



The bridge to possible



2022 Global Networking Trends Report

Special Edition: The State of SASE and
The Rise of Networking as a Service (NaaS)



Special Edition:
The State of SASE





Contents

SASE introduction	04
IT's challenge	05
The relationship between SD-WAN and SASE	07
Desired SASE capabilities	09
The importance of integration	12
SASE adoption trends	15
SASE consumption models	17
SASE conclusion	18



Embracing a secure access service edge (SASE) strategy

Hybrid work demands a cohesive SASE strategy to deliver a consistent and exceptional user experience from anywhere.

To address rising interest and confusion in the marketplace surrounding secure access service edge (SASE), we've created this special addendum to the [2022 Global Networking Trends Report: The Rise of Network as a Service \(NaaS\)](#).

Driven by the sharp rise in remote work and hybrid cloud adoption, SASE (pronounced “sassy”) provides secure and seamless connectivity to any application, over any network, from any location or device.

SASE integrates networking and security functions into a unified, cloud-native solution or service.

In contrast to traditional security solutions, it pushes security policies and enforcement closer to end users and applications that have become increasingly distributed. It expands on zero trust and eliminates the need to constantly backhaul data to a data center, effectively reducing network loads and bottlenecks and providing a superior user experience.



As an alternative to a traditional security stack, it provides secure access from edge to edge, including the data center, remote offices, roaming users, and beyond.

This addendum highlights the latest trends and insights surrounding SASE, with data from multiple market surveys and perspectives gleaned from prominent industry analysts and experts. We hope this information helps you better understand the benefits and implications of SASE as you formulate your networking, security, and cloud strategies.

– Omri Guelfand, VP, Network Services, Cisco



“Confusion still abounds in the marketplace about what constitutes SASE. However, the emerging consensus is aligning well with our standing view that SASE is not a completely new technology but an integration of existing networking, such as software-defined WAN (SD-WAN), and security technologies, such as secure web gateways (SWG), into a cloud-based secure connectivity solution.”

– Dell’Oro Group¹






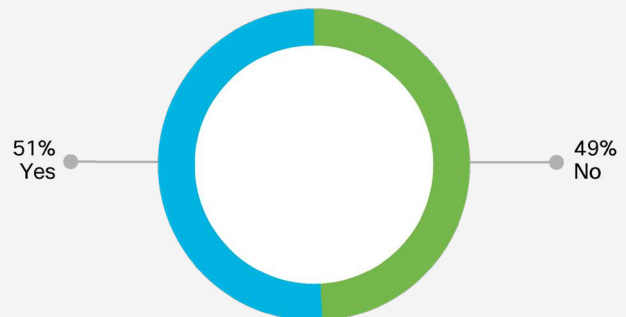
IT's challenge: Delivering a secure, cloud-first hybrid work experience

The two biggest trends IT teams are dealing with today are undeniably the continued transition to a multicloud application strategy and the adoption of hybrid work models. With users and applications more distributed than ever, the complexity of connecting and securing them has increased dramatically.

The distribution of applications across multiple private and public clouds is now amplified by the intense distribution of workers and workspaces resulting from hybrid work. With this hyperdistribution, the challenge of trying to maintain a high-quality, inclusive user experience stands in stark contrast to the once highly controllable on-premises enterprise environment.

In recent surveys, 76% of IT teams said that remote workers are harder to secure,² and 51% of organizations said they have had problems connecting workers to company resources over the past 18 months.³

   Have you/your company had trouble keeping employees connected over the last 18 months?



The ongoing transition from a data-center-centric application model to an internet-enabled cloud-centric model has forced IT teams to completely rethink their networking strategy. Likewise, security teams are struggling to provide a safe and seamless user experience when both users and applications are located off-premises, where they are more susceptible to accidental exposure or intentional attacks.

This helps explain the high level of interest in a cloud-delivered SASE model, which brings together networking solutions such as SD-WAN with cloud security solutions such as security service edge (SSE) and zero-trust network access (ZTNA).



SASE is intended to connect and protect users and applications wherever they are located or hosted, ultimately providing a better, more consistent, and more secure user experience. It also promises to reduce IT cost and complexity and improve network flexibility and performance and ultimately the application experience.



“At its 2020 apex, the pandemic drove a 450% increase in the number of U.S. employees working remotely full-time or occasionally compared to the pre-pandemic baseline. While rates have started to decline, we anticipate long-term remote work rates to settle at 200% above the pre-pandemic baseline.”

– Dell’Oro Group⁴



Bottom line:

An increasingly distributed and diverse workforce is here to stay. Implemented correctly, SASE connects and protects distributed users and applications, aligns network and security policies, and reduces the burden and risk of network and security management.



The relationship between SD-WAN and SASE

Marketplace confusion surrounding SASE has spawned a number of questions regarding existing SD-WAN solutions. Does SASE replace SD-WAN? Do they complement one another? Or are they altogether different solutions for different needs?

The answer is simple: SD-WAN is foundational to SASE.

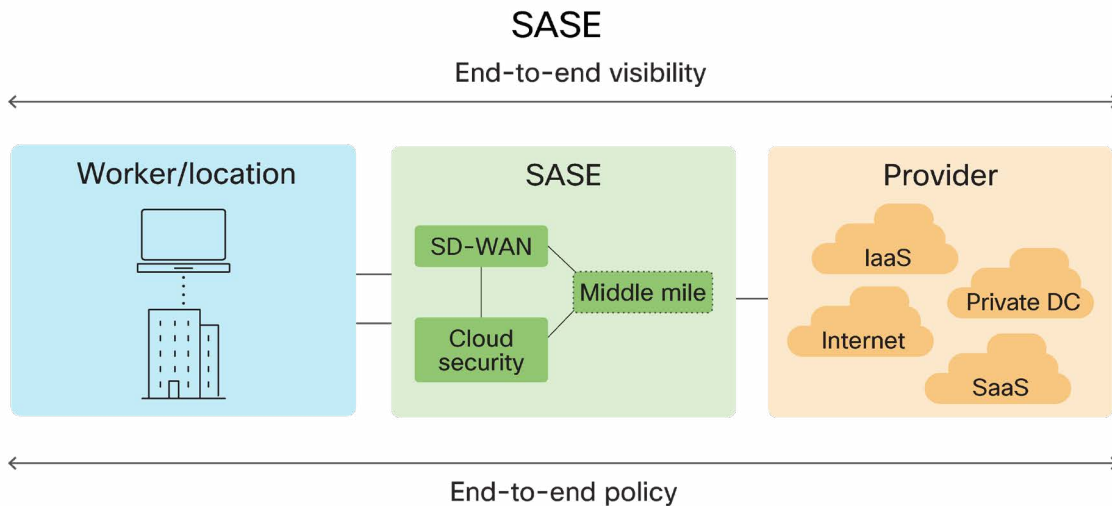
SASE combines the native security capabilities of SD-WAN with cloud-centric security to connect and protect users and applications no matter where they are located or hosted. As an overlay architecture, SASE cannot deliver ubiquitous security without the safeguards SD-WAN provides, including:

