



# 5 Things SASE Covers that SD-WAN Doesn't

# SASE is on the Rise

More and more IT leaders are realizing that SD-WAN doesn't address the complete needs of the digital business. Gartner agrees with this and predicts a rapid shift to Secure Access Service Edge (SASE).



**By 2024, more than 60% of software-defined, wide-area network (SD-WAN) customers will have implemented a secure access service edge (SASE) architecture, compared with about 35% in 2020.”**

**Gartner**

Hype Cycle for Network Security, 2020

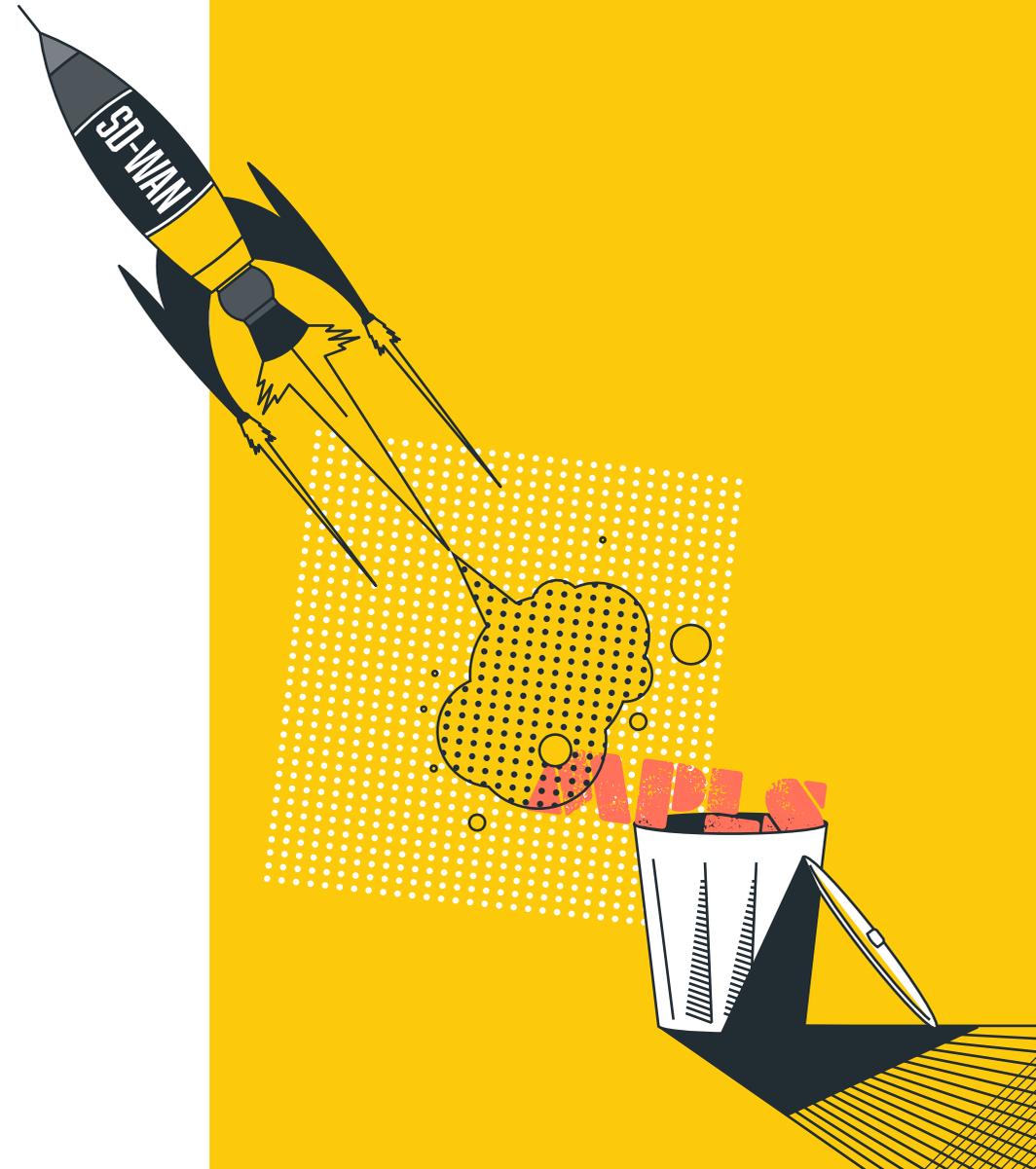
## Let's understand why...

