CLOUDFLARE

SOLUTION GUIDE

Coffee shop networking

Modernize networking at any location with SASE to minimize hardware and simplify connectivity with consistent security.

Treat any location like a coffee shop

Working from a coffee shop is simple: grab a latte, open your laptop, and connect to your apps over WiFi. Modern enterprises are taking inspiration from this simplicity to embrace more flexible and cost-effective network architectures at branches, stores, restaurants, manufacturing facilities, and other locations.

This "coffee shop networking" model promises the seamless connectivity that modern workers expect, without the complexity of a traditional private network.

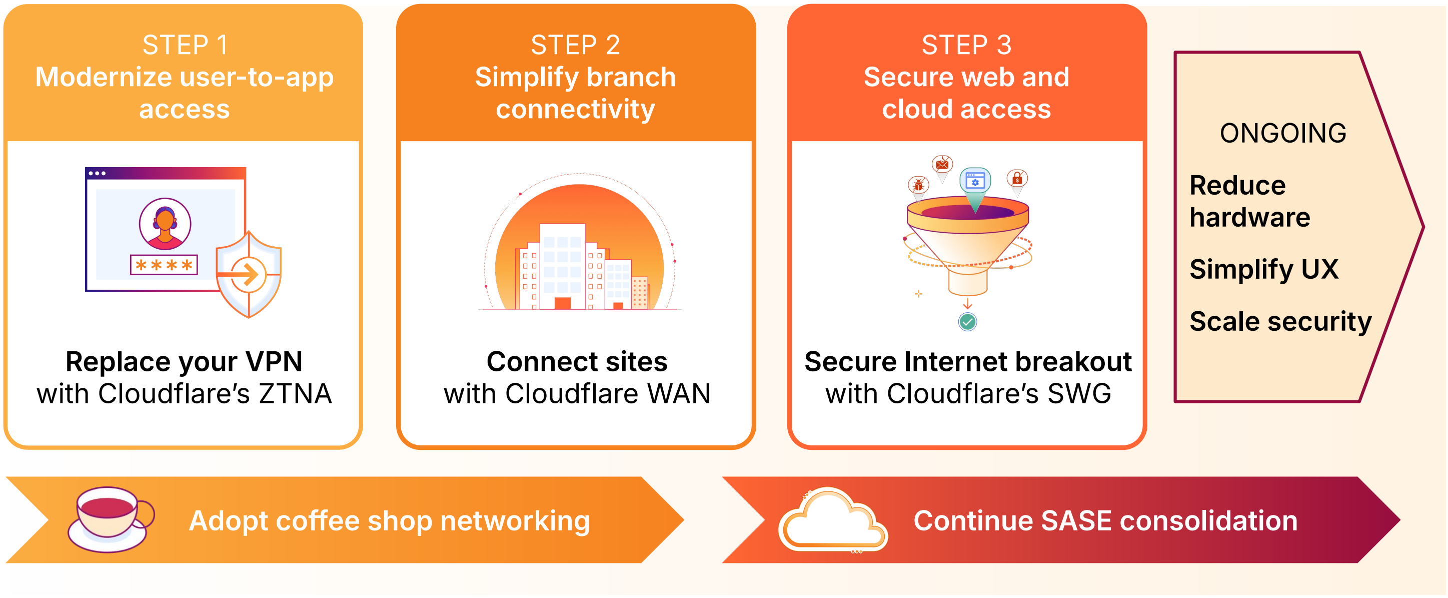
Cloudflare One, the agile SASE platform, provides the foundation for this transition. Shifting from disparate connectivity and security appliances to a unified-by-design cloud network helps you:

- **Minimize costs and your on-prem footprint** with a light-branch, heavy-cloud approach.
- **Ensure consistent experiences everywhere** at home, the office, or the coffee shop.
- **Enforce zero trust security** with granular policies based on identity, not network location.

