



MARKET BRIEF

LET'S GET SASE: CONSIDERATIONS FOR THE NEXT EVOLUTION IN SD-WAN SERVICES

SASE focuses on the identity of entities on the network, their real-time context, and active security and compliance policies and granting more flexibility in sourcing underlying network connectivity. Providing continuous risk vs. trust assessments, SASE tracks people, groups, specific devices, applications, IoT and edge locations, and other services to protect the corporate network from malicious attacks.



NETWORKING HAS COME FULL CIRCLE

In the earliest days when a company expanded into multiple locations, they put a router in front of their local area network (LAN) and connected it to their other locations with leased lines.

Then, as network evolution continued, most organizations began to trust the public Internet with their network traffic, so they put a firewall in front of each router at each location and used that to transport their data removing the leased line costs. More recently, large corporations uncomfortable with the public Internet have used Multiprotocol Label Switching (MPLS) connections for more secure data transfer.

The next great evolution came when it was decided to put the management software and intelligence into firmware installed directly inside the router. Prior to this time routers had little built-in intelligence and were managed externally using software running on a typical x86 computer. Engineers felt they could achieve far greater operating efficiency by moving that management software directly into firmware installed in the router itself.

Then came the most recent evolution, in this case a 180-degree reversal, as manufacturers removed the software and intelligence from their router appliances and returned them to their original home on computers. This software-driven management dramatically improved flexibility, agility, and scalability over firmware-driven appliances as it was much easier to make changes in software. Perhaps an even greater advantage was addition of the ability to manage multiple routers, geographically dispersed globally, from one central management console instead of having to physically visit each router separately to update it.

This is how software-defined networking (SD-WAN) came to be. Now, network managers could combine MPLS with other circuits of varying kinds and costs, to shape and re-shape the traffic as their applications required. Or, they could simply remove MPLS from their underlying network altogether and achieve the same functionality at significantly lower cost. This decision is driven by aligning network and business management teams to determine whether specific applications require the isolation and resulting increased security provided by a stand-alone MPLS circuit.

DISRUPTION GROWS

SD-WAN arrived just as the wave of transition to cloud computing was reaching its crest. Data workloads were being migrated from on-premises networks to cloud-service-providers (CSP).

Monolithic applications were being transformed into cloud-native versions using microservices in containers. Users were about to start working-from-home (WFH), and data and networking security were under assault.

These transformations had removed significant cost and management overhead from enterprises, and liberated users to work from anywhere (WFA) on any device they preferred. But each of these advantages had brought with them new security and privacy challenges.

What was needed were security solutions as agile, flexible, and scalable as the networks, applications, and workloads had become.

GETTING SASE

Secure Access Service Edge (SASE) was created by combining SD-WAN with Secure web gateways (SWG), Cloud access security brokers (CASB), Zero-trust network access (ZTNA), and Firewall as a service (FWaaS) to provide the needed robustness of security with no compromise in technology, features, or agility. Security delivered as a service, SASE focuses on the identity of entities on the network, their real-time context, and active security and compliance policies. Providing continuous risk vs. trust assessments, SASE tracks people, groups, specific devices, applications, IoT and edge locations, and other services to protect the corporate network from malicious attacks.

Since it delivers all security services from a single platform, you no longer need local firewall hardware at any of your locations. This saves not only the initial price for the equipment and software, it saves even more by removing the need to manage and administer it. Since it integrates threat prevention, sandbox, DNS protection, web filtering, identity theft, credential theft, data loss prevention (DLP), full content inspection, and next generation firewalls (NGFW), there is no longer a need to purchase point products for any of these functions.

This managed service significantly reduces complexity or management overhead and enables access to any resource from anywhere at any time.

ENABLING THE HYBRID WORKSPACE

As we begin to emerge from the COVID-19 pandemic, enterprises will start making decisions regarding who continues working from home, who returns to the office, and who splits their time between the two. Network and security managers who have struggled with how to manage security on devices connected through residential Internet access services will now be able to take over that security remotely as a service with SASE. Road warriors now equipped with smaller, lighter, thinner laptops, Bluetooth keyboards, mice, and headsets, and readily available mi-fi access will also fall within an organization's security strategy, as will all mobile devices and wearables that continue to proliferate within the enterprise.