# The Role of SD-WAN

SD-WAN emerged close to a decade ago, showing the potential to be a viable and cost-effective alternative to MPLS – thus making it the logical next step in WAN technology. SD-WAN was considered by many enterprises as the go-to-technology for preparing their network for the digital transformation.

At the time it made sense, because SD-WAN addresses the high cost, rigidity, and capacity constraints of MPLS. But, is this enough to deliver the level of network and security your enterprise demands?

To answer this, let's see what SD-WAN covers, and more importantly, understand what SD-WAN does NOT cover.



# How SASE Overcomes SD-WAN Limitations

Advanced Security

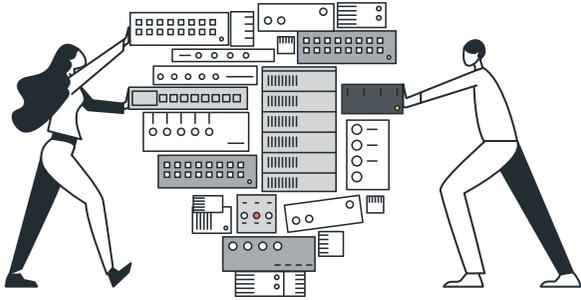
Remote Workforce

Cloud Readiness

Global Performance

Simple Management

# Advanced Security



## SD-WAN Shortcomings

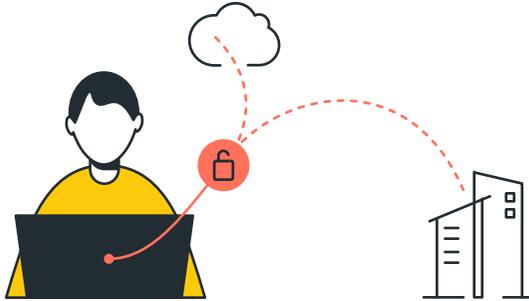
SD-WAN lacks integrated branch security, forcing IT to integrate additional security appliances such as NGFW, IPS, and SWG. This significantly increases the cost of SD-WAN deployments and complicates ongoing maintenance required for the many appliances.



## The SASE Approach

SASE's built-in network security stack delivers unified, enterprise-grade security to all edges, at all locations. There's no need to introduce and manage additional security appliances.

# Remote Workforce



## SD-WAN Shortcomings

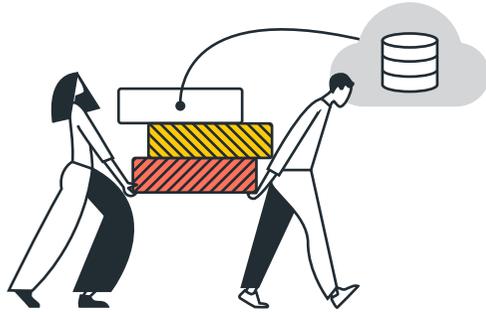
SD-WAN lacks support for remote users as it was designed to reduce spend on MPLS connectivity between physical locations only. Today, secure remote access is an essential pillar for guaranteeing business continuity, yet SD-WAN doesn't address this.



## The SASE Approach

Remote users, at all locations, dynamically connect to the nearest SASE PoP, benefiting from optimized and secure access to all applications, both on-premises and in the cloud.

