

SD-WAN and SASE security best practices

SASE and SD-WAN simplify IT operations, but how do you ensure security best practices? This quick reference guide highlights key considerations during selection and implementation.

Security basics

DO

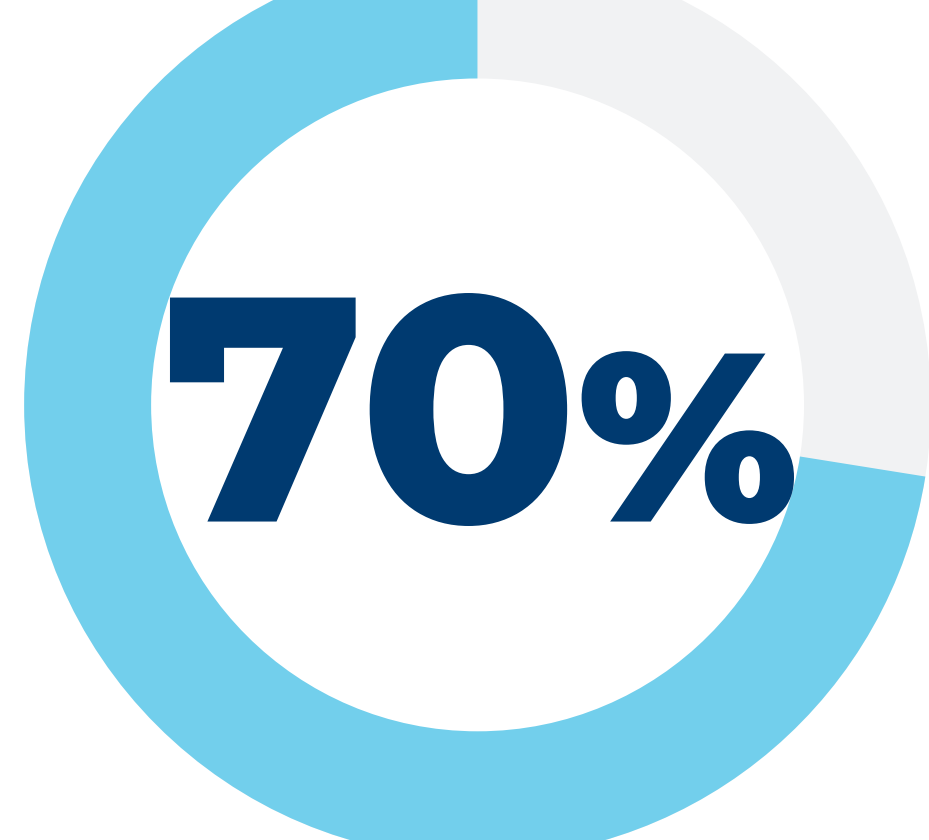
Update SD-WAN and SASE systems with the latest security patches after installation.

DON'T

Trust SD-WAN devices and technologies unless they come from well-known providers.

DO

Coordinate IT teams, as SD-WAN/SASE blur the line between network and security operations.



of IT executives consider security their **top factor** when selecting SD-WAN solutions

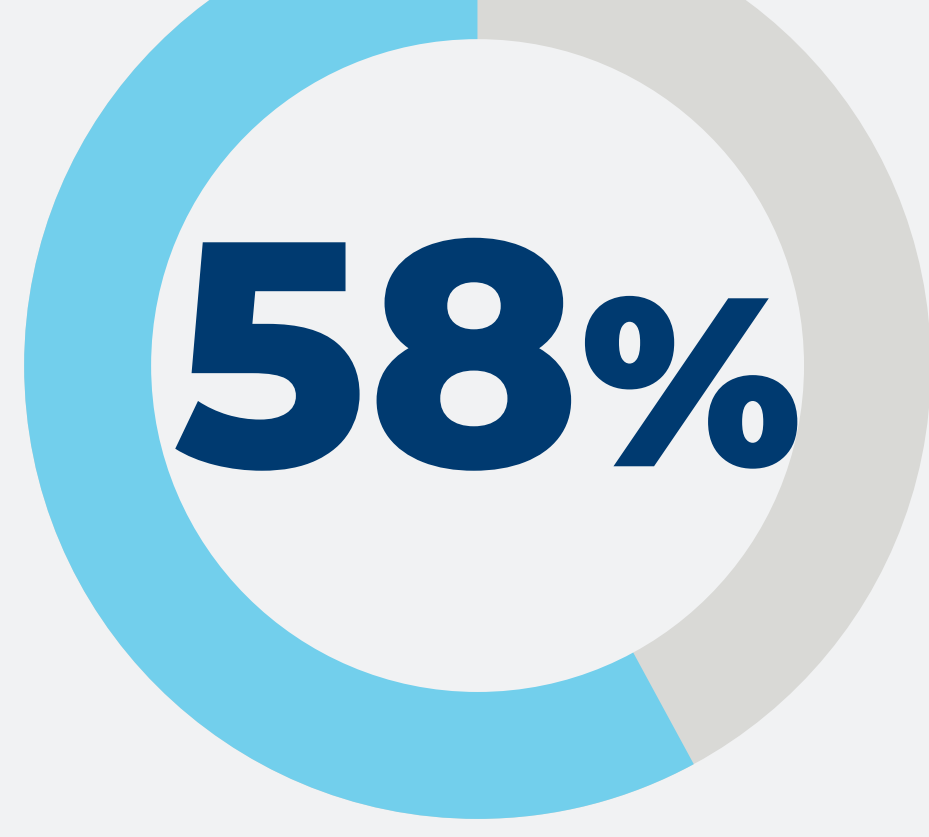
Source: IDG SD-WAN Market Trends Report

Internet security

Sidestep complexity
Secure internet breakouts and automatic encrypted tunneling require next-gen firewalls that should be built in

