ConRes
IT SOLUTIONS

SHAPING THE FUTURE OF NETWORK SECURITY

Why you should embrace the new era of efficiency and security through Secure Access Service Edge (SASE)

SASE Executive Summary

SHAPING THE FUTURE OF NETWORK SECURITY

Why you should embrace the new era of efficiency and security through Secure Access Service Edge (SASE)

SASE EXECUTIVE SUMMARY

ConRes IT SOLUTIONS

INTRODUCTION

The ConRes security practice is built upon a foundation of networking expertise and security intelligence, including the capability to implement a secure access service edge (SASE) architecture, which represents a bold step forward in securing our customers' business, employees, customers, and supply chain.

With that in mind, we have prepared this Executive Summary of SASE to encapsulate the value it offers to our customers.

No matter what your organization's size, ConRes can help you determine which steps you should take to begin building toward SASE adoption.

TABLE OF CONTENTS

The swift emergence of SASE

Why the top companies already embrace SASE adoption

The top one-third of enterprises have either adopted SASE principles or they have already begun planning and preparations to do so.

The origin of organizational conversations surrounding cloud-based secure access service edges (SASE) can be traced to a 2019 report by Gartner titled *The Future of Network Security Is in the Cloud*.

Looking back on the report now, it is remarkable how much (and how well) Gartner was able to predict about network security trends. In assessing the 2019 security landscape, Gartner concluded that organizations placing enterprise data centers at the center of connectivity requirements (such as a legacy, on-prem security hardware) suffer challenges to the dynamic access requirements that modern digital businesses require. Three years later, these requirements have only gotten more pronounced.

As businesses continues their digital transformation — and as unpredictable world events continue to shine a light on organizational vulnerabilities — there is a growing urgency for flexibility. The reason Gartner's report looks so prescient only three years later is because we have seen, firsthand, the need for secure remote access points that share to one location. This need has also coincided with the increasing adoption of many software-as-a-service (SaaS) applications that were formerly on-prem or individual licenses. And so, while there are some non-SASE networking solutions that can meet some modern organizational needs, they are missing the crucial benefits that SASE provides.

SASE is the only modern networking option built for security. That's why "secure access" is in its name.

The problem with non-SASE networking solutions is that, as more businesses rely on mobility to replace the traditional office, they are left vulnerable to attacks on employees who are no longer working behind the company firewall. And when considering how reliant most companies have become on SaaS applications, the need for organizational flexibility is essential. *So why not meet both needs at the same time?*

For some organizations, the emergence of SASE might feel like it came out of nowhere — and, in many ways, it has. However, what Gartner realized in 2019 (and what many organizations are beginning to realize now) is that the enterprise network is slowly being turned "inside out," inverting the traditional norms surrounding security and networking. It's time for efficiency and security to work toward the same ends; it's time for security staffers to begin delivering policy-based solutions; it's time for your organization to begin planning for SASE capabilities, if it hasn't already.

The world is changing rapidly. To stay ahead, you need to make sure your security doesn't keep you behind.

Exploring the state of modern network security

To understand how we arrived at SASE, consider where we've been

The birth of SASE is an outgrowth of the concept of the secure internet gateway (SIG). The goal of SIG is to offer functionality across different online traffic types, which in turn provides cloud-based broad security to protect users and their traffic. The best way to conceive of SIG is via its name: as a digital wall that stops malicious code and non-user attempted URL connections at its gates. It allows permissible traffic through and extends this protection to cloud-based applications such as SaaS — for example, by blocking uploads to SaaS applications by malignant actors.

The SASE concept is designed to broaden the security functionality of SIGs while converging network functionality. As we have seen, this ensures safe access by remote users across the same network while SASE is busy securing the cloud, data center and branch network edges. This allows organizations to effectively overcome current gaps in coverage; most importantly, it lessens the burden on security teams while doing more for organization's already limited security budget (more on this below).

But while SASE benefits are easy to observe across a wide spectrum of organization needs, what is less obvious is what characteristics make for a smooth adoption. To that end, there are two main characteristics Gartner identified in its 2019 report that digital businesses require to help facilitate this change. To be SASE ready, you organization must be:

Focused on user security

Traditionally, organizations have emphasized the security needs of the brick-and-mortar office. And in a world where on-prem systems were the only available solution, this made sense. But at a time when data usage is shifting away from one access point to a myriad of them, organizations must be willing to commit to the security of the individual.

Increased cloud commitment

By focusing to user security, organizations will necessarily commit further to the cloud as these two concepts work hand in hand. But whereas many organizations have already embraced the cloud in terms of application usage, these same organizations still store their most sensitive data outside of the cloud.

If your organization is willing to embrace user security and increase your commitment to the cloud, you are ready to plan for SASE adoption and reap the benefits of a switch. And as we enter new era of efficiency and security, there are so many benefits available.