- Enabling Network Address Translation (NAT)
- Segmenting the network into multiple subnetworks
- Monitoring and blocking malware and malicious traffic
- Restricting unauthorized users
- Preventing unwanted content or applications
- Firewalling unwanted incoming and VLAN-to-VLAN traffic
- Securing site-to-site/in-tunnel VPN
- Geofencing for location-based access control



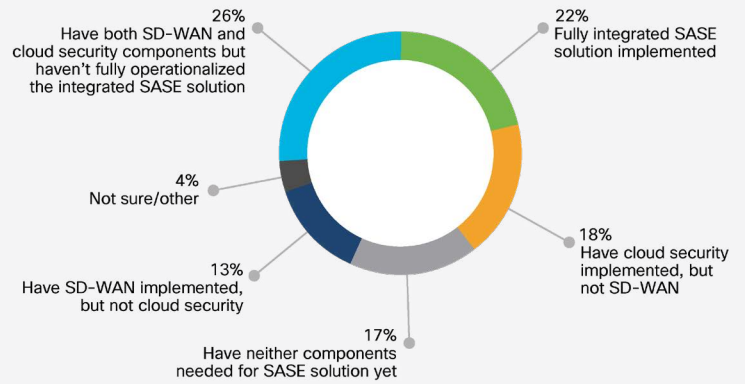
“SASE does not make SD-WAN obsolete. Instead, SD-WAN is a foundational component of SASE. SASE offerings converge multiple network and security-as-a-service capabilities, such as SD-WAN, secure web gateway (SWG), cloud access security broker (CASB), next-generation firewall (NGFW), and zero trust network access (ZTNA).”

– 2021 Gartner®, Quick Answer: Does SASE Replace SD-WAN?⁵





What stage are you at in your SASE adoption journey?



Cisco, 2021 Future of Technology Survey, N 29,506

Should IT organizations start with SD-WAN or cloud security? Many are taking a phased approach to SASE implementation. Most are in the middle of their SASE journey, with a combination of SD-WAN and cloud security components that have yet to be fully integrated or operationalized.

18% of companies have cloud security but no SD-WAN, and 13% have SD-WAN but no cloud security.⁶



Bottom line:

SD-WAN is a foundational element of SASE that works hand in hand with cloud-centric security solutions or services to protect users and data across on-premises, cloud, and edge domains.

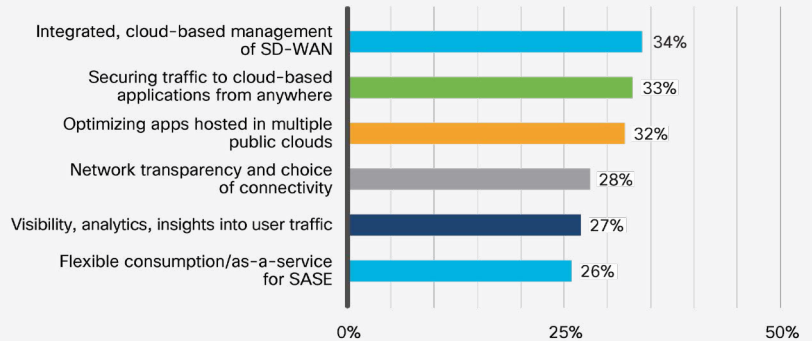


Desired SASE capabilities

With SASE representing the integration of network and security capabilities, 34% of organizations are prioritizing solutions and services that provide integrated, cloud-based management of SD-WAN. Securing traffic to cloud-based applications (33%), optimizing applications hosted in multiple public clouds (32%), and improving network transparency and flexibility (28%) have also been cited as top priorities.



In your opinion, which capabilities of SASE would be a priority for your organization?



Cisco, 2021 Global Networking Trends Survey; N 1534

To connect remote workers:

43%

43% of organizations are planning to use VPN as a service.

36%

36% are looking to adopt zero-trust network access and multifactor authentication capabilities.

35%

35% are interested in host-based unified clients.

35%

35% are looking to extend their SD-WAN to mobile and home users.



While SASE architectures, solutions, and services continue to evolve, they are fundamentally designed to bring together some or all of the core capabilities provided by SD-WAN and cloud security:

