TOP 7 PITFALLS TO AVOID WHEN

Selecting the right SSE solution

Security service edge (SSE) delivers all the security services you need from a purpose-built cloud platform. If done correctly, SSE can cut costs and complexity while improving threat and data protection. Knowing what to look for in an SSE platform is the first step in your transformation journey.

Ready to switch to SSE for threat and Data Protection? Avoid these 7 pitfalls:

1 No proven track record

Performance and scalability is key, so avoid SSE clouds that can't deliver your needs

2 Not built on zero trust

Reducing your attack surface and the impact of ransomware requires a zero trust architecture

3 Can't scale SSL inspection

Many SSE clouds struggle to inspect all traffic, but without it, you can't deliver airtight protection

4 Doesn't support flexible deployments

Avoid approaches that can't support all the different deployment scenarios you may need

5 Unable to provide a great user experience

Everything will flow through your SSE, so ensure it helps you see and optimize your users' experiences

6 Limited in third-party integrations

Your SSE will be at the heart of everything, so focus on strong integrations with peering, identity, SD-WAN, SoC, and orchestration

7 SSE cloud fails to show value

Testing and piloting SSE should be easy, but also give you the confidence that it can deliver in production at scale

If you're ready to learn more about security service edge and how it can help you reduce risk, costs, and complexity, check out our new ebook:

Top Pitfalls to Avoid When Selecting an SSE Solution

Experience your world, secured.™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com