

Security Service Edge (SSE) for Enterprises

Scalable security for the distributed workforce



Enterprises are rethinking security posture as cloud adoption grows

Modern businesses are moving to the cloud and increasing their cloud spending for various benefits like efficiency, speed, and more. As they pursue this strategy, a defensive plan built solely on perimeter-based security becomes insufficient.

Organizations have historically relied on VPN-based solutions to support a growing mobile workforce that accelerated during and since the pandemic, thanks to the dynamic, work-from-anywhere trend. But VPN solutions have deficiencies in terms of security and user experience. Organizations are moving towards the SASE framework to counter the inadequacies of historical access methods, which complements the new ways of hybrid working.

Security Service Edge

SSE is the security focus of SASE that allows different security capabilities to be bundled and delivered together for organizations.

How SSE solutions can benefit your business

Reducing risks

Security is no longer attached to a location or network – it can be uniformly cloud-delivered – which means even if the user is outside the premises, security is consistent. Unified security services remove the gaps that products from different vendors present and reduce risk. With SSE, organizations have better user visibility regardless of locations and channels.

Better user experience

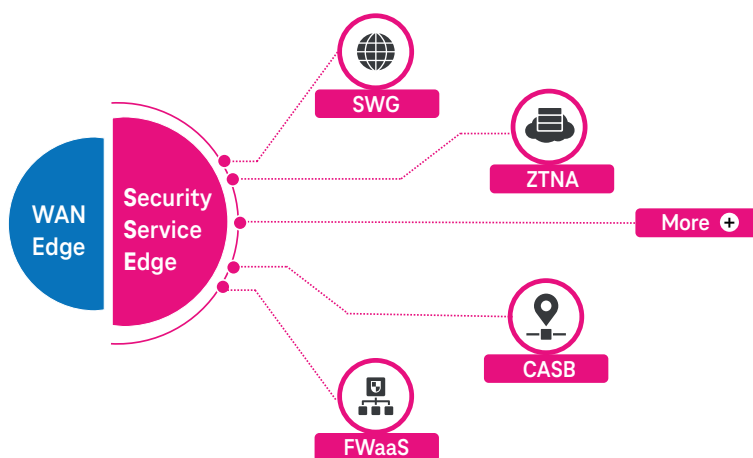
With SSE's global distribution, content is inspected when the end-user connects to the SSE cloud. As this process executes closer to the user, it reduces the latency, thus improving user experience and performance.

Reduced costs and complexities

SSE unifies multiple security services, like SWG, ZTNA, CASB, FWaaS, Cloud DLP (Data Loss Protection), and Remote Browser Isolation (RBI). With these services available under one roof, there is a reduction in cost and complexity, and security policies are applied consistently.

Components of SSE:

1. Zero Trust Network Access (ZTNA)
2. Secure Web Gateway (SWG)
3. Cloud Access Security Broker (CASB)
4. Firewall-as-a-Service (FWaaS)
5. And More



SSE has emerged as a standalone market segment in Gartner's research

Because the SSE framework is modular, the organization can prioritise relevant services and defer elements based on business priority, adding them later as they scale up. It also enforces all security updates across the cloud – thus significantly reducing the need for manual intervention.

Zero trust-based access

SSE creates secure remote access with zero trust policies for devices, applications, content, and, most importantly, users. Granting access is strictly policy-based and user-based. As apps are behind the SSE platform, they aren't exposed to the internet, minimizing the attack surface and business risks.

How SSE can help you

Secure remote workforce

With traditional VPNs presenting challenges, organisations struggle to secure remote access to private apps and cloud services. SSE enables access to apps, data, and content without exposing users to risks and vulnerabilities common with traditional access methods. Adopting a Zero Trust approach ensures that the exposure is reduced to a minimum.

Identify and eliminate threats

SSE's primary objective is to protect users and organisations from

threats (like phishing and malware) across the web, cloud, and the internet. For example, an SSE platform that includes CASB allows data inspection in SaaS-based applications and quarantines malware before it can cause damage.




Secure cloud services access

One of the most crucial aspects of SSE is policy control of user access to cloud services, the web, and the internet. As users access apps and content on and off the network, SSE enforces policies to eliminate risks. Organisations also need to implement corporate internet and access policies for compliance reasons. The SSE platform with Cloud Security Posture Management (CSPM) capability helps them avoid breaches due to misconfiguration.


Secure sensitive data

Organisations have data residing in different platforms and channels. SSE helps identify and safeguard sensitive data; the platform offers improved visibility across channels with crucial data protection technologies. Sensitive user data can be classified and secured with the help of the cloud Data Loss Protection (DLP) policy. DLP policies can be enforced for data at rest in the cloud and transit, making data protection more manageable.

How T-Systems can help you with SSE

| | | |
|--|-------------------------|---|
|  | SSE Advisory | Our expert consultants can help you determine what kind of SSE solution you need based on your current security level. |
|  | Implementation | With our network of selected partners, we can implement the right SSE solution that exactly fits your need(s). |
|  | Managed Services | We offer Managed Services to keep operations up and running with administrative support, policy configuration, device management and monitoring, etc. |

Get started with SSE today. Drop a note on the below email.

| | |
|---|---|
| Expert Contact | Contact |
|  | T-Systems International GmbH Hahnstraße 43d 60528 Frankfurt am Main, Germany E-Mail: cyber.security@t-systems.com com Internet: www.t-systems.com |
| Silvija Andjelovic Cyber Security Expert silvija.andjelovic@t-systems.com | |