
Getting started with SASE: A guide to secure and streamline your network infrastructure

SASE, or secure access service edge, simplifies traditional network architecture by merging network and security services on one global network. This whitepaper explores the evolution of network security that led to SASE, outlines the breadth of services included in a SASE solution, and offers practical steps to move toward SASE adoption.

INTRODUCTION

Coined by Gartner in 2019, secure access service edge, or 'SASE,' was initially positioned as a pivotal advancement in the digital transformation process: highly customizable network and security services seamlessly stitched into the fabric of a global cloud platform. With a 20% adoption rate expected by 2023, Gartner claimed that the demand for SASE capabilities would "redefine enterprise network and network security architecture and reshape the competitive landscape."¹

Since then, the term has spread like wildfire through the IT and enterprise security space. As network security providers and SD-WAN vendors scramble to position themselves as SASE leaders, enterprises are left with a hastily-assembled jumble of network and security services that approaches, but often doesn't fully encompass, a SASE framework.

True SASE adoption requires more than bundling existing single-point solutions — it demands a complete reconsideration of enterprise network infrastructure. Maintaining a rigid on-premise network perimeter is no longer sufficient to protect a distributed, mobile workforce, while juggling multiple security services to protect a hybrid infrastructure can be costly, create headaches for IT teams to deploy and manage, and leave massive security gaps.

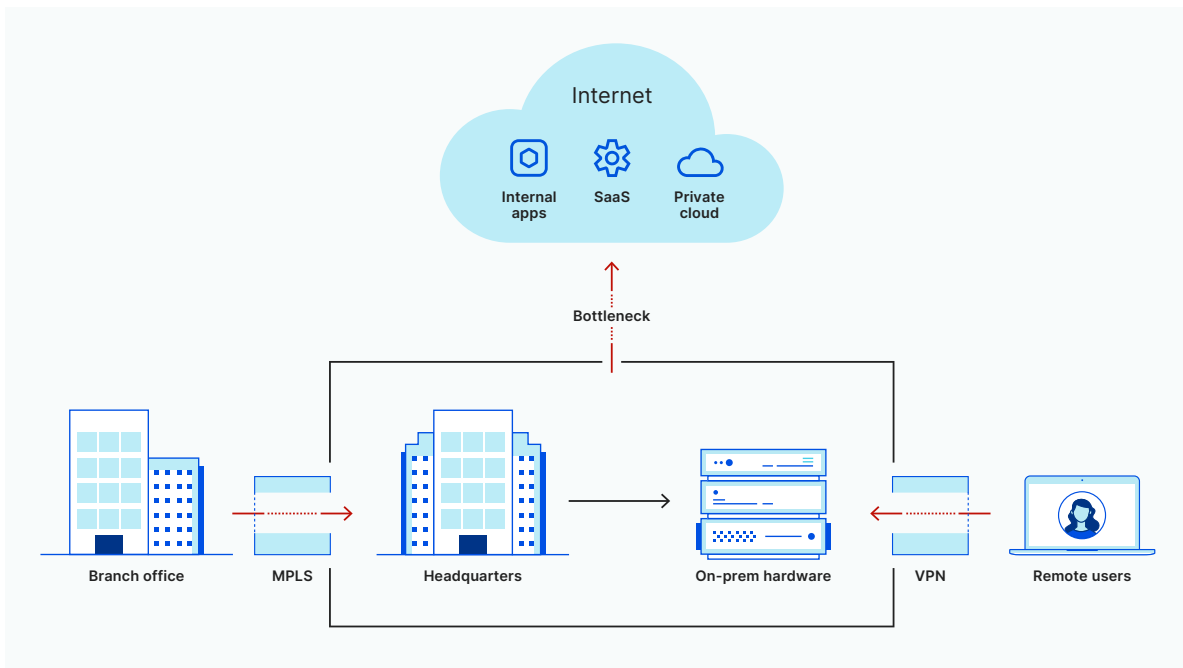
SASE addresses these challenges by shifting the network perimeter from centralized data centers to the user. By consolidating networking and network security services and delivering them from a single, cloud-based platform, SASE eliminates security gaps between services, gives IT teams greater visibility into network activity, and simplifies the cloud migration process.

