Prepared for

paloalto NETWORKS

Five Things to Consider Before Embarking on a SASE Project

March 2021 EMA White Paper
By Paula Musich

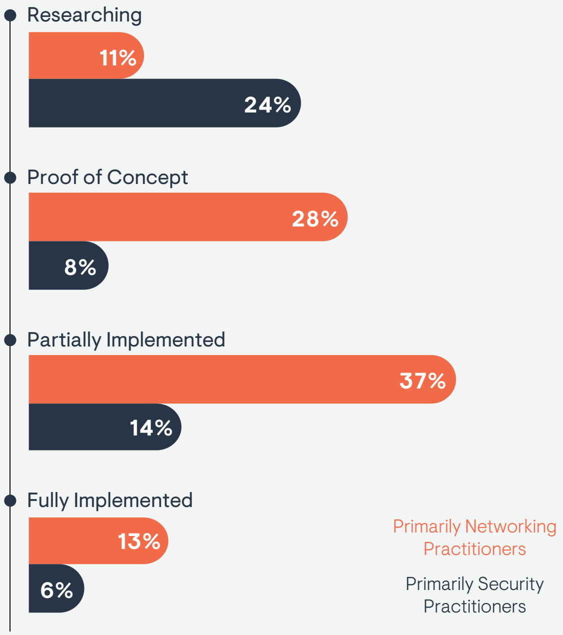
EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Introduction

The convergence of networking and security in the cloud, described as secure access service edge (SASE), is a nascent market that already has the attention of IT operations teams looking to adapt their networking and security architectures to better serve the needs of digitally transformed enterprises. Such digital transformation initiatives were put into hyperdrive in 2020 thanks to the global pandemic and sudden need to enable information workers to do their jobs from home, using their own Wi-Fi and broadband networks. The new Enterprise Management Associates research report, "Availability and Buying Options in the Emerging SASE Market" made it clear that networking professionals are leading the SASE adoption curve, with 37% of the networking professionals who were familiar with the term SASE indicating that their organizations had already partially implemented a SASE project. Another 28% indicated that their organizations were in the middle of a SASE evaluation or proof of concept exercise. Meanwhile, among IT security practitioners who were familiar with SASE, only 14% indicated their organizations had partially implemented SASE with another 8% noting that their organizations were conducting a POC. The attributes of SASE that IT networking professionals value the most include SD-WAN connectivity, with 31% of those respondents ranking that as the most important attribute, followed by cloud-based multifunction network security at 26%, and 19% ranking secure remote access as the most important SASE attribute.

No matter which group is leading the charge to SASE adoption and no matter which attributes are considered most valuable, there are many considerations that IT operations teams need to think about to ensure the success of any SASE deployment. Such considerations can include whether SASE providers take a single vendor versus multi-vendor approach, whether providers integrate with existing security and SD-WAN tools in use, how SASE offerings are architected, how to best bring together networking and security teams to execute a deployment, and how to get started with a SASE project.

Respondent Organization Engagement with SASE



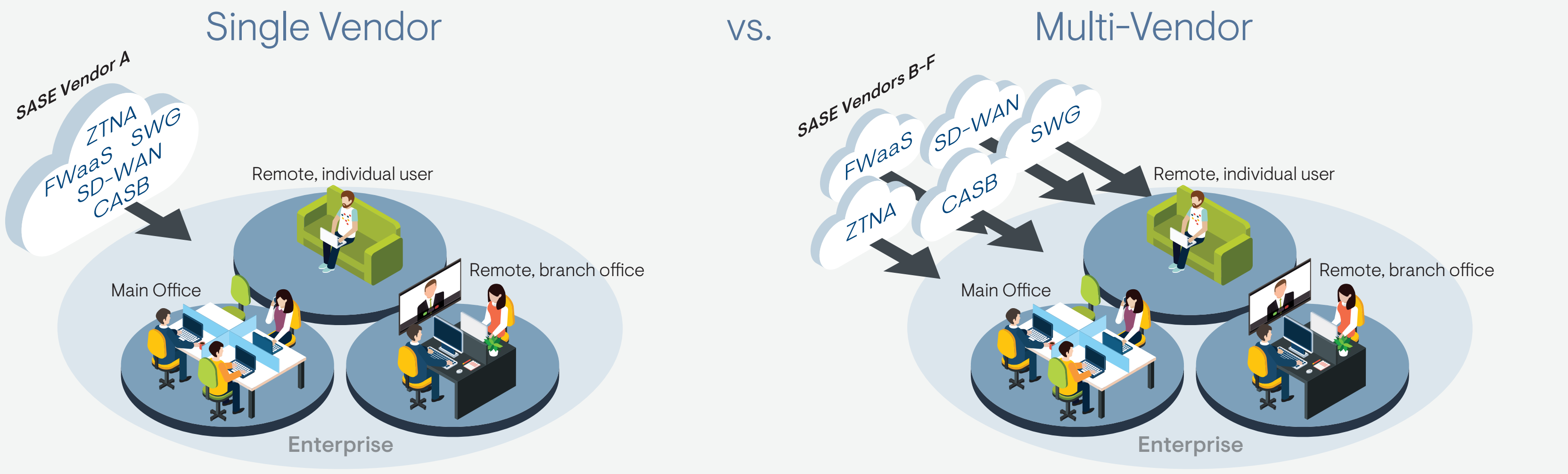
In two separate research projects conducted late in 2020 surveying primarily networking and security practitioners

