

# Cloudflare Zero Trust

The fastest Zero Trust browsing and application access platform

## Risks beyond the perimeter

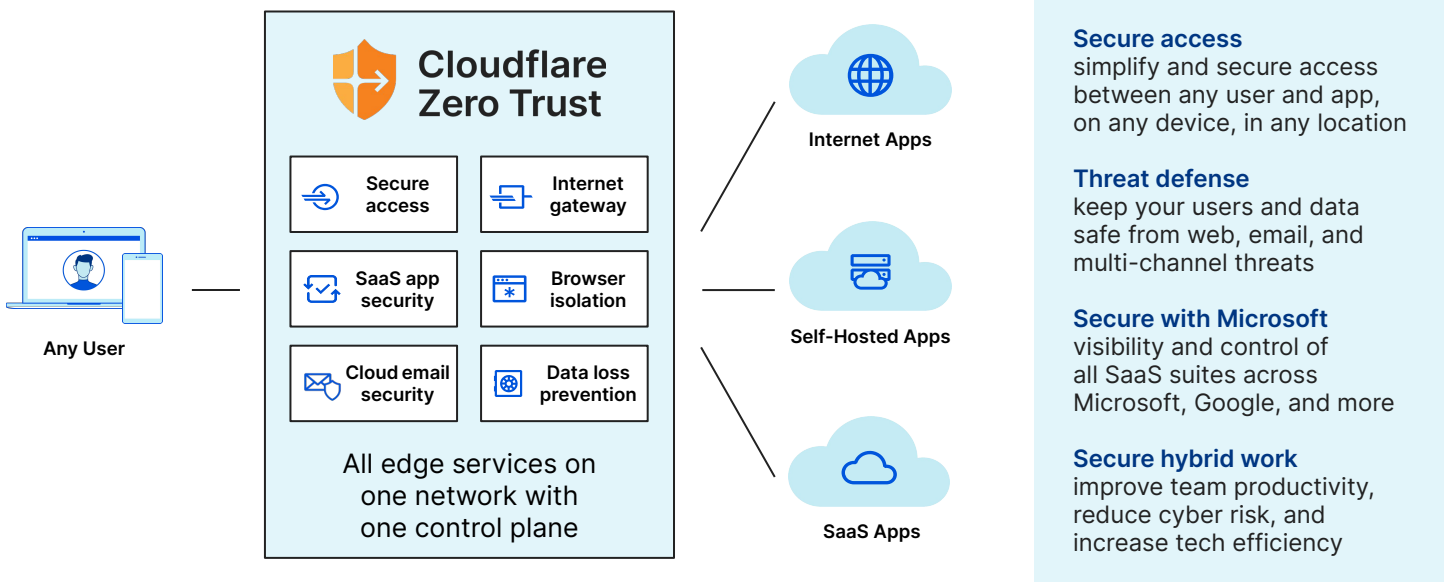
When applications and users left the walls of the corporate perimeter, security teams had to compromise on how to keep data safe. Location-centric methods of securing traffic (like VPNs, firewalls, and web proxies) have broken down under pressure, leaving organizations with limited visibility, conflicting configurations, and excessive risk.

With risks now persisting everywhere, organizations are turning towards Zero Trust delivered in the cloud to adapt.

## Adopt Internet-native Zero Trust

Cloudflare Zero Trust is a security platform that increases visibility, eliminates complexity, and reduces risks as remote and office users connect to applications and the Internet. In a single-pass architecture, traffic is verified, filtered, inspected, and isolated from threats.

It runs on one of the world's fastest Anycast networks across 275+ cities in 100+ countries to deploy faster and perform better than other providers.



## Business benefits

### Reduce excessive trust

Protect apps with identity and context-based Zero Trust rules. Block phishing, ransomware, and other online threats. Isolate endpoints from risks by keeping untrusted code away from devices and untrusted user activity away from data.

### Eliminate complexity

Reduce reliance on legacy point products and apply standard security controls to all traffic — regardless of how that connection starts or where in the network stack it lives.

