CLOUDFLARE

EBOOK

Achieving SASE success

10 key milestones to get it right

About this guide

The secure access service edge (SASE) market is expected to reach over $28.5 billion by 2028.[1]

No longer just a buzzword, SASE is a strategic foundation to drive C-level priorities:

- Helping CISOs **enforce security everywhere**, to reduce risk and safeguard data across expanding attack surfaces
- Helping CIOs **accelerate digital innovation** by simplifying IT and consolidating vendors
- Helping CTOs and CFOs **lower total cost of ownership** (TCO) and reduce technical debt

Transitioning to a cloud-native SASE architecture is not a quick pivot; it is a long-term, enterprise-wide strategy to converge network connectivity with Zero Trust security. Without planning, that journey can feel daunting: Where to begin? What to do next? And in what order?

That's where **Achieving SASE success: 10 key milestones to get it right** can help. Based on how Cloudflare customers are evolving their architectures, this guide maps out a path to SASE across three common phases:

- **Modernizing remote access** by adopting Zero Trust Network Access (ZTNA)
- **Modernizing security** with a unified security service edge (SSE) approach
- **Modernizing networking and security** for single-vendor SASE and Zero Trust everywhere

You'll also find real examples of how Cloudflare One, deployed as part of a single-vendor or multi-vendor SASE strategy, helps organizations deliver early wins and build momentum.

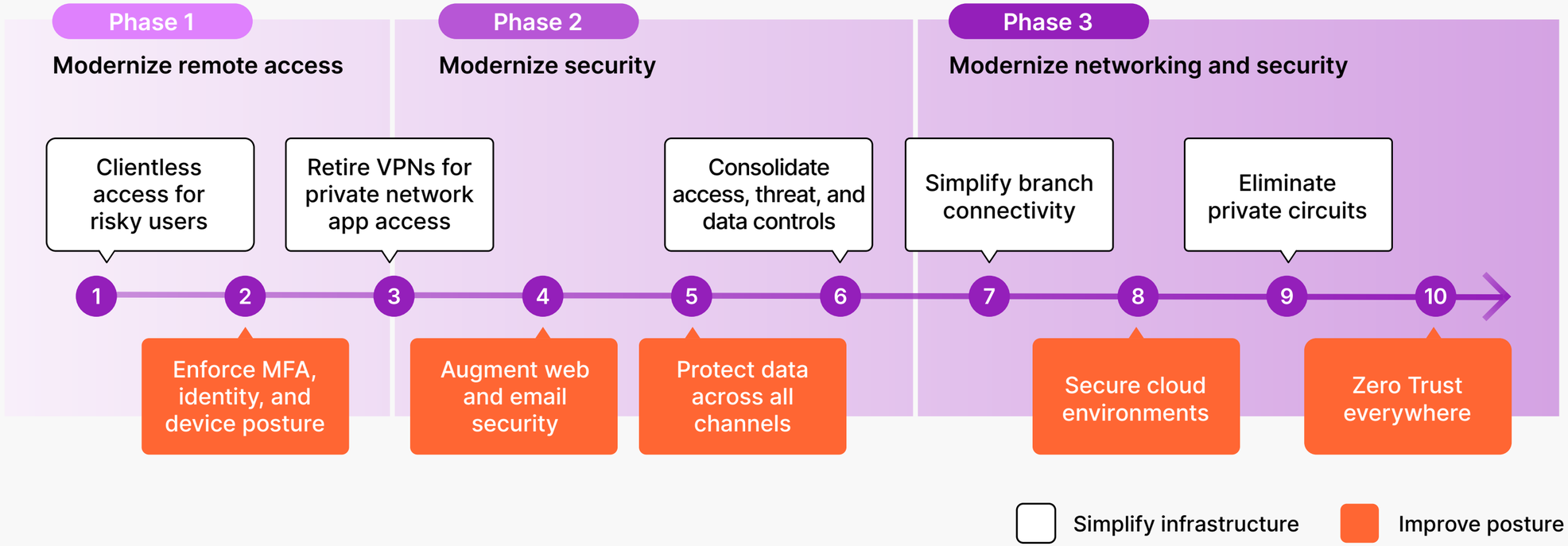
Learn more

This guide provides an executive-level overview of 10 common SASE milestones. For technical details on implementation guidance, visit Evolving to a SASE architecture.

