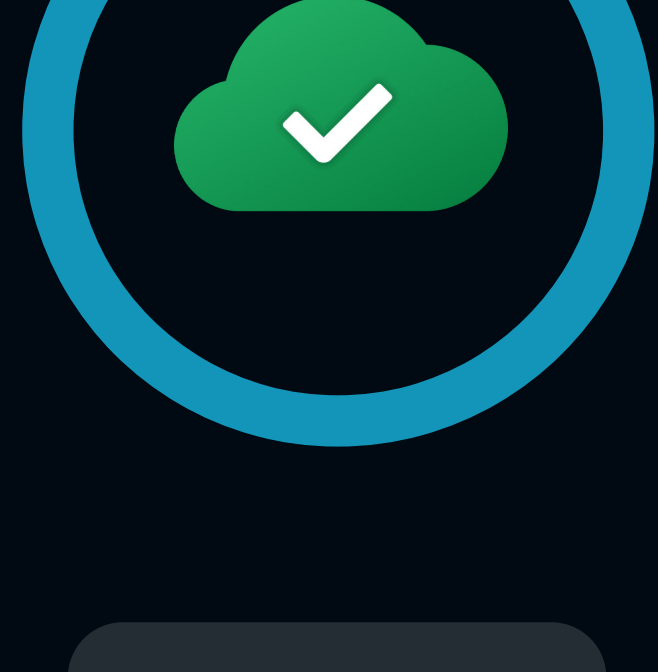


2021 SASE Trends

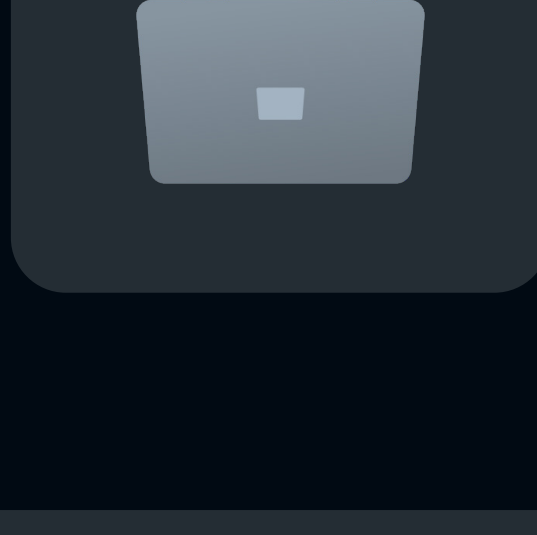
Plans Coalesce but Convergence Will Be Phased

The amount of interest in secure access service edge (SASE) architectures has exploded as organizations struggle using traditional, on-premises-based network and security solutions to support distributed, cloud-centric enterprise environments. The spike in newly remote workers pushed many organizations to a tipping point. At the same time, the broad applicability of SASE leads to some confusion about where to begin and which technologies are required, exacerbated by legacy organizational dynamics.

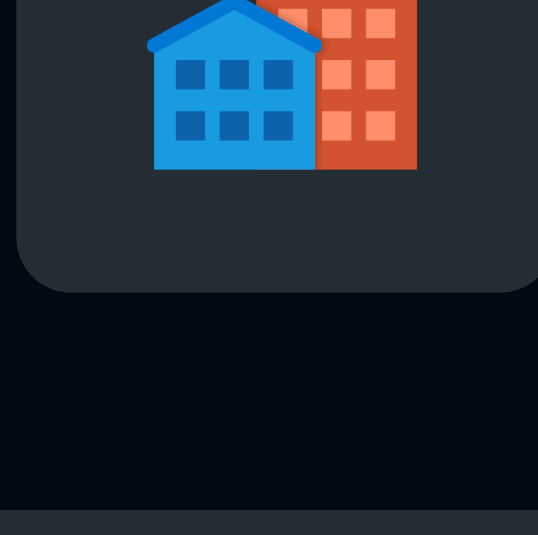
Hybrid work and public cloud drive new technology adoption.



