

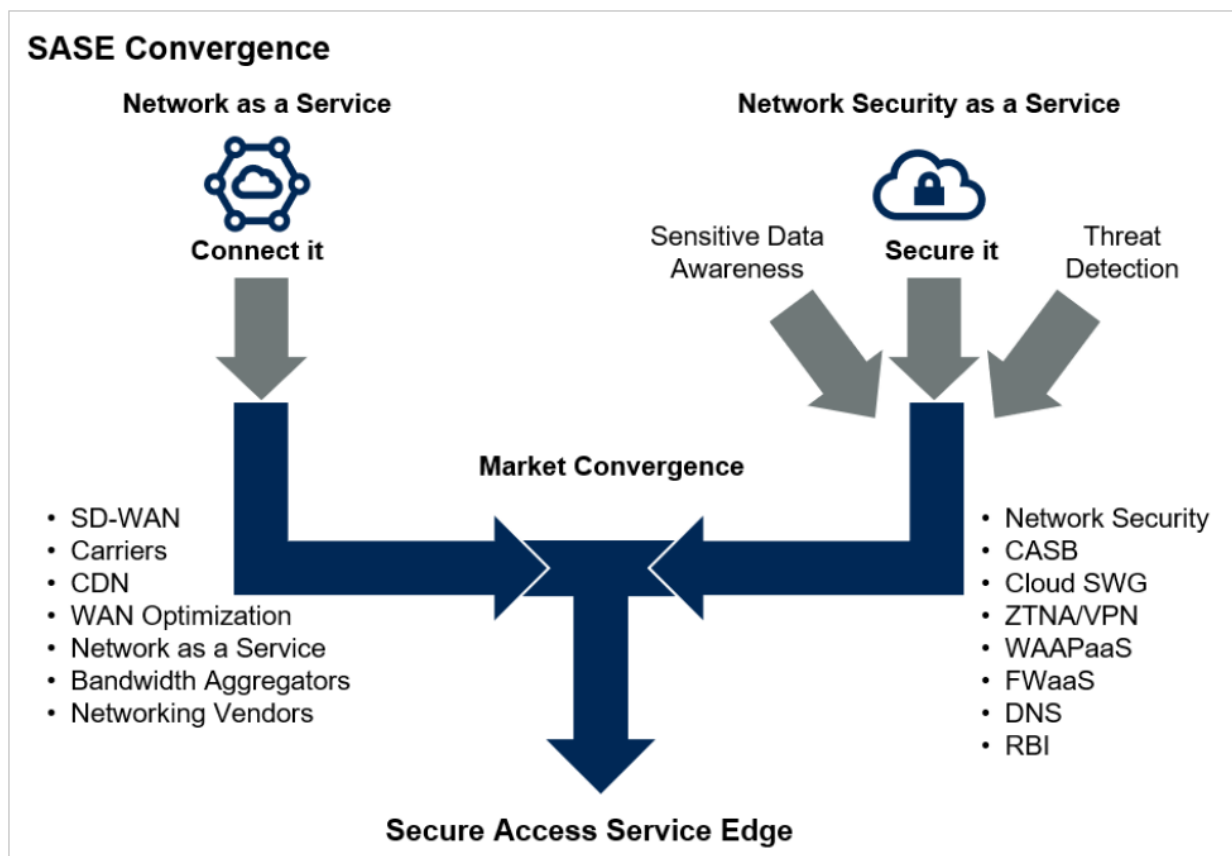
## SASE Architecture

October 21, 2021

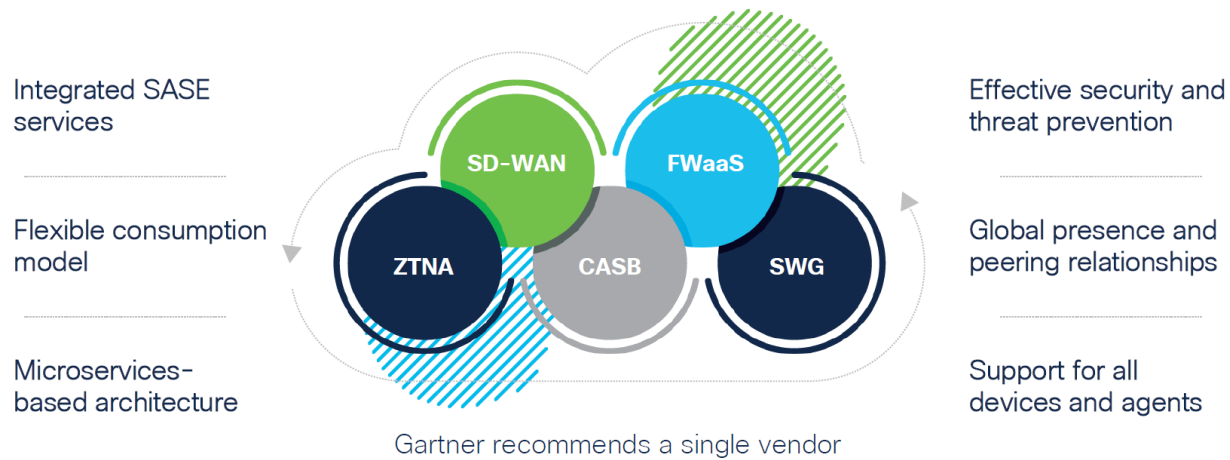
### Origins of SASE

In 2019, Gartner published a report called [“The Future of Network Security Is in the Cloud”](#). In this report, Gartner introduced the Secure Access Service Edge (SASE) concept. The SASE concept includes an even wider set of security functionality than a SIG, and it includes the convergence of networking functionality as well. A SASE solution can secure the cloud, data center, and branch network edges and deliver a secure SD-WAN fabric across disparate connections.

In that report, Gartner also shared their prediction that “by 2023, 20 percent of enterprises will have adopted SWG, CASB, [zero trust network access] and branch FWaaS capabilities from the same vendor up from less than 5 percent in 2019.”