Ease management burdens
Use one tool to centrally administer firewalls and orchestrate security policies across all deployments

Avoid alert overload
Let your provider handle security alerts via a 24/7 threat detection and response service



of adopters expect to use a hybrid mix of both public and private connectivity for SD-WAN access

Source: Altman Solon 2021 State of SD-WAN Study

Using SD-WAN & SASE to achieve Zero Trust



Take a user-based approach
Identity analytics, deep network visibility, and shadow IT discovery tools aid in building Zero Trust architectures



Facilitate segmentation
SD-WAN facilitates network segmentation — look for flexible, unlimited capabilities that don't charge per segment



Enable hybrid work
All-in-one solutions should address connectivity at home as well as security for network, cloud, and endpoints



Protect endpoints and IoT
Extend protection to every device using both endpoint security technology and 24/7 detection and response services

91%

of IT leaders are interested in SASE solutions

76%

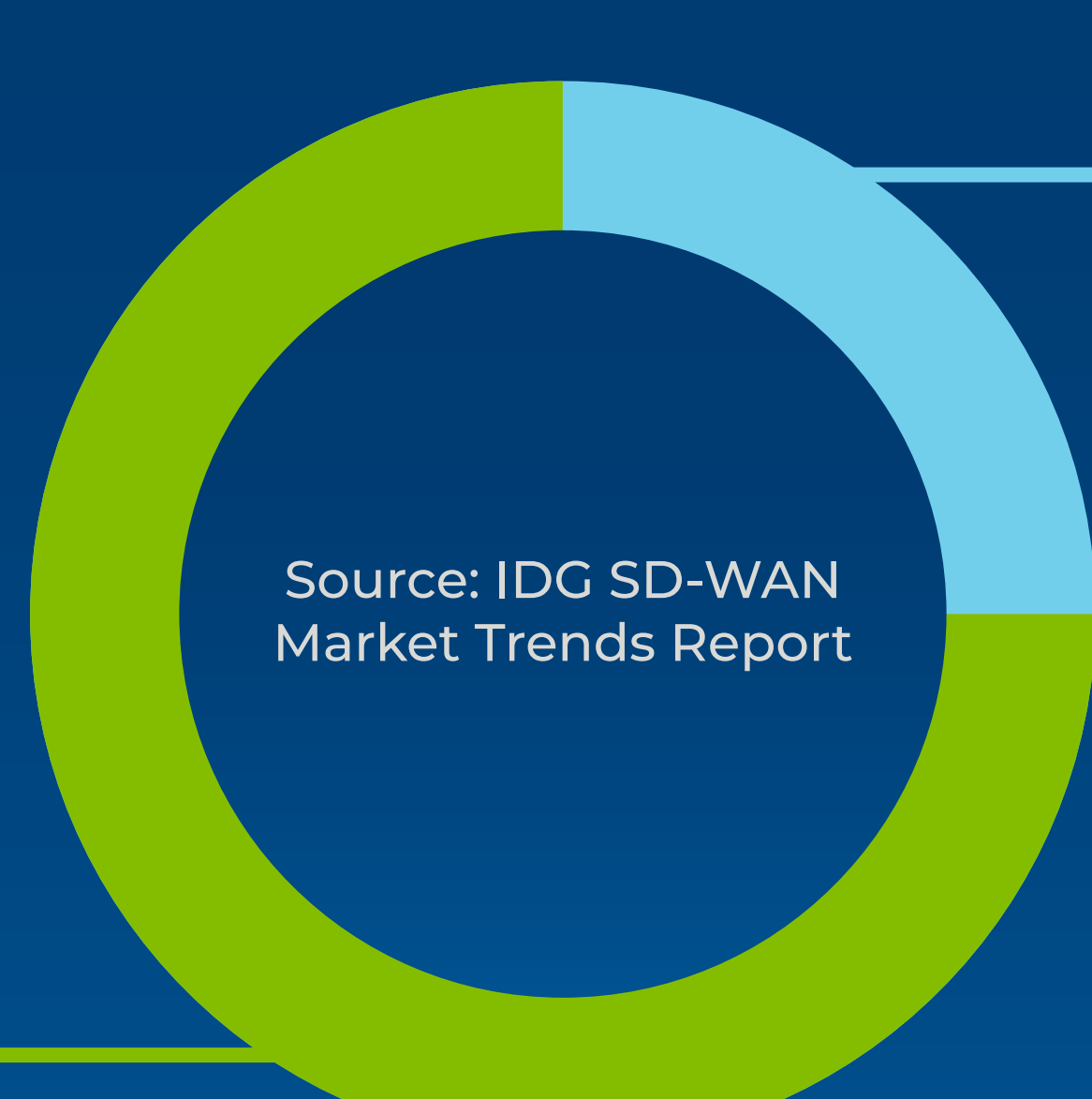
are in the process of implementing Zero Trust

Sources: IDG and Microsoft

Most prefer a managed service

75%

use managed or co-managed SD-WAN services



25%

take a DIY approach to SD-WAN

5 questions before you buy SD-WAN or SASE

- 1 Does your solution include next-gen firewalls with cloud and onsite deployment options?
- 2 Do you offer 24/7 managed threat detection and response services?
- 3 What technologies are included, and do they come from leading providers?
- 4 What network visibility and security analytics do I gain from the online portal?
- 5 What additional services can help me with network, cloud, and endpoint security?

