Whitepaper

Assess and Adopt Secure Access Service Edge (SASE) With Insight

Introduction

Most organizations believe network security is more difficult than it was just two years ago.[1] As IT environments take on increased complexity, IT leaders are seeking new, more efficient ways to handle quickly evolving security challenges. Spiraling data quantities, rising numbers of endpoints and users, applications spanning cloud and on-premises architectures, and evolving network architectures have all introduced new levels of cybersecurity risk within organizations. This complexity has left many IT teams and security operations juggling multiple disparate point solutions and vendors for IT security solutions. Unfortunately, this creates additional complexity, risk, and costs.

Organizations looking to create a comprehensive, cloud-first security posture need an alternative to traditional data center-oriented security models. The Secure Access Service Edge (SASE) model was developed to answer this change by unifying traditionally siloed networking and security services in a cloud-centric environment with a single management point.

Given their apparent need for simpler security management and a growing industry shift to SASE adoption, many organizations are now at a crossroads, wondering what SASE has to offer, how it compares to Software-Defined Wide Area Network (SD-WAN), whether and how they should implement a SASE approach, and what that would mean for investments they've already made in their security strategies.

Understanding SASE solutions

As a longtime provider of innovative IT solutions, Insight helps clients understand the features and benefits of a SASE approach and implement the solutions that work best for every client's network and security needs and challenges.

This whitepaper is intended to provide a starting point for organizations that find themselves in the position of exploring SASE options for their business.

SASE features and benefits

Importantly, SASE is not a singular tool or technology; rather, a concept defining the convergence of networking and security services within a cloud-based architecture that unifies security and delivers reliably secure connectivity for endpoints and remote offices to private and cloud-hosted services.

Built into the SASE approach are familiar security architectures and capabilities, including:

- DNS-Layer Security
- Cloud Access Security Broker (CASB)
- Secure Web Gateways (SWG)
- Zero Trust Network Access (ZTNA)
- Next-Generation Firewalls (NGFW)
- SD-WAN

The goal of SASE is to combine these security architectures for a scalable environment that delivers direct internet access, secure applications, and stronger protection against cyberthreats and security concerns.

Ideally, a well-architected SASE approach will enable organizations to:

- Reduce latency
- Gain insights for developing access policies
- Improve visibility
- Streamline security management and operations
- Protect on-premises and remote users

How SASE compares to SD-WAN

Many organizations question how SD-WAN and SASE differ architecturally. SD-WAN is a technology that helps optimize path selection and application experience within an enterprise. It provides the greatest benefit when there are multiple links at single locations to prioritize, selecting the best path for specific business-critical applications.

While SD-WAN enables optimal cloud connectivity through dynamic path selection and Direct Internal Access (DIA), modern SASE solutions are built cloud-focused and are able to provide the mechanism for secure connectivity for both remote users and branch locations to consume cloud applications as a service from the cloud.

What does SASE mean for existing SD-WAN and other prior security investments?

While SASE will help consolidate some security tools, it is not necessarily a replacement for SD-WAN and other common security technologies and protocols; rather, it is an approach that unifies these existing technologies. As such, SASE will never remove the critical need for dynamic traffic steering or application-aware routing within the enterprise — primary reasons for SD-WAN implementation.

In addition, many clients continue to refrain from expanding cloud presence or prefer to prioritize an internal approach to security and threat detection.

Enabling the convergence of network and security, SASE actually works to complement many of the solutions clients currently have in place; and as a cloud-hosted solution, SASE may offer many organizations the opportunity to replace or consolidate redundant or legacy tools that contribute to operational inefficiencies and technical debt.

Whether and how to implement a SASE approach

SASE implementations will differ between organizations based on individual needs, and SASE may not be a necessary approach for every environment. However, between the evolving challenges of the modern workforce and a competitive market that demands innovation, many clients will find SASE a promising solution for these very common use cases:

Improved access

The workforce today requires reliable access to applications from a multitude of changing locations and devices and a consistent and secure experience and interface regardless of whether access is remote or on-premises. A comprehensive approach to cloud-based security protects devices, users, and data within the network, regardless of location.

Improved security

The expansion of the edge across the growing Internet of Things (IoT), remote workforce, and dispersed IT landscape in general has created an increasing number of gaps in enterprise security. Additionally, organizations cite a lack of automation, modern solutions, and skilled cybersecurity staff as top obstacles to security operations.[2] A SASE approach not only modernizes cybersecurity across the organization's entire network architecture, but also simplifies and streamlines the management process, making it easier for teams with limited resources to achieve stronger results.

Improved scalability

Unnecessary complexity and outdated technology hold businesses back from achieving the agility needed to grow and innovate. Relying on disjointed point solutions is overburdening IT and security teams and preventing organizations from realizing the efficiencies that could help their organizations to meet modern demands at scale.

Why Insight for SASE

Insight can help guide organizations looking to solve for one or more of these use cases. Our decades of knowledge spanning both older and emerging IT technologies and solutions combined with our familiarity with a wide scope of industry offerings allows us to walk an organization through the specifics surrounding various SASE solutions and to determine how best to implement and evolve their own IT architectures for cloud-driven security.

As a leading technology partner working with multiple world-class vendors, Insight's experts understand the ins and outs of every solution available and help identify the best-fit solutions for each use case. Our vendor-agnostic approach is complemented by a range of Insight offerings, from strategic consulting and roadmap creation to technical adoption, implementation, and solutions management offerings.

Because of its nature as an integrative approach to security in the cloud, the SASE conversation spans several areas, including cloud, security, infrastructure, policy, users, and more. Insight can help gather the input needed from the various internal groups involved in network, cloud, and security strategies to help outline the best approach to implementation.

It's important for organizations to understand that SASE adoption is a multiphased, strategic approach. One of the unique benefits of working with Insight for SASE implementation is that it enables organizations to take a stair-step approach to adoption, building on capabilities as ready, with strategic support for every phase.

Summary — Simpler, stronger security is available with Insight support for SASE

As network and security challenges continue to change, IT leaders can rely on Insight to deliver the strategies, tools, and technologies it takes to simplify operations, streamline the IT environment, and introduce efficiencies that empower innovation and success. Insight has the expertise to help identify and implement solutions designed to address modern network and security challenges and equip organizations to manage and maintain security operations effectively into the future.

---

1 Cisco. (2020). A Roadmap to SASE.

2 Marketpulse Research by IDG Research Services. (February 2021). Cybersecurity at a Crossroads: The Insight 2021 Report. Commissioned by Insight.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com