Teams policy builder, allowing administrators to allow, block, or isolate any security or content category and application group.

Get started

Cloudflare Browser Isolation

- ✓ Execute all browser code in the cloud
- ✓ Mitigate the impact of attacks
- ✓ Seamless, lightning-fast end user experience

Learn more >

Starting at $10 per user (only available with paid plans)

Helping organizations worldwide progress towards Zero Trust

View case studies >

Embrace Zero Trust Security

Sign Up Contact Sales

Sales

Enterprise Sales

Become a Partner
Contact Sales:
6797 6901

Getting Started

Community

Developers

Support

Company

Billing for Cloudflare for Teams

Updated: 4 months ago

Learn more about Cloudflare for Teams subscription plans and billing cycles.

In this article

Overview

Cloudflare for Teams uses Cloudflare's global network to empower your internal teams and infrastructure with secure, fast, and seamless access to any device on the internet.

Cloudflare for Teams consists of two products: Cloudflare Access and Cloudflare Gateway. You can subscribe to each independently or together as a bundle.

Cloudflare Access replaces corporate VPNs with Cloudflare's network. Instead of placing internal tools on a private network, customers deploy them in any environment, including hybrid or multi-cloud models, and secure them consistently with Cloudflare's network. Read more on how to subscribe to the Cloudflare Access standalone plan.

Cloudflare Gateway is a modern next generation firewall between your user, device or network and the public Internet. Once you set up Cloudflare Gateway, Gateway's DNS filtering service will inspect all Internet bound DNS queries, log them and apply corresponding policies. Read more on how to subscribe to the Cloudflare Gateway standalone plan.

This article covers the mechanics of the Cloudflare for Teams plans and billing cycles. For more

There are three Cloudflare for Teams billing plans, each offering a different set of features.

Teams Free

The Cloudflare for Teams free plan is available with or without accompanying Cloudflare paid subscriptions. It provides up to 50 Cloudflare Access seats and DNS filtering for up to 3 locations, with 24 hours of logging.

Teams Standard

The Cloudflare for Teams Standard plan consists of all of the features in the Cloudflare Access standalone plan and Cloudflare Gateway standalone plan.

Seat enforcement

Within the Cloudflare for Teams Standard plan, you must pick the same number of seats used across both products. For exa udflare Access and 30 seats of Cloudflare Gateway.

Users who authenticate to eith eat.

Teams Enterprise

Cloudflare for Teams Enterprise plan offers everything in the Standard plan, plus features such as logpush of Access and Gateway logs, certificate-based authentication, and 24x7x365 support with faster response time.

The Enterprise plan is billed by invoice instead of credit card. For more information, please see the Enterprise plan page.

employees and apps protected online. Best for teams **under 50 users**, or for trying out Teams.

$0/user

billed month-to-month

Get Started

Internet, with up to 30 days of activity logging. Best for teams **over 50 users**.

$7/user

billed month-to-month

Get Started

most advanced security controls on Cloudflare's global edge network.

Custom

billed month-to-month

Contact Us

Subscription Details

Billing cycle

All Cloudflare for Teams plans bill monthly, in advance. When you select a plan, you are billed for the month at that time. For example, if you purchase a plan on January 10, you will be billed on that day, and all of your future ach month.

If you are already a Cloudflare ing date will be the same as your other Cloudflare services

Prorating plans

Cloudflare billing will prorate Cloudflare for Teams plans when you make changes.

For example, if you decide to purchase additional seats 10 days into your billing cycle, you will be charged for the partial cost of those additional seats over the remaining 20 days of your billing cycle, starting on the day of the purchase. You will be able to make use of all seats immediately.

User count

Cloudflare for Teams subscriptions consist of seats that users in your account consume. When users authenticate to an application or enroll their agent into WARP, they count against one of your active seats. Seats can be added or removed at **Settings > Account > Plan** on the Teams Dashboard. If all seats are currently consumed, you must first remove users before decreasing your purchased seat count.