1. THE ORIGINS OF SASE

To understand the pivotal shift that SASE represents, it's important to examine the gradual evolution of network infrastructure and security.

Before the widespread adoption of cloud computing, corporate resources, data, and applications lived within on-premise facilities that were safeguarded by hardware firewalls and DDoS appliances. Employees in a corporate office accessed internal resources through private connections filtered by network firewalls. Users connecting from remote locations usually did so through a VPN, which was prone to latency and overcrowding.

Underpinning this setup was a fear of the open Internet — a tool that was first and foremost built for resiliency, with little consideration for enterprise performance and security needs. Because the Internet had proven inherently vulnerable to attacks, organizations elected to establish their own private networks that secured (often ineffectively) data, applications, and corporate resources with physical firewall boxes and DDoS appliances, and tromboned all incoming traffic through centralized data centers for inspection and filtering.



Pre-SASE network infrastructure

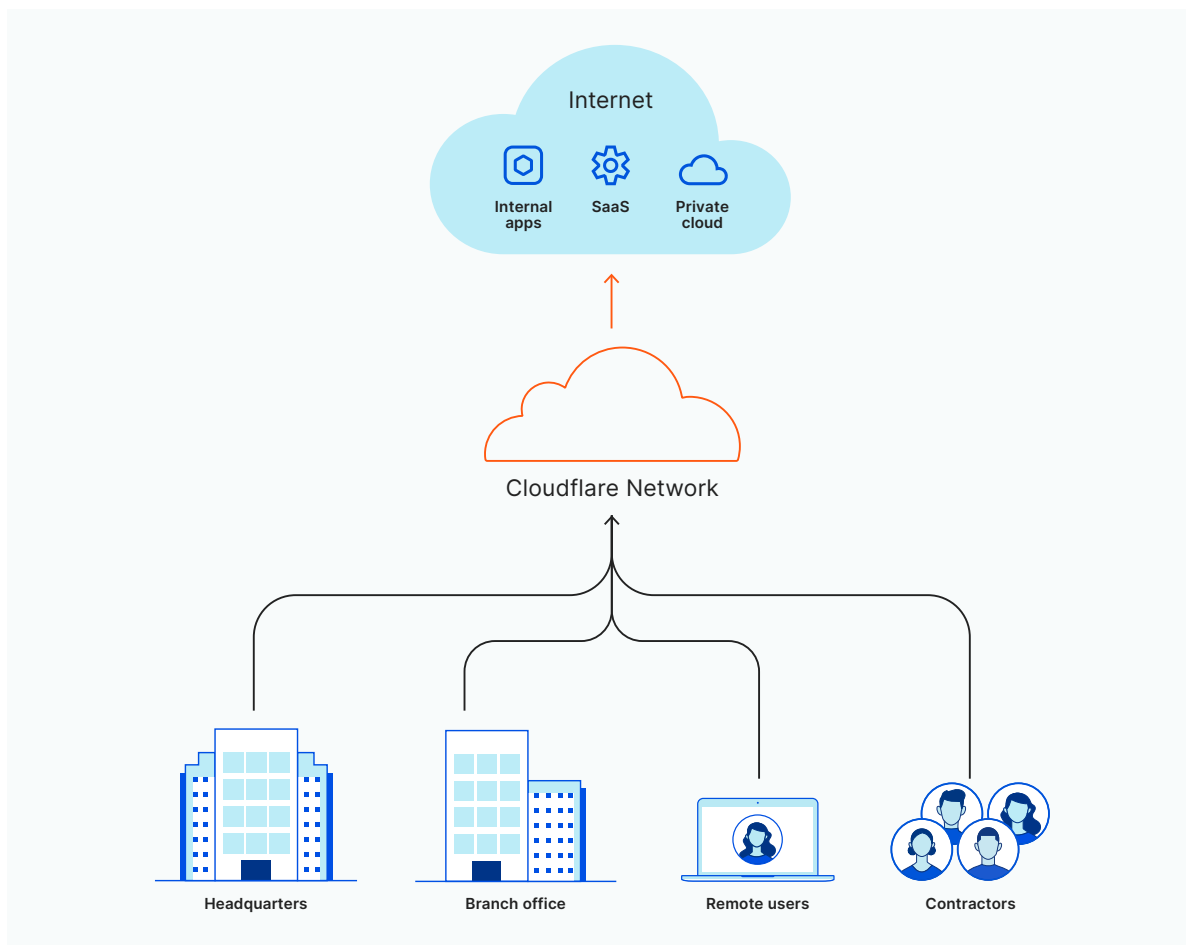
This model of network security was expensive and complex, and still left organizations vulnerable to data breaches and internal threats. Once an attacker breached the network perimeter, they could wreak significant damage within an organization by spreading malware, taking control of user accounts², and stealing valuable customer data.³

