CLOUDFLARE

Securing Hybrid Work

Reduce risk and increase visibility for all users, both on- and off-network

Secure any connection from any user, on any device, in any location

Our work-from-anywhere future: Years into the global pandemic and with a recession forthcoming, hybrid work looks here to stay. IT and security teams must deliver consistent protection and experiences for all users and devices, whether remote or in the office, and traditional location-centric tools (like VPNs and IP-based controls) are failing to meet the task.

Modern security for a modern workforce: In response, many organizations are reimagining their IT and security architecture and adopting cloud-delivered security that scales to the needs of distributed workforces and follows Zero Trust best practices.

Cloudflare makes it simple to secure any connection, so users on any device or in any location stay safe and productive when accessing applications or the Internet.

What Gartner® says:

> *By 2026, 75% of workers will continue to split time between home and traditional office locations, down slightly from 77% at the height of the pandemic in 2021.*[1]

> *Network security designs based on a collection of perimeter security appliances are ill-suited to address the dynamic anywhere, anytime needs of a modern digital business and its hybrid digital workforce.*[2]

Table of contents by page

Security modernization opportunities

Secure application access without a VPN

With users so dispersed, backhauling traffic through on-prem appliances like VPNs slows down performance and creates risk for threats to spread laterally across the corporate network.

Instead, regain visibility for all requests and enforce identity-based controls delivered closer to users to sustain productivity. No backhauling required.

Streamline SaaS security

More than ever, workforces rely on SaaS applications outside the controls of traditional corporate networks.

In response, organizations need more comprehensive visibility and control over their SaaS applications to set access policies, apply data protection controls, mitigate shadow IT, and scan apps for misconfigurations.

Protect users and data from Internet threats

Ransomware, phishing, and other Internet-threats are ever present and increasingly sophisticated.

Adopting cloud-based inspection and isolation for outbound traffic keeps users safe from malware. Plus, administrators can apply controls to prevent sensitive data from reaching local, unmanaged devices.

Hybrid work for mature enterprises

For mature enterprises, modernize security for hybrid work with confidence

Challenge: Complex, legacy environments

Organizations are experimenting with models of in-office working. But maintaining consistent protections and user experiences is challenging across these hybrid scenarios.

These companies tend to be more established, with heavier pre-existing (often complex) on-prem and legacy investments. Starting a new security project in the face of recessionary headwinds can feel too risky and difficult.

Opportunity: Simpler path to modernization

Organizations deserve to pursue digital transformation at their own pace, without needing an infinite budget, expensive 'proofs-of-concept,' complex implementation phases, or daisy-chained services.

To help these mature enterprises address their hybrid work needs, Cloudflare is designed to be easier and faster to deploy than other Zero Trust service providers like Zscaler.

Sample use cases

Telecommunications

Situation: 100+ year-old European telecoms with $20B+ in annual revenue wanted a single vendor to deploy Internet filtering and to authenticate access to legacy apps that had been recently migrated to multiple cloud environments.

Solution: Company selected Cloudflare to consolidate services and use a unified platform to secure both application and Internet access across its 100K+ employees.

Federal government

Situation: U.S. Department of Homeland Security (DHS) is leading investments in Internet threat protection across federal offices, locations, and infrastructure.

Solution: DHS selected Cloudflare and Accenture Federal Services to develop a joint solution to filter DNS queries to malicious and risky destinations that will be used across federal agencies.

Media & advertising

Situation: Media conglomerate ($10B+ revenue and 100K+ employees globally) faces cyber attacks on internal infrastructure, including a ransom note.

Solution: Cloudflare secures hundreds of web and non-web apps with identity-based Zero Trust rules. Company rolls out protection for 50K employees within 3 months and projects to expand across the entire workforce within 9 months.

Energy

Situation: Fortune 500 natural gas provider sought enhanced protection from rising cyber threats targeting the sector for both its distributed data centers and 1,500+ workforce.

Solution: Company selected Cloudflare to replace Zscaler, citing better reliability and consistency in protecting application and Internet access and longer term, an easier path to adopt advanced controls with remote browser isolation.

CUSTOMER QUOTES

> *Cloudflare is a force multiplier on our Zero Trust journey.*

John McLeod
CISO, National Oilwell Varco

> *Cloudflare has enabled Ziff Media Group to seamlessly and securely deliver our suite of internal tools to employees around the world on any device, without the need for complicated network configurations.*

Josh Butts
SVP Product & Technology,
Ziff Media Group

> *With Cloudflare, we've been able to reduce our dependence on VPNs and IP allow-listing for development environments.*

Alexandre Papadopoulos,
Director of Cyber Security,
INSEAD

Remote-first workforces for digital natives

For digital natives, prioritize agile security to support remote work flexibility

Challenge: Scale and automate cloud security

Many organizations are embracing remote-first hiring. They often tend to be younger, early cloud adopters with limited on-prem infrastructure and with business models predicated on safe, fast, and reliable digital services.

Enabling work-from-anywhere flexibility can be a differentiator, but demands security tooling that is equally flexible as users move and rely on personal devices.