98% use public cloud services (either IaaS or SaaS).



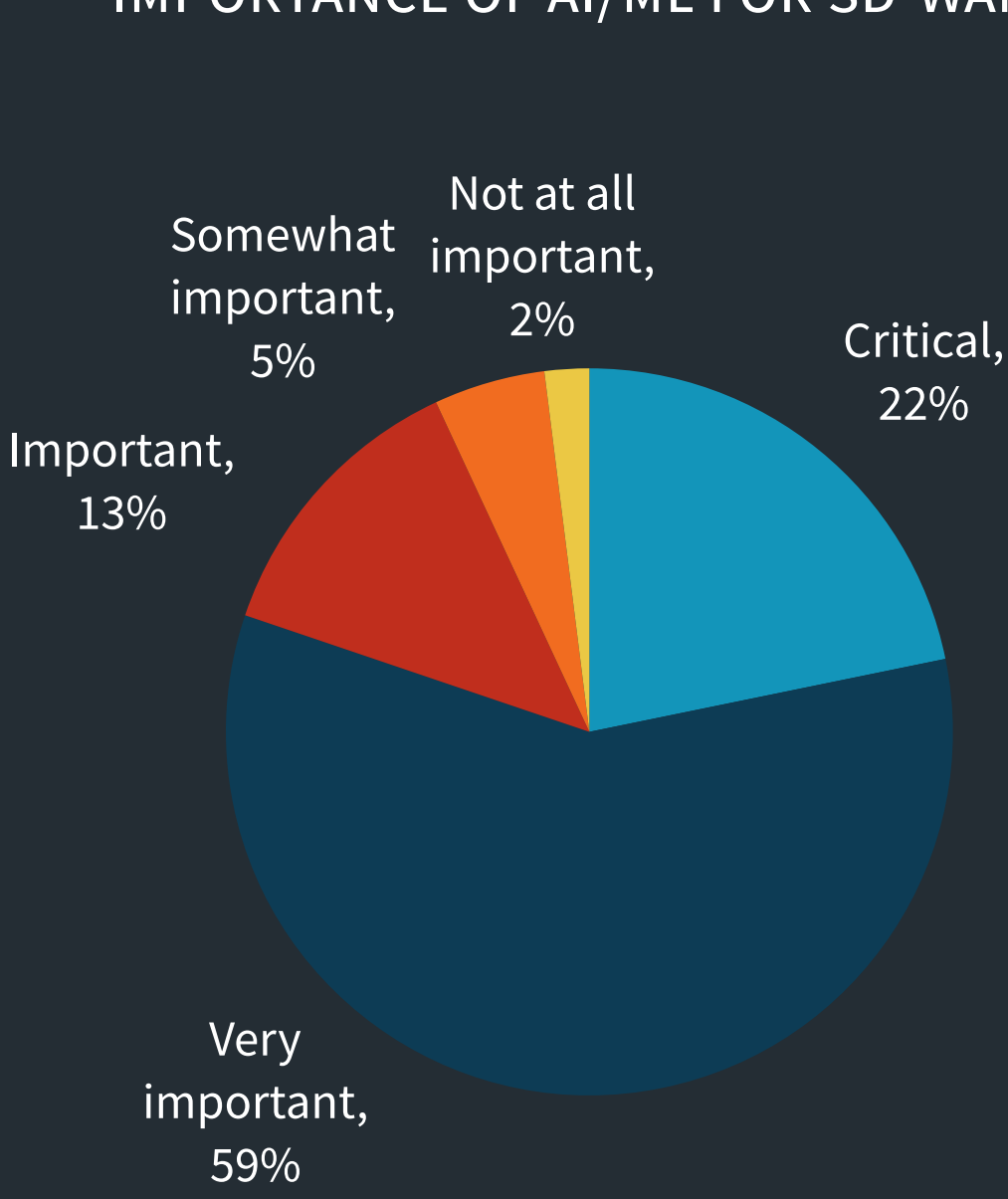
62% of employees will work remotely or in a hybrid manner.