### Restore visibility

Comprehensive logs for DNS, HTTP, SSH, network, and Shadow IT activity. Monitor user activity across all apps. Send logs to multiple of your preferred cloud storage and analytics tools.

## Secure access (ZTNA)

### A faster, easier, and safer way to connect any user to any application

#### Challenge: Slow, complex, and risky access

Traditional perimeter-based access controls (like VPNs) are increasingly a liability. Sluggish performance hurts end user productivity, administrators struggle with unwieldy configuration, and lateral movement is hard to contain.

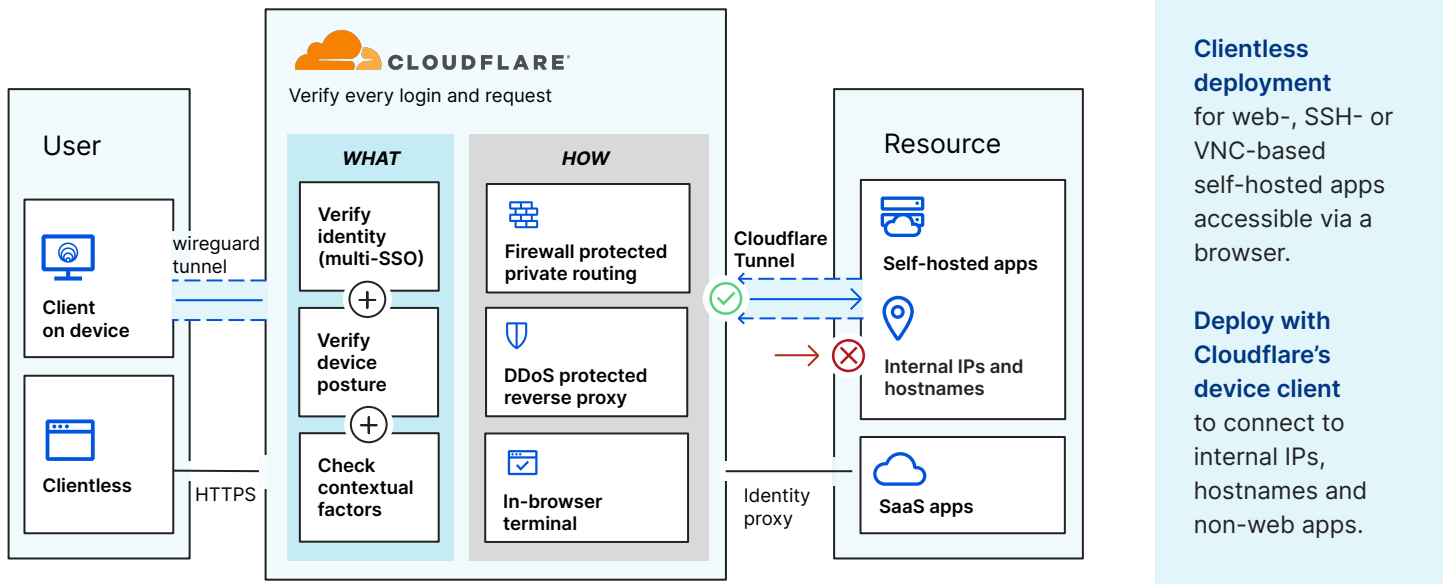
Accelerated cloud adoption and hybrid work have further exposed these flaws and made VPNs more vulnerable.

#### Zero Trust Network Access (ZTNA)

Cloudflare's ZTNA service, Access, augments or replaces VPN clients by protecting any application, in any on-premise network, public cloud, or SaaS environment.

Cloudflare's ZTNA works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules limiting access to corporate applications, private IP spaces, and hostnames.

### How it works



### Key use cases



#### Support remote work and BYOD initiatives

Verify access for all users, wherever they are, based on identity, device posture, authentication method, and other contextual factors.

