CLOUDFLARE

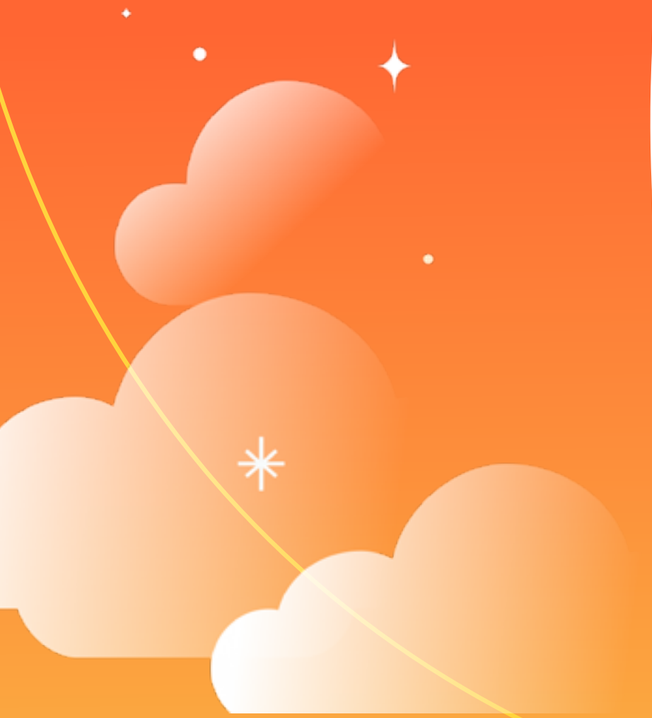
EXECUTIVE GUIDE

The CISO's guide to SASE adoption

How to evaluate SASE platforms for high-priority use cases

Table of Contents

Evaluating SASE platforms for high-priority use cases



Our customers often adopt Cloudflare services for external-facing applications. However, with trends like hybrid work, generative AI, and API-first app development, connecting and securing internal apps, people, and networks has become a challenge. Shifting compliance requirements add to this burden.

To overcome these challenges, consider a secure access service edge (SASE) architecture. Unlike past approaches, SASE unifies security and networking capabilities onto a single cloud platform and one control plane.

By placing network controls on the cloud edge, SASE helps deliver C-level priorities such as:

- Accelerating growth by removing security and connectivity obstacles
- Enforcing more consistent visibility and control across all locations, people, devices, and apps
- Reducing complexity and costs through vendor consolidation and less legacy IT management
- Enabling any-to-any connectivity between all networks, cloud environments, apps, and people

However, there is no “one size fits all” approach to SASE.

“The CISO’s guide to SASE adoption” highlights common “quick win” use cases, as well as outlines vendor assessment criteria and a long-term SASE roadmap.

It also explains why some organizations choose Cloudflare One as their single-vendor SASE platform or as part of a two-vendor solution. Built on our connectivity cloud, Cloudflare One simplifies secure, “any-to-any” connectivity and helps enterprises regain control of their IT environments.

USE CASE #1

Adopt Zero Trust Network Access (ZTNA)

Relying on traditional perimeter-based security for hybrid work arrangements, multicloud environments, and unmanaged devices limits visibility, creates conflicting configurations, and increases risk. A Zero Trust approach, where no entity is trusted by default, helps modernize an organization's security strategy in the following ways:

Replacing traditional hardware-based security

Traditional network perimeter controls like VPN are hard to scale, reduce visibility, and make it difficult to detect and remediate attacks. A cloud-based SASE model provides a secure alternative by implementing Zero Trust Network Access (ZTNA), while also routing and processing network traffic across a global cloud network. This helps reduce both end-user friction and attacker lateral movement.

Managing device access

Third-party users can pose risks when privileges are over-provisioned or unmanaged devices can connect to a network. SASE enables clientless access with Zero Trust policies, ensuring contractors only access what they need with BYOD data controls.

Mitigating ransomware attacks

In a traditional network architecture, ransomware actors can quickly move laterally to other parts of the network to eventually extract or alter valuable data. However, since SASE operates on Zero Trust principles — including the principle of "least-privilege" access (enforced with ZTNA) — even compromised accounts or devices do not have indiscriminate network-level access. This limits the range of potential lateral movement and contains the spread of ransomware.