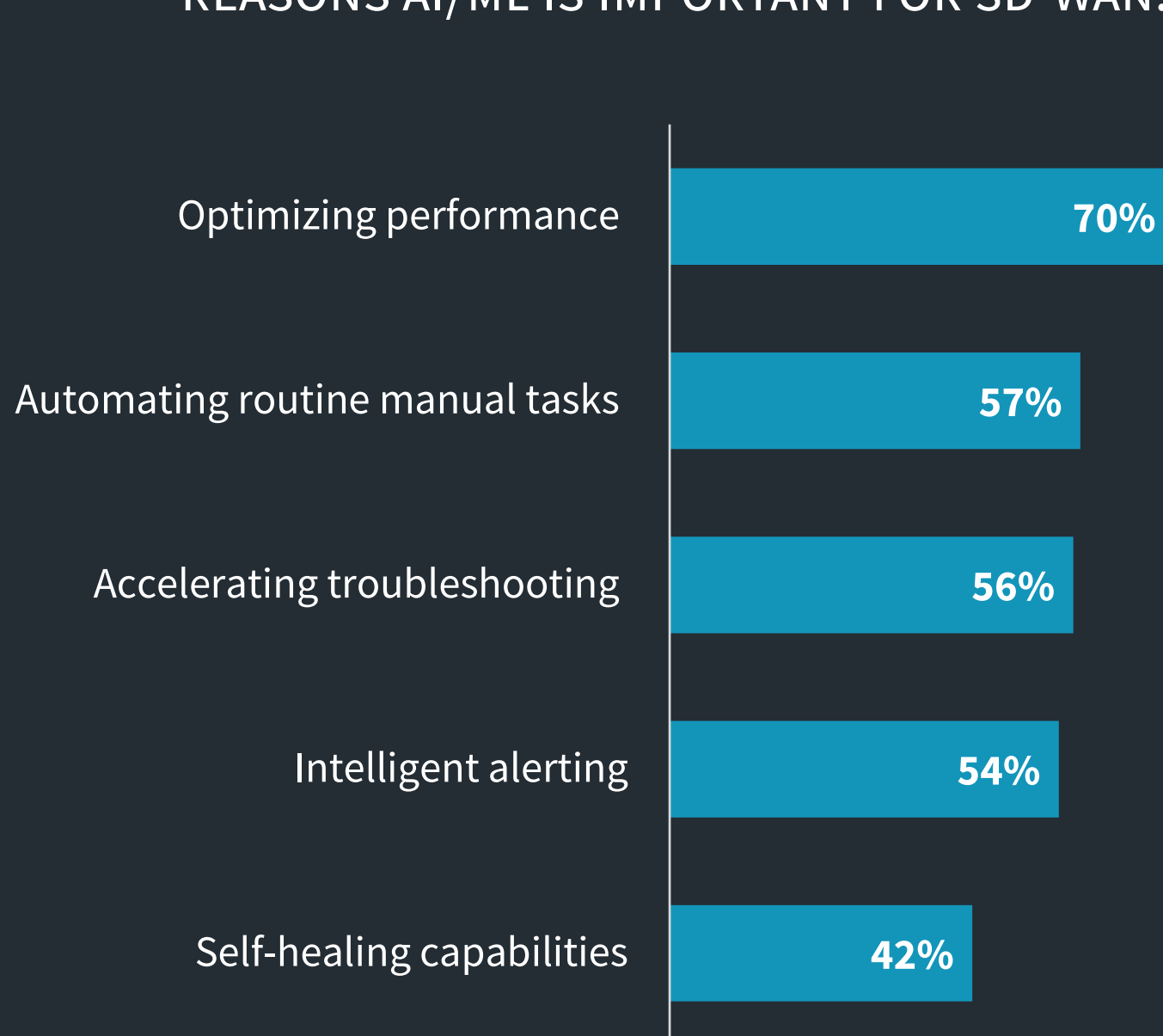
71% of organizations will support at least 25 branch or remote office locations.