01. Single vs. Multi-Vendor SASE

Single vendor SASE providers strive to deliver all of the required SD-WAN and security capabilities from within their own product portfolios, offering customers a single, integrated platform. Multi-vendor SASE providers, on the other hand, work with a range of technology integration partners to deliver a series of SD-WAN and security functions. Both offer advantages and disadvantages.

Single vendor SASE providers offer one throat to choke when support issues arise, more simplified and consistent pricing, and the potential for a more unified and consistent policy management experience for customers. However, most providers struggle to deliver the full complement of networking and security functions that customers may require. The tradeoff to achieve that breadth could come at the cost of greater depth of individual functions. This could serve to limit the range of credible vendors for prospects to consider.

Multi-vendor SASE approaches offer customers the option to create a SASE deployment that can be tailored to the customer's specific requirements, delivering integrated, best-of-breed capabilities across multiple providers. That approach raises a number of questions, including: how well are partner solutions integrated? Do integration partners have agreements in place and well-defined workflows to provide seamless support when issues arise, so the customer does not have to deal with finger pointing? At the same time, multi-vendor SASE deployments can make SASE acquisition complex and difficult to budget for, since pricing models will differ from one partner to the next.



02. Support for Existing Security and Network Management Tools

As enterprises begin to adopt SASE for specific use cases, and as they expand their new SASE deployments into other areas, IT security and networking teams will need to continue to secure and manage existing on-premises infrastructure alongside their new SASE deployments. IT security teams in particular have struggled to rationalize an outsized number of security tools by consolidating what they are using. It will be very important for these teams to be able to integrate their SASE deployments into policy engines and security management interfaces already in use within the organization to reduce operational complexity and ensure consistent policy enforcement, no matter where the user is located or how they are connecting to the converged network. At the same time, there will always be security functions or services that the SASE provider doesn't offer, and it's critical that the SASE provider offer a way for customers to enable specific integrations themselves via simplified APIs that come with support for any technical issues that crop up.

03. SASE Architectures: Thin Branch? Heavy Branch?

SASE providers often describe their architectures as either being thin branch, heavy branch, or both. Essentially, thin branch refers to security delivered from the cloud, while heavy branch executes security tasks locally. Although the latter may be desired where there is a need for deep packet inspection to secure East/West traffic locally, it obviates the SASE benefits of reduced operational complexity and overhead as well as improved agility in deployment. What's key is that provisioning, management, and policy decisions are cloud-based where the SASE service can take advantage of greater scale and flexibility, while policy enforcement takes place locally in agents, virtual appliances, or small footprint devices.

04. Successful SASE Deployments: It Takes a Village

Successfully converging networking and security infrastructure for the majority of larger enterprises requires close collaboration between networking and security teams—two IT operations teams that don't always collaborate closely with each other. To achieve such collaboration will require a cultural shift for large organizations and they will have to reevaluate how they are structured, carefully examine how they approach SASE adoption, and decide where the budget will come from. What will be key is to ensure buy-in for any SASE project from the highest levels of IT management, particularly the CIO and CISO, who can help facilitate the cultural shift by creating virtual SASE teams made up of both network and security architects to lead the deployment. These IT and security executives will need to work together to create new, more cohesive objectives and incentives to ensure these groups come together in a productive way to safeguard post-deployment operations to run smoothly.

05. How to Get Started

Those that have already started down the SASE path often advise their peers looking at a SASE deployment to start small with a specific use case, then expand to other use cases over time as new opportunities come up. Examples of use cases include remote access security for mobile users, MPLS replacement projects, or an initiative to replace edge firewalls with cloud-based security. Small sites can serve as proving grounds for new SASE deployments. As contracts for existing firewalls or web filters come up for renewal, SASE should be considered as an alternative. Among the early pioneering SASE customers, typical deployments come down to three distinctive scenarios. The first involves moving remote access security from on-premises devices into a SASE cloud, with SD-WAN integration planned for a later phase of the deployment. The second leads with a migration from MPLS to SD-WAN, with cloud security integration planned for a later phase of deployment. The third and most transformational approach is to move both security and SD-WAN to the cloud in one motion. The latter requires well-thought-out planning to ensure success, but it can deliver outsized benefits right off the bat.

About Palo Alto Networks

Palo Alto Networks, a global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world in which each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com** You can also follow EMA on **Twitter** or **LinkedIn**

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com** 4073.031221