Limiting data exposure

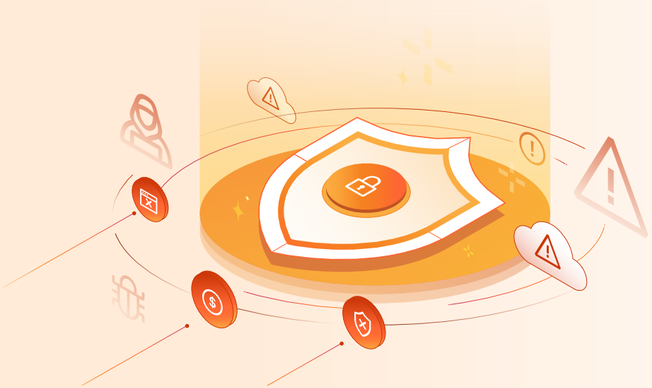
As users share sensitive information across SaaS apps and cloud storage, the risk of data exposure and exfiltration rises. SASE enforces Zero Trust policies that help prevent data exposure by limiting which apps or app tenants each user has access to, while also scanning SaaS apps and cloud storage for sensitive data and misconfigurations.

> **"Although we were familiar with Cloudflare from our application security and development transformation, the Zero Trust portfolio services truly amazed us. Comparing the different features and capabilities of Cloudflare relative to other solutions, it was a no-brainer … By simplifying things with Cloudflare, our third-party partners and internal users receive the same secure, seamless experience we provide consumers on our website."**
>
> **Abraham Ingersoll**
> Chief Security Officer, THG
>
> Read the THG & Cloudflare case study >

USE CASE #2

Protect your attack surface

Digital transformation and remote work have expanded the attack surface, with more dispersed users and unmanaged devices. But extending on-premise firewalls to the cloud and scaling networks via VPNs can increase exposure to threats, and simultaneously reduce visibility. A SASE architecture extends visibility and controls to support a “perimeter-less” model, and enforces consistent protection in these ways:



Avoiding multi-channel phishing

Attackers launch phishing attacks into channels where users tend to let their guard down about where they click. However, a SASE platform integrating ZTNA and a cloud access security broker (CASB) — alongside email security and web security with remote browser isolation (RBI) — offers a multi-layered approach to stop phishing threats across email, SMS, social media, collaboration apps, and other communication channels.

Defending remote workers

Remote work requires users to connect from multiple locations and devices, often outside their organization’s purview. A SASE architecture allows organizations to secure any connection, so users on any device in any location can stay safe and productive when using the Internet and internal resources.

Protecting distributed offices

Traditional approaches for inspecting office traffic often require backhauling the traffic to centralized corporate data centers, which can add latency and hurt productivity. But the alternative — giving users direct Internet access — introduces risks and creates inconsistent user experiences. SASE intelligently manages and optimizes direct connections to any cloud or Internet destination, and enforces policies and protections as close to end users as possible.

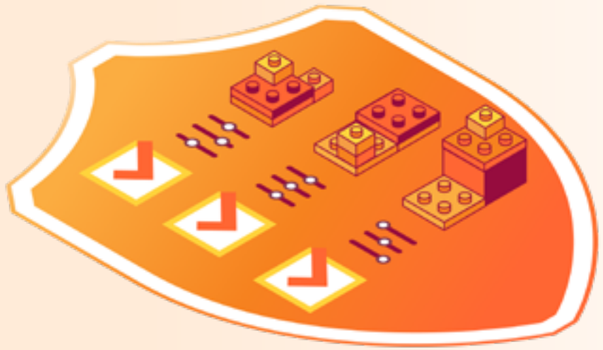
Securing wide area networks (WANs)

Some WANs bypass cloud security for traffic between branches, so integration claims between security services and software-defined WANs may not be what they initially seem. SASE simplifies and secures how organizations connect over WANs by filtering and inspecting traffic between offices, data centers, public clouds, and other locations.

> **“As we enter a new technical era, with the rapid development of generative AI, we expect to see new generations of complex online threats coming toward the industry. I believe Cloudflare has the visibility, access, and business intelligence to leverage the massive amounts of data on the global network and train defensive models to identify and mitigate these next-generation attacks.”**
>
> **Mehdi Salour**
> Senior Vice President of Global Network and DevOps, 8×8
>
> Read the 8×8 & Cloudflare case study >

Protect your data

Sensitive data may be exposed through the unsanctioned use of generative AI and shadow IT, leading to compromise or breaches that may be costly to remediate. SASE converges data visibility and controls across web, SaaS, and private application environments, helping organizations accomplish the following:



Simplifying compliance with data security regulations

Keeping up with the multitude of data security and compliance demands (GDPR, PCI DSS, HIPAA, and more) is complex. Compliance standards related to AI usage are also continuously evolving. SASE unifies data controls so security teams can lock down regulated data classes, reduce breach risks, and streamline data compliance.

