CHANNEL BYTES

REPORT

Adopting SASE:

A Strategic Approach to NextGen Network Architecture

In collaboration with:

VANDIS

HPE aruba networking

Executive Summary

Does your organization have a lot of remote offices, storefronts, or branches? Do you have a hybrid work force? **About 94% of major US corporations currently have remote employees**. Do you lose sleep at night worrying about network security? If so, you should join the ongoing strategic migration toward SASE.

Secure Access Service Edge (SASE – pronounced "sassy") is a term coined by Gartner in 2019. Although it is a rather awkward acronym, it is an exciting networking and security technology whose time has come. SASE is a cloud-based architecture designed to enable branch offices and remote workers to securely access enterprise applications.

Gartner expects that SASE will represent a $5B worldwide market in 2024[1], and it is rapidly growing. In particular, highly distributed organizations such as school districts, retail chains, banking, government services, and medical clinics will greatly benefit from this technology. In addition, companies with substantial remote workforces will also benefit from the simplified connectivity and built-in security inherent in a SASE solution.

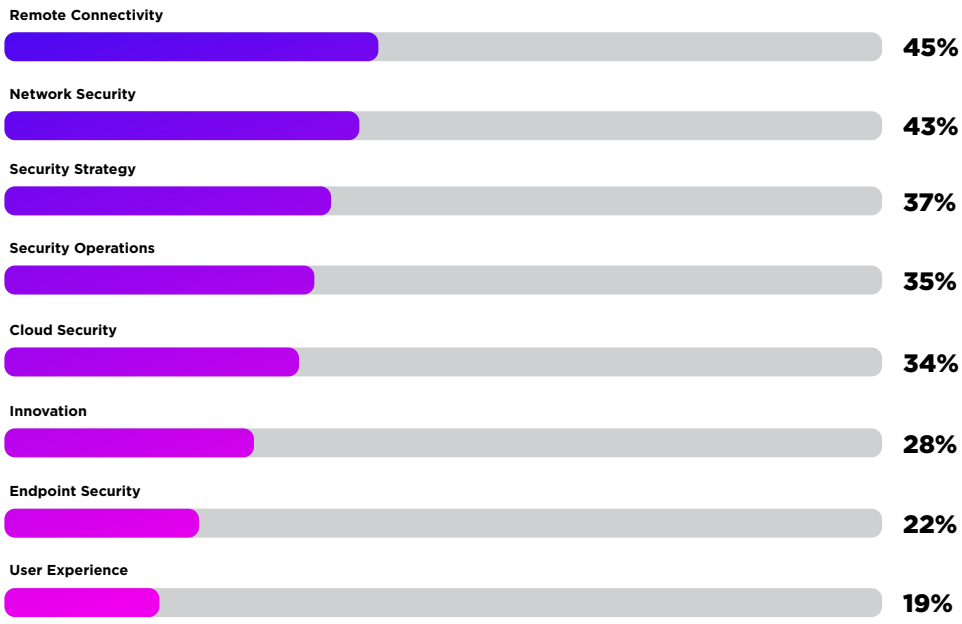
SASE improves network connectivity, enhances security, and reduces costs. In short, this technology will make all types of organizations more competitive in their respective fields.

Business Challenges

Remote branches and countless telecommuters really stretch the limits of most enterprise networks. Providing all these users with high performance connectivity, especially in rural areas, can be daunting. And then there is the greater challenge associated with securing these remote locations. In fact, **according to ESG Research in 2021, 68% of the enterprise cyber breaches used a branch office or remote worker as the source of compromise**[2].

It is a scary world. Denial of Service (DoS) attacks, phishing, ransomware, and other malware are daily occurrences. An enterprise will need a whole stack of network and security appliances in order to detect and deflect all these exploits. However, recreating that complex pile of multi-vendor hardware at each branch office isn't possible. In addition to the monumental expense, this would also create a huge management nightmare.

The SASE cloud architecture model solves this problem by bundling together network and cloud-native security technologies and delivering them in a unified cloud service. It addresses both the connectivity and the security challenges of branch offices and remote workers. This solution also helps reduce hardware, software, and maintenance costs. Some of the key challenges driving organizations to adopt SASE are listed below, as reported in a survey by Cybersecurity Insiders, sponsored by Axis Security in 2023[3].



