WHITEPAPER

CLOUDFLARE

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.

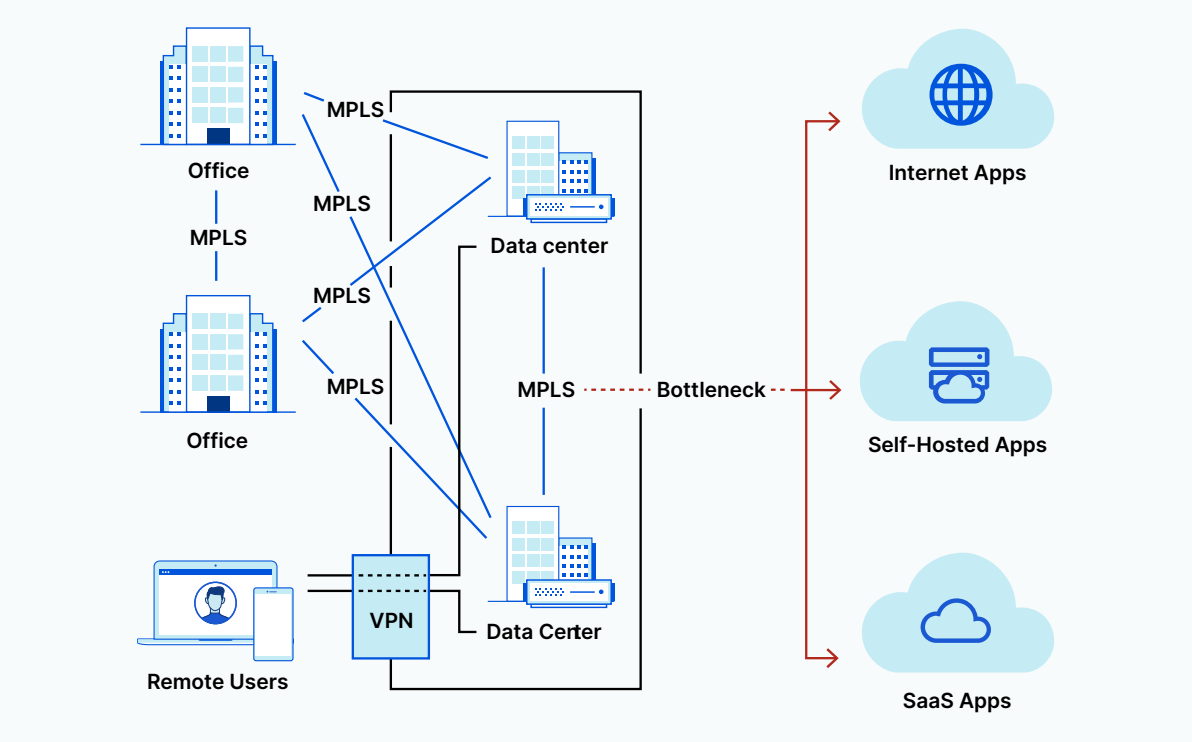
SASE addresses these challenges by shifting the network perimeter from centralized data centers to the user. By consolidating networking and network security services and delivering them from a single, cloud-native platform based on Zero Trust principles, SASE eliminates security gaps between services,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

THE ORIGINS OF SASE — OLD MODEL

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, high overhead to avoid overcrowding and patch vulnerabilities, and poor mobile experiences.

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.