With the advent of cloud and SaaS services, organizations have more freedom and flexibility to reimagine their network infrastructure, as applications, data, and employees no longer need to reside exclusively within on-premise facilities.

1. THE ORIGINS OF SASE

However, with that freedom comes new security challenges. IT teams are tasked with protecting a mixture of on-premise and cloud-based services, as well as securing an increasingly mobile and remote workforce.⁴ Doing so successfully often requires maintaining expensive hardware and layering single-point security services from multiple vendors, which can be time-consuming to implement and difficult to manage.

The next evolution of network security likely will not resemble the hardware that protected traditional 'hub-and-spoke' infrastructure or the complex workarounds required by a hybrid cloud architecture. Instead, it will look like a SASE framework, one that consolidates network and security services and delivers them as an integrated service.



SASE network infrastructure

Rather than depending on ineffective hardware appliances or patching together siloed security services, SASE offers a streamlined approach to network security. It replaces complicated backhauling with the Internet edge, allowing enterprises to route, inspect, and secure traffic in a single pass. Coupled with zero trust access policies and network-level threat protection, SASE eliminates the need for legacy VPNs, hardware firewalls, and DDoS protection appliances, giving organizations more visibility into and control over their network security configurations.

2. DEFINING SASE'S SCOPE

SASE is a cloud-based security model that combines software-defined wide area networking with core network security services and delivers them on the cloud edge. Most SASE offerings are characterized by five primary capabilities:



Building and managing networks

A software-defined wide area network (SD-WAN) enables organizations to establish private corporate networks without the assistance of hardware routers or multiprotocol label switching (MPLS) circuits. This virtual, software-based architecture gives enterprises greater flexibility when creating and maintaining their network infrastructure, though it also comes with some built-in security vulnerabilities.



Connecting users to applications

Zero trust network access (ZTNA) requires real-time verification of every user to every protected application in order to protect internal resources and defend against potential data breaches. With a “zero trust” approach, no entity is automatically trusted until their identity is authenticated — even if they are already inside the perimeter of a private network.



Filtering traffic

A secure web gateway (SWG) prevents cyber threats and data breaches by filtering unwanted content from web traffic, blocking unauthorized user behavior, and enforcing company security policies. It typically includes URL filtering, anti-malware detection and blocking, and application control, among other capabilities.



Protecting applications and infrastructure

Cloud-based firewalls (FWaaS) protect cloud infrastructure and applications from cyber attacks through a set of security features that includes URL filtering, intrusion prevention, and uniform policy management.