[1] Bhogal, Charanpal, et al. Forecast Analysis: Secure Access Service Edge, Worldwide. Gartner Research, 5 Feb. 2025

Table of contents

At-a-glance: 10-step journey to SASE consolidation and Zero Trust security

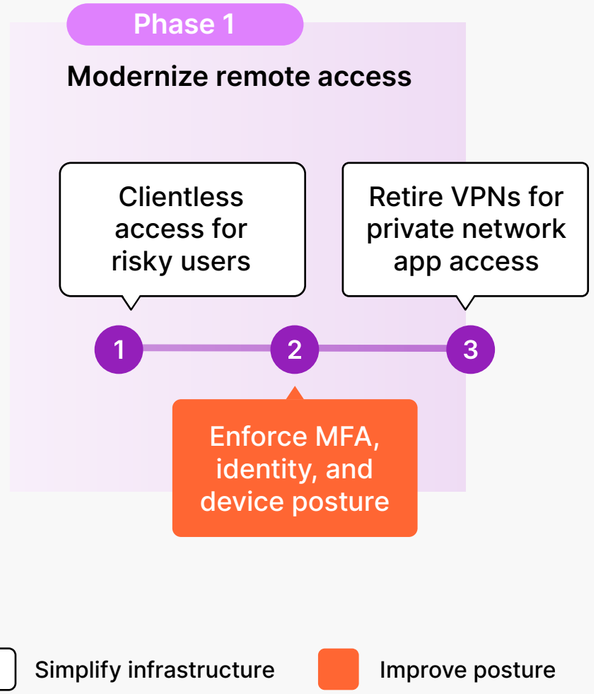


The steps in this 10-step framework are designed for organizations who are trying to achieve two major goals with SASE:

1. Simplifying their infrastructure by consolidating network connectivity and security functions, and deprecating point products

2. Improving their security posture by increasing visibility and control across environments via Zero Trust security policies between users and resources, on any device, in any location

Phase 1: Modernize remote access with ZTNA



Many organizations start their SASE journey by replacing traditional 'castle-and-moat' controls for remote access, such as virtual private networks (VPNs), and embracing cloud-delivered Zero Trust security.

Relying on perimeter-based security is increasingly a liability. Tools like VPNs, for example, increase risk with overly permissive access, hurt efficiency with manual configurations, and frustrate end users with slow experiences.

Zero Trust Network Access (ZTNA) promises a safer, simpler, and more reliable alternative, helping organizations:

- Reduce risk with increased visibility and controls
- Enable agility with streamlined operations and scaling
- Improve user experiences with fast, consistent connections

With a ZTNA service like Cloudflare Access, organizations can verify every request between any user and app based on identity, device posture, and other context — with no backhauling or on-prem appliances required.

Adopting these Zero Trust principles has been a priority in recent years as organizations embrace hybrid work and distributed cloud architectures.

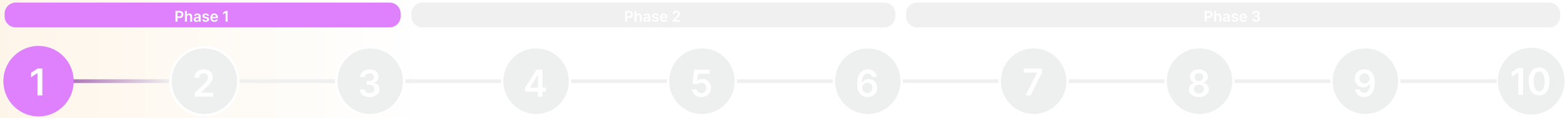
76%

of organizations have or will replace VPN with ZTNA.

98%

of IT security decision-makers agree: connecting users to applications directly — rather than the broader network — is important.[2]

[2] Source: Enterprise Strategy Group custom research commissioned by Cloudflare, "*Considerations for Implementing Zero Trust for the Workforce*", July 2024



STEP 1:

Clientless access for risky users

Many organizations start with clientless ZTNA.

This helps build familiarity with the new Zero Trust approach — without the headaches of managing client software on endpoints. In fact, 84% of senior IT and security leaders say that clientless ZTNA deployment helped them significantly accelerate Zero Trust adoption.

In this first step, they prioritize securing access for a subset of "risky users" like contractors, third parties, developers, and newly acquired teams. They often pose a risk because they interact with sensitive data or exist outside an organization's control.

These initial rollouts also typically prioritize apps like ERP, communication and collaboration, and file sharing.[3] But any web app and browser-based SSH, RDP, or VNC environment is a strong fit to get started with clientless ZTNA, and the project focus will depend on an organization's needs.

Case studies

ocado GROUP

Software and robotics platform

Securing contractor and third-party access

> Learn more

Canva

Graphic design software

Securing privileged developer access to infrastructure

> Learn more

Delivery Hero

Local delivery platform

Simplifying IT integration during M&A

> Learn more

EQT

Financial services

Maintaining business continuity as apps migrated to the cloud

> Learn more

[3] Source: Enterprise Strategy Group custom research commissioned by Cloudflare, "*Considerations for Implementing Zero Trust for the Workforce*", July 2024

Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 6 7 8 9 10

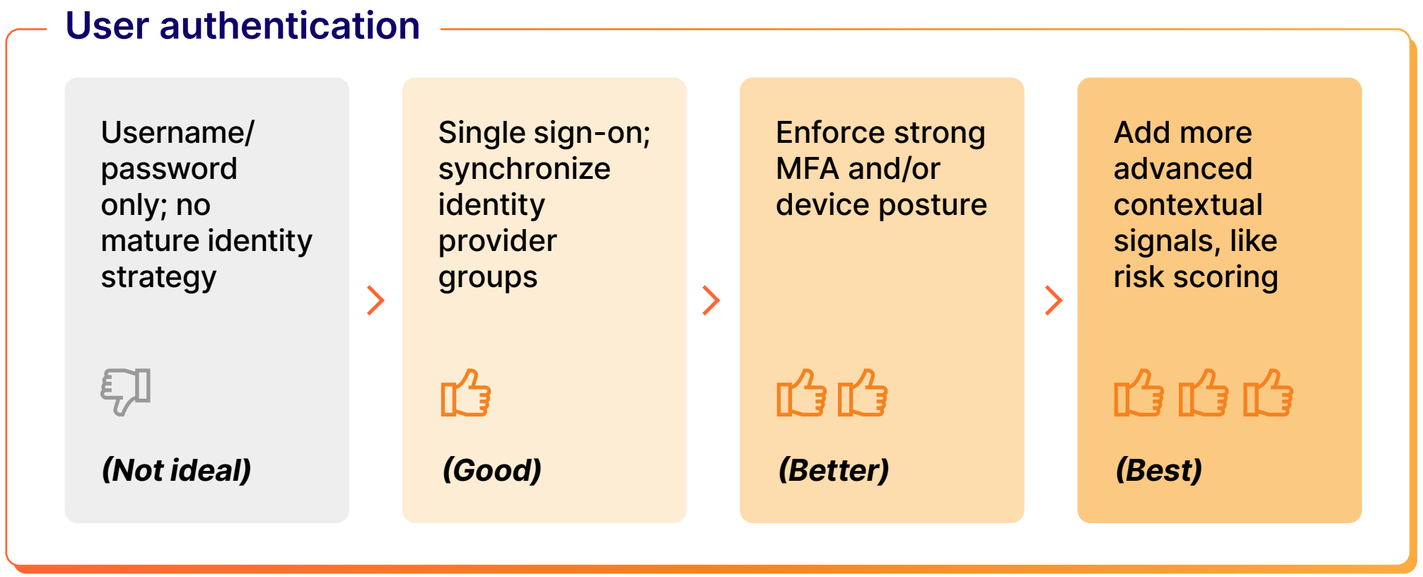
STEP 2:
Enforce MFA, identity, and device posture

Over time, organizations extend ZTNA to more users and apps (commonly CRM, financial management, DevOps CI/CD workflows, and development and collaboration).

Scaling typically requires deploying the ZTNA solution's device client, which enables per-device visibility and full proxy controls.

In parallel, they improve their security posture by layering more granular rules, including per-app policies based on the user's specific role, multifactor authentication (MFA) and hard key requirements, identity, device posture, user risk scoring, and more.

On the right is a sample maturity framework as you consider additional authentication signals and factors.



Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 6 7 8 9 10

STEP 2:

Retire VPNs for private network app access

For many organizations, the long-term goal is replacing the VPN entirely.

With VPNs, organizations too often find themselves in endless cycles of patching vulnerabilities, manually on/offboarding users, and resolving IT tickets.

Full VPN replacement typically requires extending ZTNA to non-web apps and legacy private networks for consistent context-based access controls across all internal resources. Deprecating a VPN helps not only to reduce costs (from rising bandwidth and hardware expenses), but also to unlock IT and security agility to tackle the next phases of SASE.

indeed

The world's #1 job site, **Indeed**, recognized the need to modernize an IT ecosystem that had grown increasingly complex. This complexity resulted in inconsistent traffic controls to their SaaS apps, data centers, and cloud resources. It also meant inefficient backhauling of traffic to data centers and an overreliance on an on-premises VPN.

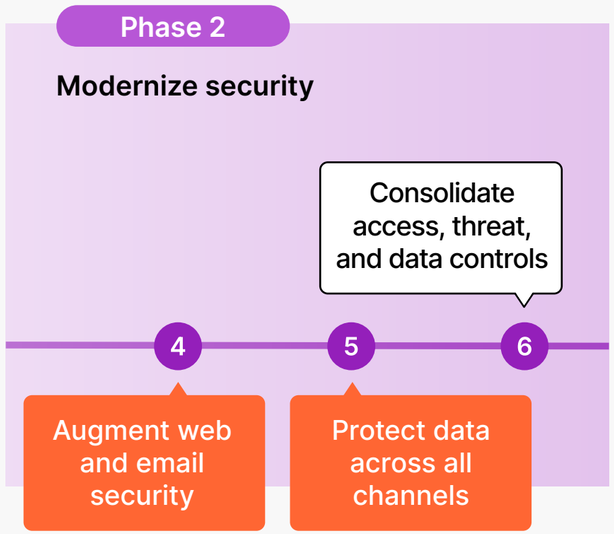
To begin modernizing their access approach, they progressively rolled out Cloudflare's ZTNA service to dedicated test groups of hundreds of users, representing different device types and roles.

