What SASE Means for Service Providers

May 12, 2021

by **Irene Zhang**

The COVID-19 pandemic and the rise of remote work have accelerated digital transformation and the shift to the cloud. It's an industry turning point. Gartner predicts that by 2022, more than 50% of enterprise data will be created and processed outside the data center or cloud[1], up from less than 10% in 2019[2].

If the future of digital business resides in the cloud, so does security. Organizations must ensure the privacy and integrity of their applications and data from the cloud and within their own data centers all the way to the edge — including branch offices, classrooms, factory floors or wherever people and "things" connect.

That's the principle behind SASE, or the Secure Access Service Edge. Gartner coined the SASE term back in 2019[3], and while "sassy" might feel silly to say, the concept is gathering momentum. It's also creating new opportunities for managed service providers.

What Does SASE Mean for Service Providers?

In essence, a SASE architecture is the embodiment of networking converged with security. By delivering networking and security together as a cohesive service, enterprises and network operators alike can provide customers with strong protection from cyberattacks, wherever they are located.

For the last several years, Juniper has talked about building threat-aware networks with the Juniper Connected Security strategy. In short, Juniper Connected Security *is* SASE.

A network that is threat-aware can detect threats and stop them from getting a foothold in the network. Policy-based software-defined secure access is extended everywhere across the network fabric. All points of connection are used to see, automate and protect against malicious activity—right down to the user and endpoint. Security is enforced everywhere endpoint identities are located.

What are the benefits of SASE for Service Providers?

SASE is a great opportunity for service providers to launch or expand their managed secure SD-WAN services portfolio to support their customers' digital transformation.

While some enterprises will build their own secure SD-WAN, many more organizations will look to the expertise and resources of a managed service provider. Customers already count on their service provider partners to keep their networks running at peak performance, and by incorporating SASE-based solutions, service providers can extend security services to the edge – wherever the edge may be.

SASE also delivers:

- **Improved customer experiences:** Customers can reduce risk and remove security as a roadblock to innovation. By integrating security directly into SD-WAN or MPLS services, network operators can extend Zero Trust security directly to the customer edge. Policies can be applied dynamically based on identity and context, with enforcement points distributed throughout the network, beyond the firewall. Customers have predictable network services that fit their use cases, whether for video meetings from home, branch office connectivity or robots on a factory floor.
- **Greater business agility:** Integrating security into the network everywhere delivers business agility—for service providers and their customers. Bad actors will continue to use any means necessary to make an attack successful, but with a threat-aware network that extends security to wherever the customer is located, it's easier to safeguard their business—and for service providers to do the same for their own infrastructure.
- **Reduced operational complexity**: Service providers have long dealt with network traffic through multiple layers of security defenses, which can create performance chokepoints and result in a proliferation of specialized security appliances. With SASE, security is integrated everywhere, whether physical, virtual or cloud-based. The focus is on the edge—the direct connection from the client to the cloud—and it doesn't stop there. SASE goes beyond the edge to connect application services to users and secure the entire data transaction. With SASE, the network architecture is simplified, leading to operational efficiency.

SASE is a Journey

With Juniper, customers control the speed of their journey to SASE. Customers can count on Juniper's Connected Security strategy and solutions like Juniper Networks® Security Director Cloud as they evolve their threat-aware network and deliver secure access to services to their customers.

Juniper Networks® Security Director Cloud is the portal to SASE, bridging the present with the future. With Security Director Cloud, customers can manage security anywhere and everywhere, from the customer edge, in the cloud and to the cloud.

We are ready to meet you wherever you are on your SASE journey.

Join us at RSA Conference 2021 from May 17th – 20th to find out how to take your first step toward SASE with Juniper.

[1] https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/

[2] https://www.gartner.com/smarterwithgartner/gartner-top-10-trends-impacting-infrastructure-operations-for-2020/

[3] https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/