## Realizing a SASE framework requires a long-term vision for consolidation



### Today's Challenges

We are now realizing the need for SASE. IT teams face a common challenge: how to securely enable the growing universe of roaming users, devices, and software as a service (SaaS) apps without adding complexity or reducing end-user performance - all while leveraging their existing security investments.

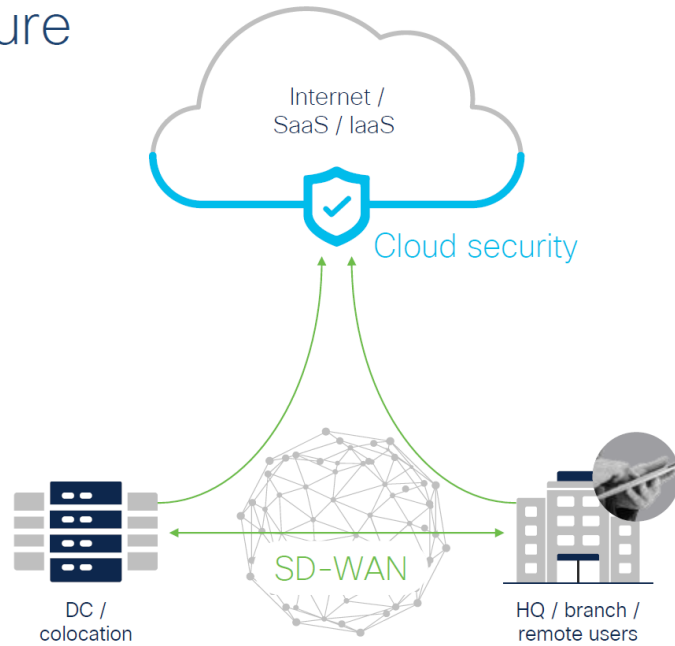
Likewise, users in remote and branch offices need the same level of network performance and security as users in central locations. IT must develop strategies to protect users - wherever they work and on any device they use - from a variety of threats, including malware infections, command-and-control callbacks, phishing attacks, unauthorized access, and unacceptable use, among others.

## SASE Architecture

Cisco addresses these challenges with three key pillars of [SASE architecture](#): **Connect**, **Control**, and **Converge**.

