SASE with Savvy: The Keys to an Effective Secure Access Service Edge Solution
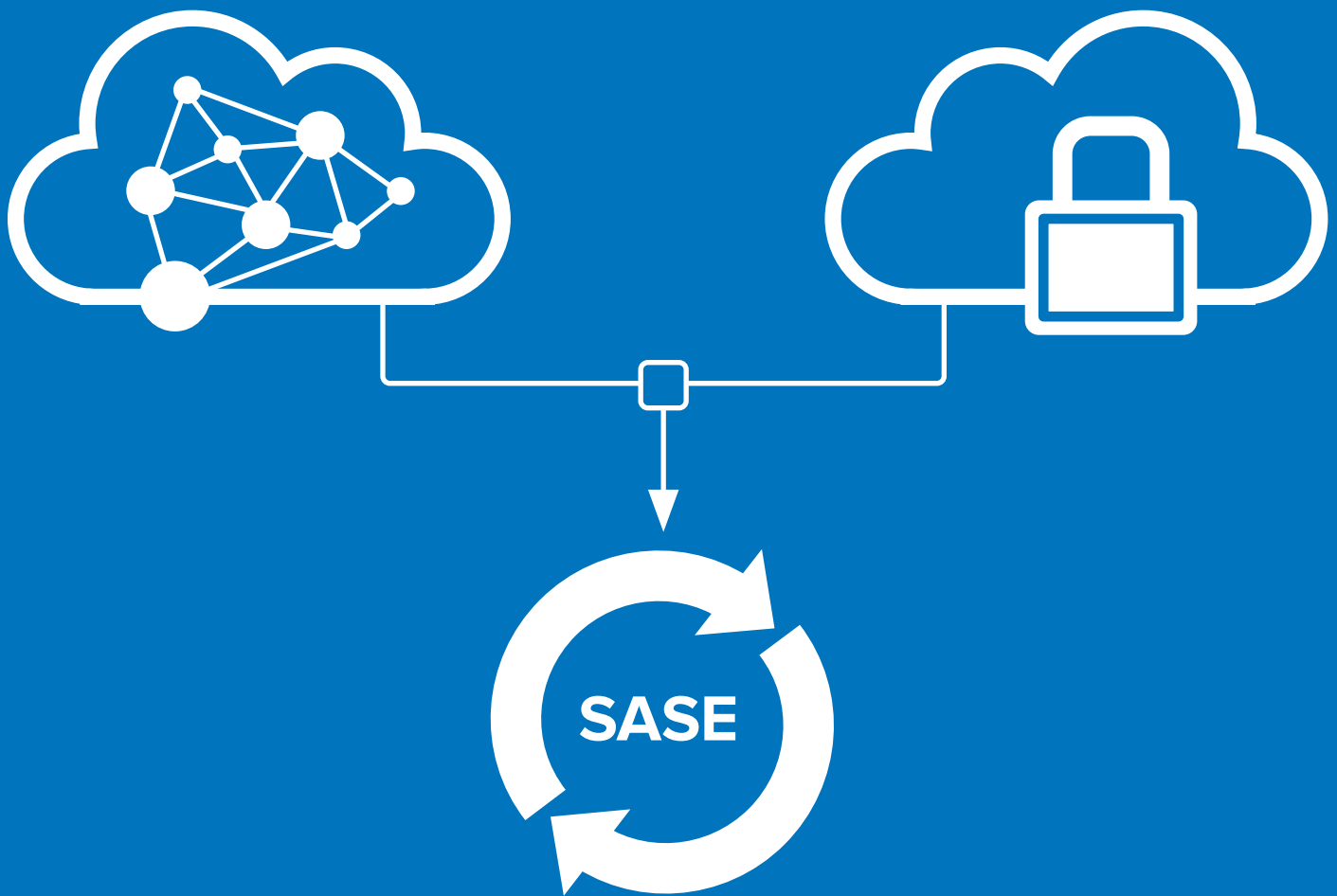
Based on real user reviews of Cisco SD-WAN and Cisco Umbrella

IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

Secure Access Service Edge (SASE) is becoming a standard approach for securing the increasingly distributed users, data and applications in a modern organization. A solution developed to handle the unusual needs of digitalization and cloud-based computing, SASE enables secure, anywhere, anytime access from any device. An effective SASE implementation depends on many factors, as users of Cisco Umbrella and Cisco SD-WAN solutions explain in this paper. Architecture and performance are important, as are the way an organization deploys SASE's core elements of Cloud Access Service Broker (CASB), Zero Trust Network Access (ZTNA), Domain Name Server (DNS) security, Software-Defined Wide Area Network (SD-WAN) and Firewall-as-a-Service (FWaaS).
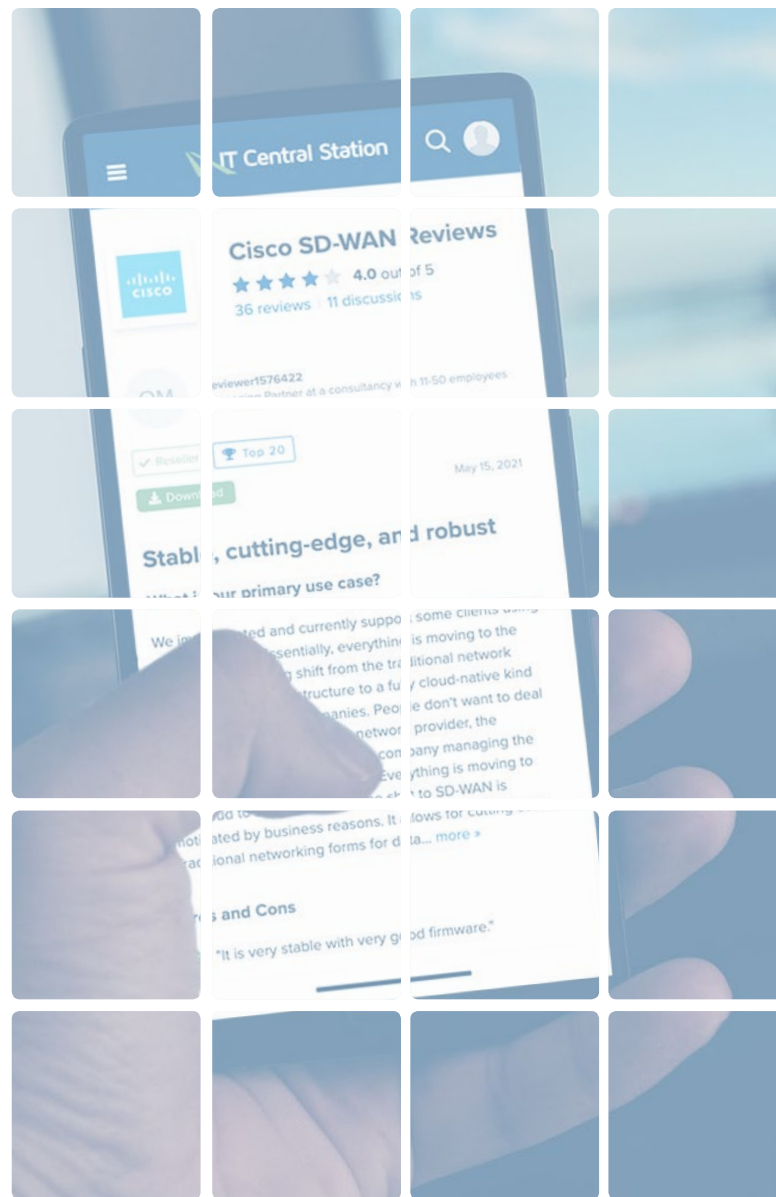
CONTENTS

INTRODUCTION

Secure Access Service Edge (SASE) has become the predominant approach to securing sprawling networks and heterogeneous endpoints, including the increasingly common hybrid work environment. What makes for a good SASE implementation? Answers vary widely, partly because organizations are at different stages of SASE maturity, while also electing to build their SASE architecture in their own unique ways. In this paper, users of the Cisco Umbrella and Cisco SD-WAN (Software-Defined Wide Area Network) solutions discuss the keys to an effective SASE solution. They comment on evolving SASE use cases, as well as the elements of SASE, including the Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Domain Name Server (DNS) security and Zero Trust Network Access (ZTNA).

Note: Companies in this paper referred to as "large" have over 5,000 employees. Mid-sized companies in the paper have between 500 and 5,000 employees, while companies with fewer than 500 employees are identified as "small."