Challenges Driving SASE Investment 2023

Technical Insights and Benefits

SASE is becoming increasingly more significant in the information networking and cybersecurity worlds. Over the past year, deployments have dramatically increased, technology has substantially evolved, vendor solutions have multiplied, and end-user prices have declined. **Some estimates suggest that up to 65% of North American distributed enterprises intend to adopt SASE within the next two years**[4]. In short, SASE is now mainstream.

SASE is an architecture that combines network security functions with Wide Area Network (WAN) capabilities to support distributed organizations and aims to provide enterprises with an integrated and comprehensive cloud-based approach to network security and connectivity. As a cloud-based technology, SASE supports multiple levels of security throughout the technology stack commonly referred to as the Security Service Edge (SSE).

In SASE, the "E" represents "edge" – a crucial component since cloud-based security services are dispersed to the network's edges, aligning closely with the locations where the users are actually situated. By doing so, SASE can address the challenges posed by the evolving IT landscape, including remote workers, along with the shift to cloud services, and the urgent need for more agile and scalable solutions.

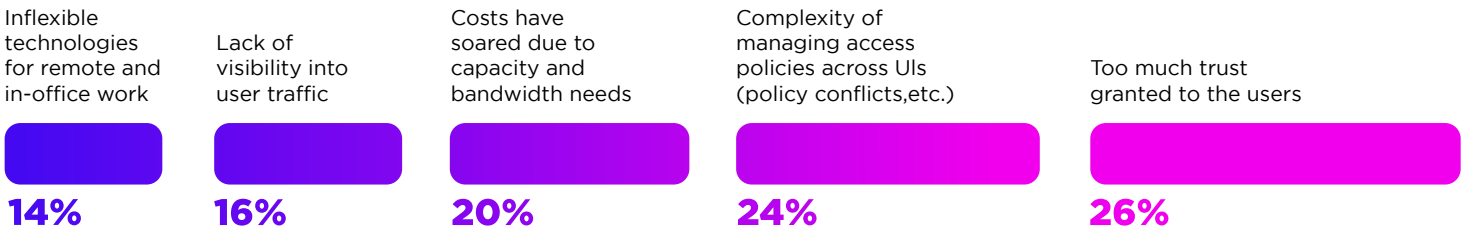
SASE Components and Benefits:

1. **WAN Connectivity:** Typically, SD-WAN is proposed as the underlying connectivity solution. SD-WAN offers users, regardless of location, reliable and high-performance access to applications in the cloud or the data center.
2. **Security Service Edge (SSE):** This cloud-based security model provides a high degree of both scalability and flexibility. Users can dynamically add, change, delete, or even bundle services based upon their ever-changing requirements. Solutions commonly integrated into SSE include:
   a. Secure Web Gateways
   b. Firewall as a Service (FWaaS)
   c. Zero Trust Network Architecture (ZTNA)
   d. Cloud Access Security Brokers (CASB)
   e. Data Loss Prevention (DLP)
   f. Malware Detection
   g. Web/URL Filtering
   h. Identity and Access Management (IAM)
   i. Data Encryption
   j. Analytics, Logging, and Reporting
3. **Policy Organization and Enforcement:** SASE deploys centralized policy management and enforcement for networking and security services. Policies can be dynamically applied based upon users, devices, locations, or applications. This helps organizations implement and enforce intent-based policies.
4. **Centralized Cloud Management:** Users can view, monitor, and manage the entire network from a single centralized platform.
5. **AI/ML-Based Security:** SASE solutions often incorporate Artificial Intelligence (AI) and Machine Learning (ML) to enhance threat detection and response capabilities. These technologies analyze and correlate vast amounts of data to identify and remediate anomalies and threats in real-time. This improves the network's overall security and greatly reduces response times.

By combining these components into a unified architecture, SASE provides an agile, scalable, and comprehensive approach to addressing the networking and security needs of modern enterprises, especially in large distributed environments. As part of the journey to adopting SASE, end-users can take a phased approach to selecting the feature set that is consistent with their unique requirements.