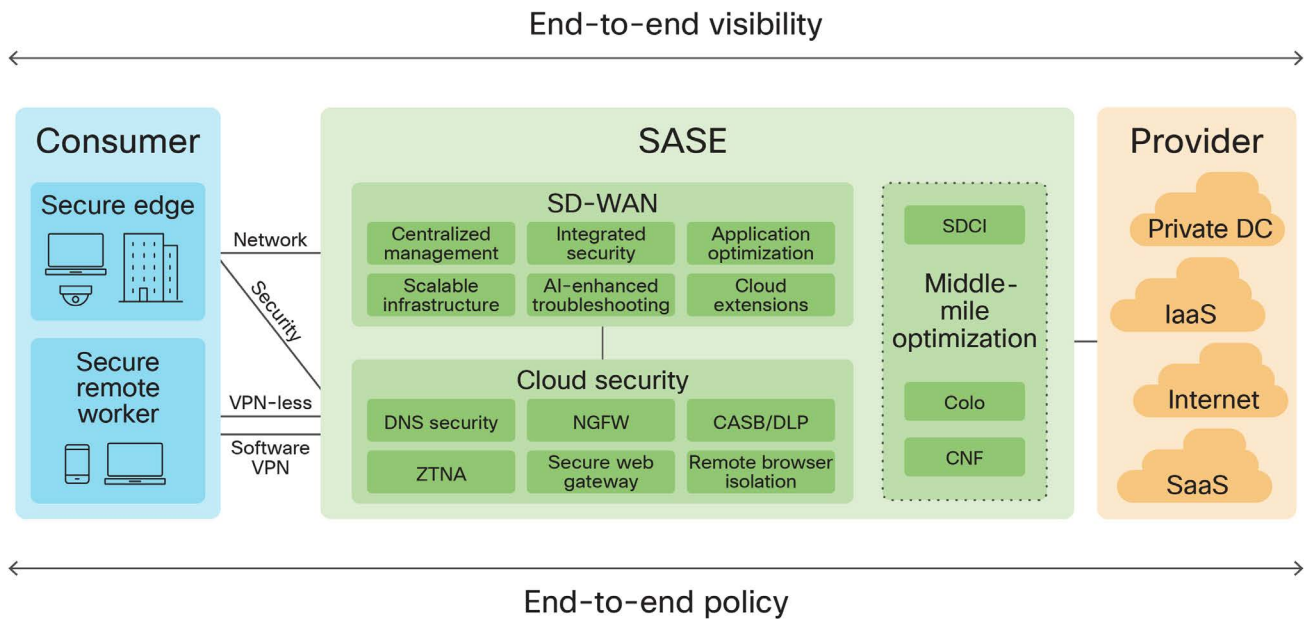
SD-WAN	Cloud security
<p>Centralized management A centralized, highly visual dashboard that facilitates device configuration, network management, monitoring, and automation. Includes zero-touch provisioning at the network edge.</p>	<p>Zero-trust network access (ZTNA) A security framework that mitigates unauthorized access, contains breaches, and reduces attackers' lateral movement across the network. ZTNA should be coupled with strong identity and access management to verify users' identity and establish device trust before granting access to authorized applications.</p>
<p>Cloud network extension and middle-mile optimization Extensive cloud on-ramp integrations to enable seamless, automated connectivity with any site-to-cloud and site-to-site configuration. Includes optimized middle-mile connectivity through software-defined cloud interconnect (SDCI) and colocation integrations.</p>	<p>Secure web gateway (SWG) A gateway that logs and inspects web traffic to provide full visibility, URL filtering, and application control and protection against malware.</p>
<p>Application experience The ability to monitor and validate the usability and performance of web applications. The detailed metrics and waterfalls show the sequential fetching and loading of web components to identify errors and bottlenecks and understand the impact on application performance.</p>	<p>Cloud-delivered firewall with intrusion prevention system (IPS) Software-based, cloud-deployed services that help manage and inspect network traffic.</p>
<p>Flexible and scalable infrastructure A wide range of physical and virtual platforms that deliver high availability and throughput, multigigabit port options, 5G cellular links, and powerful encryption capabilities. Optimizes WAN traffic by dynamically selecting the most efficient WAN links that meet the service-level requirements.</p>	<p>Cloud access security broker (CASB) Software that detects and reports on cloud applications in use across a network, exposing shadow IT and enabling risky SaaS apps and specific actions, such as posts and uploads, to be blocked.</p>
<p>AI-enhanced troubleshooting Robust AI/ML for optimizing network performance, automating routine manual tasks, and accelerating troubleshooting. Provides intelligent alerting, self-healing, and predictive internet rerouting capabilities.</p>	<p>Data loss prevention (DLP) Software that analyzes data inline to provide visibility and control over sensitive data being pushed or pulled beyond the organization's network or cloud.</p>
<p>Integrated security Robust security capabilities that work hand in hand with cloud security to protect branches, home users, and cloud-based applications from infiltration.</p>	<p>Remote browser isolation (RBI) Software that isolates web traffic from user devices to mitigate the risk of browser-delivered threats.</p>
<p>Identity-based policy management Microsegmentation and identity-based policy management across multiple locations and domains.</p>	<p>DNS-layer security Software that acts as the first line of defense against threats on the internet, blocking malicious DNS requests before a connection to an IP address is even established. Strong DNS security can greatly reduce the number of threats a security team has to triage on a daily basis.</p>
<p>Advanced insights Enhanced visibility into application, internet, cloud, and SaaS environments with comprehensive, hop-by-hop analysis. Enables the isolation of fault domains and provides actionable insights to accelerate troubleshooting and minimize or eliminate the impact on users.</p>	<p>Threat intelligence Threat researchers, engineers, and data scientists who use telemetry and sophisticated systems to create accurate, rapid, and actionable threat intelligence to identify emerging threats, discover new vulnerabilities, and interdict threats in the wild before they spread, with rule sets that support the tooling in your security stack.</p>



In addition to integrating SD-WAN and cloud security capabilities, SASE models can help break down operational silos and foster greater alignment between network and security teams. With standardized policies, shared telemetry, and coordinated alerts across all security and networking components, SASE enables NetOps and SecOps teams to improve IT efficiency, visibility, and protection.

With this in mind, it is important for organizations to have a comprehensive SASE strategy that accommodates both NetOps and SecOps goals, increases operational alignment, and is capable of supporting the organization’s needs for the foreseeable future.

SASE: Detail



“By 2024, 30% of enterprises will adopt cloud-delivered secure web gateway (SWG), cloud access security broker (CASB), zero trust network access (ZTNA), and branch office firewall as a service (FWaaS) capabilities from the same vendor, up from less than 5% in 2020.”

– Gartner⁷



Bottom line:

As they evaluate SASE strategies and offerings, organizations are seeking solutions and services that deliver the fundamental capabilities of both SD-WAN *and* cloud security to meet their current and evolving needs.



The importance of integration

Modern enterprises rely on a number of network environments (data center networks, local area networks, wide area networks) and security solutions (firewalls, gateways, and access control for on-premises and cloud-based systems). Through technology and service integrations, SASE can provide visibility, policy orchestration, and protection across all of them.

With the ultimate goal of securely connecting users and applications wherever they are located or hosted, these integrations also help:

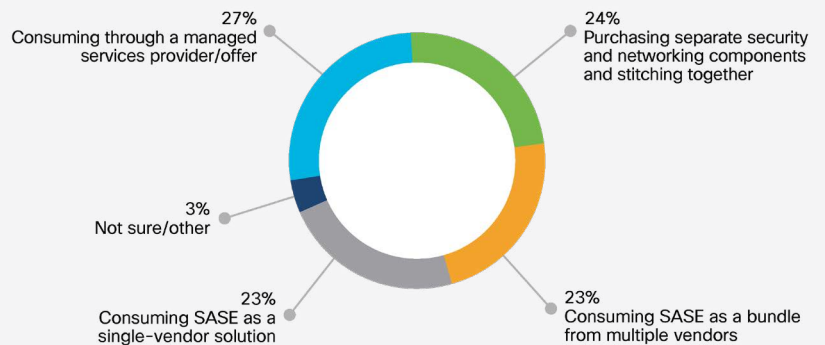
- Reduce the volume of security incidents.
- Accelerate troubleshooting and problem resolution.
- Simplify systems monitoring and management.
- Improve policy standardization and enforcement.
- Support regional compliance and data requirements.
- Reduce capital and operational costs.

