Security Service Edge (SSE)

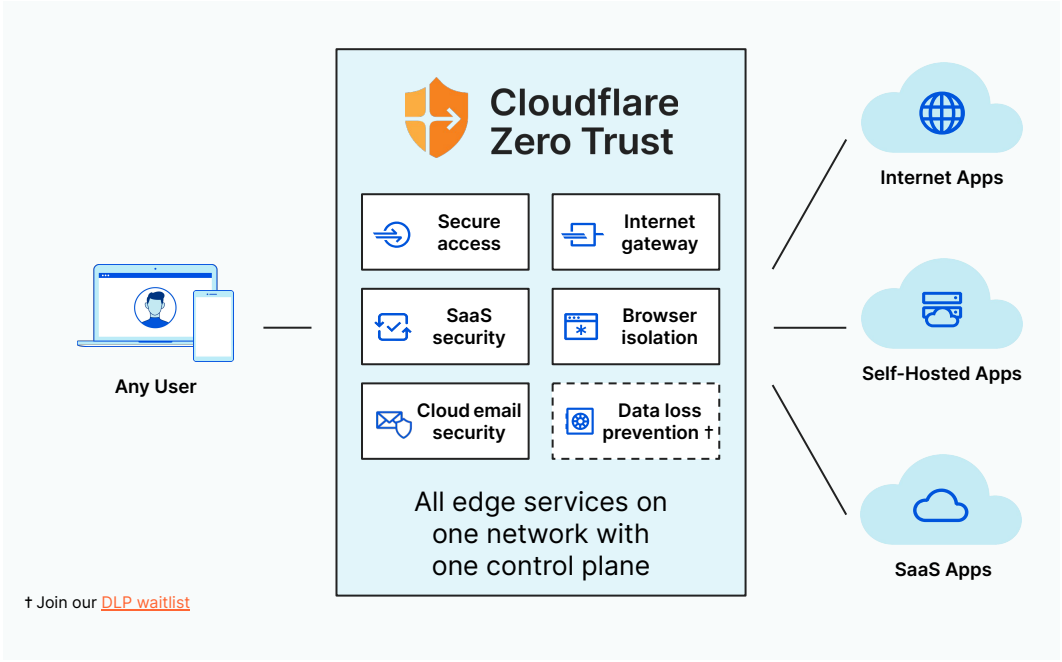
Planning for security service consolidation while adopting at your own pace

Cloud-centric convergence

The complexity of maintaining multiple point solutions is driving most organizations to consolidate their preferred vendors. Today, "best-of-breed" capabilities and broad platforms don't have to be mutually exclusive. As the majority of IT buyers lean toward consolidation, security vendors are meeting the moment by amplifying the value of their security platforms beyond what each service could accomplish individually.

The SSE approach — which straddles point products and full consolidation — focuses more deeply on security capabilities than most Secure Access Service Edge (SASE) offerings, as it is not tied to network infrastructure. In our opinion, our Zero Trust platform matches Gartner's SSE and converges formerly-distinct point products: ZTNA, VPN, SWG, DNS Filtering, CASB, RBI, and Firewall as a Service (FWaaS).

> *"Consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs (replacing with a ZTNA approach). Leverage a converged market that emerges by combining these services."* [1]
>
> Gartner



† Join our DLP waitlist

VPN replacement
simplify and secure connecting any user to any resource

SaaS security
visibility and control of applications including email

Internet protection
keep your data safe from threats over any port and protocol

Security modernization
improved productivity, simpler operations, reduced attack surface

SSE as a bridge to SASE

While converging security and network edge services is the ultimate goal of SASE, some companies may never look to fully consolidate to a single vendor, based on their history and current infrastructure. Regardless of your long-term SASE strategy, Cloudflare can help you modernize security, transform your corporate network, or both.

Single-vendor SASE
For businesses aiming to fully unify security and network edge services from a single vendor, Cloudflare One, our SASE platform, provides Zero Trust network-as-a-service built on our 270+ city global network.

Multi-vendor SASE
For those with mature SD-WAN deployments or disjointed security and network teams, Cloudflare Zero Trust can help modernize security and achieve an SSE implementation, leveraging SD-WAN partnerships for multi-vendor SASE.

Composable SSE adoption

The move to cloud-based SSE is not intended to be an overnight switch; Cloudflare Zero Trust helps organizations phase out hardware at their desired pace. Many businesses will start their Zero Trust journey by augmenting their VPN with ZTNA, on a path to full replacement. Streamlining SaaS security is a close second priority for most, with broader threat and data protection strategies following soon thereafter.

Our uniform, composable architecture facilitates modular adoption of security services. Businesses can deploy custom combinations of services to fit their prioritized use cases—no "all or nothing" mindset necessary.

> *"Inventory equipment and contracts to implement a multiyear phase out of on-premises perimeter and branch security hardware in favor of cloud-based delivery of SSE. Target consolidation of on-premises equipment ideally to a single appliance."* [1]
>
> Gartner

Integration fuels innovation

All Cloudflare services run on every server in every data center across our massive global network, so there are no gaps in coverage or inconsistencies. This helps us deliver single-pass inspection and ensure the highest level of security, performance, and reliability.

Natively integrated services also surface more creative opportunities to combine functionality across multiple services and deliver on our customers' desired use cases. As these product lines blur, cross-service interaction helps us solve more advanced scenarios and truly modernize security.

Strengthen third-party access security

- ZTNA and RBI integrate to provide safe access for third parties like contractors and partners
- Verify contextual information for authorization, and serve apps in isolated browsers to protect data
- Clientless operation for both services simplifies rollout with no downloads required

Visualize and audit SSH sessions

- ZTNA and SWG integrate to provide visibility across entire SSH sessions to monitor privileged access
- Simplify SSH access with clientless, browser-based SSH sessions through ZTNA
- Provide SSH session visibility at a network layer; log every command using SWG as a proxy

Simplify SaaS remediation workflows

- SWG and CASB integrate to enable a "find and fix" workflow; block some or all suspicious SaaS activity straight from CASB security findings
- Expand SaaS visibility to help detect and remediate issues that could lead to data leaks or compliance violations

Better protect against phishing

- Email security and RBI integrate to combat sophisticated phishing attacks and business email compromise (BEC)
- No predictive threat intelligence is perfect; opening email links in an isolated browser provides an extra layer of protection

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

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

[1] Gartner Hype Cycle™ for Network Security, 2021