Complex and distributed network environments require AI/ML for SD-WAN.

IMPORTANCE OF AI/ML FOR SD-WAN.



REASONS AI/ML IS IMPORTANT FOR SD-WAN.



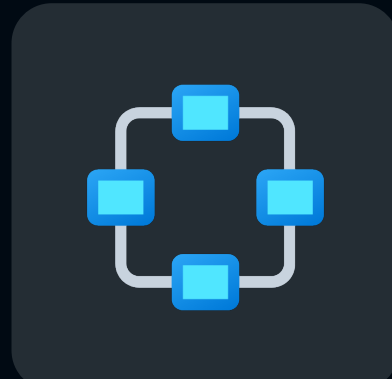
SASE convergence strategies will be targeted to start.

INITIAL APPROACH TO SASE:



48%

We will focus on the security aspect first



31%

We will focus on the network aspect first



21%

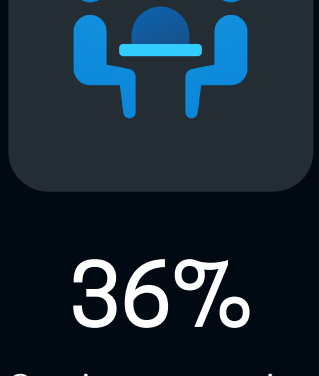
We will focus on both security and networking from the start

TOP 5 DRIVERS FOR EXPANDING SASE STRATEGIES.



37%

Long-term strategy to support work-from-home environment



36%

Getting executive support for SASE initiatives



34%

Getting company to approve training/skills required



33%

Getting internal agreement on a broader strategy



32%

Contracts ending/refresh cycles of the different tools/network connections

Divergent SASE approaches drive different functional needs.

TOP 10 TOOLS CONSIDERED STARTING POINTS FOR BUILDING OUT SASE.



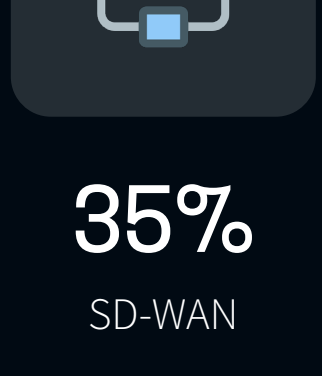
45%

Zero trust network access



37%

Data loss prevention (DLP)