“Two major SASE implementation types exist in the market, unified and disaggregated. The unified implementation consists of single-vendor, tightly integrated SASE platforms. The disaggregated implementation is a multiple-vendor or multi-product implementation with less integration in comparison to the unified variant.”

– Dell’Oro Group⁹



How will you deploy and operationalize your SASE solution?



Cisco, 2021 Future of Technology Survey; N 29,506

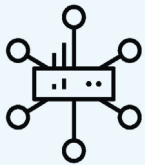


With the emergence of single-vendor and multivendor solutions and services, as well as the possibility of custom-built architectures that stitch together a number of point solutions, organizations have a number of options for how to deploy and operationalize SASE.

Because building and integrating a custom solution or operationalizing a multivendor SASE bundle can introduce unwanted complexities, operational challenges, and security vulnerabilities, many (50%) are seeking a unified and/or managed solution from a single vendor.

- 70% agree or strongly agree that it has become increasingly complex to manage a multivendor networking and security stack effectively.
- 26% have both cloud security and SD-WAN capabilities but have not fully operationalized and integrated them into a full SASE model.¹⁰

Whether it is a custom-built architecture, a multivendor bundle, a fully managed service from a single vendor, or a variation thereof, every SASE solution should provide better alignment and integration between:



SD-WAN and cloud security

- Automate the routing of traffic between the SD-WAN device and cloud security points of presence (PoPs).
- Automatically reroute traffic to an alternative PoP for resilience when there is a performance problem.
- Use AI-enabled predictive analytics to automatically reroute traffic to alternate PoPs before the user experience is impacted.



NetOps and SecOps teams

- Become able to continuously share security policies (such as access authorizations and segmentation) between SD-WAN and cloud security implementations.
- Allow data exchange between SD-WAN and cloud security management platforms to provide consistent visibility into policy and events.
- Extend and propagate enterprise network constructs (such as VPNs and Security Group Tags) and policies into cloud security platforms.
- Use single sign-on (SSO) administrative authentication across SD-WAN and cloud security management platforms.



End users and applications

- Enable direct connectivity between SD-WAN, middle-mile (such as SDCI), multicloud, and SaaS services.
- Monitor and optimize the user experience with full visibility and analytics across SD-WAN, cloud security PoPs, and IaaS/SaaS connections.



“It’s impossible to do networking well without integrating security. I need to look at security holistically, from the endpoint through the network all the way to the application. With network-as-a-service, I need the provider to take responsibility for the network and security. If they only take responsibility for the network, I need the visibility and control necessary to assure full protection and rapid threat mitigation. In the ideal state, the provider would do both networking and security very well.”

– Director of IT infrastructure, global consumer products company



Bottom line:

Whether custom-built or delivered from one or more vendors, SASE solutions and services should provide tight integration between SD-WAN and cloud security systems, to optimize a secure user experience and streamline NetOps and SecOps collaboration.

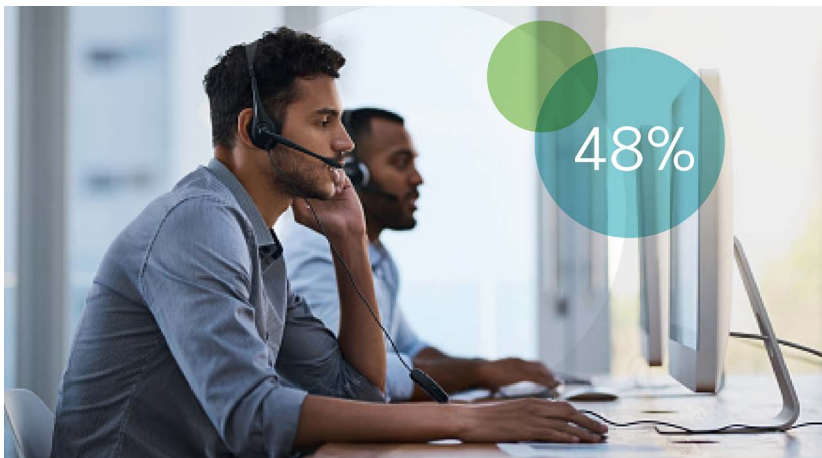
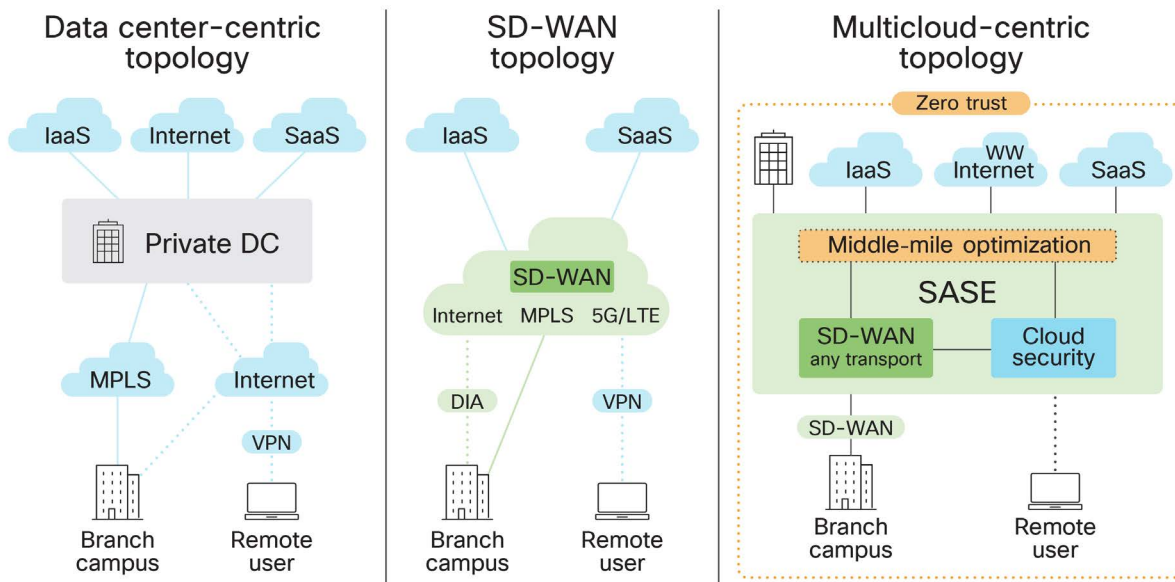


SASE adoption trends

As with any technology decision, the right SASE model and deployment approach will be unique for each organization. The network and security solutions already in place, as well as overarching operational strategies and business priorities, should be driving factors in any SASE decision. Critical initiatives, regulatory demands, mergers and acquisitions, supply chain operations, and business resilience requirements should also be considered.