The Cloudflare difference

- **Unified WAN and zero trust security** services built to work together on one SASE platform. No more complex SD-WAN overlay configurations that are disjointed from security capabilities.
- **Global scale and consistency** with 3x more network locations than other SASE vendors.
- **Composable and flexible on-ramps** to support any-to-any connectivity L1–L7 on one control plane. No more navigating the caveats of separate SD-WAN and security architectures.
- **Never pay for user bandwidth.** With Cloudflare, user traffic is excluded from WAN pricing. No double paying for user seats and bandwidth.

Recommended roadmap



STEP 1
Modernize user-to-app access

Replace your VPN with Cloudflare's ZTNA

STEP 2
Simplify branch connectivity

Connect sites with Cloudflare WAN

STEP 3
Secure web and cloud access

Secure Internet breakout with Cloudflare's SWG

ONGOING

Reduce hardware

Simplify UX

Scale security

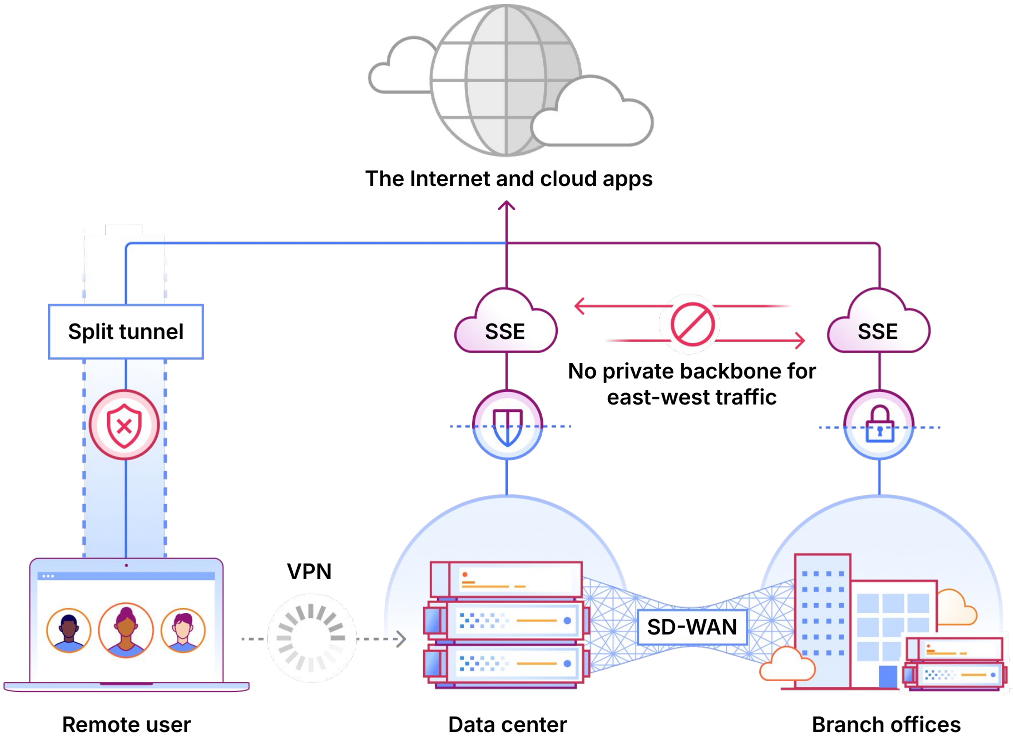
Adopt coffee shop networking

Continue SASE consolidation

Challenge: Disjointed SD-WAN and service-chained SSE solutions

While SD-WAN reduced costs in the 2010s by mixing Internet and MPLS, it was built for connecting buildings, not people. This often results in:

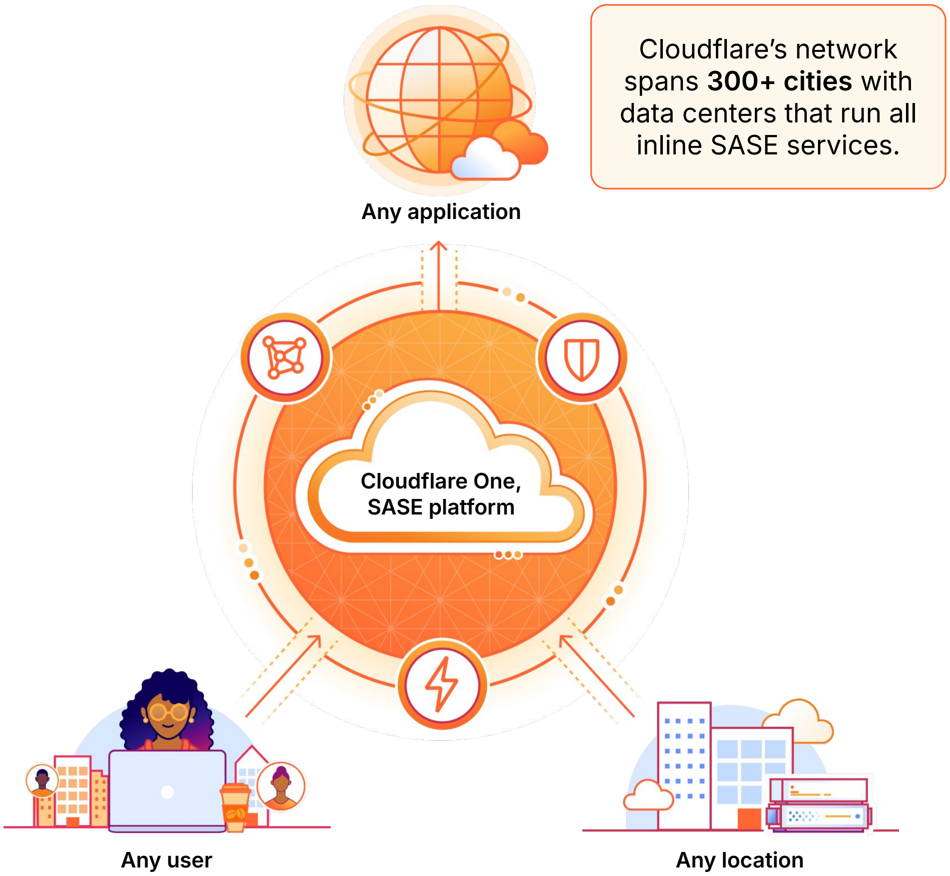
- **High overhead and costs:** Overlay configurations are too complex. Plus, teams double pay for both user security licenses and site bandwidth.
- **Slow performance:** Remote users remain tethered to slow VPNs.
- **Fragmented security:** Many vendors acquire and stitch together disjointed SD-WAN and SSE services, leading to inconsistent policy enforcement.


The Internet and cloud apps
Split tunnel
SSE
No private backbone for east-west traffic
SSE
VPN
SD-WAN
Remote user
Data center
Branch offices

