TAKING A SMART APPROACH TO MAKING SINGLE-VENDOR SASE A REALITY

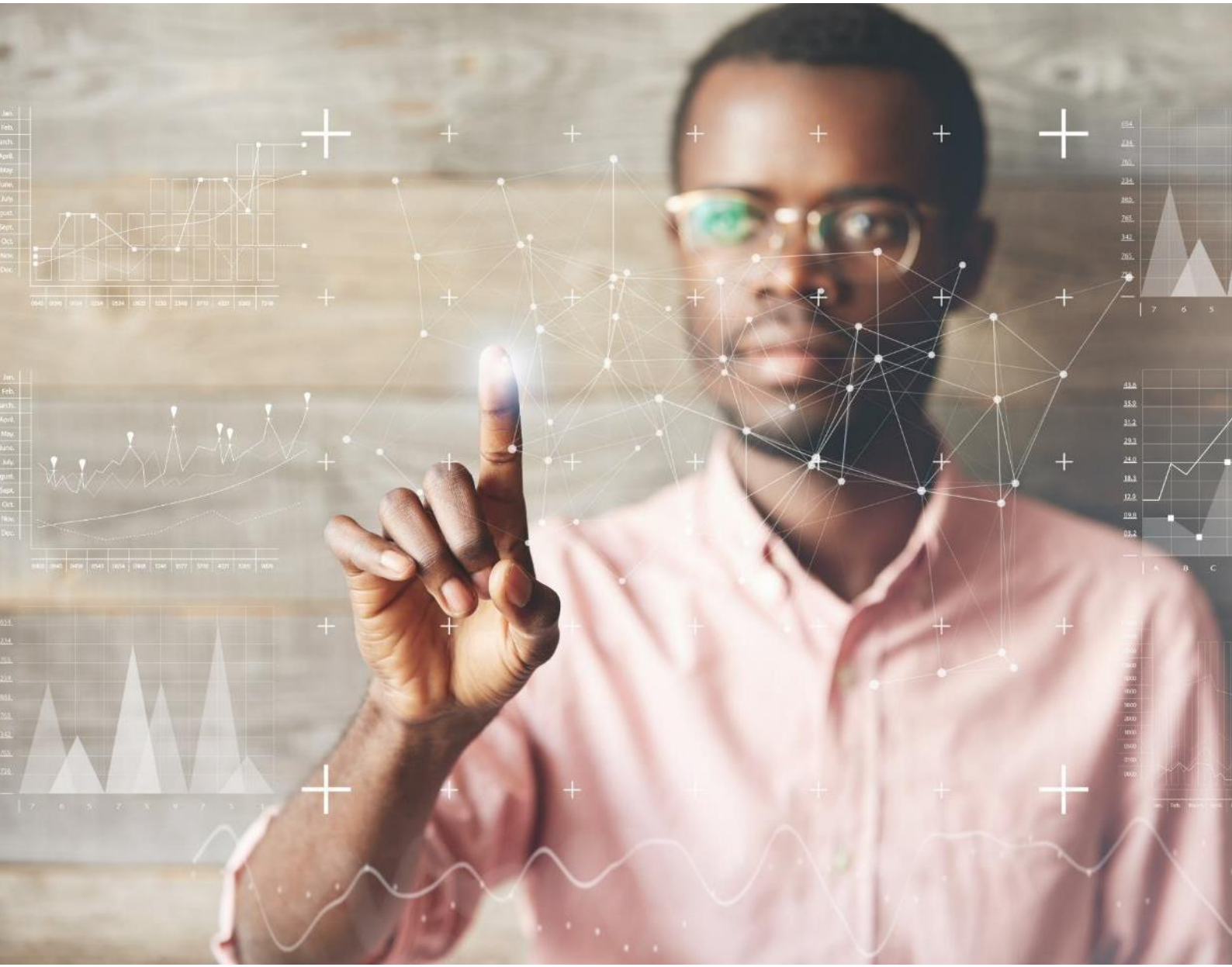
Authors:

Pete Finalle,
Chris Rodriguez

October 2023

An IDC Analyst Connection sponsored by HPE Aruba

IDC #EUR151262023



IDC ANALYST CONNECTION
Sponsored by: HPE Aruba Networking

Taking A Smart Approach to Making Single-Vendor SASE a Reality

October 2023

Questions posed by: HPE Aruba Networking

Answers by: Pete Finalle, Research Manager, IDC and Christopher Rodriguez, Research Director, IDC

Q1: Why are businesses looking to modernize their networking and security practices?