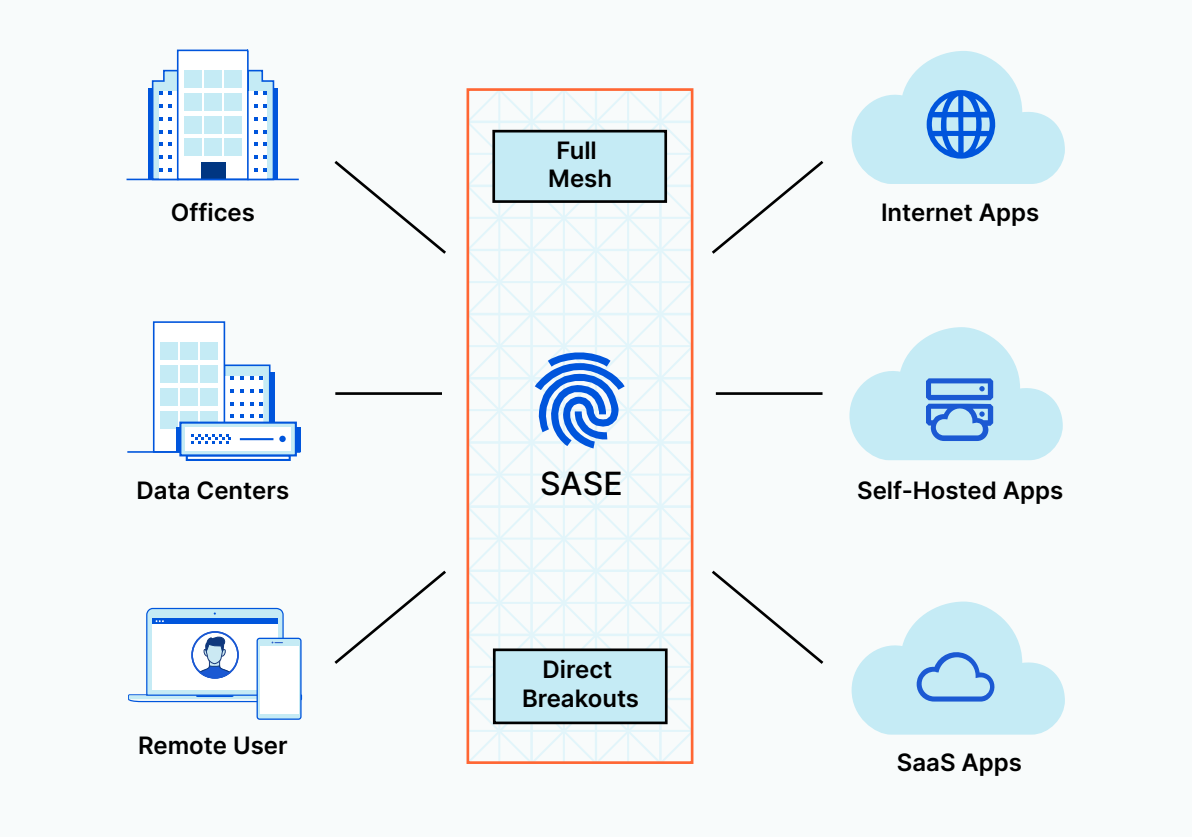
This model of network security was expensive and complex, and still left organizations vulnerable to data breaches and internal threats. Once an attacker breached the network perimeter, they could wreak significant damage within an organization by spreading ransomware, taking control of user accounts[2], 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.

THE ORIGINS OF SASE — NEW MODEL

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.



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, accelerate, verify, filter, isolate and inspect traffic in a single pass. Coupled with full mesh WAN connectivity, zero trust access policies, and network-level threat protection; SASE eliminates the need for legacy VPNs and MPLS circuits plus hardware firewall, proxy, and DDoS protection appliances, giving organizations more visibility into and control over their network security configurations.

DEFINING SASE'S SCOPE — CORE CAPABILITIES

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.

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.

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.