Organizations migrating from a data-center-centric application model to a cloud- or multicloud-centric model may start their SASE journey with SD-WAN, for example, followed by middle-mile optimization and cloud security integration.

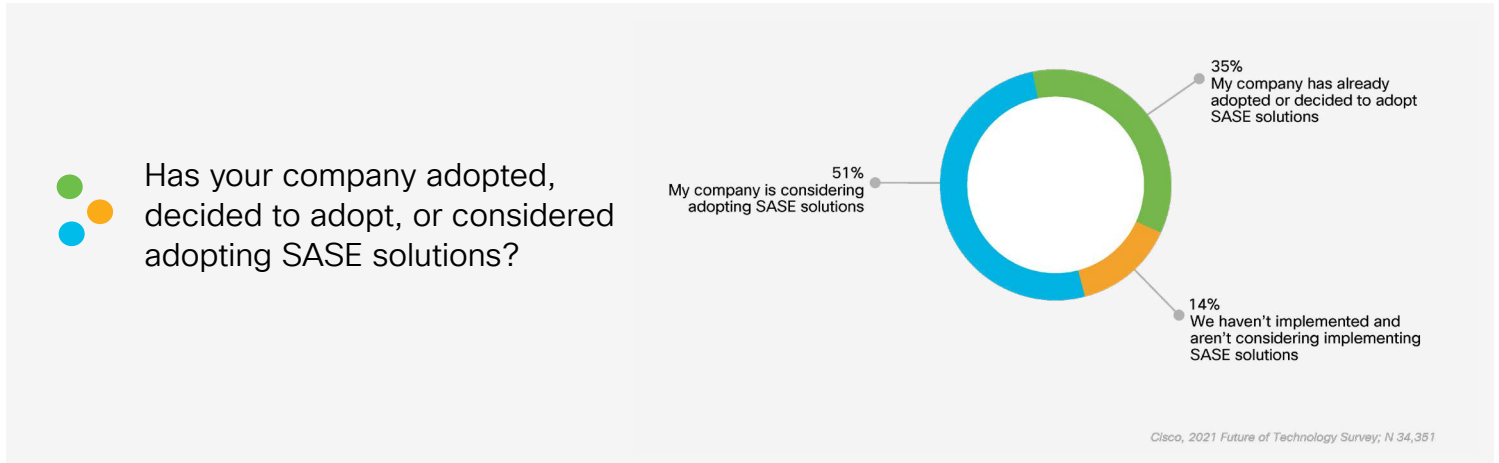
From DC-centric to multicloud-centric topology



48% of companies interested in SASE will start with security, 31% will start with the network, and 21% plan to address security and networking simultaneously.⁸



Regardless of the particular model or deployment approach, many companies say they are already well underway with SASE adoption: 86% of organizations are either considering adopting or have already adopted SASE.¹¹



“By 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020.”

– Gartner¹²



Bottom line:

SASE deployment approaches are influenced by existing infrastructure lifecycles, operational priorities, and business initiatives. IT teams should adopt a strategic planning approach aimed at incrementally building toward a complete SASE architecture.



SASE consumption models

There are three primary consumption models for SASE solutions and services. While these consumption models have varying impacts on internal teams and operations, all of them break down traditional networking and security silos. As a result, SASE can be a forcing function that improves operational alignment and efficiency.



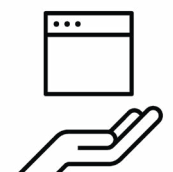
As a service

For those wanting fast deployment, minimal impact on operations and staff, and the reduced risk that comes with SLAs, SASE as a service provides a host of fully integrated, cloud-delivered capabilities with a single dashboard and full lifecycle support. 26% of organizations cite SASE as a service as their preferred consumption model.



Hybrid or co-managed

Organizations that are not yet ready for a full as-a-service model or that want more customization than those services provide can take a hybrid approach. This involves integrating cloud-based security capabilities with an existing SD-WAN solution and/or sharing network and security responsibilities with a managed service provider. These hybrid approaches provide additional security and support and allow IT teams to maintain a measure of visibility and control while reducing overall lifecycle management demands.



Highly customized or DIY

Organizations wanting full customization and control of their network and security footprint can build, integrate, and manage SASE capabilities on their own. This level of customization and control typically comes at the expense of speed and agility; requires additional lifecycle management of hardware, software, and licenses; and necessitates extra security and compliance specialists. This is a good option for organizations that have very specialized demands and an existing network and staff that can meet the architectural and operational requirements of SASE.

Read about our lessons learned in this [Cisco Secure Access Service Edge \(SASE\) Deployment Case Study](#).



Bottom line:

There are multiple SASE consumption models with varying operational impacts. The right model for each organization depends on a number of factors, including the size, skill sets, and bandwidth of the internal IT team and the prioritization of specialized needs, speed, agility, visibility, and control.



SASE conclusion

SASE architectures, solutions, and services provide secure connectivity between any user and any application, no matter where they are located or hosted. But the journey to SASE will be unique for each organization. The right model and approach will depend on existing technology investments as well as IT and business priorities.

Cisco and our ecosystem of partners can help address your unique network and security needs with the most complete, flexible, and resilient SASE solution in the market.

You can choose from our broad SASE portfolio that combines best-in-class networking, client connectivity, security, and unique internet observability capabilities to deliver the outcomes you need. You can also choose from a range of simple, flexible SASE deployment and consumption models that address a variety of situations and requirements.

Our highly available global cloud security infrastructure provides secure access wherever users and applications reside. And our market-leading SD-WAN solutions provide the agility and features needed to deliver consistently high-quality experiences for your users. Together, our cloud security and SD-WAN solutions provide the industry's most complete and uniquely integrated SASE capabilities.