Managing shadow IT

SASE helps minimize the risks associated with shadow IT by proxying traffic through an inline cloud access security broker (CASB), which reveals the use of unsanctioned applications and controls how those apps are accessed and used.

Using generative AI safely

A SASE approach enables organizations to detect and approve AI application usage and scan for misconfigurations that risk data leaks. AI apps can also be run in isolated web browsers to restrict data inputs and output.

Protecting sensitive data

Detect and control how sensitive data moves into, around, and out of IT environments. This includes scanning apps and inspecting traffic for regulated personal data and intellectual property, blocking Internet threats like phishing and ransomware, and implementing additional protections against data theft and inadvertent leaks.

> **“Despite its many legitimate users, AI presents major security and privacy concerns. Cloudflare helps us find what shadow AI risks exist and block unsanctioned AI apps and chatbots.”**
>
> **Matthew Ortiz**
> Senior Manager Information Security, Indeed
>
> Read the Indeed & Cloudflare case study >

Choosing a SASE solution

Multi-vendor vs. single-vendor SASE

Imagine a Tour de France team of riders from different squads, with different strategies and gear. They have not trained together before, but each cyclist has a specialty for every stage. In SASE, this is like having two or more vendors for different SASE functions. This approach lets organizations customize their tech stack and leverage the strengths of each vendor.

Multi-vendor SASE also requires having the time and resources to orchestrate and integrate the services — with limitations due to a subset of data and features exposed to or interoperable with third parties. Otherwise, the lack of coordination can be inefficient, leave security gaps, decrease visibility, and increase costs and complexity.

Organizations seeking a simpler approach to solving a wide range of problems should consider single-vendor SASE (SV-SASE). This approach consolidates different point products and drives down TCO. To further reduce complexity, look for a vendor who has architected their services to be unified, natively integrated, and developer-friendly from the outset. Plugging in users, apps, devices, locations, and clouds into one network ensures consistent visibility, control, and policy enforcement from day 1.

Key criteria

Whatever approach you choose, keep the following criteria (and sample questions) in mind when assessing solutions:

Risk reduction:

- Is application traffic decrypted and inspected by threat and sensitive data detection engines in a single pass? Are there any deployment caveats?
- Are all data flows and communications through SaaS suites protected across every channel?
- What user/device risk scoring and analytics are available?
- Are any security functions bypassed based on any network on-ramps?
- Can you integrate my threat intelligence feeds into your architecture?

Network resiliency:

- Are the security and networking functions natively integrated by default?
- Is each connectivity method and SASE service interoperable with each other in every location?
- Is every function delivered from every data center location?
- Do you offer uptime and/or end-user latency guarantees with any SASE service?