Connecting users to applications

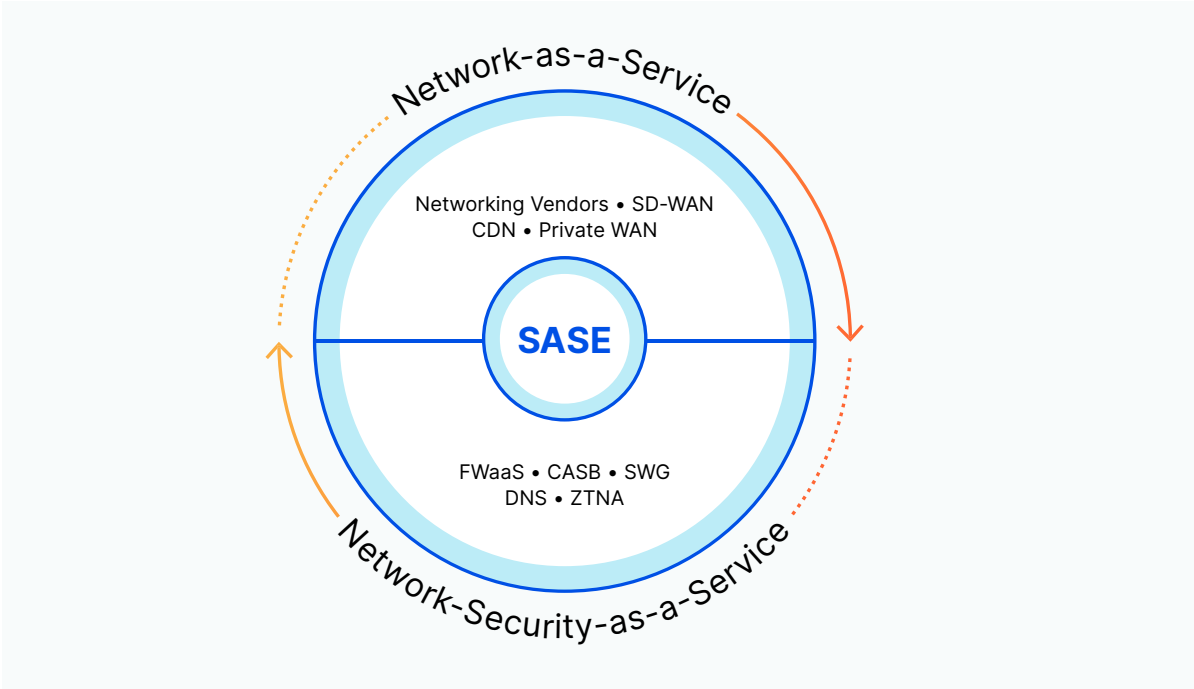
Zero trust network access (ZTNA) requires real-time verification of every user to every protected application in order to protect internal resources and defend against potential data breaches. With a "zero trust" approach, no entity is automatically trusted until their identity is authenticated — even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

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.

DEFINING SASE'S SCOPE — BEST-IN-CLASS CAPABILITIES

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.



While SD-WAN helps customers manage the last-mile of network connectivity, it cannot directly ensure the security, performance and reliability of the middle-mile between users and applications. At best, it can optimize end-to-end connections by relying on multiple global networks and chaining multiple security services, which is complex and costly. A SASE provider that has built WAN-as-a-service from scratch -- with or without SD-WAN -- enables customers to manage only one global network with security, performance, and reliability built-in by default. SWG, CASB and ZTNA together greatly reduce security risks, yet the combination still leaves many gaps to threat and data protection in all use cases. A SASE provider that has built remote browser isolation from scratch to natively integrate with SWG, CASB and ZTNA within every data center eliminates those gaps.

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.

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 reduce reliance on or even replace your VPN, shield corporate data and resources from internal and external threats, and improve user experience. By bringing your secure web gateway, firewall, and devices' browsers to the edge, you can filter, isolate, and inspect 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 on-prem security appliances (unified threat management, 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 DDoS appliances and defend corporate networks from attacks with cloud-native, network-layer DDoS protection that can detect and mitigate threats in real time.

4. Migrate applications to the cloud.

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

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

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

CLOUDFLARE'S SASE IS CLOUDFLARE ONE

Cloudflare One is a Zero Trust network-as-a-service platform that dynamically connects users to enterprise resources, with identity-based security controls delivered close to users, wherever they are.

With Cloudflare One's network services, infrastructure teams can:	With Cloudflare One's Zero Trust services, IT security teams can:
• Use the Cloudflare global network as your WAN. • Replace legacy appliances with a cloud-native network firewall. • Improve application performance and end user latency.	• Connect users to resources simply and securely with no VPN. • Block lateral movement, ransomware, malware, and phishing. • Improve end user experience and administration effort, especially onboarding time.

Why Cloudflare?

