Unlocking SASE Protection for Mid-Market Organizations

1. What Is SASE

Secure access service edge (SASE) combines the offerings of Network-as-a-Service as well as Software-as-a-Service applications. Before SASE, many of these applications were accessed through a VPN or were hidden behind cloud security; however, SASE secures user access via integrated service capabilities, including SD-WAN and cloud native security functions (e.g., secure web gateways, cloud access security brokers, zero-trust network access and more).

As hybrid work models have increased, so has the need for SASE: endpoint users are now spread across main campuses, as well as branch and home offices, all of which are working through a unified data center to access the internet and SaaS. This exponentially raises your number of stress points and slows your company's internet traffic. It also increases exposure—when every endpoint user is utilizing a different form of security, your company's vulnerability increases. This is reflected in the data: according to a Gartner survey of 500 businesses, 45% of those polled cited reliable network performance as their number one challenge for hybrid work adoption.

2. Benefits of SASE

In contrast, what companies want is security that is simple and scalable across all endpoints. SASE creates multiple layers of security with less effort and fewer resources than traditional security solutions. This means fast user protection across your distributed network with simple, flexible deployment options and off-network protection. Because SASE enables secure, agile cloud transformation, it also allows for SSL decryption at a scale that is unachievable with on-prem hardware. The result is consistent, high-performance security for multi-cloud demands.

The bottom line is that SASE addresses critical modern business challenges, such as digital business transformation, edge computing and workforce mobility. With an efficient as-a-service model, you can efficiently deploy your resources and reduce your reliance on other applications. Effectively, SASE empowers your business to continue adapting to the future of security while accounting for the new landscape of diverse workforce locations. This means secure direct-to-internet access, cloud app usage and roaming users across any device, anywhere.

3. What Is Cisco+ Secure Connect?

Cisco has created a robust, end-to-end SASE solution by combining native Cisco Meraki® SD-WAN and Cisco SD-WAN (vManage). This single-provider solution integrates Secure Edge, Secure Client and Cisco Umbrella into one offering hosted on Meraki's cloud networking platform. In other words, it merges the industry's highest threat catch rate (96%) with a platform that hosts 3.5 million networks, 10 million devices—and counting.

The aim of this SASE solution is to increase network security protections while simultaneously lowering the barrier for entry. CISCO's SASE components have an overall emphasis on SD-Wan and Security Service Edge networking security. Your central campus, branch campuses and remote workers all need

coverage, which can increase the burden placed on your IT Team (assuming you have one to begin with). Cisco+ Secure Connect is a “set it and forget it” solution that limits that burden through ease of use and a quick window from purchase to operation. Plus, CISCO has engineered an easy setup to connect existing Meraki branches to Cisco+ Secure Connect as well as to add and remove sites. Furthermore, this subscription model ensures that companies do not need to juggle best-of-breed subscriptions.

Cisco+ Secure Connect also supports your overall network by allowing you to realize the full scope of its capabilities. The main piece of feedback CISCO has addressed from customers is the scalability of the system. CISCO services the bandwidth per branch on the backend to limit your overall latency. Additionally, when you add CISCO+ Secure Connect to your Meraki network, you stack application offerings. CISCO has built zero-trust security controls and remote access VPN specifically for this solution—CISCO Umbrella does not offer these applications by itself. They have also prioritized a secure web gateway with data loss prevention.

4. Overview of Use Cases

Secure Internet Access – This allows endpoint users to securely access applications from companies’ data centers/clouds as well as the internet and public applications. It also blocks malicious activity. Companies are able to apply policies to ensure least-privileged access private applications.

Secure Private Access – This allows users to access private applications through a cloud VPN, thereby enhancing internet security, private applications and IoT devices. It also enforces usage policies and manages access to public SaaS-based applications.

Site Interconnect – This allows for an efficiently operating network through native Cisco Meraki® Secure SD-WAN and Cisco SD-WAN (vManage) integration. Users and companies avoid bottlenecks with a dramatically simplified architecture that inherently links anything you connect to the SASE Fabric.

5. How Does Cisco+ Secure Connect Protect You?

The Cisco solution offers three main features that will increase your current SASE protection:

1. Comprehensive security controls: ZTNA, RA-VPN, SWG & DLP
2. Simplified and centralized visibility and management
3. Unified networking and security with traffic optimization

Here are some of the key protection feature highlights:

Clientless ZTNA Access: Makes it possible to leverage a web browser for remote access to private web-based applications. This is critical for situations where it is not possible to install Cisco Secure Client on a remote user’s device. Both the user and device are verified and validated before access is permitted.

Cloud Access Security Broker: Gives organizations insight into their overall cloud activity. Not only does this feature offer the ability to detect and report on any cloud applications in use, but it also provides information regarding current risk levels as well as the ability to block or control usage to reduce risk.

Data Loss Prevention: Scans all outbound web traffic and blocks sensitive data from external exposure or attacks. Cisco+ Secure Connect supports real-time rules that inspect web traffic and extend support for all cloud applications, along with SaaS API-based rules that scan data at rest in the cloud.

Secure Web Gateway: Logs activity, inspects web traffic and enforces acceptable internet use policies. All files are scanned, and any known bad items are blocked. If the SWG encounters new or suspicious files, it can route them to a sandbox for deeper inspection and retrospective alerts can be generated.

Traffic Steering: Determines what traffic is sent (inclusion) or not sent (exclusion) through the Cisco+ Secure Connect tunnel. When the tunnel is not active, this feature can send web traffic to Cisco+ Secure Connect for enhanced internet security for web-based applications.