Opportunity: Composable security fit to scale

With less legacy IT to deprecate, these digital natives can leverage our Internet-native architecture and deployment flexibility to stay agile in their security modernization.

Our composable services, API-first design, and single-pane management make it easy to get started and adapt security. The speed, scale, and reliability of our global network meet the needs of a fully remote workforce.

Sample use cases

B2B SaaS

Situation: Australian graphic design platform Canva (valued at $40B in 2021) deployed Cloudflare pre-pandemic to streamline access for third-party users and avoid the hassles of implementing a VPN.

Solution: Over time, Canva has rolled out Zero Trust application access policies across its entire growing workforce, plus has extended Internet filtering and inspection.

Fintech & blockchain

Situation: BlockFi – a series-D wealth management platform powered by blockchain technology – needed to level up security in the face of cyber threats against its growing assets under management and remote-first workforce.

Solution: Cloudflare enabled BlockFi to transition to identity-based authentication for application access and away from time-consuming IP-based controls.

Social Media

Situation: Global social media platform experienced a high-profile breach exploiting internal application access and VPN configurations.

Solution: In response, the company decided to overhaul its remote access approach by adopting Cloudflare's Zero Trust Network Access (ZTNA) solution for 13K employees and contractors and retiring its VPN deployments.

E-commerce

Situation: Global e-commerce platform ($4B+ revenue and 15K+ employees) sought better protection for remote users browsing the Internet and accessing sensitive SaaS apps while off-network.

Solution: Company deploys Cloudflare to layer threat protection capabilities like DNS filtering while also providing enhanced visibility into SaaS application usage.

CUSTOMER QUOTES

> *At Delivery Hero, we always strive to deliver an amazing experience to our customers. Cloudflare helps us do the same for our internal teams: offering them a secure working environment across the globe and an easy way to build fast, reliable, and privacy-respecting applications.*

Christina von Hardenberg
CTO, Delivery Hero

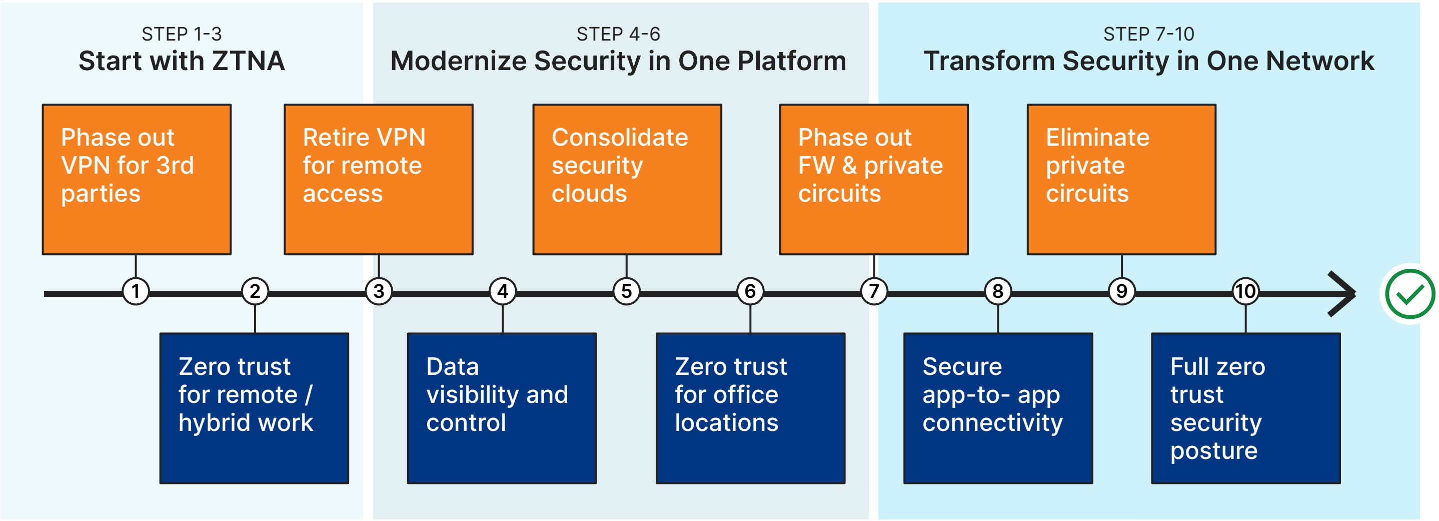
> *Cloudflare is essential to how we secure our rapidly growing, remote workforce. Adopting Zero Trust for application access gave our admins enhanced visibility and granular controls they could never get with prior legacy tools.*

Marccio Alcaide
Head, IT Security, Facily

Illustrative hybrid work roadmap

How customers plan to modernize security

🟧 Infrastructure Consolidation 🟦 Security Policy



STEP 1-3
Start with ZTNA

STEP 4-6
Modernize Security in One Platform

STEP 7-10
Transform Security in One Network

1 Phase out VPN for 3rd parties

2 Zero trust for remote / hybrid work

3 Retire VPN for remote access

4 Data visibility and control

5 Consolidate security clouds

6 Zero trust for office locations

7 Phase out FW & private circuits

8 Secure app-to- app connectivity

9 Eliminate private circuits

10 Full zero trust security posture

✓

Security modernization roadmap

The above roadmap is illustrative of the approach we see organizations take when modernizing their security to adapt to hybrid work. This roadmap has two key goals:

1) **Top row (in orange):** To consolidate connectivity and security infrastructure away from point products and hardware to one cloud-native platform.
2) **Bottom row (in blue):** To gain the visibility and controls to adopt Zero Trust security between users and resources on any device, in any location.