Simple deployment and management

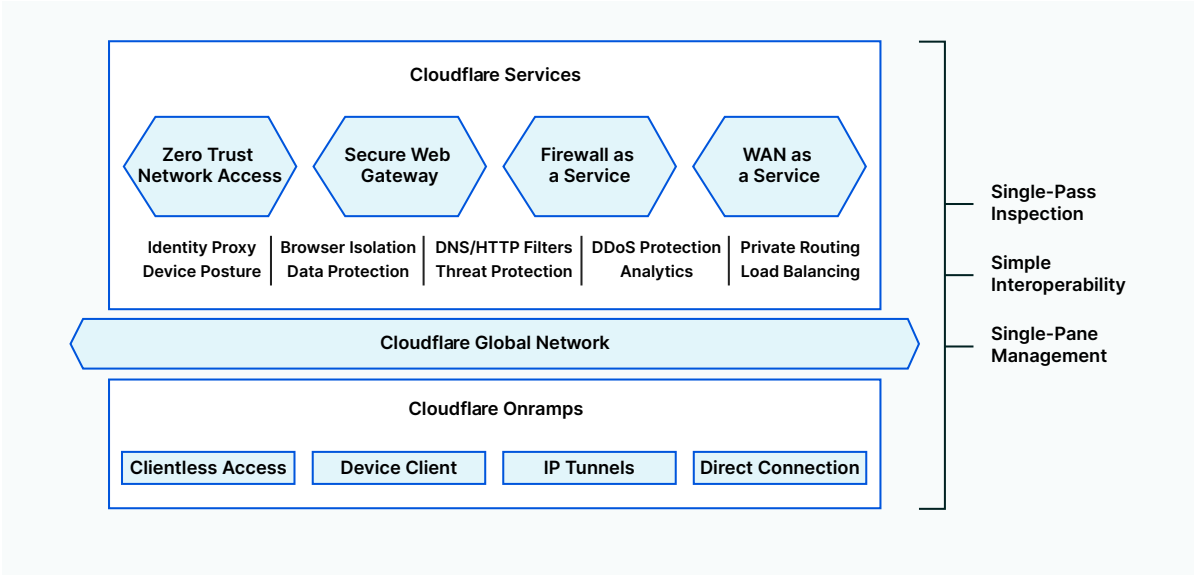
Every Cloudflare One service runs in every one of our 250+ cities around the world. No need to manually integrate multiple point products as you progress to a SASE model.

Consistent security and speed anywhere on Earth

Every Cloudflare data center provides single-pass traffic inspection and routing, giving users anywhere on Earth the same protection — without losing speed due to latency or the 'trombone effect.'

Connects to what you already use

Cloudflare runs the world's most powerful, most-peered network, and Cloudflare One supports the identity, endpoint, and cloud providers you already use. Easy to use, integrate once.



CLOUDFLARE'S SASE IS CLOUDFLARE ONE

Cloudflare One provides the security and connectivity capabilities you need to connect users, applications, and branch offices in a work-from-anywhere world.

<table>
<tr><th colspan="2">Cloudflare One</th></tr>
<tr><td>Zero Trust Network Access
Connect any user to any application and private network faster and more securely than a VPN by enforcing identity- and context-based rules and limiting lateral movement.

Core SASE Capabilities:
• Connecting users to applications
• Securing data</td><td>WAN as a Service
Enable any-to-any connectivity with faster performance, built-in security, and increased resiliency by replacing your legacy WAN architecture with our global private backbone.

Core SASE Capability:
• Building and managing networks</td></tr>
<tr><td>Secure Web Gateway
Block known and unknown Internet threats — and easily control data flows — by enforcing DNS, HTTP, network, and browser isolation rules with unlimited SSL inspection.

Core SASE Capabilities:
• Filtering and inspecting traffic
• Securing data</td><td>Firewall as a Service
Control access — and block DDoS attacks and other threats — by enforcing stateful inspection rules on all inbound and outbound traffic, while maintaining fast performance.