Even those returning to the office benefit. It's very possible those who are chosen to return, or especially those who will be alternate between home and office, will very likely not find themselves returning to their own desk, cubicle, or office. Instead, they will likely be welcome to choose the next available "hoteling" space which is completely ready to connect them to the network. Wherever they end up, SASE enables the IT department to enforce all security and compliance policies to ensure safety for all data and all users.



Gartner predicts that by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at the end of 2018.

Gartner

Gartner Hype Cycle for Cloud Security, 2020

BETTER SUPPORT THROUGH TECHNOLOGY

Perhaps the most important advantage gained by using SASE is the ability to give all users what they want most, responsive support. Since SASE can be controlled from literally anywhere, a support specialist need not be in the data center to respond to calls for help. They can simply whip out their laptop, tablet, or smartphone and make the changes the user needs to solve their problem.

When you think about it, SASE is the next logical step after you've moved all workloads, applications, resources, and users to the cloud in that it moves security and compliance to the cloud as well. It is a technology that truly enables the business to operate better, faster, and more efficiently.



Why Advantage?

We optimize the technology lifecycle

Advantage is a managed service provider that drives value to your organization through five key stages in the technology journey. Employing expert practitioners, efficient processes, and a unique software platform, we solve the challenges of managing technology in the modern enterprise.



DESIGN

Based on your business drivers and global best practices, we create purpose-built solutions leveraging leading technologies and ideal providers.



SOURCE

Leverage our experience, benchmarking, and global partner network to select service providers, negotiate the best possible terms, and contract for the lowest rates.



INSTALL

Capitalize on our project management leadership for a seamless rollout of new solutions and the timely disconnect of legacy services.



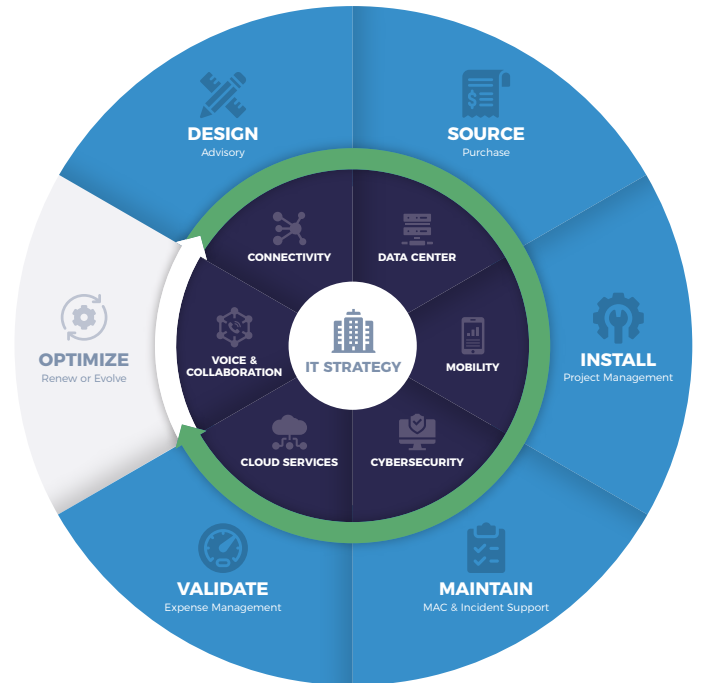
MAINTAIN

Ongoing managed support of daily activities such as moves, adds and changes to your services, while having full visibility into your inventory through our Command Center platform.



VALIDATE

Receive ongoing managed services to support the invoice lifecycle, including contract management, expense validation, dispute resolution, and AP/GL feeds for payment.



From procurement and provisioning through inventory and expense management, we optimize your communications solutions across voice, data, cloud, and mobility. Advantage is your team behind the scenes—so you can focus on success.

Learn more at [AdvantageCG.com](https://www.advantagecg.com)
info@AdvantageCG.com | +1 212.872.1700