A Brief Overview of SASE

SASE has rounded the corner from being an analyst's paradigm to serving as the new standard for securing connections to business critical applications and other digital assets. It is a response to the growing trend of digitalization, work from anywhere and cloud-based computing. Network managers and their colleagues in security began to see that users needed access from anywhere while maintaining a consistent level of security. They recognized that the traditional perimeter was vanishing — if not becoming totally obsolete — as a countermeasure to attacks on digital assets. People and devices needed access at the edge, and not just to the data center, but to any number of cloud-based systems. SASE addresses these new requirements.
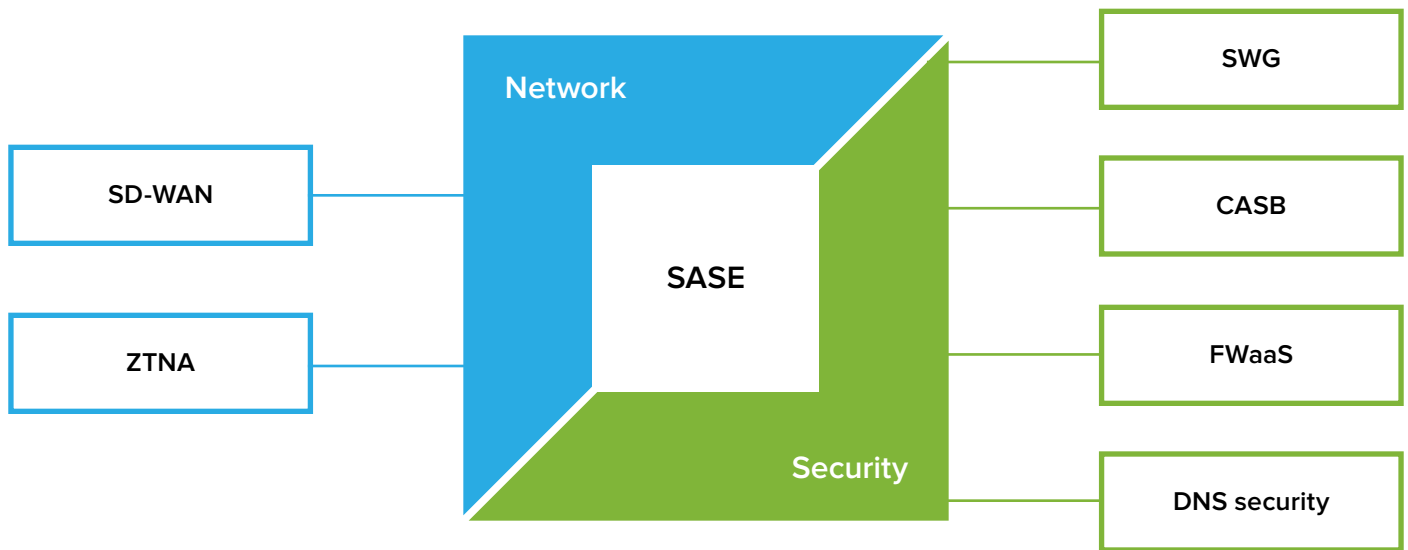
Figure 1
Elements of SASE, which blend network and security

A great deal has been written about the benefits of SASE. Briefly, SASE adopters are finding that the model helps cut costs in security and network operations. This comes partly from SASE's ability to combine security and network management. In addition, security is more holistic with SASE, as there are fewer disjointed point solutions required to protect digital assets. Management grows simpler with this convergence, as well. The technology also tends to be highly scalable.

Definitions and implementations of SASE vary, but industry consensus holds that SASE comprises a collection of six core technologies that blend network operations with cloud security. These include the Software-Defined Wide Area Network (SD-WAN), Secure Web Gateways (SWGs), Cloud Access Service Brokers (CASBs), Firewall-as-a-Service (FWaaS), DNS security and Zero Trust Network Access (ZTNA). Figure 1 depicts these essential components of the SASE model.

"
.. security is more holistic with SASE, as there are fewer disjointed point solutions required to protect digital assets.

Evolving SASE Use Cases

IT Central Station members are putting Cisco solutions to work in evolving SASE use cases. Given the relatively early stage of SASE in the enterprise technology lifecycle, some of the use cases are incremental and preliminary. However, the direction is clear. As a Managing Partner who uses Cisco SD-WAN at a small consultancy put it, "Essentially, everything is moving to the cloud. There is a big shift from the traditional network operator-based infrastructure to a fully cloud-native infrastructure for companies. Today with the SASE architecture, it's very easy to immediately deploy the cloud to have one subscription for one set of services. People don't want to deal with so many providers."