35%

SD-WAN



34%

Secure web gateway



34%

Cloud access security broker



33%

Advanced threat protection/sandboxing



33%

VPN



33%

Next-generation firewall



32%

WAN optimization



32%

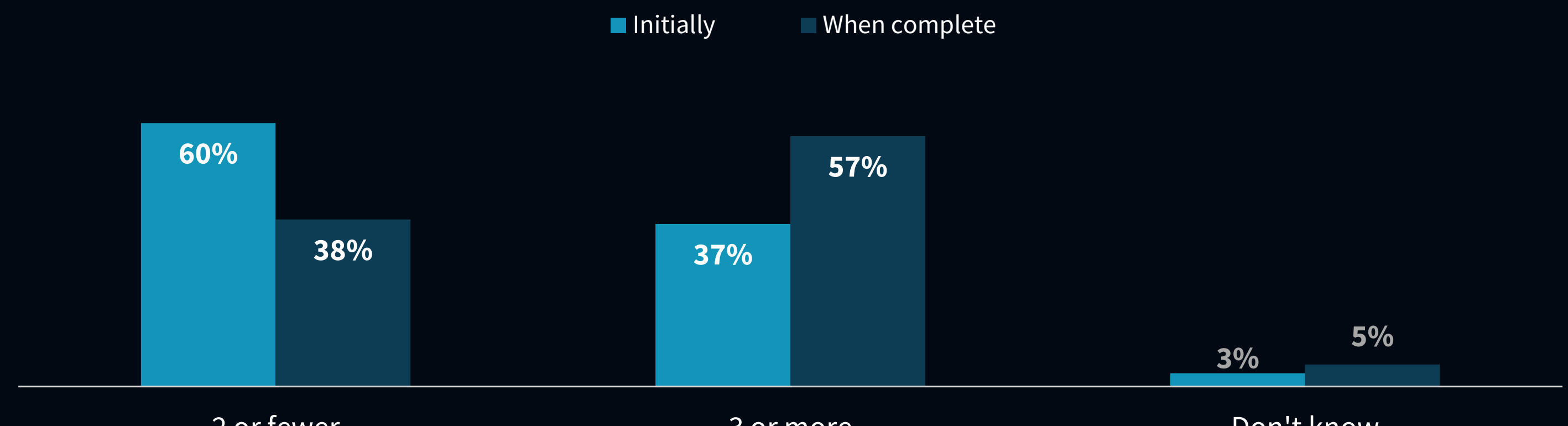
Firewall-as-a-service

TOP 5 CRITICAL SASE SOLUTION ATTRIBUTES.



Most envision a multi-vendor SASE approach to begin.

NUMBER OF SASE VENDORS.

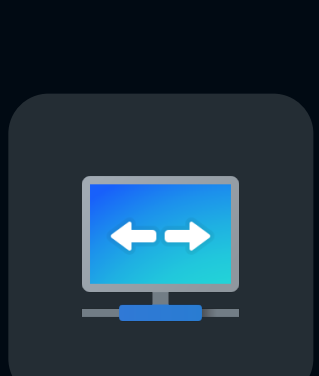


TOP 5 SASE VENDOR CRITERIA.



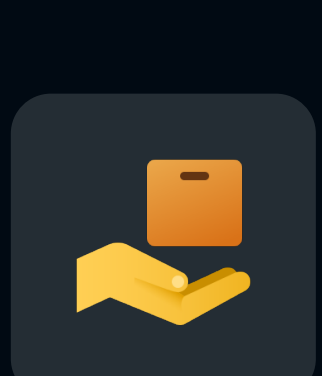
39%

Network security expertise



31%

Network expertise



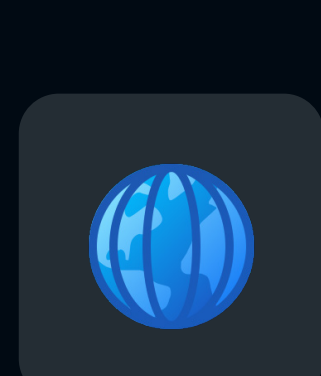
25%

Availability of managed services



25%

A strong history with cloud-delivered solutions



23%

A global network with strong latency/uptime SLAs

Early SASE adopters report benefits, but work remains.

TOP 5 BENEFITS SEEN BY ORGANIZATIONS IMPLEMENTING SASE.



38%

Faster network or security problem resolution



38%

Reduced security solution costs



37%

Ease of management



37%

Better alignment of network and security policies



37%

Fewer security incidents



45% will work with managed services providers to manage SASE solutions.

Improving internal alignment will be critical.

TOP 5 ROLES WITH INPUT INTO SASE PLANNING, EVALUATION, AND/OR DECISION MAKING.



90%

Senior IT management



77%

Senior security management



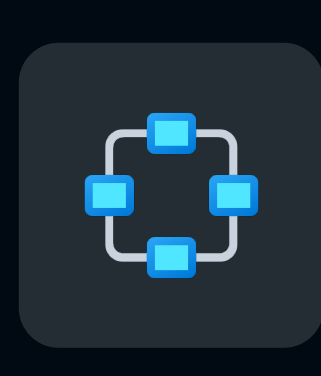
66%

IT operations



63%

Senior network management



60%

Network security team



48% say getting cross-functional agreement on SASE strategy and/or vendors is a challenge.

[LEARN MORE](#)

For more data and analysis from this ESG research study, as well as specific recommendations for IT organizations navigating these transitions, see our research report, *SASE Trends: Plans Coalesce but Convergence Will Be Phased*.