Enforce these Zero Trust policies for your hybrid workforce. Support bring-your-own-device (BYOD) initiatives by securing both managed or unmanaged devices.



#### Streamline third party access with flexibility

Speed up access setup for contractors, suppliers, agencies, collaborators, etc.

Onboard multiple identity providers (IDPs) at once. Set least privilege rules based on the IDPs they already use.

Avoid provisioning SSO licenses, deploying VPNs, or creating one-off permissions.



#### Simplify administrative config and support

Add new users, identity providers, or Zero Trust rules in minutes.

Unlock new productivity by reducing employee onboarding time ([eTeacher Group](#)) and moving away from IP-based access configuration ([BlockFi](#)). No need to hire dedicated staff to manage VPNs ([ezCater](#)).

## Threat defense (SWG & RBI)

### Filter, inspect, and isolate Internet-bound traffic

#### Challenge: Evolving threat landscape

Leveling up security while keeping users productive has never been trickier. Remote work means more unmanaged devices storing more sensitive data locally. Meanwhile, ransomware, phishing, shadow IT, and other Internet-based threats have been exploding in volume and sophistication.

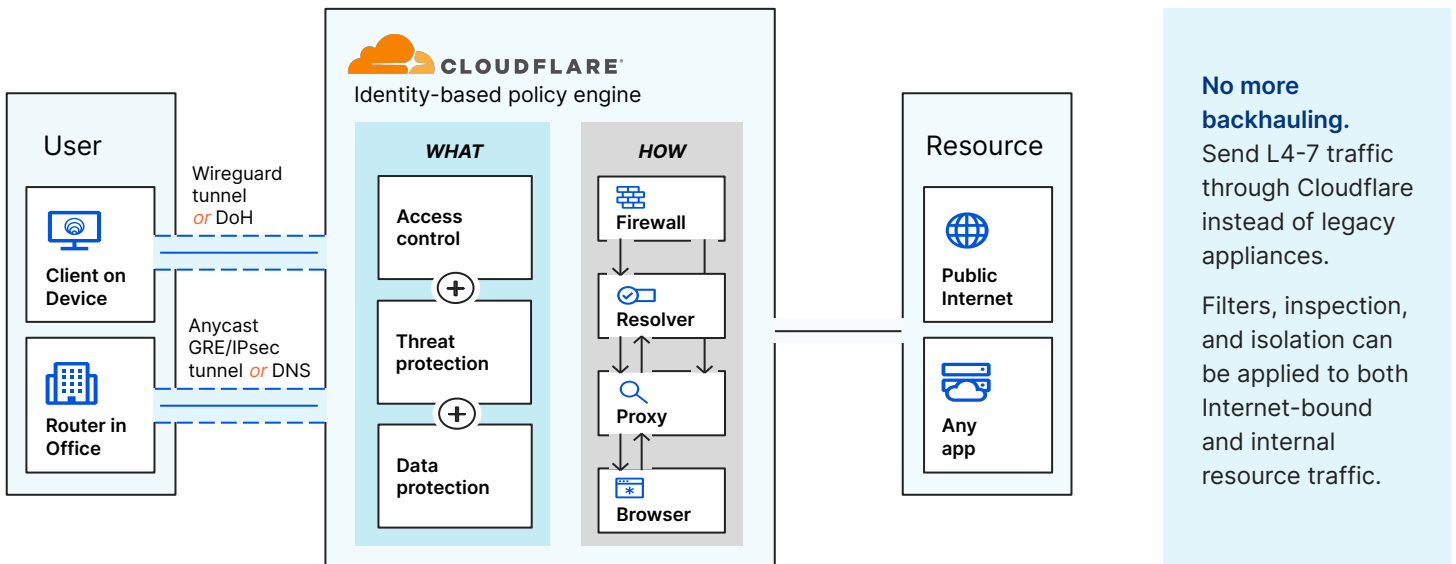
Relying on legacy point solutions and data backups is a risky strategy to guard against multi-channel threats.