# Cloud Readiness



## SD-WAN Shortcomings

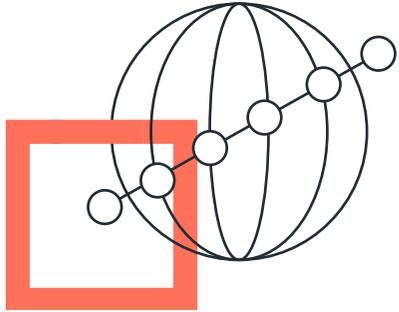
SD-WAN is limited in its cloud readiness. As an appliance-based architecture, SD-WAN requires the management and integration of proprietary appliances to add security and remote support, and expensive premium cloud connectivity solutions like AWS Direct Connect for optimized cloud connectivity.



## The SASE Approach

Cloud datacenters are connected to the SASE cloud as an integral part of the network, benefiting from all network optimization and security controls. Cloud applications require no integration, and application-specific traffic from any edge is automatically detected and sent to the PoP closest to the cloud instance serving the business.

# Global Performance



## SD-WAN Shortcomings

SD-WAN can't guarantee global performance without a private backbone. All SD-WAN players have had to integrate with third-party backbone providers to address this issue.



## The SASE Approach

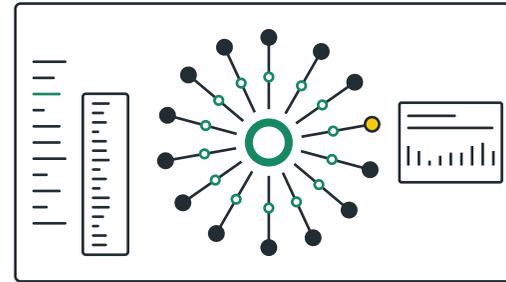
Optimal global performance is guaranteed everywhere through the SASE's global private backbone and built-in WAN optimization.

# Simple Management



## SD-WAN Shortcomings

SD-WAN and security solutions that aren't converged lack a single pane of glass for policy management. IT has to manage all functions separately, which makes troubleshooting and operations more complex.



## The SASE Approach

SASE converges all networking and security functions, enabling full visibility into the network, and simplifying management via a unified, enterprise-wide, centralized policy.

# SASE Takes Up Where SD-WAN Left Off

SASE creates a holistic platform that connects all edges to the network and security capabilities an enterprise requires. This lowers the cost, complexity, and risk of supporting the business in a dynamic environment. True SASE is the only architecture that allows you to move beyond the network complexity of today and prepare you for the opportunities of tomorrow.



**True SASE services are cloud-native – dynamically scalable, globally accessible.”**

**Gartner**

Hype Cycle for Network Security, 2020

## Learn more about Cato's SASE service

## How to Identify a True SASE Platform

Gartner defined essential capabilities a true SASE platform must provide:



### Converged SD-WAN and Security

SASE delivers network and security, including SD-WAN, SWG, CASB, SDP/ZTNA, DNS and FWaaS, all from a unified software stack with single-pass processing.



### Cloud-Native Architecture

SASE delivers elasticity, adaptability, self-healing, and self-maintenance capabilities, providing a platform that is always available and easily adapts to emerging business needs.



### Service Delivered via Globally Distributed PoPs

SASE PoPs need to be globally distributed, expanding their footprint to deliver a low-latency service to enterprise edges.



### Support for all Network Edges

SASE creates one network for delivering equal service to all enterprise resources: datacenters, branch offices, cloud resources, and remote users.

### Further explore the value of SASE

and learn how to easily differentiate between a True SASE Vendor vs. a SASE Wannabe, check out the resources below.



Answering the Top Questions About SASE Asked by IT Professional

[Read Whitepaper](#)



The Dark Side of SD-WAN

[Watch Webinar](#)



Why SASE is the Future of SD-WAN & Security

[Watch Webinar](#)



MPLS, SD-WAN, Internet and SASE

[Get the eBook](#)



SASE vs. SD-WAN: Achieving Cloud-Native WAN Security

[Read Article](#)



SD-WAN or SASE: The Power is in the Platform

[Read Article](#)