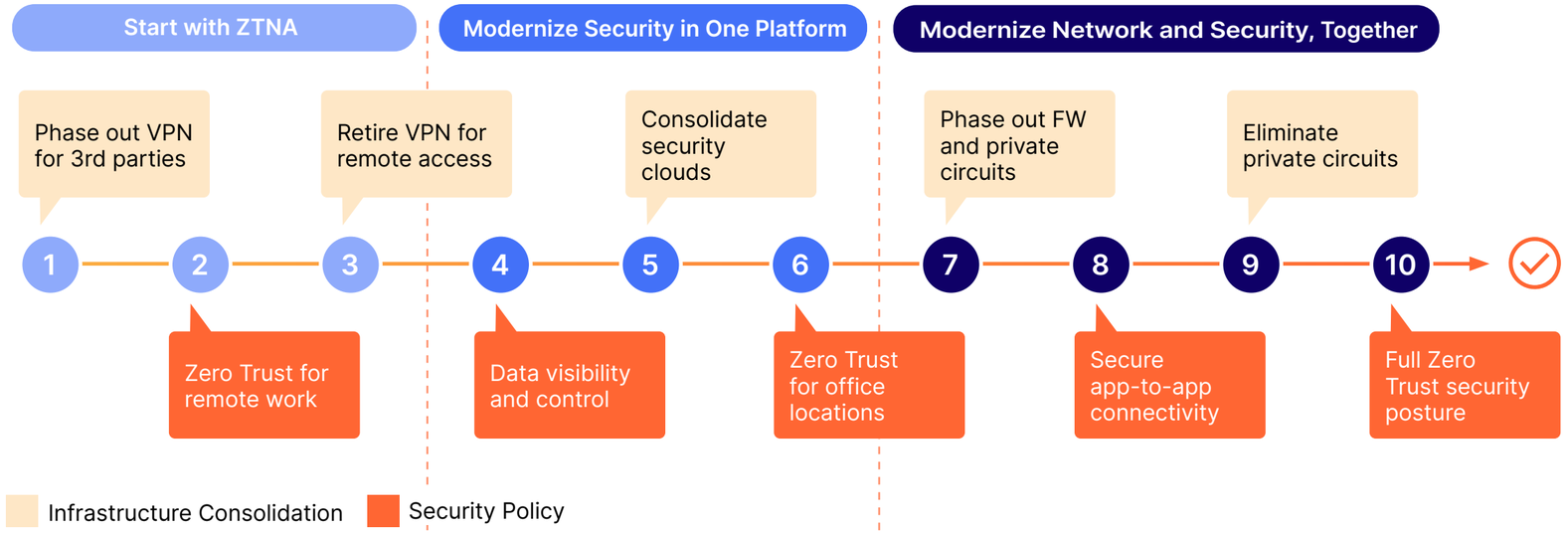
Future-proof architecture:

- What happens to our SASE services/costs if we switch between clouds?
- Is your platform developer-friendly? Will future SASE functions work seamlessly with my current apps?
- What data localization and compliance capabilities are built-in?

Structuring your SASE roadmap

One of the best aspects of a composable SASE architecture is that there is no perfect order of operations. The many use cases solved by a SASE architecture can be considered cumulative: effort towards one or two use cases still make an organization's security posture stronger.

Starting small on the journey to SASE can prove efficacy, gain internal momentum, increase support from stakeholders — and improve the likelihood of buy-in for future, larger projects.



For instance, your long-term roadmap for a complete SASE architecture may follow a flow similar to that of other Cloudflare customers:

Phases 1-3

Modernize how workforces reach corporate resources, by offloading or eventually replacing VPNs and legacy private networks with Zero Trust.

Phases 4-6

Improve visibility and controls for SaaS apps, including mitigating shadow IT, managing tenants, and preventing data exfiltration. Consolidate controls for outbound Internet access and threat protection tools.

Phases 7-10

Bring access consistency such that users and devices in any network location gain the same Zero Trust security posture. Phase out network appliances and private circuits, and enable Zero Trust app-to-app connectivity across cloud environments. Finally, true network modernization eliminates any remaining excessive trust.

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." Consolidate network services onto our single-vendor SASE, Cloudflare One, to simplify even more of your tech stack — and deliver the greatest cost reduction possible.

All Cloudflare services are built on Cloudflare's connectivity cloud — a unified platform of cloud-native services designed to help organizations regain control over their IT environments.

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

Up to 25%
Reduced risk of breach

29%
Improvement in security team efficiency

13%
Improvement in IT team efficiency

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

Gartner

- Named for the first time in 2024 Gartner® Magic Quadrant™ for **Single-Vendor SASE**
- Named in the Gartner® Magic Quadrant™ for **Security Service Edge** (SSE) for 2nd consecutive year
- Named a Customers' Choice in the 2024 Gartner® Peer Insights™ Voice of the Customer: **Zero Trust Network Access**

FORRESTER®

- Strong Performer in the Forrester Wave™ for **Security Service Edge** (SSE) Solutions, Q1 2024
- Strong Performer in the Forrester Wave™ for **Zero Trust Platforms** (ZTP), Q3 2023
- Leader in the Forrester Wave™ for **Enterprise Email Security**, Q2 2023

IDC

- Leader in the IDC MarketScape for **Zero Trust Network Access** (ZTNA) 2023
- Leader in the IDC MarketScape for **Network Edge Security as a Service** 2023