Phases 1 - 5: Securing app and Internet access

For many, adapting to hybrid work means first modernizing how how workforces reach corporate resources.

Phase 1: Often their first step is to start offloading VPN traffic and transition to Internet-native controls for select users – such as contractors, developers, partners, or newly acquired teams. Cloudflare makes it particularly easy to secure self-hosted apps accessible via a browser without the need to deploy any software on endpoints.

Phase 2: This modern tooling enables the visibility necessary to build per-app policies based on role, MFA and hard key requirements, and identity and device posture.

Phase 3: As teams build confidence in this approach, they move to retire their VPN entirely and protect non-web and legacy private networks with Zero Trust.

Phase 4: Focus then shifts to improving visibility and controls for SaaS apps, including mitigating Shadow IT, managing tenants, and preventing data exfiltration.

Phase 5: With internal and SaaS apps now managed from a single platform, organizations look to expand controls for outbound Internet access and consolidate threat protection tools like DNS filters and Secure Web Gateways.

Phases 6-10: Shifting connectivity to the cloud

The remaining roadmap phases are in planning for most organizations, but their aspiration is to shift all network connectivity and security onto one unified cloud network.

Phase 6: Here, organizations seek to extend consistent Zero Trust to any network location like HQ, branch, data centers, and satellite offices to support hybrid work.

Phase 7: As office traffic is increasingly sent to Cloudflare for security, organizations can phase out traditional on-prem firewalls and other private network appliances.

Phase 8: These advanced use cases focus on securing app to app connectivity across hybrid multi-cloud environments, which readies the network infrastructure team to end telco MPLS contracts in Phase 9.

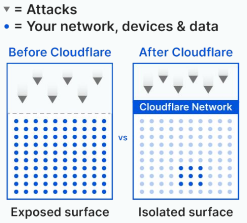
Phase 10: Although modernization is never truly over, the aspiration is that Zero Trust now extends to all users, devices, data, applications, and environments.

Business and security outcomes

5 ways Zero Trust saves your business time and money

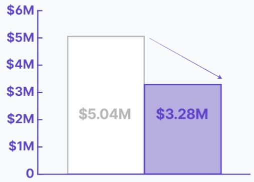
Reduce attack surface

91%↓



Reduce breach costs

35%↓

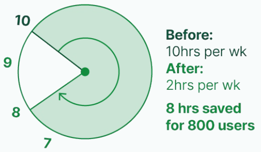


Accelerate employee onboarding

60%↑

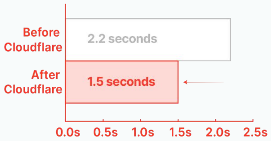
Reduce IT ticket burden

80%↓



Reduce user latency

39%↓



Other business drivers

Unlock workforce productivity

For administrators

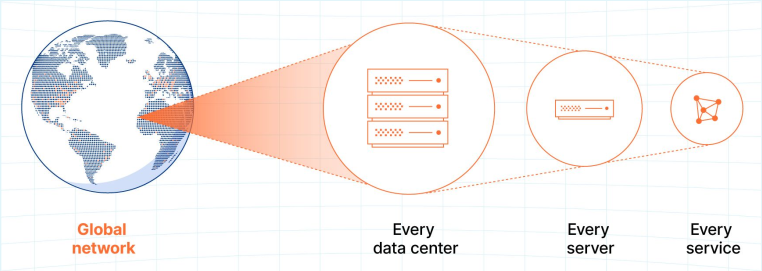
- Simplify configuration with a single management interface to set policies across application and Internet access
- Configure all integrations with identity providers, endpoint protections, cloud providers, and network on-ramps from that same management interface

For end users

- Frictionless authentication and native browsing experiences with security that stays out of the way

Reduce costs on legacy services

- Replace or augment your virtual private network (VPN) appliances and instead adopt Zero Trust Network Access (ZTNA)
- Transition from on-prem web proxy or firewall to cloud-native L3-L7 security services
- Offload use cases from virtual desktop infrastructure with Remote Browser Isolation (RBI)
- Swap out traditional secure email gateway for modern cloud email security



Consistent speed and scale to protect all remote or office users

All security, performance, and reliability functions are designed to run on every single server in every Cloudflare data center on our network that today spans 270+ cities.

Accelerate your Zero Trust roadmap

Try it now

Contact us

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

REV: PMM-2022JJUL

[1] *Top Network Practices to Support Hybrid Work,* Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 04/08/2022
[2] *2022 Strategic Roadmap for SASE Convergence,* Gartner, Neil MacDonald, Andrew Lerner, John Watts 06/24/2022

GARTNER is a 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.