The digital business era is highly interconnected, massively distributed, and "always on." Today's business requirements emphasize the need to connect people, things, applications, and resources while ensuring maximum security and minimal latency and providing a frictionless experience. This has made the traditional network security approach, focused primarily on fortifying the perimeter, obsolete. Devices and personnel are increasingly accessing both on-premises and cloud resources regardless of their location (the main office, a branch office, or a remote location). Additionally, sensitive resources are not only becoming more decentralized themselves, but are also often available to users regardless of their physical location or the network they are using.

This has made securing the network a complex task — the perimeter has dissipated, necessitating a more modern approach to security. With sensitive data and communications no longer confined to a centralized safe haven, identity has become the new perimeter, which is flexible and dynamic to meet modern hybrid work requirements. Furthermore, hybrid work has resulted in the need for a more consistent security stack across the entire business, extending the policies and posture present in the main office to the new hybrid environment. This requires a complete network security stack as a service — which can be delivered with a high level of performance — to secure and enable business operations without negatively impacting service quality.

Additionally, the sprawl of stand-alone products to address modern work ecosystems' growing complexity has reached an untenable level for security and networking personnel to manage. Individual products with separate interfaces and agents and varying integration levels are not only difficult to manage but can lead to significant security and networking gaps due to non-complementary feature sets, misconfigurations, underutilized tools, and operational inconsistencies. Security personnel are a finite resource; spreading their expertise over dozens of dissimilar products and hoping they will fill the gaps themselves is unrealistic.

Q2: Where does single-vendor SASE fit into the security and network transformation process?

Hybrid work and the transformation of networks and resources has left glaring gaps for on-premises hardware and virtualized software security, creating new opportunities for security-as-a-service tools to fill these gaps and reach increasingly decentralized resources and personnel. Thus, concepts such as security service edge (SSE) and secure access service edge (SASE) have emerged as highly consolidated solutions that offer deep integration (if not a shared common codebase), single-agent functionality, and a unified management console. Serving as a Swiss army knife of networking and security, these tools can simultaneously reduce the complexity of à la carte products and fill the gaps resulting from modern hybrid work environments.

In terms of providing connectivity for the growing number of remote resources and personnel, the consistency of the service and its security are equally important. A location-agnostic, high-quality service, consistently delivered to users based on their identity, ensures a consistent work experience regardless of employees' distance from corporate main offices. Single-vendor SASE takes the concept of SASE further — tighter integration between networking and security, as well as between components and capabilities, can improve security posture, reduce misconfiguration challenges, and simplify the solution's overall deployment.

Q3: What is a pragmatic SASE adoption path?

SASE adoption is a unique journey for each end customer, with no suitable one-size-fits-all approach to their immediate SASE requirements and ideal internal roadmap. Existing gaps in security vary by vendor, depending on previous technology purchases; replacing existing security tools is not always straightforward, as these tools can be deeply entrenched. Additionally, existing upgrade cycles often set the pace for SASE expansion, as few customers are willing to sacrifice their current investments. As existing contracts come up for renewal, windows of opportunity open up for greater SASE component adoption. Thus, it is ultimately up to the adopting organization to define its SASE journey, while the SASE provider adheres to the organization's security requirements, timing, and existing product and infrastructure complexities.

SASE is a twofold solution, and adoption may begin with security technologies (e.g., zero trust network access [ZTNA]) or networking technologies (e.g., SD-WAN). However, the goal is consistent: Achieving secure connectivity for the entire enterprise is not about following a fixed path, but rather about a business outcome that fits the unique needs of an individual business. Thus, the components of a SASE solution must be modular in terms of adoption and consolidated in terms of functionality, providing the benefits of stand-alone products for flexibility and the benefits of consolidated products for functionality. This level of flexibility is a key differentiator for single-vendor SASE providers who can achieve the broad adoption of features and capabilities beyond the bare minimum.

Q4: What have businesses been overlooking in their SASE adoption plans?