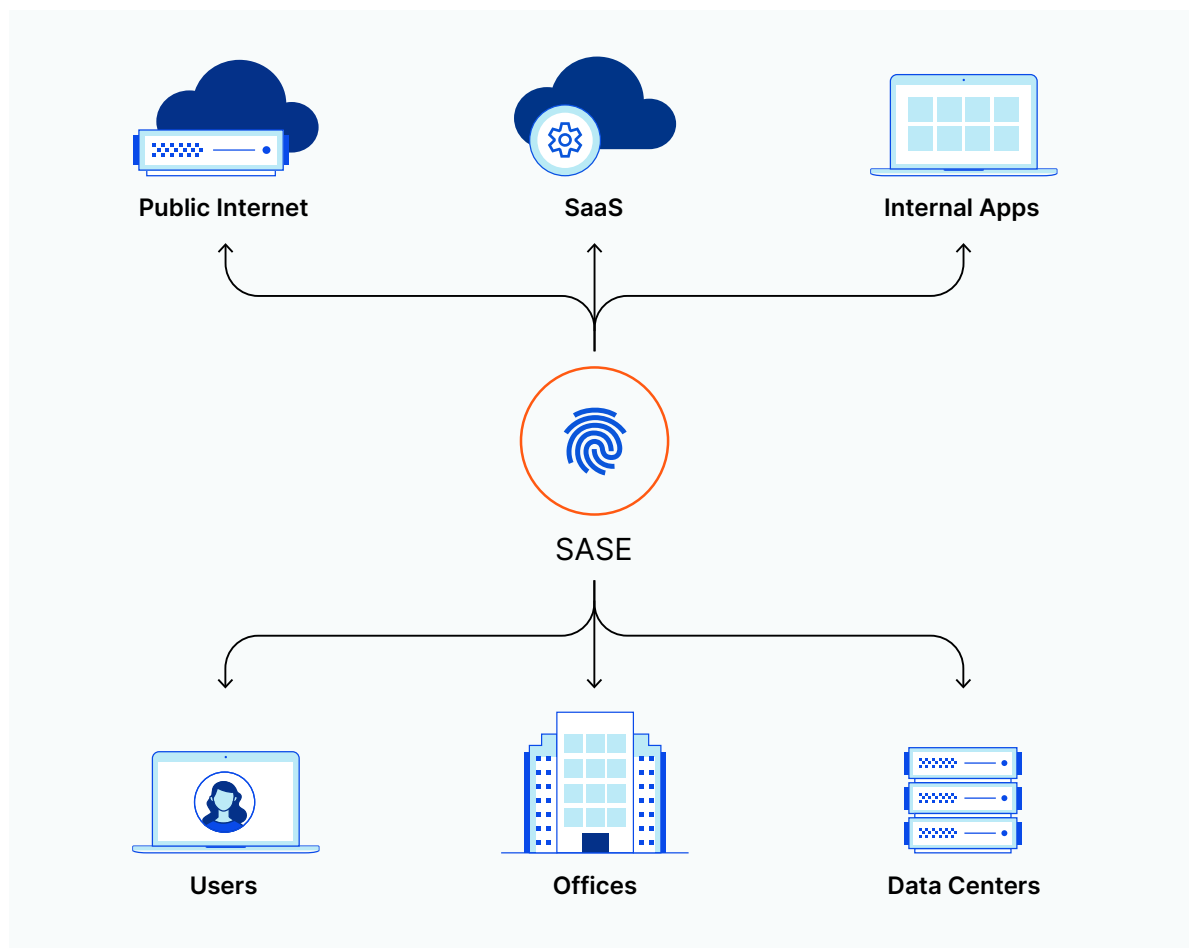


Securing data

A cloud access security broker, or CASB, performs several security functions for cloud-hosted services (e.g. SaaS, IaaS, and PaaS applications). Standard CASBs secure confidential data through access control and data loss prevention, reveal shadow IT, and ensure compliance with data privacy regulations.

2. DEFINING SASE'S SCOPE

Although a conventional SASE solution includes the five services outlined above, the list is more of a starting point than a strict set of requirements. SASE, at its core, converges two fundamental and separate capabilities — software-based network architecture and cloud-based security services — beyond that, vendors may add or subtract additional services as needed.



3. BENEFITS OF A SASE APPROACH

As it continues to evolve, SASE implementation may vary considerably from vendor to vendor and organization to organization. Most SASE solutions, however, share several key advantages over on-premise and hybrid network security configurations:



Streamlined implementation

By consolidating networking and security services, SASE eliminates the need to onboard cloud-based services, set up on-premise appliances, and invest time, money, and internal resources to keep both updated against the latest threats.