In his view, having separate vendors for the network, along with multiple cybersecurity providers managing routers and firewalls and so forth, is no longer tenable. He said, "Everything is moving to the cloud to simplify things. Traditional networking forms for data centers are simply too expensive, too slow, and very time-consuming to maintain." Now, with Cisco driving his SASE approach, he has one subscription that provides full access to a dedicated network that is faster than the traditional MPLS networks he used to use. And, he shared, "You have integrated cybersecurity and a fully dedicated private backbone that is essentially spreading across the globe. With SD-WAN, especially with solutions based on the SASE framework, they pay one subscription fee each month, and one single company is managing everything."

> ❝
> **Many of our customers are moving to the cloud, which can handle both on-prem and cloud services, a hybrid solution.**

Hybrid and multi-cloud use cases are favorably mentioned by IT Central Station members. For example, according to a pre-sales consultant who uses Cisco SD-WAN at a large tech services company, "Many of our customers are moving to the cloud, which can handle both on-prem and cloud services, a hybrid solution." A Senior Director, Network Engineering at a mid-sized tech vendor remarked that Cisco SD-WAN "securely connects to our hybrid cloud using transit VPCs and cloud on-ramp for fast deployments." A Sr. Network Engineer Consulting Services at a comparably-sized consumer goods company

echoed this idea, commenting that Cisco SD-WAN was good for cloud- based integrations.

Other notable prototypical SASE use cases included:

- "One of the more important use cases for clients is using the product as a web proxy. A second thing would be a situation where a customer wants to block access to an employee's personal email account and allow only corporate email accounts. A third would be the cloud-delivered firewall.." - Technical Presales Consultant who uses Cisco Umbrella at a mid-sized software company

- "We primarily use the solution as cloud security for our branches. It protects us from direct internet outbreaks." Network Specialist who uses Cisco Umbrella at Syswind Kft., a small tech services company

- "The solution allows organizations to have visibility into the application traffic. After implementing the solution, we can see what types of traffic we have. We can see how users are using the internet and will be able to tell if anyone is downloading something that they shouldn't be or if they are consuming a lot of data." - System Engineer who uses Cisco SD-WAN at a small tech services company

- "We use it to control how the end users can access our data center services and internet services, which gives us an inner view of the user behavior and how they are doing, and if any malicious activity is going on, knowingly, unknowingly, or both." - Senior Manager, Information Technology who uses Cisco Umbrella at Emami Ltd, a mid-sized consumer goods company

The Importance of Architecture and Performance

SASE combines networking and security, so architecture is an important consideration for system owners. A SASE solution has to be adaptable and stable, but also high performing. A Network Engineer & Security Specialist who uses Cisco Umbrella at a small tech services company put it this way: "The solution is extremely stable. It has excellent performance."

A Head of IT Operations who uses Cisco SD-WAN at a small tech services company spoke highly about the architecture of the solution when he said, "In a software-defined network architecture, it heals itself and the management of the solution is very easy." A Senior Global Product Manager at a large comms service provider characterized Cisco SD-WAN as a global scale solution providing an open architecture design with good technical support.

A "10 out of 10" score for Cisco SD-WAN came from an Executive Vice President of Operations and IT who uses Cisco SD-WAN at Robinson Management Service, a mid-sized financial services firm. He cited cost savings of 80% and a performance boost of 400% as his reasons

for providing such a positive review. He further revealed, "It worked right from the beginning and saved them a ton of money."

> ❝
> **The solution is extremely stable. It has excellent performance.**

"Cisco is definitely cutting edge, absolutely cutting edge in terms of robustness on the capability of the network to be very stable with very low delay," said the consultancy's Managing Partner. He then added, "It is a proven, tried, and tested technology. It is very reliable software. It is rock solid and very stable with respect to delivering top-performance networking functions."

Understanding the Elements of SASE

A SASE implementation depends on its individual elements. SASE owners should understand how each part of the construct functions and adds to the value of the whole. The following user experiences provide details and insights in each of the major SASE solution segments.

Secure Web Gateway

A secure web gateway is a cloud-based full proxy that can log and inspect all of an organization's web traffic for greater transparency, control and protection. IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls and advanced threat protection.

This is how a Network Engineer at LADWP, a large energy/utilities company, uses Cisco Umbrella. In his case, the solution ensures that employees don't visit websites they are not supposed to be accessing. A Security Team Leader at a mid-sized tech services company

also uses Cisco Umbrella at a banking client as a gateway to the web with a broad set of control and protection for all of their internet traffic.