Adopting organizations tend to have a technical view of their requirements and which boxes need to be checked. However, adopting a comprehensive security solution is not always straightforward and can be challenging. In fact, it is not uncommon for adopting organizations to get hung up on deployment complexities after rolling out either net new capabilities (usually ZTNA) or relatively simple capabilities (often secure web gateway [SWG]). IDC finds that SASE security component adoption begins to drop off once customers face the challenge of replacing more complex products, such as cloud access security broker (CASB). A flexible solution is the remedy for navigating such complex roadblocks, allowing continued SASE expansion to fill existing security gaps, while entrenched or complex technologies require additional time and planning for adoption.

Additionally, simply defining the structure and timeline of a SASE solution ignores many of the nuances of these often complex environments and their stakeholders.

- **Machine environments:** Internet of Things and OT devices and ecosystems are increasingly connected to IT networks, and cloud resources have become a critical part of corporate network infrastructure. Securing these environments requires unique discovery capabilities, contextual identification, and industry-specific security policies, which few vendors are able to provide in tandem with IT security.
- **Networking personas:** Single-vendor SASE solutions require the alignment of networking and security decision makers and their priorities with a single product that addresses the needs of both. Neglecting the needs of one in favor of the other can make meeting overall business needs a challenge. In general, neither party is seeking a compromise; therefore, finding a solution that emphasizes networking and security capabilities equally is a necessary step in bringing these two siloed IT personalities together.

Q5: What does the next stage of SASE look like?

While current customers may be content with SWG, ZTNA, CASB, and SD-WAN from a single vendor, the appetite for more exhaustive security products from single vendors is growing. Therefore, while single-vendor SASE has become the here and now, a more comprehensive security stack from a single vendor is the future, with components such as remote browser isolation (RBI), data loss prevention (DLP), network access control (NAC), and digital experience monitoring (DEM) added to the mix. However, as with traditional SASE components, the tight integration between these capabilities is what brings value to customers. Of a growing number of security and networking capabilities, a simplified management/interface, a unified agent, shared telemetry, and strengthened security posture remain key to continued product consolidation.

Additionally, the SASE market is still in its infancy, and security vendors are focusing on realizing their aggressive security development roadmaps. As this market continues to evolve and expand beyond existing concepts and definitions, customers should be forward-thinking. SASE adoption is a long-term journey, and comparing internal adoption roadmaps with vendor development roadmaps can provide insights into the benefits of a long-term commitment to a single vendor. Additionally, organizations just starting to adopt SASE can ensure efficient future investment by pausing to evaluate their solution's performance and comparing it with newly developed or updated solutions. SASE solutions are evolving rapidly, and navigating the growing sea of products and capabilities requires continued active assessment and evaluation.

MESSAGE FROM THE SPONSOR

About HPE Aruba Networking

HPE Aruba Networking helps businesses capture, secure, and transport data to users and applications from edge to cloud. With a market-leading product line (from wireless and switching to datacenter, WAN, and SSE), HPE Aruba Networking provides customers with everything they require to connect and protect their organization. HPE Aruba Networking's unified SASE integrates award-winning SSE and industry-leading SD-WAN into one simplified, cost-effective solution. IT teams gain full visibility into and centralized control of all traffic and locations, enabling faster responses to both threats and business needs.

To learn more about HPE Aruba Networking's unified SASE, visit https://www.arubanetworks.com/solutions/sase/. For real-time news updates, follow us on Twitter and Facebook, and for the latest technical discussions on mobility and HPE Aruba Networking products, visit the Airheads Community on https://community.arubanetworks.com/.

About the Analysts

Pete Finalle, Research Manager

Pete Finalle is a Research Manager for IDC's Security and Trust team, currently responsible for the Trusted Access and Network Security coverage area. Pete's core research coverage is focused on network security hardware, software, and public cloud services; spanning foundational components like firewall, IDS/IPS, VPN, NAC, and SWG, as well as new concepts like Zero Trust Network Access (ZTNA), Network Edge Security as a Service (NESaaS).

Christopher Rodriguez, Research Director

Christopher is a Research Director in IDC's Security & Trust research practice focused on the products designed to protect critical enterprise applications and infrastructure. IDC's Security & Trust research services to which Chris contributes include Active Application Security and Fraud, where he covers web application firewall, DDoS mitigation, bot management, and API security.

IDC Custom Solutions

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com