Reduced latency

SASE reduces latency and improves performance by routing network traffic across an expansive edge network in which traffic is processed as close to the user as possible. Routing optimizations can help determine the fastest network path based on network congestion and other factors.



Simplified policy management

SASE allows organizations to set, monitor, adjust, and enforce access policies across all locations, users, devices, and applications. Attacks and incoming threats can be identified and mitigated from a single portal, rather than individually monitored and managed with multiple single-purpose security tools.



Global network

A SASE framework is constructed on top of a single global network, enabling organizations to expand their network perimeter to any remote user, branch office, device, or application and gain more visibility and control across their entire network infrastructure.



Identity-based network access

SASE leans heavily on a zero trust security model, in which user identity and access is granted based on a combination of factors: user location, time of day, enterprise security standards, compliance policies, and an ongoing evaluation of risk/trust. This level of security — a significant step up from the overly permissive and inherently vulnerable VPN — protects against both external and internal data breaches and other attacks.

4. GETTING STARTED WITH SASE

For enterprises that have invested serious time, resources, and money in elaborate on-premise setups, manage complex webs of cloud-based security services, or are still adjusting to the future of remote work, SASE adoption can feel daunting — but it doesn't have to be.

Here are five practical steps you can take to get started with SASE:

1. Secure your remote workforce.

Implement a ZTNA solution that will allow you to eliminate your VPN, shield corporate data and resources from internal and external threats, and improve user experience. By bringing your secure web gateway and cloud-based firewall to the edge, you can inspect and filter traffic without backhauling it through a central data center.

2. Place branch offices behind a cloud perimeter.

Apply a zero trust architecture to branch offices that will remove the need for onsite security appliances (hardware firewalls, DDoS protection, etc.), which can be expensive to maintain and ineffective against a quickly-evolving threat landscape.

3. Move DDoS protection to the edge.

Get rid of hardware DDoS appliances and defend corporate networks from attacks with cloud-based, network-layer DDoS protection that can detect and mitigate threats in real time.

4. Migrate applications to the cloud.

As your organization scales, move applications from on-premise data centers to the cloud and make sure to apply consistent cloud security policies across all traffic.

5. Replace on-premise security appliances with unified, cloud-based policy enforcement.

Reduce the cost and complexity of maintaining network hardware appliances by shifting policy enforcement to the edge, where you can monitor and manage all traffic, attack patterns, and security policies from a single pane of glass.

5. HOW CLOUDFLARE DELIVERS SASE

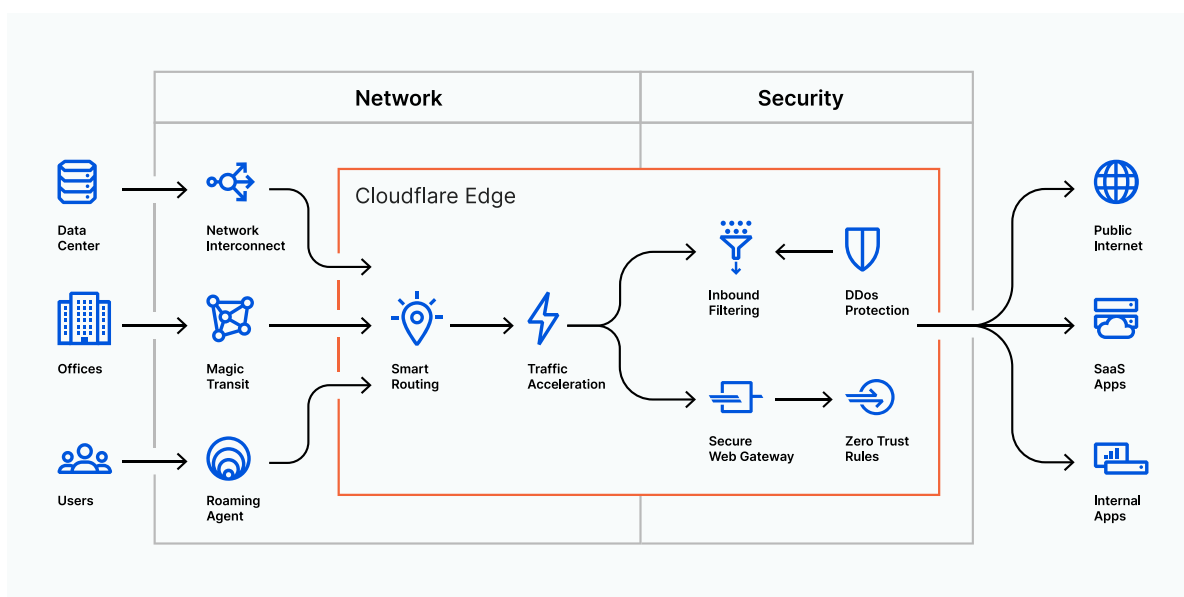
Whether you call it SASE or simply the new reality, enterprises need flexibility at every layer of the network and application stack. Users need secure, authenticated access wherever they are: at the office, on a mobile device, or working from home.