Combining plans

You cannot combine subscription plans with free plans. For example, if you have a team of 55 who need Cloudflare Access, you must purchase Cloudflare Access for 55 users. You will not be able

to cover 50 users with the free plan and pay for the excess users.

I'm an Access customer. Where is my current plan?

With the new Access standalone subscription and Teams bundles, price distinctions based on tiers of available identity provider sources are going away. Starting on September 2, 2020, you can modify your Access subscription to a Teams bundle, or to Access standalone, at $3 per user, per month. If you pay for Access Basic or Access Premium today, you can continue to use your plan at the monthly rate you pay now.

How many Gateway seats do I get on the Cloudflare for Teams free plan?

On the free plan, you can use the Cloudflare Gateway DNS filtering features for up to 50 users across 3 locations. A user amounts to 5,000 DNS queries per day.

Can I change my plan?

You can choose to upgrade or downgrade your plan at any time. If you downgrade during a billing cycle, your downgraded pricing will apply in the next billing cycle. If you upgrade during a billing cycle, you will be billed for the upgraded plan at the moment you select it.

How can I stay up to date with what's new with Teams?

We're constantly enhancing the Teams platform, and will be announcing new capabilities like Remote Browser Isolation and the Teams Client Application later this year. To stay informed on what's new, we recommend joining the Cloudflare Community and subscribing to the Cloudflare blog.

Not finding what you need?

Searching can help answer 95% of support questions. This is the quickest way to get answers.

Ask the Community Submit a request

Can I cancel my subscription anytime?

Yes, you can change your plan at any time.

Return to top

Recently viewed articles

4xx Client Error

Troubleshooting Cloudflare 1XXX errors

Setting up Multi-User accounts on Cloudflare

Understanding Cloudflare DDoS protection

Billing for Cloudflare for Teams

Updated: 4 months ago

Learn more about Cloudflare for Teams subscription plans and billing cycles.

In this article

Overview

Cloudflare for Teams uses Cloudflare's global network to empower your internal teams and infrastructure with secure, fast, and seamless access to any device on the internet.

Cloudflare for Teams consists of two products: Cloudflare Access and Cloudflare Gateway. You can subscribe to each independently or together as a bundle.

Cloudflare Access replaces corporate VPNs with Cloudflare's network. Instead of placing internal tools on a private network, customers deploy them in any environment, including hybrid or multi-cloud models, and secure them consistently with Cloudflare's network. Read more on how to subscribe to the Cloudflare Access standalone plan.

Cloudflare Gateway is a modern next generation firewall between your user, device or network and the public Internet. Once you set up Cloudflare Gateway, Gateway's DNS filtering service will inspect all Internet bound DNS queries, log them and apply corresponding policies. Read more on how to subscribe to the Cloudflare Gateway standalone plan.

This article covers the mechanics of the Cloudflare for Teams plans and billing cycles. For more

There are three Cloudflare for Teams billing plans, each offering a different set of features.

Teams Free

The Cloudflare for Teams free plan is available with or without accompanying Cloudflare paid subscriptions. It provides up to 50 Cloudflare Access seats and DNS filtering for up to 3 locations, with 24 hours of logging.

Teams Standard

The Cloudflare for Teams Standard plan consists of all of the features in the Cloudflare Access standalone plan and Cloudflare Gateway standalone plan.

Seat enforcement

Within the Cloudflare for Teams Standard plan, you must pick the same number of seats used across both products. For exa udflare Access and 30 seats of Cloudflare Gateway.

Users who authenticate to eith eat.

Teams Enterprise

Cloudflare for Teams Enterprise plan offers everything in the Standard plan, plus features such as logpush of Access and Gateway logs, certificate-based authentication, and 24x7x365 support with faster response time.

The Enterprise plan is billed by invoice instead of credit card. For more information, please see the Enterprise plan page.

employees and apps protected online. Best for teams **under 50 users**, or for trying out Teams.

$0/user

billed month-to-month

Get Started

Internet, with up to 30 days of activity logging. Best for teams **over 50 users**.

