CLOUDFLARE

SOLUTION BRIEF

Securing distributed workplaces

Consistent protection on one unified control plane for all requests, from any office location

Shift security to the cloud

Reduce complexity and risk for offices with Cloudflare

With employees working in offices and remotely, many organizations are re-evaluating how they secure offices today – whether they rely on appliances in data centers or allow direct, unsecured Internet access.

Their new focus is delivering consistent protection and experiences across users on- and off-network. Most times, this means shifting controls away from disparate tools like VPNs, web proxies, and firewalls, and toward a single cloud-delivered security platform.

Cloudflare sees organizations modernizing office security with two common use cases.

> **Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the numbers of vendors required. Deploy ZTNA to augment or replace legacy VPN to limit investment in legacy technology.[1]**
>
> Gartner

Recommended use case:

Secure application access with Zero Trust to replace VPNs

Enforce granular, identity-aware policies per app, instead of allowing lateral movement across the corporate network.

- **Step 1:** Integrate with your identity provider(s)
- **Step 2:** Protect any web app via a browser
- **Step 3:** Secure SSH, VNC, and RDP environments via a browser

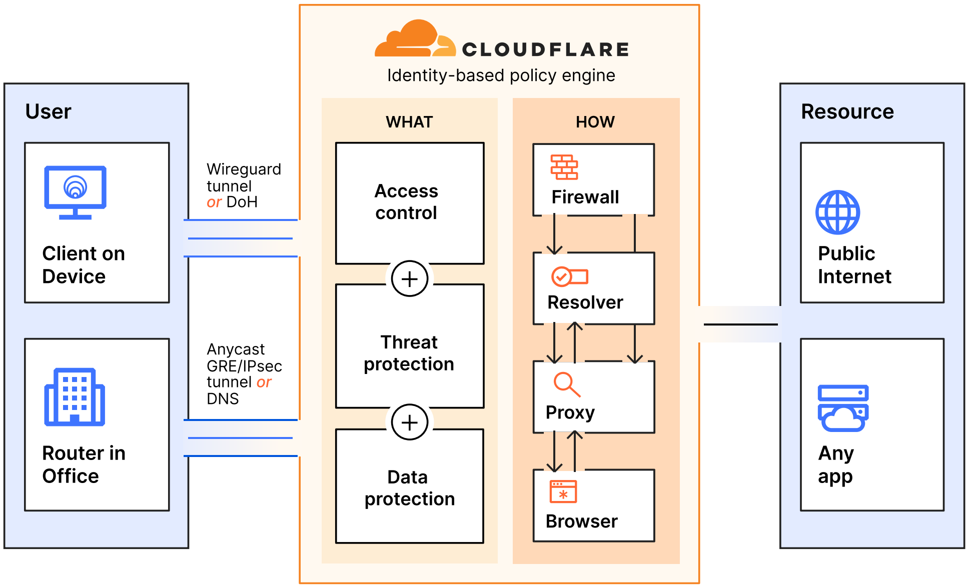
Recommended use case:

Filter Internet access for consistent security with fast time to value

Protect office users first with DNS filtering and later, more comprehensive inspections across all locations. No more backhauling traffic through on-premises security appliances in data centers.

- **Step 1:** Point DNS traffic to Cloudflare's global network
- **Step 2:** Set up location-based DNS filtering to protect from ransomware, phishing, and other Internet threats
- **Step 3:** Control data flows by enforcing HTTP, network, and browser isolation rules with unlimited TLS 1.3 inspection.

How it works



Clientless deployment to verify access and filter DNS queries from office locations.

Deploy with Cloudflare's device client to unlock enhanced visibility and controls per user and device.

Figure 1: Verify, filter, isolate, and inspect office traffic in a single pass with [Cloudflare Zero Trust]

Flexible on-ramps from any source

Start by using Cloudflare for DNS resolution via network routers. Over time, send L3 traffic to our global network via your GRE or IPsec tunnels – or use your existing SD-WAN routing method.

Alternatively, deploy Cloudflare's client for DNS and HTTP filtering and inspection on managed devices.

Fast policy enforcement, built to scale globally

All security, performance and reliability functions are built to run on every server in every data center across our 275+ locations and 100+ countries.

Our network scale means that protections are always enforced close to offices and end users, wherever they are, at high speed with single-pass inspection.

Other use cases to explore over the next six to twelve months

Regain control over SaaS apps

Discover and mitigate the risks of shadow IT that employees use in offices and at home.

Prevent data leaks and compliance violations with CASB policies enabled from the same, single Cloudflare dashboard. Learn how.

Offload MPLS traffic

Replace expensive, aging, and slow private MPLS connections.

Simplify legacy WAN architecture by using Cloudflare's global network to manage traffic across branch offices, data centers, and public cloud services. Learn how.

[1] Gartner Hype Cycle for Network Security, 2021 | GARTNER and HYPE CYCLE are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.