Cloudflare One™ is a comprehensive network-as-a-service (NaaS) solution that simplifies and secures corporate networking for teams of all sizes.

With Cloudflare One, you can:

- **Embrace zero trust access.** Replace broad security perimeters with one-to-one verification of every request to every resource. Enforce zero trust rules on every connection to your corporate applications, no matter where or who users are.
- **Secure Internet traffic.** When threats on the Internet move fast, the defenses you use to stop them need to move faster. Cloudflare One protects remote employees from threats on the Internet and enforces policies that prevent valuable data from leaving your organization.
- **Protect and connect offices and data centers.** Corporate networking has become overly complicated, which means user traffic often has to travel through multiple hops to get to where it needs to go. Protect offices and data centers through one consistent cloud platform with Cloudflare One.

Cloudflare is uniquely architected to deliver integrated network and security services across 200+ locations worldwide, eliminating the need for enterprises to run traffic through a centralized data center or manage multiple point solutions in the cloud.



How Cloudflare One protects network infrastructure

5. HOW CLOUDFLARE DELIVERS SASE

Cloudflare One	Core capability	SASE service
Cloudflare Gateway inspects user traffic and blocks malicious content from reaching user devices and spreading within an organization.	Filtering traffic	SWG, CASB, FWaaS
Cloudflare Access strengthens access requirements by applying identity and context filters to every inbound and outbound request.	Connecting users to applications	ZTNA, CASB
Cloudflare Magic WAN <i>provides a control plane to accelerate and route traffic across the Cloudflare network using WARP, Magic Transit, and Cloudflare Network Interconnect (CNI).*</i>	<i>Building and managing networks</i>	SD-WAN
Cloudflare Magic Firewall <i>replaces on-premise firewalls with network-level protection for remote users, branch offices, data centers, and cloud-based infrastructure.*</i>	<i>Protecting applications and infrastructure</i>	FWaaS
Cloudflare Browser Isolation <i>protects user devices from zero-day threats by separating the browser from potentially harmful code.*</i>	<i>Securing devices and data</i>	<i>Remote browser isolation</i>

* = coming soon

To learn more about Cloudflare One, visit www.cloudflare.com/cloudflare-one/.

REFERENCES

1. Gartner, "The Future of Network Security Is in the Cloud." Analyst(s): Neil MacDonald, Lawrence Orans, Joe Skorupa. August 30, 2019. [Gartner](#).
2. Twitter Inc. "An update on our security incident." [Twitter](#). Accessed 27 October 2020.
3. Marriott International News Center. "Marriott International Notifies Guests of Property System Incident." [Marriott](#). Accessed 27 October 2020.
4. Bursztynsky, Jessica. "Dropbox is the latest San Francisco tech company to make remote work permanent." [CNBC](#). CNBC. Accessed 27 October 2020.

© 2020 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.