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

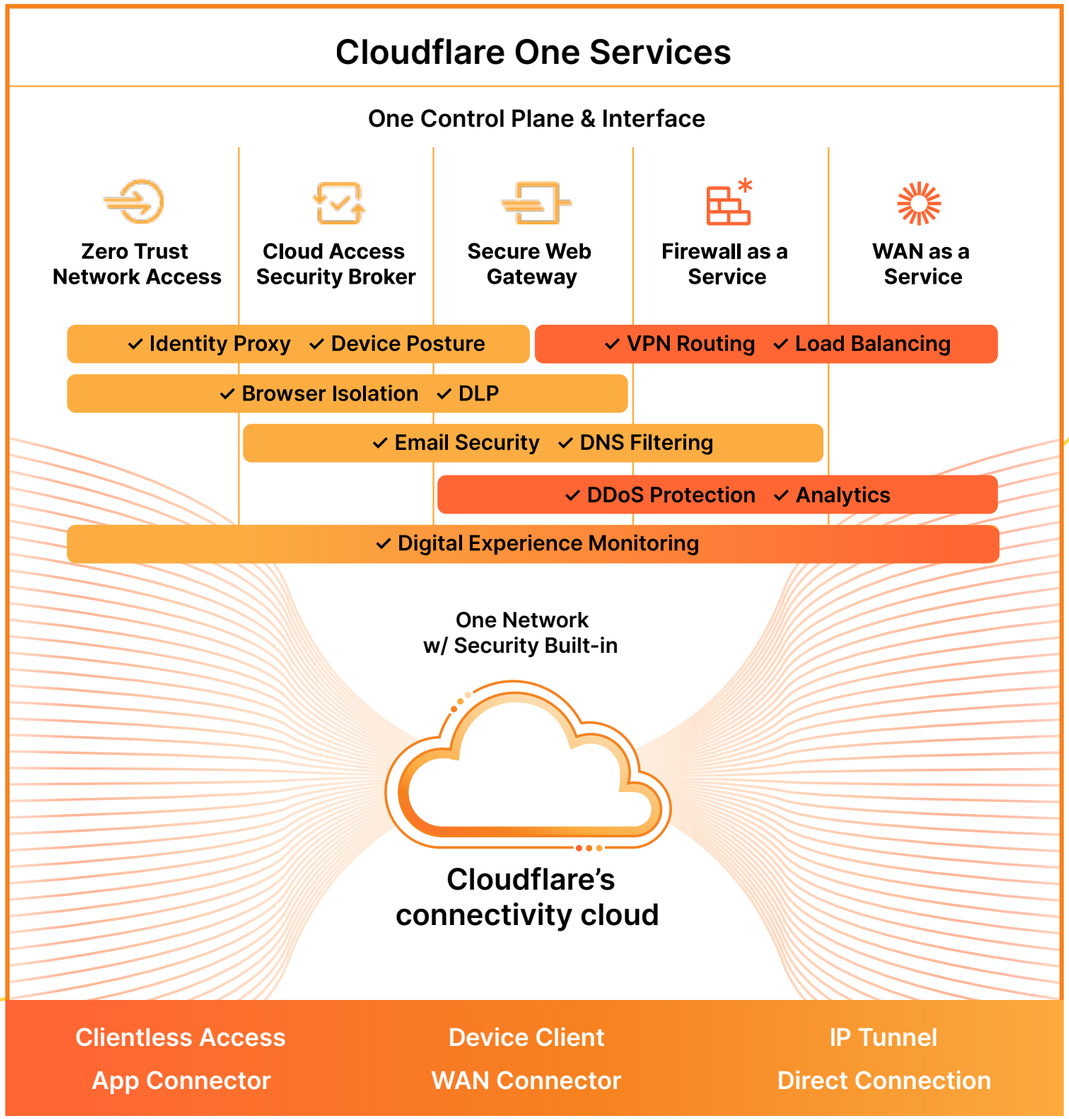
How Cloudflare delivers SASE: One composable, Internet-native platform

Cloudflare is the only SASE provider to start with a Zero Trust Network architecture with identity and context-based connectivity built-in across our entire platform.