$7/user

billed month-to-month

Get Started

most advanced security controls on Cloudflare's global edge network.

Custom

billed month-to-month

Contact Us

Subscription Details

Billing cycle

All Cloudflare for Teams plans bill monthly, in advance. When you select a plan, you are billed for the month at that time. For example, if you purchase a plan on January 10, you will be billed on that day, and all of your future ach month.

If you are already a Cloudflare ing date will be the same as your other Cloudflare services

Prorating plans

Cloudflare billing will prorate Cloudflare for Teams plans when you make changes.

For example, if you decide to purchase additional seats 10 days into your billing cycle, you will be charged for the partial cost of those additional seats over the remaining 20 days of your billing cycle, starting on the day of the purchase. You will be able to make use of all seats immediately.

User count

Cloudflare for Teams subscriptions consist of seats that users in your account consume. When users authenticate to an application or enroll their agent into WARP, they count against one of your active seats. Seats can be added or removed at **Settings > Account > Plan** on the Teams Dashboard. If all seats are currently consumed, you must first remove users before decreasing your purchased seat count.

Combining plans

You cannot combine subscription plans with free plans. For example, if you have a team of 55 who need Cloudflare Access, you must purchase Cloudflare Access for 55 users. You will not be able

to cover 50 users with the free plan and pay for the excess users.

I'm an Access customer. Where is my current plan?

With the new Access standalone subscription and Teams bundles, price distinctions based on tiers of available identity provider sources are going away. Starting on September 2, 2020, you can modify your Access subscription to a Teams bundle, or to Access standalone, at $3 per user, per month. If you pay for Access Basic or Access Premium today, you can continue to use your plan at the monthly rate you pay now.

How many Gateway seats do I get on the Cloudflare for Teams free plan?

On the free plan, you can use the Cloudflare Gateway DNS filtering features for up to 50 users across 3 locations. A user amounts to 5,000 DNS queries per day.

Can I change my plan?

You can choose to upgrade or downgrade your plan at any time. If you downgrade during a billing cycle, your downgraded pricing will apply in the next billing cycle. If you upgrade during a billing cycle, you will be billed for the upgraded plan at the moment you select it.

How can I stay up to date with what's new with Teams?

We're constantly enhancing the Teams platform, and will be announcing new capabilities like Remote Browser Isolation and the Teams Client Application later this year. To stay informed on what's new, we recommend joining the Cloudflare Community and subscribing to the Cloudflare blog.

Not finding what you need?

Searching can help answer 95% of support questions. This is the quickest way to get answers.

Ask the Community Submit a request

Can I cancel my subscription anytime?

Yes, you can change your plan at any time.

Return to top

Recently viewed articles

4xx Client Error

Troubleshooting Cloudflare 1XXX errors

Setting up Multi-User accounts on Cloudflare

Understanding Cloudflare DDoS protection

Billing for Cloudflare for Teams

Updated: 4 months ago

Learn more about Cloudflare for Teams subscription plans and billing cycles.

In this article

Overview

Cloudflare for Teams uses Cloudflare's global network to empower your internal teams and infrastructure with secure, fast, and seamless access to any device on the internet.

Cloudflare for Teams consists of two products: Cloudflare Access and Cloudflare Gateway. You can subscribe to each independently or together as a bundle.

Cloudflare Access replaces corporate VPNs with Cloudflare's network. Instead of placing internal tools on a private network, customers deploy them in any environment, including hybrid or multi-cloud models, and secure them consistently with Cloudflare's network. Read more on how to subscribe to the Cloudflare Access standalone plan.

Cloudflare Gateway is a modern next generation firewall between your user, device or network and the public Internet. Once you set up Cloudflare Gateway, Gateway's DNS filtering service will inspect all Internet bound DNS queries, log them and apply corresponding policies. Read more on how to subscribe to the Cloudflare Gateway standalone plan.

This article covers the mechanics of the Cloudflare for Teams plans and billing cycles. For more

There are three Cloudflare for Teams billing plans, each offering a different set of features.