Importance of SSE

Cybersecurity professionals have identified their top concerns with existing remote access security solutions. These, as summarized by Comcast Business in their "2023 SASE Trends Report"[5], are listed below:



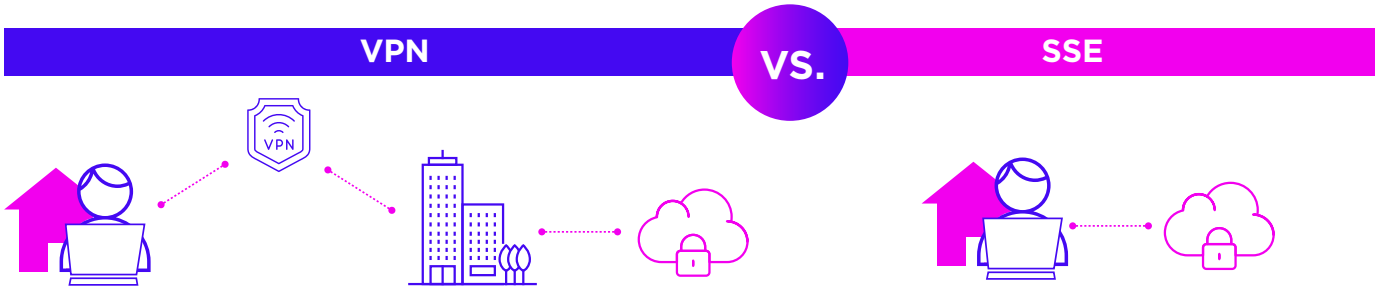
These issues are easily addressed by the Security Service Edge (SSE). This term is another Gartner creation; SSE is the security subset of SASE. SSE provides a single consolidated cloud-based platform for all of the core security services. This ensures that specific security profiles are available for all remote branches and users, regardless of their locations. Furthermore, a user's security profile will be able to follow him/her to different offices or remote destinations.

SSE solutions often consist of a collection of point products (a.k.a. "best of breed") from multiple vendors. However, the ideal solution for most end-users would be a single-vendor SSE bundle. This would consist of a cloud native platform specifically built to support a zero trust architecture. Other services such as firewalls, web gateways, etc., will also be integrated into this single platform.

Why Consider Alternatives?

Traditional networks typically consist of VPNs connecting branch offices or remote workers into the main corporate network. While this certainly is a functional solution, it is also sub-optimal for many reasons:

- All VPNs carry traffic back to the hub of the network. This can cause bottlenecks and scalability limitations while also creating security risks.
- Not all enterprise applications are centralized anymore. Instead, they are often cloud-based. Therefore, the central data center is not always the optimal destination for remote traffic.
- VPNs can require cumbersome manual connect/disconnect routines in order to be activated.
- Traditional VPNs often add latency, especially when all of the traffic needs to be backhauled to a central location before being forwarded to the actual destination.
- Rising costs have impacted several types of VPNs.



SSE solutions can overcome these challenges. These solutions replace the complexity of VPNs. Not only are they often more cost effective, they also enable better productivity of the users.
SSE ultimately makes organizations more competitive in their respective markets.

By the end of 2024, it is anticipated that 40% of all major corporations will have SASE adoption strategies in place[6]. The most common type of SASE deployments will be single-vendor SSE solutions.

Economic and Operational Advantages

The economic and operational benefits associated with implementing SASE cannot be overstated. For starters, SASE eliminates the need for large caches of hardware and software at remote locations. Instead, all of the connectivity and security functions are neatly consolidated in the cloud. This leads to immediate capital savings. This consolidation also greatly reduces the complexity of the overall network, which in turn simplifies the associated network management requirements.

Through the WAN optimization benefits of SD-WAN, SASE also reduces connectivity costs since all of the remote branches will probably only need local Internet connections. Network performance is also enhanced, which also leads to further economic efficiencies, since cloud-based resources will appear to be closer to the users.

All of the cost-effective features associated with SASE will directly benefit an organization's bottom line. In short, SASE will make your enterprise more competitive in the global market.

Adoption Roadmap for Enterprises

2024 is the year for SASE. According to Gartner, over 75% of major North American corporations are already exploring this solution. Most of those are very likely to begin deployments before the end of the year. Although SASE is simple to implement, any major IT undertaking requires considerable care and planning. Some of the recommended steps are listed below:

1. **Network Design:** A skilled networking and security architect should work with your organization to see where SASE may be applicable. SASE should become an integral and complimentary part of your existing networking, security, and management infrastructure.
2. **Vendor Selection:** Many leading industry vendors have SASE solutions. These can consist of specialized components, strategic partnerships, or the entire solution. Evaluate these options based upon your requirements. Request demos. – Note: single-vendor solutions are often preferable.
3. **Testing:** Test a couple of the leading contenders in a lab environment. Then roll-out a handful of remote offices and/or telecommuters. This is an opportunity to evaluate the system's performance, functionality, and user interfaces. Test all applications.
4. **Phased Deployment:** Flash cuts are neither necessary nor recommended. After the test sites are complete, SASE can be rolled-out in an orderly manner based upon physical locations, logical regions, branch types, etc.
5. **Post-Success:** Once deployed, work with your vendors to fine-tune the network, and plan for possible expansion.