In just over three months after they began onboarding Cloudflare, Indeed had deprecated their VPN entirely.

By turning to Cloudflare for any-to-any connectivity, Indeed:

- **Automated configuration of access policies** for any new users, devices, and applications
- **Mitigated unauthorized AI use**, preventing potential sensitive data exposure
- **Improved global security posture and user experience**, eliminating problematic regional connectivity issues

Phase 2: Modernize security



Simplify infrastructure Improve posture

This next phase focuses on simplifying and consolidating threat defense and data protection across web, email, SaaS, cloud, private app, and AI environments.

Here, organizations shift protections traditionally delivered by on-prem or standalone tools to a unified security service edge (SSE) platform[4] — a model that converges the security capabilities of SASE. In this way, they expand consistent identity-based visibility and controls they honed in phase 1 beyond internal apps to reduce risk across more of their attack surface.

Common strategic priorities include:

- **Stopping Internet and email threats** like malware, ransomware, and phishing
- **Supporting compliance** with regulations, government directives, and standards
- **Blocking access to unauthorized** SaaS and cloud apps to mitigate the risks of shadow IT
- **Preventing leaks and exposure** of sensitive data, including within AI tools

[4] Steps 4 and 5 can be taken with an SSE — a subset of SASE functionality that prioritizes securing access to the web, cloud services, and applications, rather than modernizing both security and networking. Cloudflare One is both a SASE and SSE platform.

Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 6 7 8 9 10

STEP 4:
Augment web and email security

To defend against cyber threats, Cloudflare customers progressively layer these Internet protections, often on top of existing on-prem capabilities:

- DNS filtering as a lightweight, effective way to block harmful and inappropriate content that can coexist with existing firewalls and web gateways
- More comprehensive secure web gateway (SWG) policies to control and monitor L4-L7 traffic with HTTP, network, and egress rules
- Browser isolation to insulate users from threats, even zero-days, by running webpage code in the cloud instead of locally on devices

Email inboxes remain a popular target for attackers, including as part of multi-channel phishing attacks. In response, many customers implement Cloudflare Email Security in parallel as a key step in protecting their broader workspace. Whether set up in-line, via API, or both, initial deployments often augment the built-in filters of Microsoft and Google email suites.

If you're trying to improve your defenses against malware/ransomware and phishing, email security is a a key component of workspace security—and it doesn't need to be deployed and managed separately. Your inbox is simply one of your top apps where users communicate, and with a SASE platform, you can protect email alongside the rest of your workspace in a unified, streamlined way.

Case studies

In the United Kingdom, Cloudflare has implemented Protective Domain Name Service, in partnership with Accenture, to block Internet threats and encrypt all web traffic for privacy for government and public service organizations.

Werner Enterprises, the North American transportation company, reduced malicious emails in their user inboxes by more than 50% and cut manual email triage efforts by several hours each day, unlocking productivity for more strategic projects.

THG, the global ecommerce retailer, replaced Zscaler with Cloudflare to unify security across internal apps and the Internet for 7,000+ hybrid workers. Cloudflare automated migration of initial Internet filtering policies from Zscaler in just one week.

Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 6 7 8 9 10

STEP 5:
Protect data across all channels

Mitigating data risks is always imperative, and in this step, organizations often focus on extending visibility and controls to prevent exposure across sprawling SaaS, cloud, and AI environments.

To that end, organizations typically onboard two key SSE technologies:

- Cloud access security broker (CASB) to scan SaaS apps and cloud storage via API to uncover risky misconfigurations that expose data, unauthorized user activity, shadow IT, and other threats
- Data loss prevention (DLP) to detect and block sensitive data in transit, at rest, and in use

Now with a full range of SSE capabilities, customers take on priorities to protect data across several key areas, such as:

- **Securing developer code** by remediating misconfigured public repositories (like GitHub) and controlling movement of source code
- **Mitigating risks of SaaS apps and cloud storage** by identifying and blocking unsanctioned apps, and remediating misconfigurations in common enterprise tools (e.g., Salesforce, Dropbox, and AWS S3)
- **Protecting data in AI tools** like ChatGPT by restricting inputs, copy-paste, uploads, and other user actions via DLP and browser isolation controls
- **Complying with regulations** by discovering and applying controls to regulated data classes (like PII, health, and financial), and maintaining detailed audit trails for compliance reporting and investigations

Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 **6** 7 8 9 10

STEP 6:

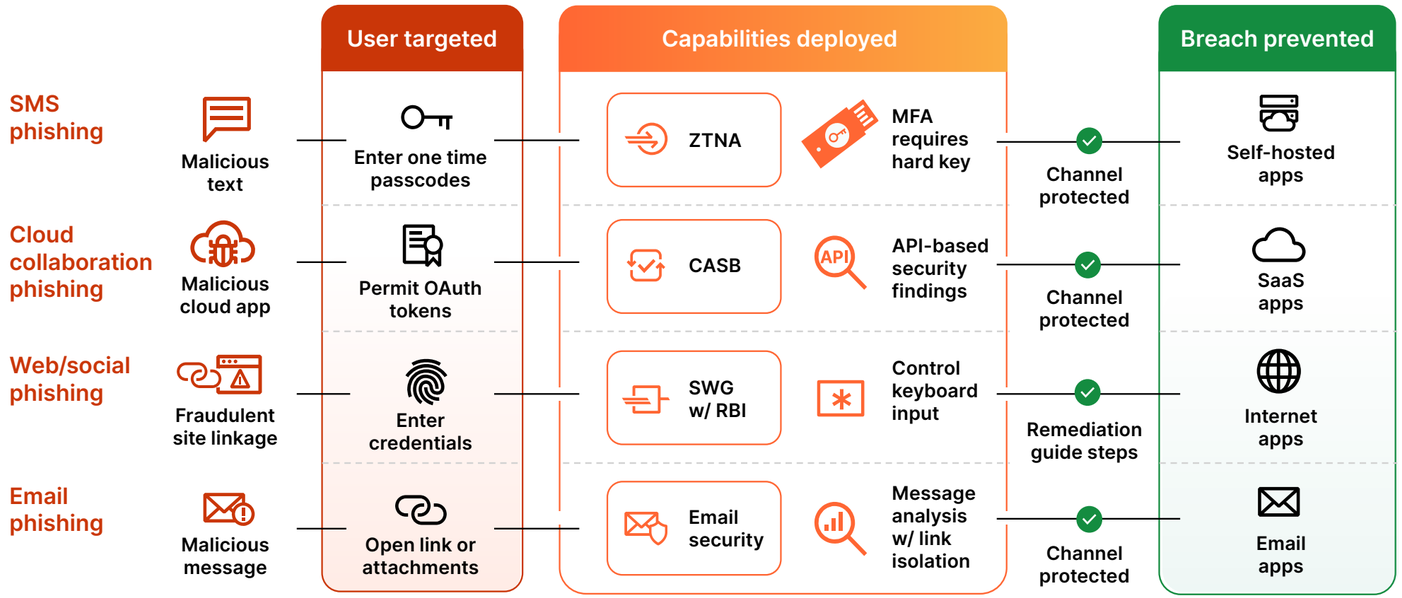
Consolidate access, threat, and data controls

As organizations progress in phase 2, they gain familiarity over the full range of SSE capabilities across ZTNA, SWG, CASB, DLP, RBI, and email security.

Unifying workspace security in this way helps strengthen their overall posture with consistent policies across environments, unlock efficiency with simpler management, and enable agility to protect growing digital footprints.

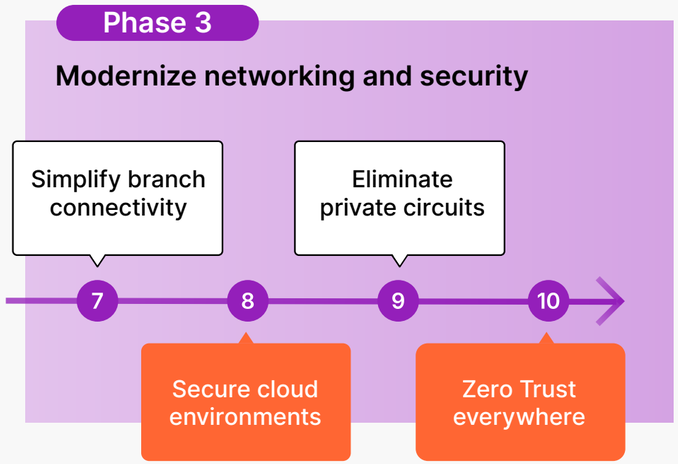
To see an SSE platform in action, let's look at how multiple protections work together to prevent phishing across multiple channels, specifically via email, text, SaaS apps, and the Internet:

Use case: Stop multi-channel phishing



- **ZTNA** with hard key authentication deters attacks that seek to harvest one-time passcodes delivered via SMS texts;
- **CASB** detects OAuth permissions in SaaS apps that have been inappropriately shared, potentially with malicious third parties who can then exploit that access;
- **SWG** can block web traffic entirely or isolate webpage activity and restrict keyboard inputs into a potential harvester; and
- **Email security** blocks multi-channel phishing attacks and isolates suspicious links to insulate users from threats.

Phase 3: Modernize networking and security



With a complete SASE transformation, organizations simplify connectivity by shifting all network and security services to the cloud.

Relying on routers, firewalls, multiprotocol label switching (MPLS) lines, WAN optimizers, and other traditional networking appliances holds back agility.

Organizations struggle with complex on-prem architectures that are:

Inflexible

Scaling capacity requires new hardware and lengthy configurations, and cloud adoption requires backhauling.