Teams Free

The Cloudflare for Teams free plan is available with or without accompanying Cloudflare paid subscriptions. It provides up to 50 Cloudflare Access seats and DNS filtering for up to 3 locations, with 24 hours of logging.

Teams Standard

The Cloudflare for Teams Standard plan consists of all of the features in the Cloudflare Access standalone plan and Cloudflare Gateway standalone plan.

Seat enforcement

Within the Cloudflare for Teams Standard plan, you must pick the same number of seats used across both products. For exa udflare Access and 30 seats of Cloudflare Gateway.

Users who authenticate to eith eat.

Teams Enterprise

Cloudflare for Teams Enterprise plan offers everything in the Standard plan, plus features such as logpush of Access and Gateway logs, certificate-based authentication, and 24x7x365 support with faster response time.

The Enterprise plan is billed by invoice instead of credit card. For more information, please see the Enterprise plan page.

employees and apps protected online. Best for teams **under 50 users**, or for trying out Teams.

$0/user

billed month-to-month

Get Started

Internet, with up to 30 days of activity logging. Best for teams **over 50 users**.

$7/user

billed month-to-month

Get Started

most advanced security controls on Cloudflare's global edge network.

Custom

billed month-to-month

Contact Us

Subscription Details

Billing cycle

All Cloudflare for Teams plans bill monthly, in advance. When you select a plan, you are billed for the month at that time. For example, if you purchase a plan on January 10, you will be billed on that day, and all of your future ach month.

If you are already a Cloudflare ing date will be the same as your other Cloudflare services

Prorating plans

Cloudflare billing will prorate Cloudflare for Teams plans when you make changes.

For example, if you decide to purchase additional seats 10 days into your billing cycle, you will be charged for the partial cost of those additional seats over the remaining 20 days of your billing cycle, starting on the day of the purchase. You will be able to make use of all seats immediately.

User count

Cloudflare for Teams subscriptions consist of seats that users in your account consume. When users authenticate to an application or enroll their agent into WARP, they count against one of your active seats. Seats can be added or removed at **Settings > Account > Plan** on the Teams Dashboard. If all seats are currently consumed, you must first remove users before decreasing your purchased seat count.

Combining plans

You cannot combine subscription plans with free plans. For example, if you have a team of 55 who need Cloudflare Access, you must purchase Cloudflare Access for 55 users. You will not be able

to cover 50 users with the free plan and pay for the excess users.

I'm an Access customer. Where is my current plan?

With the new Access standalone subscription and Teams bundles, price distinctions based on tiers of available identity provider sources are going away. Starting on September 2, 2020, you can modify your Access subscription to a Teams bundle, or to Access standalone, at $3 per user, per month. If you pay for Access Basic or Access Premium today, you can continue to use your plan at the monthly rate you pay now.

How many Gateway seats do I get on the Cloudflare for Teams free plan?

On the free plan, you can use the Cloudflare Gateway DNS filtering features for up to 50 users across 3 locations. A user amounts to 5,000 DNS queries per day.

Can I change my plan?

You can choose to upgrade or downgrade your plan at any time. If you downgrade during a billing cycle, your downgraded pricing will apply in the next billing cycle. If you upgrade during a billing cycle, you will be billed for the upgraded plan at the moment you select it.

How can I stay up to date with what's new with Teams?

We're constantly enhancing the Teams platform, and will be announcing new capabilities like Remote Browser Isolation and the Teams Client Application later this year. To stay informed on what's new, we recommend joining the Cloudflare Community and subscribing to the Cloudflare blog.

Not finding what you need?

Searching can help answer 95% of support questions. This is the quickest way to get answers.

Ask the Community Submit a request

Can I cancel my subscription anytime?

Yes, you can change your plan at any time.

Return to top

Recently viewed articles

4xx Client Error

Troubleshooting Cloudflare 1XXX errors

Setting up Multi-User accounts on Cloudflare

Understanding Cloudflare DDoS protection