SASE Deployments

Initially, back in the pre-pandemic days, SASE was perceived to be a solution for organizations such as retail chains that have a dozen or more stores. Additionally, SASE was also ideal for corporations with multiple branch offices. The SASE architecture also fully supported banks with remote branches, medical clinics, school districts, and distributed governmental organizations like the Department of Motor Vehicles (DMV). The common factor for all of these types of organizations, is the need to provide networking and security services to many remote locations.

Once the pandemic upended the entire workforce, there was an urgent need for a highly scalable and secure solution for remote workers. Now, post-pandemic, remote workers continue to dominate the market – over 50% of traditional office workers currently work from home full-time. SASE quickly became an ideal solution for these employees. Since SASE is cloud-based, no complicated local hardware or software is required. Also, SASE provides remote workers with significantly better security than most VPNs or other legacy remote access solutions.

Organizations that use cloud services to host their applications and data will also see a distinct performance benefit associated with SASE. Since SASE also resides in the cloud, the users and applications will essentially be co-located. Instead of sending the traffic to a corporate location and then to the cloud, remote users will now be able to access their applications directly.

In sum, a truly exemplary SASE user would be:

A security conscious organization with branch offices and remote workers that primarily houses its applications in hybrid and SaaS environments.

An organization such as that would be very shortsighted to overlook SASE. However, any organization that has just one or two of those attributes could also greatly benefit from a strategic SASE initiative. In fact, Gartner estimates that **75% of such enterprises are already actively considering SASE**.

Future Trends and Innovations

SASE is an evolving and progressive technology. **The market is growing by nearly 30% annually**. It is an excellent connectivity and security solution today, and it will continue to improve over time. Ongoing innovations have been aimed at improving security, performance, and the overall user experience. Based upon the established trends, here are some potential future expectations for SASE:

Increased Adoption and Maturation: This is the most noticeable and significant trend. SASE adoption continues to flourish as organizations increasingly prioritize cloud-based security and the need for simple, secure, and agile network architectures.

Enhanced Edge Security: With the rise of edge computing and the Internet of Things (IoT), SASE is likely to evolve to provide even more robust security at the edge of the network.

Further Integration with AI: Deeper integration with AI and ML will continue to enhance SASE's threat detection and response capabilities.

Development of Standards: As SASE increases in popularity, inevitably standards, procedures, guidelines, certifications, and best practices will be developed. These standards will greatly improve multi-vendor interoperability. These will be pursued and welcomed by both the users and the vendors.

Conclusion

SASE is not just a fashionable new networking trend; it is a strategic imperative for modern distributed businesses. Its time has come. SASE provides a cloud-based solution that integrates networking and security to support remote locations, branch offices, and remote workers. It provides both connectivity and security, and it reduces the organization's overhead expenses. Your organization will become more competitive when you embrace SASE.

CIOs, CTOs, and other visionary leaders are strongly encouraged to explore the benefits of a SASE solution. Now is the time to simplify your operations, fortify your security, and refine your strategic initiatives with SASE.

CHANNEL BYTES

References

1. Gartner Research, “2024 Strategic Roadmap for SASE Convergence”, 15 December 2023.
2. ESG Showcase, “A Guide to Adopting Secure Access Service Edge Network Security”, March 2021, Sponsored by Checkpoint.
3. Cybersecurity Insiders & Axis Security. (2023). 2023 SASE Adoption Survey.
4. Cybersecurity Insiders & Axis Security. (2023). 2023 SASE Adoption Survey.
5. Comcast Business, “2023 SASE Trends Report: Beating Expectations on Security While Easing IT Ops.”
6. Gartner Research, “2024 Strategic Roadmap for SASE Convergence”, 15 December 2023.

In collaboration with:

VANDIS

HPE aruba networking