What matters in a gateway, according to a Technical Presales Consultant at a mid-sized software company is the ability to segment personal accounts from corporate accounts.

> " IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls.

Specifically, he utilizes Umbrella's feature that lets his team add the ID of the customer's Gmail account or the Azure account. That ID is then used as a filter to separate access so that only corporate Gmail will be accessible. It can block personal accounts. Additionally, he values Umbrella's web proxy, which is effective in determining if web traffic may be malicious.

CASB

One of the CASB's main jobs is to protect corporate data that sits in cloud-based applications. To work well in a SASE setting, a CASB needs good app discovery, visibility and control capabilities. A System Engineer at a small tech services company found this to be the case with the CASB features available in Cisco Umbrella. He noted, "The solution's application control and application traffic steering tool are its

most valuable aspects in terms of how we utilize the product. The solution allows organizations to have visibility into the application traffic."

> **The solution's application control and application traffic steering tool are its most valuable aspects in terms of how we utilize the product.**

He added, "After implementing the solution, we can see what types of traffic we have. We can see how users are using the internet and will be able to tell if anyone is downloading something that they shouldn't be or if they are consuming a lot of data." This latter comment reflects the need for CASB to help with data loss prevention strategies, which is part of the SASE reference architecture for Network-as-a-Service shown in figure 2.
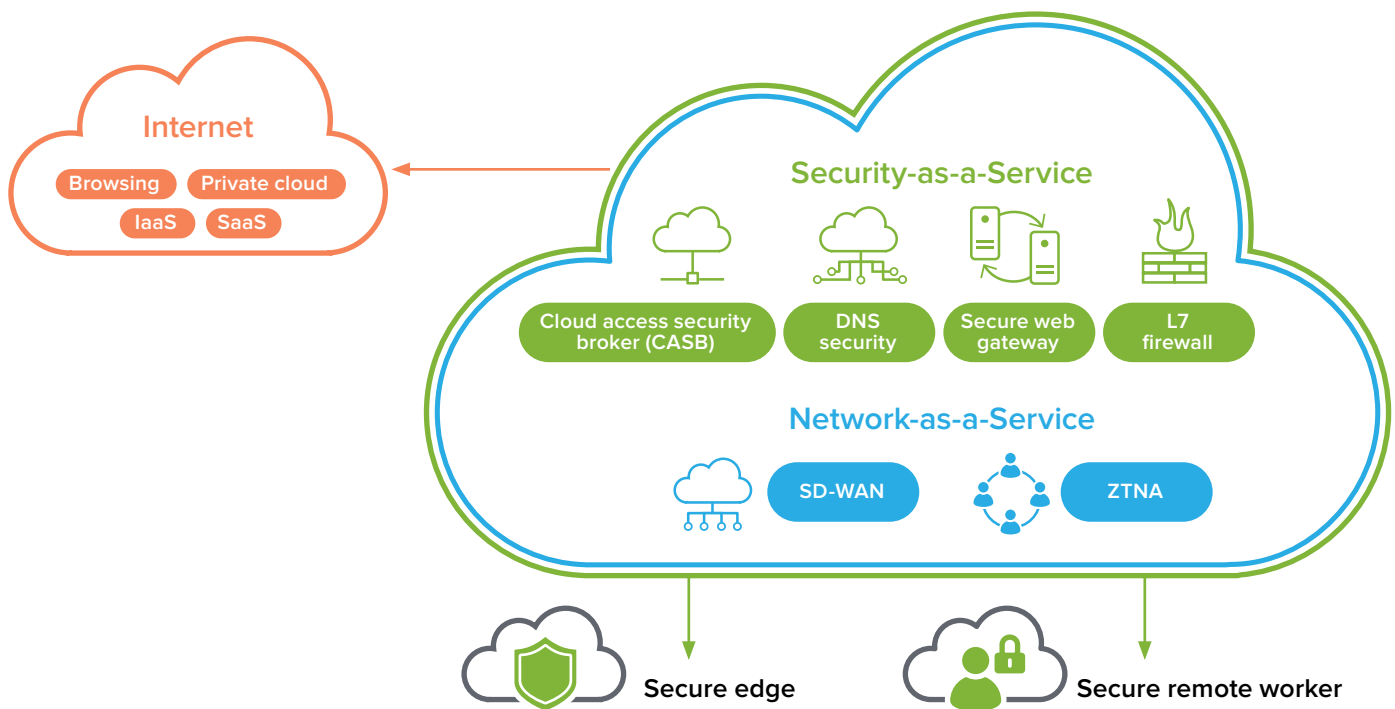

Figure 2
SASE reference architecture, based on the Network-as-a-Service model.

