



# Adopting a Secure Access Service Edge (SASE) Approach With Insight and Cisco

---

## Abstract

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. These complex and dispersed IT environments require built-in security architectures integrated throughout the infrastructure to protect users, endpoints, and data.

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.

Longtime partners in innovative IT solutions, Insight and Cisco are helping 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.

## Problem statement

Most organizations believe network security is more difficult than it was just two years ago.<sup>1</sup> 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. With the apparent need for simpler security management and the growing shift to SASE adoption, many of these organizations are 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.

## Background

Insight and Cisco possess a deep partnership and strong reputation for working together to solve client IT challenges. For more than 20 years, Insight has played an integral role in delivering innovative Cisco® solutions and managing hundreds of Cisco networks and thousands of devices for clients worldwide.

As organizations have accelerated cloud, multicloud, and hybrid cloud adoption, Cisco solutions have played a critical role in Insight's ability to help clients adopt and manage best-fit cloud tools and technologies. Cisco is leading the evolution of secure network access in the cloud with Cisco Umbrella®, a key component in Cisco's SASE framework. With an approach to SASE that combines leading network and security functionality rolled into one cloud-native service platform, Cisco Umbrella enables clients to create secure access for users in any location.

## Solution

Insight's decades of knowledge spanning both older and emerging IT technologies and solutions combined with our familiarity with Cisco solutions allows us to walk clients through the specifics surrounding Cisco's SASE solutions and to determine how best to implement and evolve their own Cisco-driven IT architectures. Insight solutions range from strategic consulting and roadmap creation to technical adoption, implementation, and solutions management offerings.

This whitepaper is intended to provide a starting point for Insight and/or Cisco clients that find themselves in the position of exploring SASE options for their organizations.



### 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)



Software-Defined Wide Area Network (SD-WAN)

Cisco Umbrella delivers leading SASE solutions, unifying the above primary SASE use cases with the SecureX-integrated security platform.<sup>2</sup> Cisco Umbrella, built on Cisco's highly available, global cloud infrastructure, delivers flexible deployment and consumption models to scale with client needs, allowing businesses to benefit from direct internet access, secure applications, and stronger protection against cyberthreats and security concerns.

Equipped with Cisco Umbrella, users can:



Connect users and devices to applications with reduced latency



Achieve visibility and control over all Software as a Service (SaaS) applications



Monitor and secure enterprise traffic from a single, cloud-native platform



Capture deep insights from the endpoint to cloud services



Protect and defend roaming users

In addition to the security benefits outlined, SASE with Cisco delivers operational benefits, including immediate value and a low total cost of ownership, rapid deployment, and efficient management, which enables internal security teams to streamline operations and better utilize resources.



## How SASE compares to SD-WAN

Many clients 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), SASE solutions like Cisco Umbrella were built cloud-focused and provide the mechanism for secure connectivity for both remote users and branch locations to consume cloud applications in the most effective manner — all delivered 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 fact, Cisco's SASE architecture enables existing consumers of Cisco's leading WAN Edge solutions to seamlessly adopt a SASE approach to security.

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 all organizations. 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.<sup>3</sup> 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.

Insight can help guide clients looking to solve for one or more of these use cases. Our teams will help a client identify when Cisco Umbrella is the appropriate solution for the organization's needs and assist with developing a strategy for implementation.

It's important for clients to understand that SASE adoption is a multiphased, strategic approach. One of the unique benefits of Cisco's SASE offering is that it enables clients to start small with DNS-layer security and take a stair-step approach to adoption, building on capabilities as the organization is ready.

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 is able to help clients gather the input needed from the various internal groups involved in network, cloud, and security strategies to help outline the best approach to Cisco Umbrella implementation. 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 client use cases.

Understanding the unique benefits of Cisco's SASE offering, and the ways it integrates with Cisco's comprehensive portfolio of cloud, data center, and network solutions, allows Insight to partner with Cisco in meeting client needs and driving meaningful IT modernization as we help existing Cisco clients build out their Cisco environments for improved value and identify new clients whose needs are best met by all that Cisco has to offer.



## Conclusion

As network and security challenges continue to change, IT leaders can rely on Cisco and 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. Cisco Umbrella is an exceptional solution designed to address modern network and security challenges and equip organizations to manage and maintain security operations effectively into the future. Insight has the expertise to help identify and implement this solution and more to the increased benefit of vendors, clients, and end users.

## References

<sup>1</sup> Cisco. (2020). A Roadmap to SASE.

<sup>2</sup> Miller, L. (2020). Secure Access Service Edge (SASE) for Dummies. Cisco Special Edition.

<sup>3</sup> Marketpulse Research by IDG Research Services. (February 2021). Cybersecurity at a Crossroads: The Insight 2021 Report. Commissioned by Insight.