All Cloudflare One services are:

- Managed via one interface to simplify how you build policies and reduce operational overhead
- Composable, so you can make progress adopting services and layering capabilities at your own pace
- Available to run across all of our 335+ data center locations, delivering consistent speed and scale everywhere

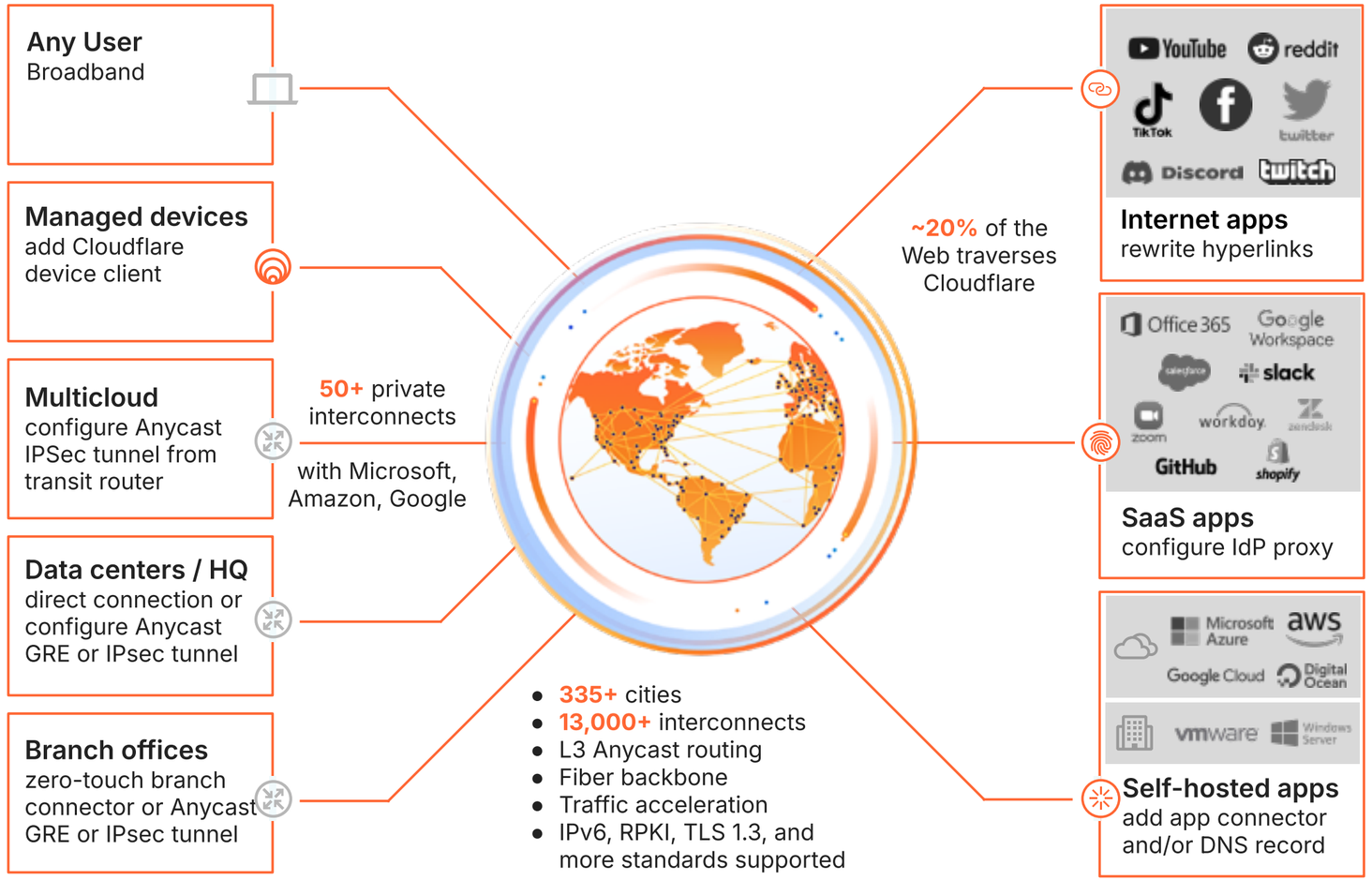
Cloudflare One also converges security and performance capabilities not typically built into SASE platforms (such as authoritative DNS, DDoS protection, and email security), which further reduces vendor complexity.



Cloudflare On-ramps

Deploying with confidence

However your teams currently use Cloudflare services today, we make it easy to send traffic to our global network with multiple, flexible on-ramps.



One

programmable network and control plane to build new capabilities on and enforce security controls

100%

uptime SLA for paid plans than only an Anycast-enabled architecture can deliver

40-65%

faster than Zscaler, Netskope, and Palo Alto Networks for security services [Learn more >]

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

Support determined by contract entitlements.

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-6743.2025FEB05