

Quick Answer: Does SASE Replace SD-WAN?

Published 28 December 2021 - ID G00759760 - 2 min read

By Andrew Lerner, Neil MacDonald

Most Gartner clients are planning for or deploying SD-WAN. There is also high client interest in SASE, and some security vendors are claiming the death of SD-WAN. This research helps guide I&O networking leaders to make the appropriate investments while navigating SD-WAN and SASE initiatives.

Quick Answer

Does SASE Make SD-WAN Obsolete?

- Short Answer: No, SASE includes SD-WAN. SD-WAN is not dead.
- SD-WAN can be either a stand-alone implementation, part of a single-vendor SASE offering or paired with a cloud-centric security vendor.
- Enterprises will need SD-WAN in order to support dynamic, application-centric traffic steering and rapid dynamic failover at remote branch locations.

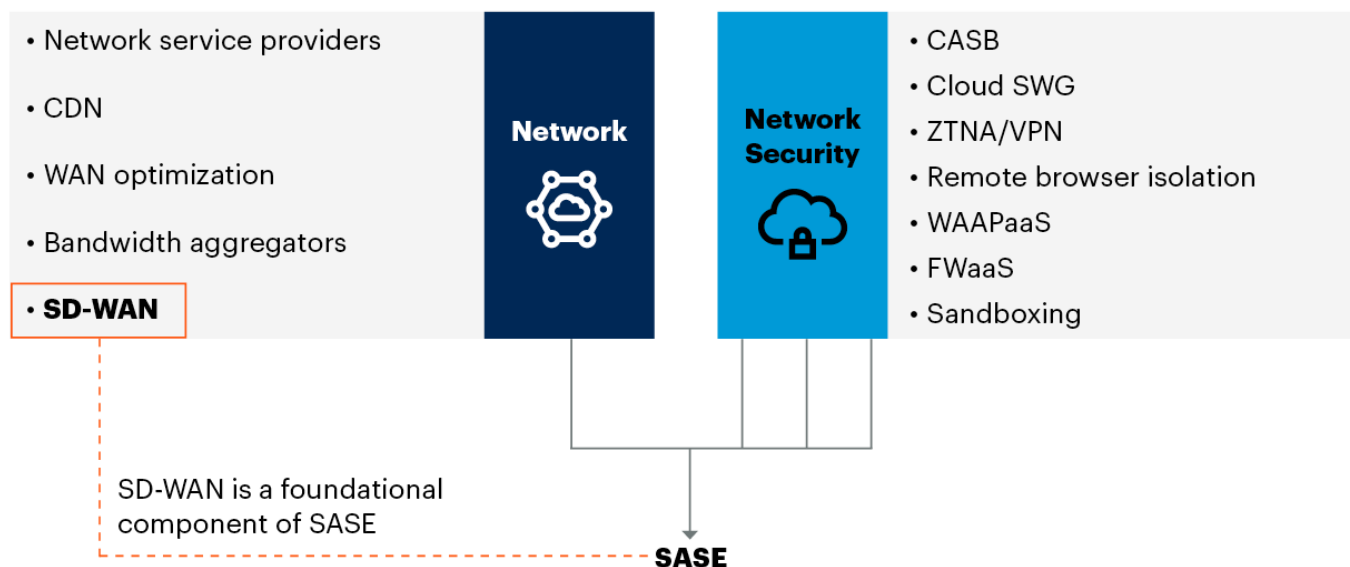
More Detail

Secure access service edge (SASE) connects and secures users, devices and locations accessing applications. Software-defined wide-area network (SD-WAN) products replace traditional branch routers. SASE does not make SD-WAN obsolete. Instead, SD-WAN is a foundational component of SASE. SASE offerings converge multiple network and security as a service capabilities, such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). See Figure 1 below.

Figure 1. The Relationship Between SASE and SD-WAN



The Relationship Between SASE and SD-WAN



Source: Gartner
759760_C

Gartner

A complete SASE offering requires SD-WAN. By contrast, SD-WAN can be implemented independent of SASE. There are both single-vendor SASE offerings and integrated multivendor SASE options in which SD-WAN products are integrated with a cloud security vendor. Not all of these vendor integrations are at the same depth. We recommend “tight integration,” which is less common in the market today, as it includes the following:

- Automated traffic routing and tunnel creation between SD-WAN device and cloud security POPs
- Automated deployment of resilient connections and associated dynamic failover
- Cross visibility between platforms to provide awareness into cloud security via SD-WAN console and vice versa
- Ability to consume and share security policies (such as segmentation) between SD-WAN and cloud security vendors
- Integration such that consoles are automatically opened with SSO

Is SD-WAN dead? Do I really need SD-WAN?

SD-WAN is not dead and most enterprises with branches will need SD-WAN products. Remote enterprise locations that require application-centric traffic steering with dynamic failover across multiple transports will best be served by SD-WAN products for at least the next three years. For locations where diverse physical connections aren't required or rapid dynamic failover isn't necessary, SD-WAN may be overkill.

Top Recommendations:

I&O leaders responsible for networking should:

- Align SD-WAN initiatives with cloud-security initiatives to avoid suboptimal selection and implementation by leveraging [2021 Strategic Roadmap for SASE Convergence](#).
- Continue existing SD-WAN rollouts but include how security will be refactored to a cloud-centric model as branch offices directly connect to the internet.
- Mandate that both networking and security groups are involved when refreshing or selecting products in the following markets: SD-WAN, SWG, ZTNA, CASB and firewall.
- Over the next three years, consolidate SASE implementation to a single vendor or to two explicitly partnered vendors (SD-WAN and SSE) that are tightly integrated.

Recommended by the Authors

[Critical Capabilities for WAN Edge Infrastructure](#)

[2021 Strategic Roadmap for SASE Convergence](#)

[Magic Quadrant for Security Service Edge](#)

Evidence

From the period of November 2020 through November 2021, Gartner analysts had over 800 interactions on the topic of SD-WAN and over 2,500 interactions on the topic of SASE.

**Learn how Gartner
can help you succeed**

Become a Client

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

[About](#) [Careers](#) [Newsroom](#) [Policies](#) [Site Index](#) [IT Glossary](#) [Gartner Blog Network](#) [Contact](#) [Send Feedback](#)



© 2022 Gartner, Inc. and/or its Affiliates. All Rights Reserved.