### Cisco SASE Architecture

- 1 Connect**  
Simple, automated transport from any user, any device, to any application
- 2 Control**  
Zero trust access control and leading threat protection
- 3 Converge**  
Cloud delivered, integrated networking and security



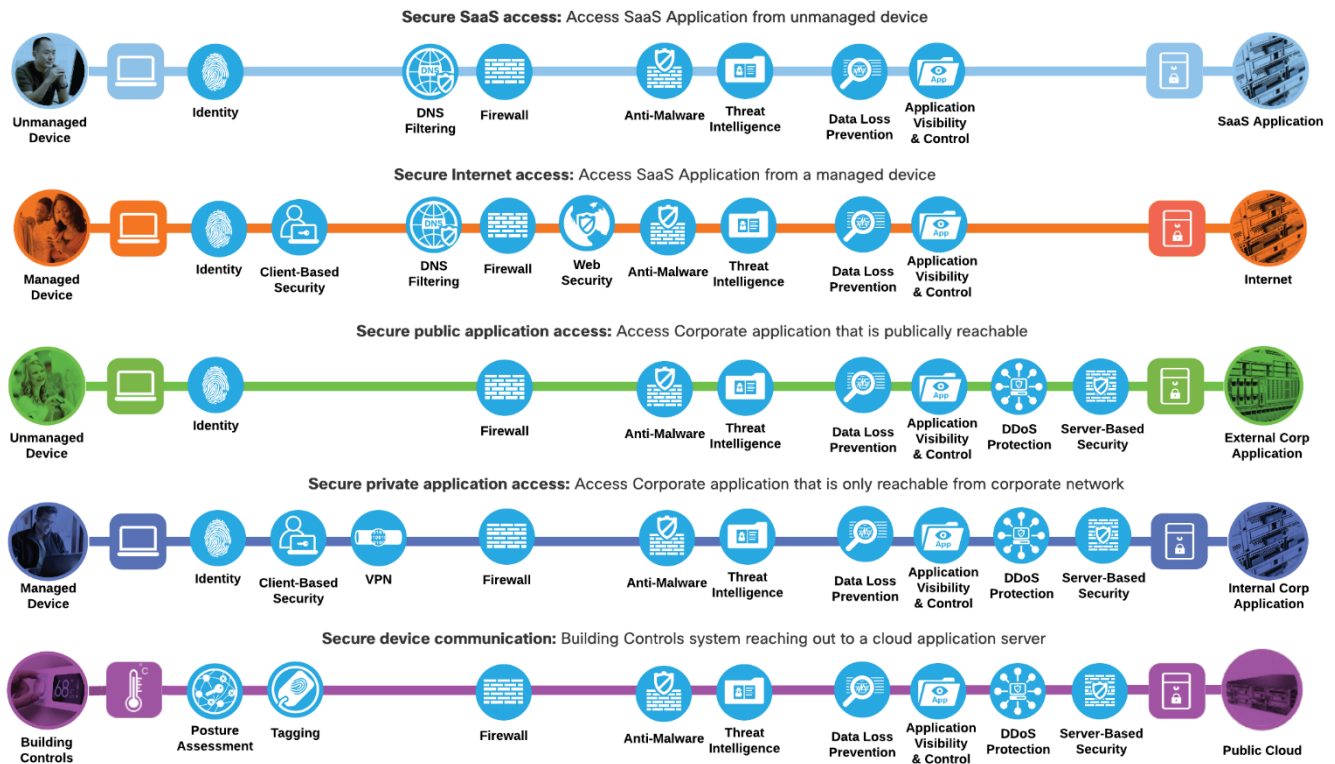
Below, you see how the Cisco products are mapped into a single package to realize the SASE architecture vision:

### Cisco SASE Architecture



## SASE Business Flows with Required Capabilities

Look at your business flow and compare it with the picture below. Ask yourself how your devices/users connect today when they are at campus or roaming and when they use corporate owned devices vs. personal devices.



If you don't see your organization with the correct flow, then that's something to be discussed with DSI and we can help you realize the SASE vision.

## Conclusion

If you have any questions or would like help with SASE, please reach out to your DSI account manager or email [sales@dsitech.com](mailto:sales@dsitech.com). They can put you in touch with me directly and we can discuss it further.

Thank you for reading and we look forward to discussing a new topic in the next newsletter!

## Resources

[“The Future of Network Security is in the Cloud” Gartner Report](#)

[Cisco Secure Access Service Edge \(SASE\)](#)

[The three C’s approach to SASE](#)

## About the Author

Ambuj M. is a Cisco Certified Internetwork Expert (CCIE) and Certified Wireless Network Expert (CWNE) with 15 years of industry experience. He currently works as a Network Solutions Architect for DISYS Solutions Inc. (DSI).