Expensive

Purchasing and maintaining circuits and appliances (often manually) require significant money, time, and expertise.

Insecure

Visibility and policies are inconsistent across multi-cloud and hybrid work environments.

However, with a complete SASE transformation, organizations reduce overhead and enhance security across their offices, branches, data centers, and physical locations.

Phase 1 | Phase 2 | Phase 3

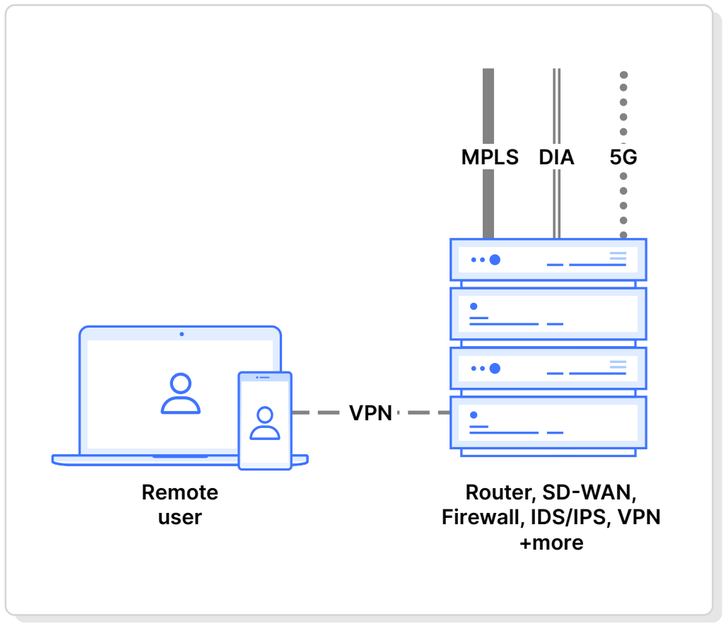
1 2 3 4 5 6 **7** 8 9 10

STEP 7:
Simplify branch connectivity

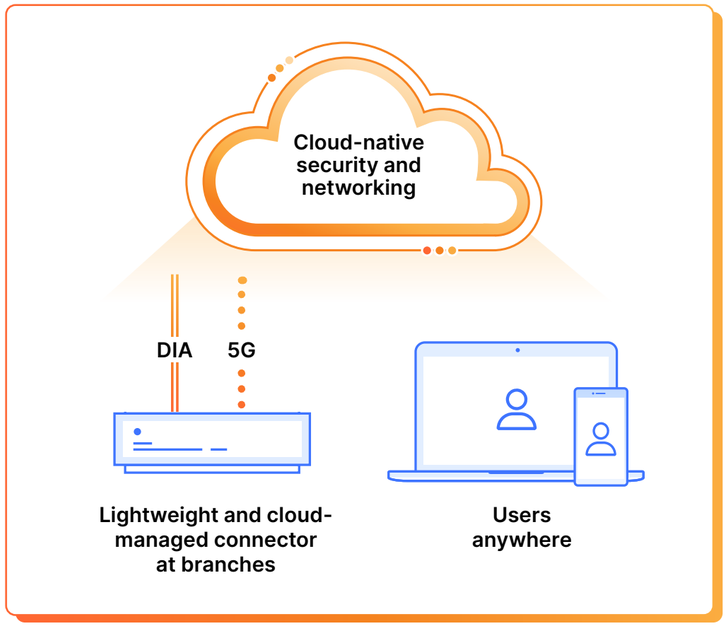
Many organizations prioritize transitioning from bulky appliance stacks at their branch offices to a lighter-weight, cloud-native approach.

The goal is for connectivity to be as simple and seamless as connecting to WiFi at a coffee shop, with minimal infrastructure or configuration required. In this "**coffee shop networking**" approach (as it's often called), the SASE platform — not an on-prem firewall — provides consistent protection, whether the user is at a branch or remote.

In this step and throughout this phase, we see customers onboard traffic to Cloudflare's Network-as-a-Service (NaaS) for more efficient and secure routing policies.



Traditional branch networking and security stack



Coffee shop networking via Cloudflare's NaaS

The simplest and easiest way to on-ramp existing network locations to the Magic WAN service is to deploy Cloudflare Magic WAN Connector. This is a plug-and-play, fully cloud-managed network device that can be deployed in any physical or cloud network as either hardware or a virtual appliance.

Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 6 7 8 9 10

STEP 8:

Secure cloud environments

The next goal is to extend that consistency and flexibility to the management of multi-cloud infrastructure.

By on-ramping traffic from public clouds like AWS, GCP, and Azure to Cloudflare, organizations can centralize visibility and orchestration.

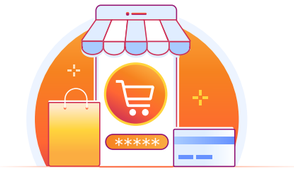
For example, Cloudflare helps organizations automatically discover and manage the native functionality of their cloud resources — like virtual private clouds (VPCs), subnets, virtual machines, route tables, and routes — without requiring any additional compute virtual machines.

