CLOUDFLARE

SOLUTION BRIEF

Secure Access Service Edge (SASE)

Accelerating network transformation and security modernization

What is SASE?

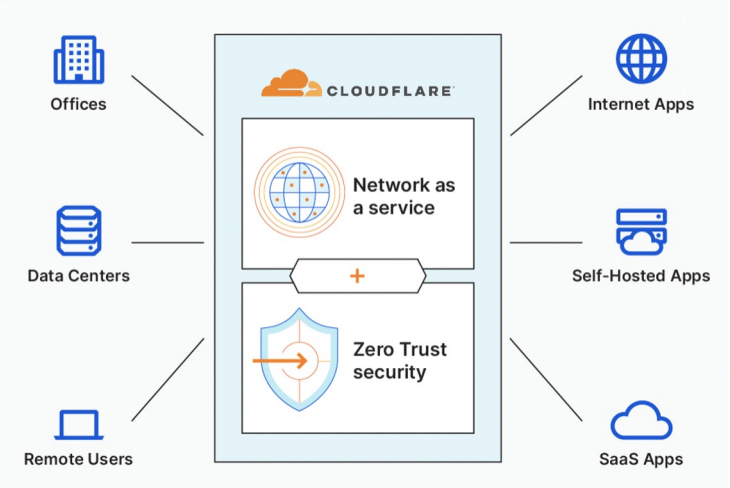
The emergence of digital and cloud initiatives has shifted the applications from centralized data centers to distributed locations such as the public cloud, private cloud, and SaaS. In parallel, users work from their home, office, hybrid, or any remote location. This new traffic pattern (any-to-any) has expanded the attack surface of the legacy network architecture resulting in an increased cyber risk.

Adopting a SASE architecture addresses the shift in the application access. SASE is the convergence of network and network security functions for any-to-any traffic with better security controls leveraging Zero Trust principles. Gartner expects that "By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch and edge access, up from 10% in 2020." [1]

How Cloudflare enables SASE

Cloudflare's SASE platform, Cloudflare One, is a Zero Trust network-as-a-service built on a single, unified Internet-native network platform. It places identity-based security controls, firewall, WAN-as-a-Service and more close to users everywhere on Earth, helping them quickly and securely connect to any enterprise resource.

Instead of granting full trust and access to applications once they're on the corporate network, Zero Trust uses a proxy-based, default-deny architecture that dictates verifying and authorizing every request into, out of, and between entities on your network — ensuring that users can only get to applications they're explicitly allowed to access.



Obstacles to SASE

Per Gartner, one of the obstacles to SASE is global coverage. On average, Fortune 500 companies have a presence in 32 countries. Yet many SASE vendors offer services in a few regions and countries. Lack of global coverage results in inconsistent security policy enforcement and performance issues.

For businesses aiming to fully unify security and network edge services from a single vendor, Cloudflare One provides services built on our 275+ city global network in 100+ countries and ~50ms from 95% of the Internet population.

"SASE depends upon cloud-delivery, and a vendor's cloud footprint may prevent deployments in certain geographies, such as China, Russia and the Middle East, where vendors may have limited cloud presence." [2]

Gartner

Composability expedites SASE

Depending on existing investments, customers embarking on the SASE journey often have several vendors spanning the end-to-end solution. Using more than 1-2 vendors leads to an increased total cost of ownership, operational complexities, performance issues, and, most importantly, reduced business agility. Dozens of SASE vendors exist—some specialize in security, others in networking—very few are experts in both.

Consolidating hardware and point products can take years as hardware gets refreshed in 5-7 year cycles. Refreshing network hardware first can cause interoperability issues with existing security service and vice versa. To expedite SASE adoption at own pace, customers require a SASE platform that is composable. Composability enabled services are available on-demand, plug-n-play with each other, and interoperable within existing infrastructure.

Cloudflare One is a composable SASE platform. With our platform, security and networking services all live on the same infrastructure, and are architecturally unified at every level—not just in a single pane-of-glass. One control plane to one data plane with single-pass inspection as close to the user as possible, so there's no added latency. With one control plane, any network on-ramps can connect and secure traffic to any resource with one-time integrations. One management interface —UI, API and CLI.

> "Strive for not more than two vendors for all core services to minimize complexity and improve performance..."[2]
>
> Gartner

One global, comprehensive service edge

Cloudflare

✓ Zero Trust Network Access	✓ Identity/Context	✓ Threat prevention
✓ CASB	✓ Device profile rules	✓ Data Loss Prevention
✓ Secure Web Gateway	✓ Role-Based Access Control	✓ Cloud app discovery
✓ Firewall as a Service	✓ Encryption/Decryption	✓ SaaS acceleration
✓ WAN-as-a-Service	✓ Browser Isolation	✓ Geo restrictions
✓ Caching/CDN	✓ DNS protection	✓ Obfuscation/Privacy
✓ Middle mile cost opt	✓ WAF/WAAPaaS	✓ Wi-fi protection

Why customers use Cloudflare to adopt SASE

Deployment simplicity

Cloudflare delivers a uniform and composable platform for easy setup and operations. With software-only connectors and one-time integrations, our Cloudflare on-ramps and edge services all work together. This leads to a better experience for your IT practitioners and end users.

Network resiliency

Our end-to-end traffic automation ensures reliable and scalable network connectivity with consistent protection from any location. With Cloudflare, every edge service is built to run in every network location, available to every customer — unlike with other security providers

Innovation velocity

Our future-proof architecture helps us build and ship new security and networking capabilities very quickly. Whether it's our rapid adoption of new Internet and security standards or building out customer-led use cases, our history of technical prowess speaks for itself, and our foundation provides extreme optionality.

Start your journey to a faster, more reliable, more secure network

Try it now

Not ready to try it out? Keep learning more about Cloudflare One

1. 2021 Gartner Strategic Roadmap for SASE Convergence 2. Gartner Hype Cycle™ for Network Security, 2021