Moving forward, Cisco is innovating around SASE at an accelerated pace through continuous integrations and continuous feature enhancements. We are evolving our offerings to provide the most flexible and easily consumable SASE services on your terms.

To learn more, visit the [Cisco SASE Resource Center](#).

Cisco was recognized as a Leader in the Gartner Magic Quadrant™ for WAN Edge Infrastructure for its ability to execute and completeness of vision.¹³



Additional resources and assistance

[Link to SASE Roadmap >](#)

[Find a Cisco Partner >](#)

[Contact Cisco Sales >](#)

Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER and MAGIC QUADRANT are trademarks and service marks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

SASE sources

1. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, September 2021.
2. The State of Security 2021, Splunk, February 2021.
3. Future of Technology, Cisco, November 2021.
4. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, September 2021.
5. Gartner Quick Answer: Does SASE Replace SD-WAN?, Andrew Lerner, Neil MacDonald, December 2021.
6. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service, Cisco, October 2021.
7. Gartner 2021 Strategic Roadmap for SASE Convergence, March 2021.
8. SASE Trends: Plans Coalesce but Convergence Will Be Phased, ESG Research Report, December 2021.
9. Advanced Research Report: SASE Market Forecast, Vol. 2, No. 1, Dell'Oro Group, September 2021.
10. 2022 Cisco Global Networking Trends Report: The Rise of Network as a Service, Cisco, October 2021.
11. Future of Technology, Cisco, November 2021.
12. 2021 Strategic Roadmap for SASE Convergence, Gartner, March 2021.
13. Gartner Magic Quadrant for WAN Edge Infrastructure, September 2021.



The Rise of Networking as a Service (NaaS)





Contents

Welcome	22
Key findings	23
A different networking model	25
Addressing challenges, delivering benefits	27
How NaaS changes network operations	29
Roles, responsibilities, and skill sets	31
Concerns and hesitations	33
Adoption trends	35
Choosing a NaaS provider	36
SASE and the different flavors of NaaS	38
Conclusion	40
Additional resources and assistance	40
About this report	41
Permissions for using this report	42



Welcome

Welcome to the *2022 Global Networking Trends Report: The Rise of Network as a Service (NaaS)*.

What a remarkable time we are experiencing, both as humans and as network professionals. Over the past year, IT leaders and network professionals have been tasked with enabling remote workers, protecting data across a more distributed computing landscape, and delivering new services for users, customers, and partners. Many businesses accelerated their digital transformation efforts to meet these new requirements, leveraging the cloud and software as a service (SaaS) for increased flexibility, agility, and speed.

In our [2021 Global Networking Trends Report](#), we highlighted the ways network technologies are being used to improve business resilience—regardless of circumstance.

In this year's report, we focus on an emerging trend that has big implications for the future: network as a service.

On the heels of increasingly popular as-a-service (aaS) models such as SaaS and infrastructure as a service (IaaS), NaaS will invariably change how many companies acquire, deliver, and manage their networking capabilities. To learn more, we spoke with 20 IT leaders and surveyed 1534 IT professionals in 13 countries about how they perceive NaaS, its strengths and limitations, and whether they plan to adopt the emerging network consumption model.

We hope the data, perspectives, and guidance in this report help you better understand the benefits and implications of NaaS as you evolve your networking strategies.

— James Mobley, SVP Network Services, Cisco



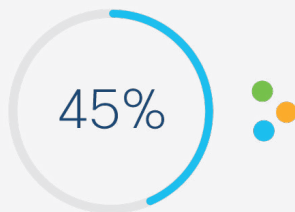


Key findings

It's no trivial proposition to completely transform the way you consume and operate your network. You need some good business and technology reasons to make this transition to an as-a-service model. And you also need trusted partners you can rely on to keep your organization humming. Still, many organizations are highly motivated to make the move. Here are some key findings from our 2022 NaaS research:

Key finding 1: Challenges

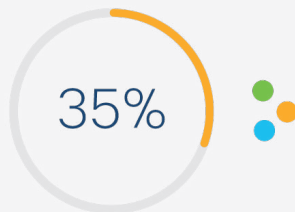
If resilience and agility are the question, for many, NaaS is the answer.



- Responding to disruptions (45%) and accommodating new business needs (40%) are cited as the top network challenges for 2021.
- At the same time, IT teams recognize the top NaaS benefit as freeing up IT teams to deliver innovation and business value (46%). Another 40% recognize NaaS as improving response to disruptions and 34% as improving network agility.

Key finding 2: Benefits

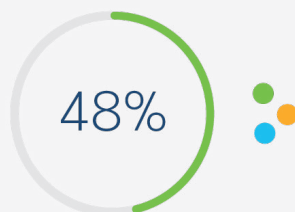
Big expectations—fast access to the latest technologies is the big prize.



- Technology continues to evolve faster than organizations can adopt it. Thirty-five percent of respondents recognize the requirement to continually deploy the latest networking technologies such as Wi-Fi 6, software-defined WAN (SD-WAN), secure access service edge (SASE), 5G, AI, and others as their top driver for NaaS.

Key finding 3: Operations

NaaS is great, but only if it helps the networking team meet service-level agreements (SLAs).

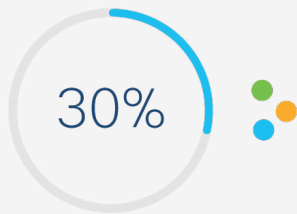


- The top services required from NaaS providers are network lifecycle management (48%), network resiliency (42%), and monitoring and troubleshooting to meet SLAs (38%).



Key finding 4: Concerns

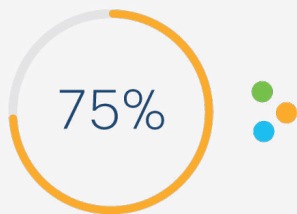
But it's not all smooth sailing; there are some concerns about giving up control and cost.



- Concerns range from whether NaaS can support unseen emerging demands (30%) to loss of security control (26%).
- The cost and disruption of transitioning also ranks high (28%).

Key finding 5: Roles

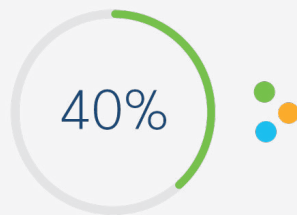
NaaS opens up new horizons for IT professionals, but they will need to up their game.