Solution: Cloudflare's truly unified SASE architecture

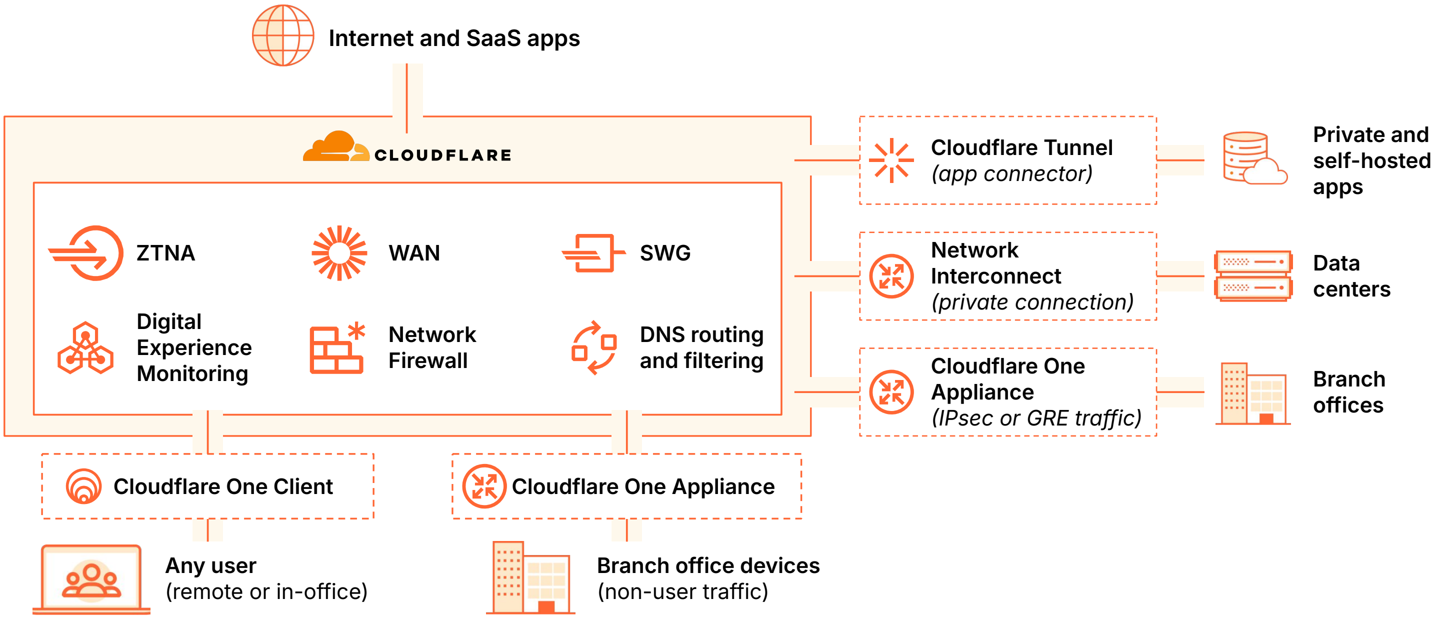
Cloudflare One unifies networking and security on a single control plane. Key benefits include:

- **No more service chaining:** Every service is available in every location with single-pass inspection for consistency as you scale.
- **Optimized connectivity:** East-west traffic traverses Cloudflare's private network backbone with AI-driven automated routing across our data centers to avoid Internet issues and avoid full reliance on peering networks.
- **Composable architecture:** All services are interoperable, so you can layer controls at your own pace and in any order. On-ramps like our device client, appliance, and physical interconnects are too, so you retain flexibility over how traffic reaches Cloudflare.



Cloudflare's network spans **300+ cities** with data centers that run all inline SASE services.

How it works


Internet and SaaS apps
CLOUDFLARE
ZTNA
WAN
SWG
Digital Experience Monitoring
Network Firewall
DNS routing and filtering
Cloudflare Tunnel (app connector)
Private and self-hosted apps
Network Interconnect (private connection)
Data centers
Cloudflare One Appliance (IPsec or GRE traffic)
Branch offices
Cloudflare One Client
Cloudflare One Appliance
Any user (remote or in-office)
Branch office devices (non-user traffic)

Step 1: Modernize user-to-app access

Replace legacy VPNs with Cloudflare Access to secure web, SaaS, and private applications. This zero trust network access (ZTNA) service enforces per-app rules based on identity. On-ramps and other capabilities for this step include:

- **Cloudflare One Client**: Deploy to all devices for full proxy controls and post-quantum encrypted connectivity.
- **Cloudflare Tunnel**: Connect apps or private subnets to Cloudflare without requiring VM infrastructure.
- **Cloudflare Digital Experience Monitoring**: Proactively troubleshoot and resolve device, network, and app performance issues.

Cloudflare recommends that ZTNA with the device client serve all user-to-app access needs for consistency across remote and physical locations.

Step 2: Simplify connectivity for branch devices

Secure connectivity from devices that cannot authenticate the way a human can (like printers, cameras, WiFi access points, IoT / OT devices).