DNS Security

DNS layer attacks can be devastating, as they hit at a fundamental point of trust and connection between end users and the Internet. SASE incorporates DNS security to mitigate this risk. A Security Engineering Senior Manager at a large retailer talked about this issue, saying, that Cisco Umbrella, which he found easy to configure and operate, "has fixed the gap in our DNS protection." They use the solution for DNS and IP reputation.

> 66
>
> **The most valuable feature is the DNS security.. used to watch all the traffic which we are routing through the endpoint and organization firewalls.**

A Network Operations Center (NOC) Lead who uses Cisco Umbrella at a small tech services company similarly remarked, "The most valuable feature is the DNS security. It is used to watch all the traffic which we are routing through the endpoint and organization firewalls." In their case, internet requests from all users and devices are routed through DNS security which scans each and every request. It notifies the team if it is not safe and allows those that are. He said, "It is like an alarm center application near our firewall."

"The primary use case for this solution is for DNS based attacks and for malware protection," said a Sr. Network and Security Consultant who uses Cisco Umbrella at a mid-sized media company. In his experience, the tools provide protection from a variety of web-based attack methods and improve visibility. He explained the process, saying, "DNS is the first step in the internet connection process. Based on the Umbrella and Talos threat intelligence, DNS security blocks the connection to millions of malicious sites before they can infect the user's device or our network.

Stopping the majority of attacks this early in the process saves us time and money by helping us avoid investigation and remediation costs. Cisco Umbrella is a fitting solution for DNS-based attacks and malware protection."

Firewall-as-a-Service (FWaaS)

The edge requires a different kind of firewall. Traffic and digital assets are located in many new places, all of which need protection. The FWaaS offers a solution, where, as the Technical Presales Consultant explained, "A customer would create a tunnel between their on-prem firewall to the Cisco Umbrella cloud. This would make it so that all the traffic is filtered by the Umbrella Firewall-as-a-Service."

> 66
>
> **..it's a cloud-based solution, you can access this over the cloud anywhere in the world.**

"If you have this solution you don't need a big firewall," said the media company Sr. Network and Security Consultant. He then related, "Because it's a cloud-based solution, you can access this over the cloud anywhere in the world. You don't need to build a big infrastructure. It will give you more return on investment."

SD-WAN

SD-WAN is an essential element of SASE because organizations need to provision secure, flexible networking to people and devices who are spread out, geographically. A Network Security Associate who uses Cisco SD-WAN at VPS, a small software company, deals with this

reality frequently. He shared that he recommends Cisco SD-WAN for clients who have multiple locations and want to have a centralized management view of all activity. He observed, "Every architecture is moving towards the cloud. Centralized management makes accessibility easier for one person."

In his case, with SD-WAN they can know what is going on at a location and what is going into the devices. He said, "Whatever configuration changes are required, we can do them from one place. We don't have to go to the client's location. We also don't have to log in to different devices to do configuration or something like that. We can do it from one centralized management console."

❝

In terms of performance, it's absolutely best of breed, and world-class.

The financial services Executive Vice President of Operations and IT described Cisco SD-WAN as a solution for integrating services to enhance up-time, performance and lower costs, while the consultancy's Managing Partner felt Cisco SD-WAN was stable, with "very minimal movement and very minimal packet loss." He said, "There is very minimal delay in the network. In terms of performance, it's absolutely best of breed, and world-class. There is no discussion about that."

CONCLUSION

SASE is maturing, though its implementations vary according to organizational priorities and existing architectures. There is no one right way to do SASE, at least not yet. However, as users of the Cisco Umbrella and Cisco SD-WAN reveal, patterns and preferences are emerging. Users recognize that workloads are increasingly moving to the cloud, so one of the main keys to an effective SASE solution is support for hybrid and multi-cloud environments. Performance and architecture matter, as well. Each SASE element must work well on its own, and in tandem with the other core components of the model.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT CISCO

Cisco is driving the revolution of secure access everywhere.

Cisco's approach to SASE combines leading network and security functionality in a single, cloud-native service to help secure access wherever users and applications reside.

Learn more about Cisco and SASE here.