INFOGRAPHIC

7 questions to help you choose the right SASE partner

A service provider with the right expertise can help you stay ahead of cyberthreats and improve your organization's experience across its end users, devices and applications. With the emergence of secure access service edge (SASE) solutions on the market, it's essential to have the know-how to select a framework that fits your organization's needs. The service provider you choose should offer a complete framework that includes onboarding, application integration and ongoing management.

Consider these questions to help find the best partner for your SASE deployment:

1

How can I ensure seamless migration and integration with our operations?

A trusted solution provider can design, deploy and support a software-defined wide area network (SD-WAN) in a way that allows a controlled migration away from physical infrastructure to a cloud-based network. Cloud-based security, multi-factor authentication (MFA) and other SASE components can also be implemented at your pace. Thorough project planning ensures successful integration with your key network applications and avoids impacts to productivity or user experience.

How can I make SASE easy to provision and manage for my users, devices and locations?

2

SASE is new to many organizations. A managed service provider can fill knowledge gaps during deployment. IT departments should insist on solutions that reduce time spent managing security activities, licenses and infrastructure. A scalable SASE framework with a single, intuitive portal can provide simplified control and visibility across your organization to secure hybrid or remote users. Look for support to integrate your network, users and applications.

3

What can I achieve with zero trust network access (ZTNA) when I already have VPNs for my remote users?

While VPNs confirm user identity and encrypted sessions, ZTNA solutions go further by continuously checking user credentials and permissions. In addition to user identity, they apply access policies based on device details, user location and other factors to help ensure data is not compromised. ZTNA can be further enhanced with MFA to help protect against an even broader array of identity-based threats.

How does SASE extend network security across multiple locations?

4

SASE enables IT administrators to apply a granular security policy to users, regardless of where they work. SASE allows a security policy that traditionally applies to a physical location to be applied to users and data outside the office, extending the security perimeter to wherever users and data exist. Real-time visibility into user activity can help organizations immediately respond to security threats. Remote users also have the same network experience as their colleagues in the office.

5

What kind of SASE support should I look for from a managed service provider?

Leading providers offer co-management options to allow clients to have as much or as little control over their services as they are comfortable with. The right partner can integrate or adjust solutions to accomodate new applications, users, security policies and clouds with rapid service restoration if problems arise. Consider an end-to-end solution provider that can offer a single point of contact across both connectivity and SASE solutions with 24/7/365 U.S.-based support and local technicians nationwide.

What other steps can I take to enhance my network and connectivity when implementing SASE?

6

A trusted national service provider with its own fiber infrastructure can apply your SASE security framework to a stable, reliable network. Using a single partner across networking, connectivity and security can give you a powerful resource for your long-term IT planning and growth — as well as a single resource for support — as you evolve your organization's security. A service provider with a 360-degree view of your infrastructure will better understand your applications, office requirements, data center and relationships to resources in the cloud to deliver the best user experience.

7

How can I improve the experience for both users and IT staff?

SASE solutions are built on cloud-native architecture — they are agile, scalable and accessible wherever business takes place. Users' essential applications are typically faster and perform better with security measures, like a secure web gateway (SWG), that do not require internet traffic to be routed through a central data center. IT teams benefit from solutions, like a cloud access security broker (CASB), that provide visibility and policy enforcement across cloud services. Consolidating multiple security solutions also offers simpler operations, plus improved network visibility, better traffic prioritization and the assistance of a skilled managed service provider.

Simplify your network and protect your resources with SASE solutions from a partner you can trust. Spectrum Enterprise offers extensive security, connectivity and SD-WAN technology backed by end-to-end support. As a managed services provider, we can help you extend your organization's network wherever employees do business while prioritizing essential applications and enhancing reliability for a better user experience.

Learn more about how Spectrum Enterprise can help secure your business.

SE-MS-IG009

Spectrum ENTERPRISE™