Core SASE Capability:
• Protecting applications and infrastructure</td></tr>
<tr><td colspan="2">Cloudflare Global Network
Sitting within 50ms of 95% of Internet-connected population, our network operates in 250+ cities with 100+ Tbps capacity, 10,000+ interconnects, and a 100% uptime SLA.</td></tr>
<tr><td>Clientless Access
Onboard any user or device in minutes — including third-parties and BYOD — with secure browser-based access to self-hosted and SaaS applications, beyond just HTTP.</td><td>IP Tunnels
Onboard entire public and private IP subnets via BGP Anycast route announcements with GRE tunnels, or our own Tunnel connector in cloud or on-prem environments.</td></tr>
<tr><td>Device Client
Onboard Windows, macOS, iOS, Android, ChromeOS, and Linux devices for secure client-based access to any application, private network, or Internet destination.</td><td>Direct Connection
Onboard your network infrastructure physically or virtually within 1600+ co-location facilities — rather than over the public Internet — for a more reliable and secure experience.</td></tr>
</table>

BUSINESS OUTCOMES USING CLOUDFLARE ONE

↓91%

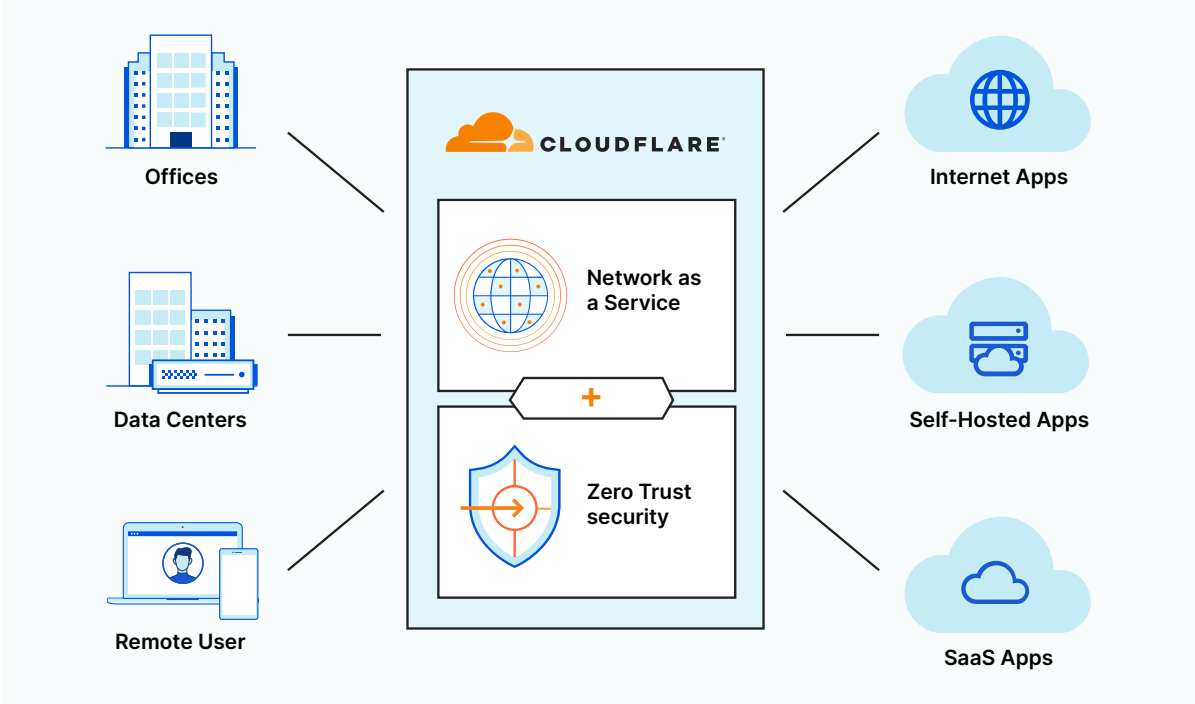
Reduce attack surface by up to 91% when you isolate high-risk browsing from end user systems and isolate application access from networks.

10→1

Lower TCO and accelerate your business by consolidating up to 10 point products into one platform.

↑60%

Onboard new employees and contractors up to 60% faster when you connect users to resources through Cloudflare instead of a VPN.



Learn more about Cloudflare One

Click here

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.