#### SWG with Zero Trust Browsing

Cloudflare Gateway, our Secure Web Gateway (SWG), protects users with identity-based web filtering, plus natively-integrated remote browser isolation (RBI).

Start with DNS filtering to achieve quick time-to-value for remote or office users. Next, apply more comprehensive HTTPS inspection, and finally, extend RBI controls to embrace Zero Trust for all Internet activity.

### How it works



### Key use cases



#### Stop ransomware

Block ransomware sites and domains based on our global network intelligence. Isolate browsing on risky sites to bolster protection.

Combine SWG filtering and RBI with default-deny, ZTNA to mitigate the risk of ransomware infection spreading laterally and escalating privileges across your network.



#### Block phishing

Filter known and 'new' / 'newly seen' phishing domains. Isolate browsing to stop harmful payloads from executing locally. Stop submission of sensitive information on suspicious phishing sites via RBI's keyboard input controls.

Plus, coming soon, admins will be able to activate email filtering with a single click – powered by [Area 1](#).



#### Prevent data leakage

Implement data loss prevention (DLP) with file type controls that can stop users from uploading files to sites.

Deploy Zero Trust browsing to control and protect the data that lives within web-based apps. Control user actions within the browser – like download, upload, copy-paste, keyboard input, and printing functionalities.

## Secure with Microsoft (CASB)

### Streamline SaaS security for more visibility and control, with less overhead

#### Challenge: SaaS app proliferation

Modern workforces rely on SaaS applications like the Microsoft 365 now more than ever. But each SaaS app requires different security considerations, and operate outside the safeguards of the traditional perimeter.

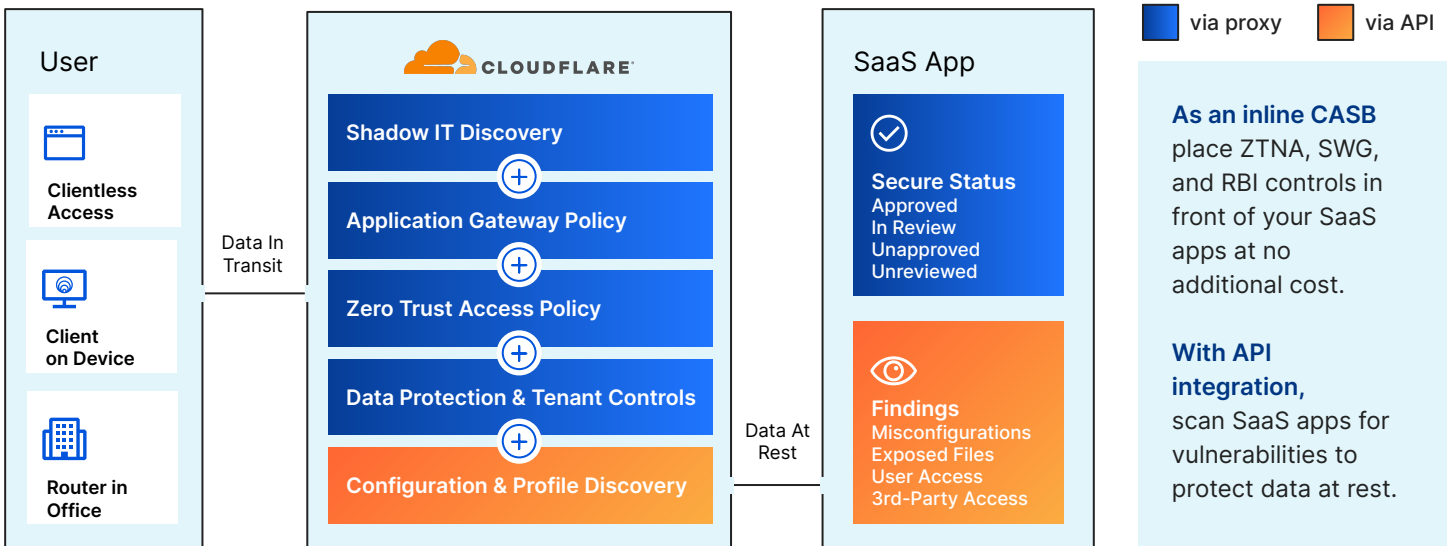
As organizations adopt dozens SaaS apps, it comes increasingly challenging to maintain consistent security, visibility, and performance.