- More than 75% of organizations agree or strongly agree that NaaS will give IT teams opportunities to advance their skill sets.
- However, today only 1 in 4 organizations are likely to trust their own IT staff over a systems integrator, managed service provider, or NaaS vendor to translate their business needs to technical policies.

Key finding 6: Adoption

There are multiple ways to get started with NaaS, and one of them is SASE.



- SASE is a likely entry point to NaaS, since 40% of organizations cited multicloud access and 34% cited security as good fits for NaaS.
- Forty-nine percent of organizations plan to get started with NaaS during a refresh or upgrade cycle, and 34% said they would start by adapting an existing site.



A different networking model

After more than 18 months of disruption and adaptation, the role that network technologies play in business survival and success has never been clearer—or more essential. Already a key enabler of remote work, networks are now being asked to support safer workplaces, hybrid work models, and evolving business

operations. To do so, they need to work seamlessly across on-premises, multicloud, and edge environments. They need to provide a secure and consistent experience for all users, regardless of location, device, or method of connectivity. And they need to support both traditional and modern microservice-driven applications.

Because resources and bandwidth are often limited, many IT and networking leaders are investigating NaaS as an alternative way to address these challenges. But what exactly is it?

When we asked IT leaders for their definition of NaaS, it was quickly apparent that it means different things to different people. In fact, in our survey, a surprising 36% of respondents claimed they already have NaaS. While this may seem high for a nascent technology, from our interviews we realized that many consider themselves as having NaaS if any portion of their network is managed by a third-party provider. We believe this definition is far too broad and needs to be more specific.



NaaS is a cloud-enabled, usage-based consumption model that allows users to acquire and orchestrate network capabilities without owning, building, or maintaining their own infrastructure.



“Organizations are trying to determine the right mix of internal and partner-provided resources. Many are choosing to invest in their people, analytics, observability, and automation, and they’re thinking hard about how to leverage strategic vendors to offload infrastructure management and maintenance.”

– Mary Turner, Research Vice President, IDC



NaaS can provide an alternative consumption model for a broad range of network elements, including wired and wireless LANs, WANs, and VPNs, as well as branch, data center, edge, multicloud, and hybrid cloud environments. It can be used to deliver new network models such as SASE. It can enable shifts in organizational models, such as the move to hybrid work. And as an on-demand service, NaaS can allow IT teams to more easily scale up or down, rapidly deploy new services, and optimize the balance between CapEx and OpEx.

For some IT leaders with whom we spoke, NaaS represents a new and better form of networking that is greatly needed.

They recognize that they are falling behind and losing the confidence of their users. And they believe NaaS can help them attain the latest technologies, meet a growing set of requirements, and match the accelerating pace of business.



“With the level of networking complexity being so high, the speed at which businesses need to respond to market changes, and the extensive reach of modern networks, there are a lot of people realizing, ‘We just can’t do this anymore, and we need help.’”

– Mark Leary, Research Director, Network Analytics, IDC



Bottom line:

NaaS adoption is expected to grow at a compound annual growth rate of 40.7% from 2021 through 2027.¹

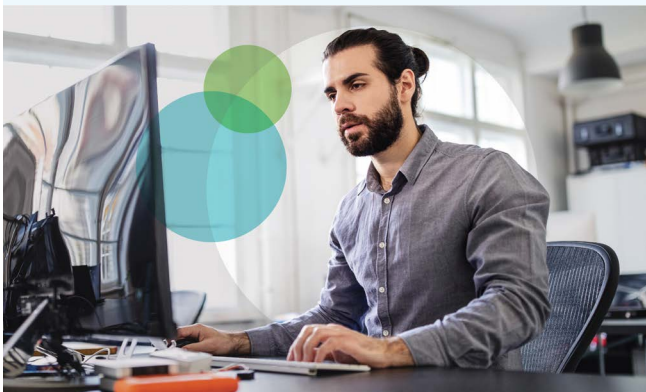


Addressing challenges, delivering benefits

Choosing whether to adopt a NaaS model ultimately comes down to the business and technology challenges it addresses, as well as the benefits it delivers.

For the organizations we polled, agility remains top of mind. When asked about the biggest business challenges their network must address, nearly 50% of IT pros said responding to disruptions and 40% said accommodating new business applications and business projects. More than one-third of respondents identified the need for network agility as a major driver for NaaS, and half of the respondents said they anticipate NaaS allowing them to deliver increased innovation and business value.

As part of their push to be more agile, many IT organizations are shifting their applications and services to the cloud, which can introduce new security, governance, and compliance challenges.

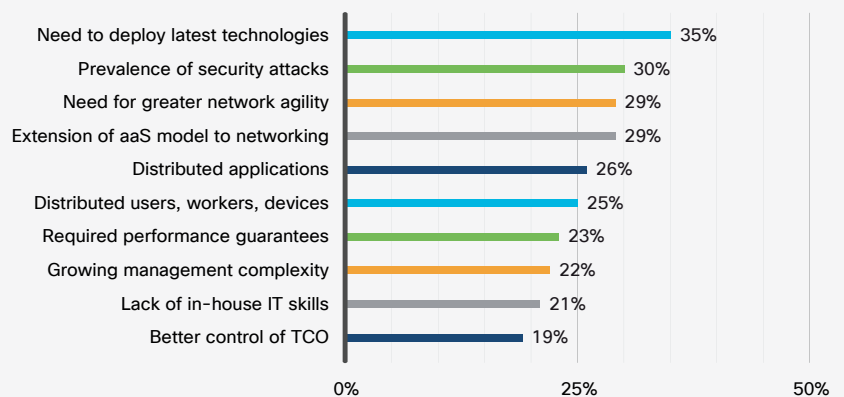


According to the IT pros we polled, the biggest technology challenges they are facing in managing their networks today are connecting to multiple clouds (36%); securing their network, users, and applications (34%); and identifying root causes and quickly remediating security or performance issues (31%).

At the same time, one-third of respondents identified the need to continually deploy the latest networking technologies (such as Wi-Fi 6, SD-WAN, SASE, 5G, AI, etc.) as a key motivation for moving to NaaS, and a third cited the ability to defend against security threats, which are becoming more frequent and sophisticated.



What would most likely cause your organization to move to a NaaS model?





“Our executives see no value in my staff configuring devices or operating infrastructure. They want IT thinking in terms of business objectives. Using outside services for basic operations allows my staff to get closer to business outcomes.”