STEP 9:

Eliminate private circuits

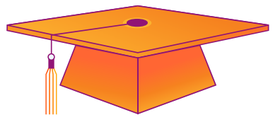
Over time, the goal is to eliminate all private network circuits, especially expensive MPLS and leased lines. By instead routing all site-to-site traffic through the SASE platform, organizations can reduce complexity, lower costs, improve performance, and enforce more consistent security.

Use cases driven by network modernization



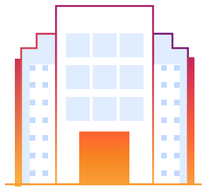
Llifestyle apparel retailer

Connecting and protecting an expanding retail store footprint without legacy hardware



Large public university

Securing Internet access across campuses without backhauling traffic to a centralized data center



Global manufacturer

Consolidate networking and security architecture to support multiple acquisitions annually

Phase 1 | Phase 2 | Phase 3

1 2 3 4 5 6 7 8 9 10

STEP 10:

Zero Trust everywhere

Throughout this third phase, organizations can eliminate remaining IP-based controls and other forms of implicit trust that are based on presence on the corporate network.

This shift provides an architectural foundation to continue maturing their Zero Trust approach — a journey that is never really "done."

As digital environments expand, organizations should continue to evolve policies to adapt with ever-changing business context, threats, and risk factors.

Future-proofing security against emerging post-quantum threats

Conventional cryptography that underpins today's Internet faces an existential threat as quantum computing advances. "Harvest now, decrypt later" adversaries actively collect encrypted communications, with the expectation that quantum computers will be able to decrypt the harvested communications in the future.

Post-quantum cryptography (PQC) represents the strongest countermeasure to quantum threats.

Even if your systems are not PQC-ready, you can begin transitioning to post-quantum cryptography while protecting against emerging threats, with Cloudflare.

Customers can enable post-quantum Zero Trust access with Cloudflare today — without disrupting performance or requiring specialized expertise.

Unlock more benefits from Cloudflare's connectivity cloud

Evolving your partnership with Cloudflare to include SASE architecture helps address the inefficiencies and risks caused by disjointed "platforms."

All Cloudflare services, including Cloudflare One, are built on Cloudflare's connectivity cloud. This provides secure, low-latency, and infinitely scalable connectivity across networks, applications, and users.

Cut network and operational complexity, boost security and regulatory compliance, and gain faster time-to-value from digital investments like cloud migration, app modernization, and AI-powered transformation.

In a commissioned, independent cost-benefit analysis of Cloudflare's connectivity cloud, Forrester Consulting found that, over three years, a composite organization representative of interviewed customers achieved benefits like:

- 238% ROI, with payback in less than six months
- A 29% improvement in security team efficiency
- A 13% improvement in IT team efficiency
- Reduced risk of breach by up to 25%

Analyst-recognized SASE platform

Gartner®

Named in Gartner® Magic Quadrant™ reports for **Single-Vendor SASE, Security Service Edge (SSE), and Email Security Platforms**

FORRESTER®

Named in Forrester Wave™ reports for **Security Service Edge (SSE), Zero Trust Platforms, Email, Messaging, and Collaboration Security Solutions**

IDC

Named in IDC MarketScape reports for **Zero Trust Network Access (ZTNA) and Network Edge Security as a Service**

Read the "Total Economic Impact™ of Cloudflare's connectivity cloud" study

Ready to fast-track your SASE journey?

Contact your representative

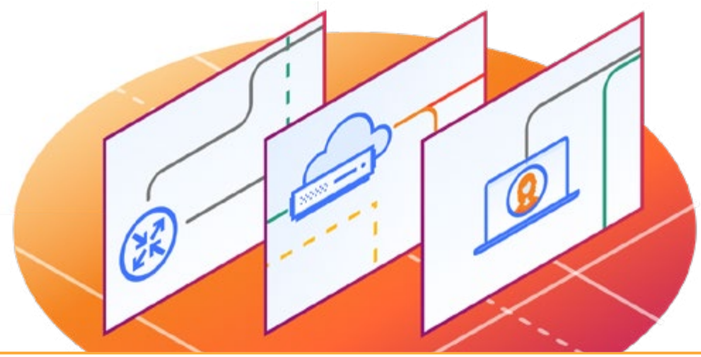
Contact your Cloudflare representative for personalized, expert advice and support.

Learn more

Visit cloudflare.com/zero-trust to dive deeper into what Cloudflare One offers.

Review documentation

Explore our reference architectures for details on how Cloudflare One is designed.