#### Cloud Access Security Broker (CASB)

Cloudflare's CASB service gives comprehensive visibility and control over SaaS apps, so you can easily prevent data leaks and compliance violations.

Block insider threats, risky data sharing, and bad actors. Log every HTTP request to reveal unsanctioned SaaS applications. Scan SaaS apps to detect misconfigurations and suspicious activity.

### How it works



### Key use cases



#### Apply tenant and data protection controls

Apply tenant control through HTTP gateway policies to prevent users from accessing and storing data in the wrong versions of popular SaaS apps, either inadvertently or maliciously.

Control user actions (e.g. copy/paste, downloads, printing, etc.) within web-based SaaS applications to minimize the risk of data loss.



#### Mitigate and control Shadow IT

Minimize the risks introduced by unapproved SaaS applications.

Cloudflare aggregates and automatically categorizes all HTTP requests in our activity log by application type. Administrators can then set the status and track the usage of both approved and unapproved apps across your organization.



#### Identify new threats and misconfigurations

Connect to popular SaaS apps (Google Workspace, Microsoft 365, etc.) via API and scan for risks.

Empower your IT and security teams with visibility into permissions, misconfigurations, improper access, and control issues that could leave their data and employees at risk.

## Phishing protection (CES)

### Extend Zero Trust to email for comprehensive threat protection

#### Challenge: Email is the #1 threat vector

Email is the #1 way teams communicate, but also the #1 way attackers get through. In fact, a recent study found that **91%** of all cyber attacks begin with a phishing email.

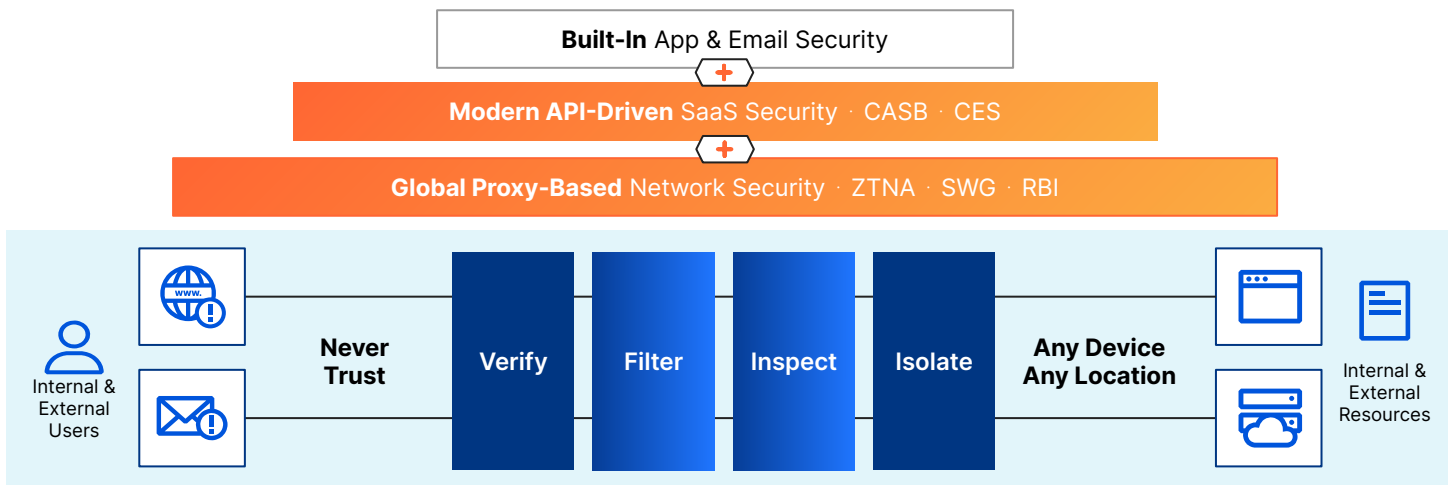
Attackers are frequently targeting and successfully exploiting the high level of trust that is often given to email communication.