Cloudflare WAN manages traffic across locations without the complexity of legacy hardware or SD-WAN overlays. On-ramps and other capabilities include:

- **Cloudflare One Appliance**: On-ramp traffic via secure IPsec tunnels using this lightweight, cloud-managed hardware or virtual appliance.
- **Cloudflare Network Interconnect**: Connect data center infrastructure directly to Cloudflare via dedicated physical or virtual links.
- **Cloudflare Network Firewall**: Filter L3 / L4 traffic and enable Intrusion Detection System.

Taking steps 1 and 2 reduces reliance on on-prem appliances and requires less on-site staff.

Step 3: Secure Internet breakout

Protect traffic egressing to the public Internet and SaaS apps with Cloudflare Gateway. This secure web gateway (SWG) filters and inspects web-bound traffic with DNS, HTTP, and network policies. Take advantage of other SASE capabilities:

- **Protect data:** Layer other SASE controls like data loss prevention, browser isolation, and out-of-band cloud access security broker.
- **DNS routing and filtering:** Take advantage of Cloudflare's unique strengths as both a recursive and authoritative DNS provider.
- For example, manage DNS records for internal resources on a private network, and then set DNS policies to resolve queries to private and self-hosted resources.

Shift security from on-prem firewalls to the SASE platform.

Customer stories

DTLR

US retailer
Learn more

Small IT team needed simpler, automation-friendly way to manage connectivity for **250+ store locations**

French research institute

Reducing reliance on VPNs and MPLS lines for **50+ branch offices** and field researchers around the world

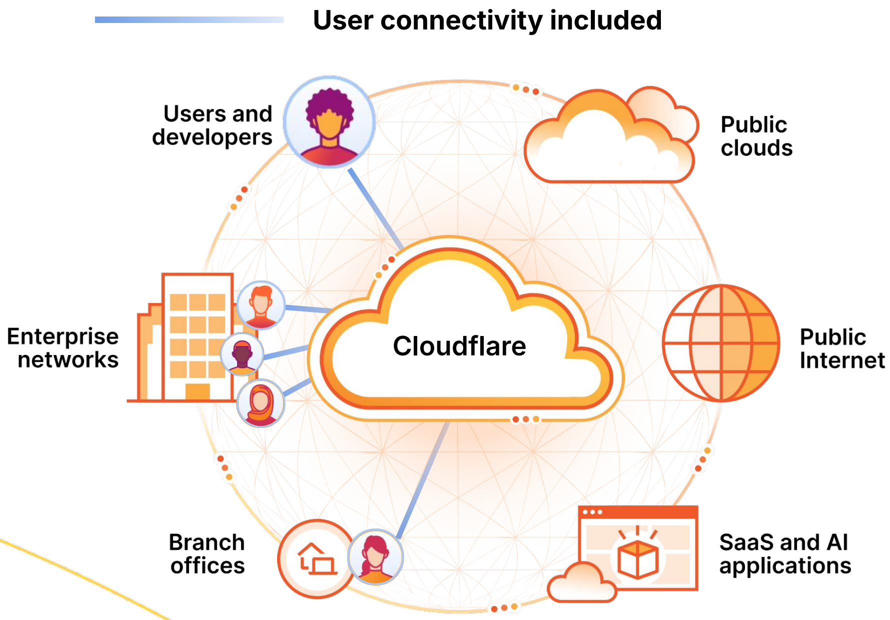
Ticketing and entertainment

Scaling connectivity across **250+ venues** from Australia to new regions globally

Global manufacturer

Pursuing single-vendor SASE consolidation to reduce tech sprawl, including multiple VPNs across **70 countries**

Simple pricing for SASE



Never pay for user bandwidth

Connect your remote, hybrid, and branch users with a single per-seat price. You'll never see bandwidth charges for devices with our user agent installed.

Each license expands your WAN

Replace expensive WAN contracts. Every user license contributes to a shared bandwidth pool that connects your entire network of offices and data centers.

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