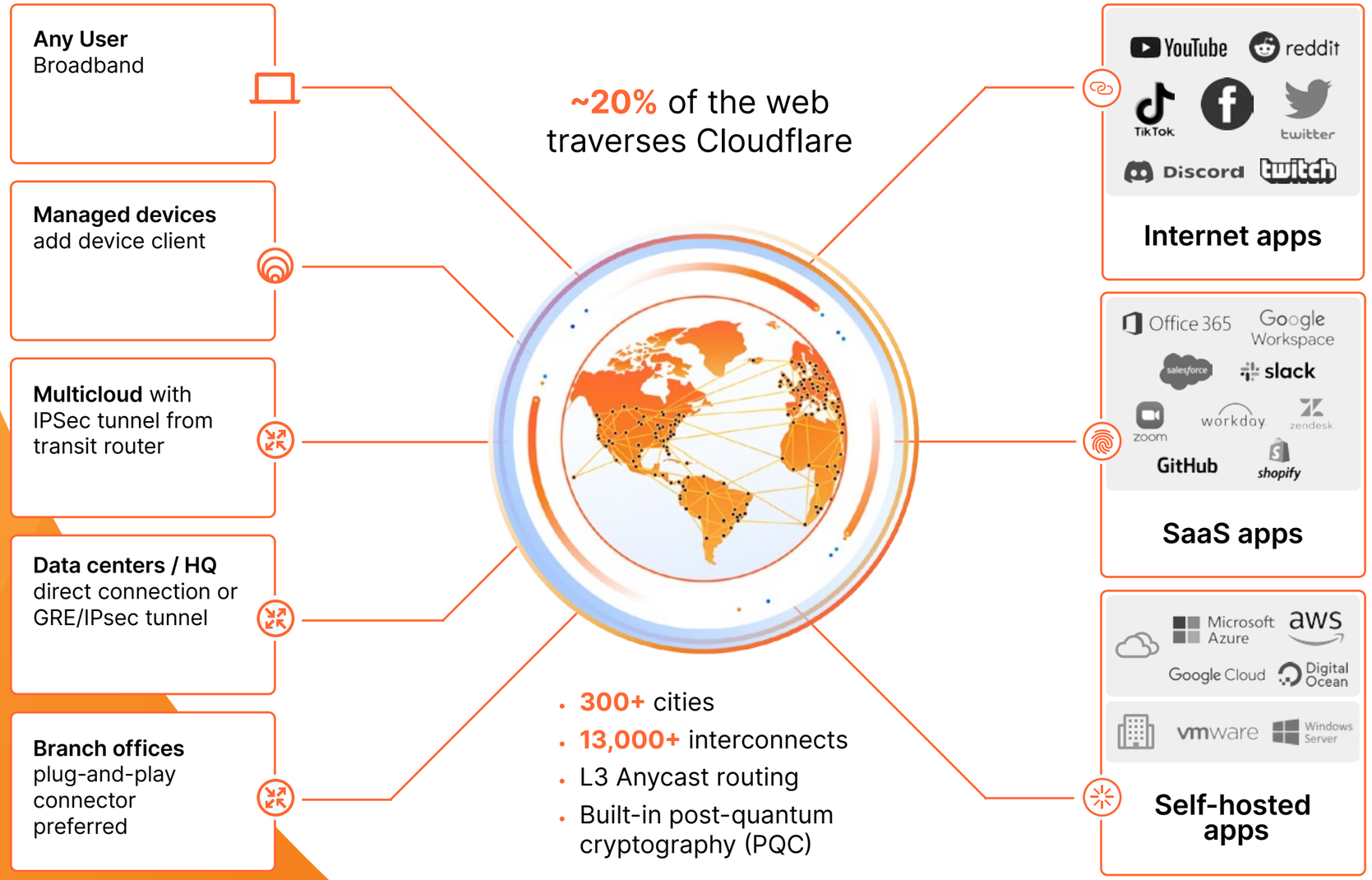
Appendix

APPENDIX

Deploying with confidence

However your teams currently use Cloudflare services today, we make it easy to send traffic to our global network with composable on-ramps for any source to any destination.

- **Clientless access** to rapidly adopt Zero Trust
- **Device clients** to fully replace your VPN
- **IP tunnels** through branch connector or Anycast GRE/IPsec to phase out legacy MPLS networks
- **Direct connections** with your on-prem locations or your VPCs



APPENDIX

Cloudflare Support and Professional Services

Professional services

Expert-led implementation

- Quickstart advisory onboarding
- Migration services
  including Descaler and Deskope programs
- Expert implementation

Success options

Curated to maximize time and value

- Standard
- Premium

Available success and support upgrades for more focused optimization services.

Technical support

Break-fix and focused services

- Technical support
- Technical account management
- Security operations service

Self-guided resources

Tutorials, best practices, how-tos, and other learning tools

- Support portal
- Reference architectures
- Product docs
- Learning paths
- Communities
  Cloudflare · Developer
- Cloudflare blog

+ Global ecosystem of Authorized Service Delivery Partners and Global System Integrators

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

REV:BDES-7212.2025JUN09