#### Integrating cloud-native email security

Adding Area 1 cloud email security (CES) as part of a comprehensive Zero Trust strategy removes implicit trust from email to preemptively stop phishing and business email compromise (BEC) attacks.

All user traffic, including email, is verified, filtered, inspected, and isolated from both known and unknown threats. Area 1 helps customers to block email-borne threats, adopt a proactive security posture, and reduce phishing incident response times by 90%.

### How it works: Zero Trust for all email, web & network traffic



### Key use cases

#### Prevent BEC and email-based fraud

Stop sophisticated Business Email Compromise (BEC) attacks and supplier account takeovers through sentiment analysis, partner social graphing, message classification, and campaign source analysis.

Automatically block, quarantine, and escalate fraudulent financial communications.

#### Protect against multi-channel attacks

Effortlessly block attack campaigns that target individuals through multiple communication channels, such as email and web, by enabling users to safely load suspicious or unknown links in a remote, isolated browser.

Catch deferred phishing attacks that weaponize links post-delivery with time-of-click link classification.

#### Accelerate phishing triage and response

Free up security investigation cycles, gain useful insights into your email environment, and reduce response times with dedicated resources that augment your existing team to quickly neutralize phishing threats.

Gain additional support and security expertise with managed email security services.

## Secure hybrid work: The Cloudflare difference

### Modern security for a modern workforce

#### Deployment simplicity

Cloudflare delivers a uniform and composable platform for easy setup and operations. With software-only connectors and one-time integrations, our Cloudflare on-ramps and edge services all work together.

This leads to a better experience for your IT practitioners and end users.

#### Network resiliency

Our end-to-end traffic automation ensures reliable and scalable network connectivity with consistent protection from any location.

With Cloudflare, every edge service is built to run in every network location, available to every customer – unlike with other security providers.

#### Innovation velocity

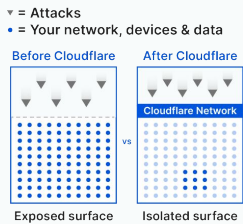
Our future-proof architecture helps us build and ship new security and networking capabilities very quickly.

Whether it's our rapid adoption of new Internet and security standards or building out customer-led use cases, our history of technical prowess speaks for itself, and our foundation provides extreme optionality.

### 5 ways Zero Trust saves your business time and money

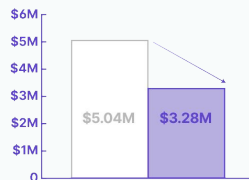
#### Reduce attack surface

91% ↓



#### Reduce breach costs

35% ↓



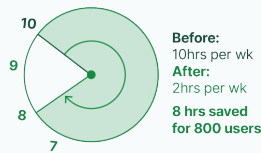
#### Accelerate employee onboarding

60% ↑



#### Reduce IT ticket burden

80% ↓



#### Reduce user latency

39% ↓



### Optimized for usability

#### One management interface

Simplify configuration with a natively built dashboard for both application and Internet access policies.

Use one dashboard to integrate with identity providers, endpoint protections, and network onramps.

#### One consolidated platform

Replace a patchwork of VPN clients, on-premise firewalls, and other point security solutions with one platform and one control plane.

Drive down costs and complexity as you move security to the edge.

#### Unrivaled user experience

Cloudflare sits closer to your users and services and routes requests faster utilizing optimized, intelligence-driven routing across our vast Anycast network, with 275+ locations in more than 100 countries around the world.



Accelerate your Zero Trust journey

Try it now

Contact us