Evolving efficiency for modern organizations

Enhancing network and security effectiveness takes time

[1]Gartner: *2021 Strategic Roadmap for SASE Convergence.*

We are still a long way from the 60% of SASE adoption that Gartner expects to see by 2025.[1] This is due to a number of factors tied to the on-the-ground operations of many organizations. One such factor is a series of substantial investments in legacy hardware systems. Compounding this factor is the shifting landscape of where employees work — are they in the office or working remotely? One final problem is especially significant for both large enterprises and small businesses alike: on the one end, there are two distinct network security/network operations teams, or on the other end, a single employee devoted to network security.

With these factors at play, even organizations that intend to adopt SASE need time to take the necessary steps toward implementation. But there are immediate benefits to planning for an SASE model, and the sooner organizations make this decision, the faster they will have a leg up on their competition.

The name of the game is efficiency, and that is one benefit SASE provides.

Rise of SaaS Apps: With the importance of software-as-a-service (SaaS) applications, organizations can no longer avoid cloud-based operations. However, these applications suffer from security limitations, including weak access control and security mechanisms. To maximize the SaaS experience, organizations must ensure that their network security does not trail behind their software operations.

New Demands for a New World: But this problem is not restricted just to SaaS applications — efficiency desires also complicate security concerns. Nowhere is this experienced more than in remote work: as soon your employees have an internet connection, your organization is open to attacks. And this threat will persist until your security team can ship necessary equipment to every worker at every branch.

Evolution of Networking: As new options have arisen for organizations, old networking solutions are proving both more expensive and slower than their SASE counterparts. Prior to Gartner's report, there was a collective reliance of remote branch locations to connect to a corporate headquarters. But as we continue to move into the 2020s, that infrastructure is growing increasingly antiquated.

Secure Your Operations Team: The simple rule of security is that for every 10 businesses searching for a security expert, nine will have to settle for a less-qualified candidate. However, although there is a dearth of qualified security professionals, by implementing security solutions that simplify the process and integrate functionality into a single platform, organizations can more easily attract top talent.

The cost of comprehensive security

Can you afford to not have SASE?

While there are some organizations who believe their legacy security systems are meeting the 2020s' standard of efficiency needs, no organization should want to pay more than they have to for security. The current problem? Many businesses are paying more for worse results. This leads to a question that every good organization must ask themselves when it comes to SASE: can we afford not to adopt?

This question becomes especially important as organizations begin to cast out and plan their future budgets. For many organizations lacking the budget for robust on-prem protection, this makes planning for SASE necessary. Especially when one considers the benefits SASE has over on-prem solutions.

Importance of Network Performance: For every enterprise-level organization, network performance is a key predictor of success. A major benefit of SASE is that it solves two key problems at once: it provides quality network solutions in situations where, previously, employees would attempt to solve the problem on their own (which increased the chances of a security breach). Consolidating networking and security functions into a single, fully integrated platform reduces cost and complexity of both. And it is worth noting that cost reductions on the network side are potentially just as significant as those on the security side within these organizations.

Security as a Mindset: As security continues to improve, cyberthreats are improving with them step by step. Formerly easy-to-spot methods have become more sophisticated, and malignant actors have begun to use ransomware-as-a-service (similar to organizational SaaS deployment). Organizations that are not fully invested in their security solutions will face hackers who are fully invested in their attacks.

Rapid Increase of Remote Users: If the last few years have taught us anything, it's that flexibility in our workspaces is essential for the today's businesses to survive. However, as organizations continues to shift the location of their employees, these workers will be the most susceptible targets for attack. Whereas public access points like Wi-Fi leave users vulnerable, secure connections keep security threats at bay.

Reduce Cost, Reduce Complexity: Traditionally, organizations have employed multiple security solutions from multiple vendors to address single-purpose needs. But this was not user-friendly: instead, these individual products required separate operating systems, making integration difficult. SASE allows your organization to keep your security under one roof — even if that roof is in the cloud.

What's on the horizon?

Moving from SASE *inquiry* to SASE *adoption*

One year ago, Gartner issued a follow-up report from its 2019 study titled: *2021 Strategic Roadmap for SASE Convergence*. The findings were remarkable: in just two years, SASE interest has skyrocketed. As organizations have quickly realized their security needs can be better met, what was previously a negligible market has grown. The percentage of end-user inquiries into SASE has risen from 3% to 15%. Perhaps Gartner's most notable assessment came regarding security systems as a whole:

> **The legacy perimeter must transform into a set of cloud-based, converged capabilities created when and where an enterprise needs them—that is, a dynamically created, policy-based secure access service edge.**

To that end, Gartner reinforces its belief that SASE is a pragmatic and compelling model that can be partially or fully implemented as soon as possible by outlining a migration plan that your organization can take advantage of today. **And that will take building relationships with new vendors and finding companies that can offer a comprehensive SASE solution.**

Regardless, it appears inevitable that SASE will be the defining security solution of the 2020s. The only question left is whether your organization can afford to avoid moving to the forefront of network security.

CONCLUSION

ConRes views SASE as an emerging security architecture with unlimited potential. This innovative approach addresses enterprise-level networking and security challenges. We are uniquely suited to offer a comprehensive SASE solution tailored to fit your organization, and we can walk you through the steps to get there.

Contact us to discover how this emerging security architecture can benefit you.

ConRes IT SOLUTIONS