– Director of IT infrastructure, global consumer products company

When we asked about the main benefits that IT pros expect from NaaS, primary decision makers cited the ability to focus on delivering business value instead of day-to-day infrastructure management.

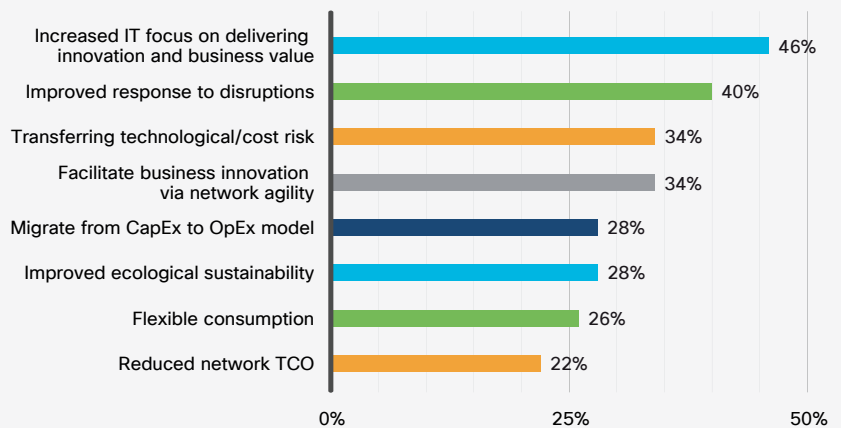
Improving the response to network and security disruptions was another highly rated benefit of NaaS, as cited by 45% of network practitioners and 40% of primary decision makers. While the prioritization of security improvements came as no surprise, we were interested to learn that more than 25% of network practitioners and 33% of primary decision makers identified improved ecological sustainability as a big benefit of NaaS.

Even more surprising was the low ranking of NaaS’s financial benefits.

With a flexible consumption model and subscription-based pricing, NaaS enables IT teams to shift from CapEx to OpEx spending and avoid large, recurrent investments in network infrastructure. Instead, spending becomes more consistent and predictable, and companies pay only for the resources they use. And yet these fiscal benefits were ranked much lower by IT leaders and network professionals compared to the agility, innovation, and management-offloading benefits of NaaS.



In your opinion, what are the top 3 business benefits that could be derived from using a NaaS model?



Bottom line:

TCO is low on the priority list when it comes to NaaS, because companies are far more concerned with delivering business value and quickly responding to disruptions. Sixty-eight percent of IT leaders agree or strongly agree that NaaS will free their teams from day-to-day network management, allowing more time to focus on delivering innovation and business value.



How NaaS changes network operations (NetOps)

A common concern we heard about NaaS is that it requires a complete handoff of network operations, giving all responsibilities to the NaaS provider and leaving nothing left for the organization's NetOps team to do. But the reality is, NaaS is not an all-or-nothing game when it comes to operational responsibility.

In a NaaS model, the provider takes responsibility for all aspects of network lifecycle management. That includes deploying, integrating, controlling, updating, monitoring,

and repairing all elements of network infrastructure—including any of their customer's on-premises equipment—required to deliver the contractual outcomes. Outcomes can include the number of connected users, sites, cloud providers, and applications, as well as the agreed-upon service levels, bandwidth, application performance, security provisions, compliance, and other requirements.

So what's left to manage? The NaaS customer's NetOps team will be able to focus more of their time on core or value-added activities.

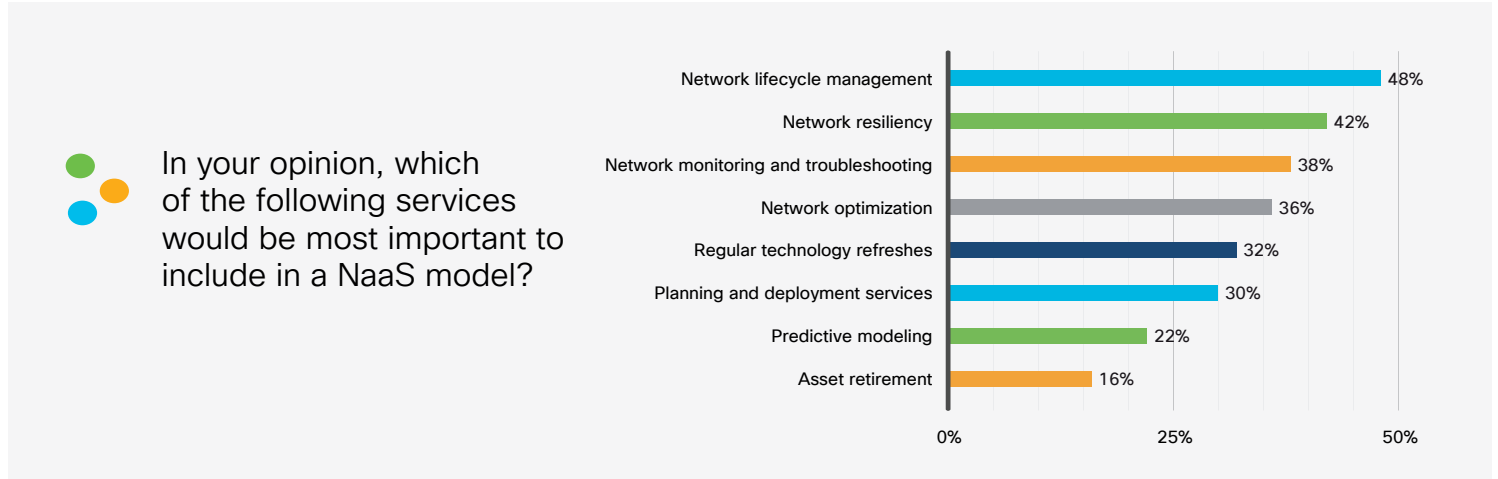
That might include, for example, defining and monitoring the desired network outcomes, such as user and application access policies and application performance levels. By monitoring network performance and insights, the customer's NetOps team can continually adapt and optimize network policies and behaviors across domains.



Using APIs, the customer's NetOps team can also manage the integrations between NaaS and their existing systems to streamline IT workflows and processes. And they'll likely want to work closely with the NaaS provider to ensure that SLAs and service-level objectives (SLOs) are being met. Regardless of operational responsibilities and handoffs, it's clear that IT professionals are keen to reduce the burdens of infrastructure management.



Forty-eight percent of the IT pros we polled said network lifecycle management is the most important service to include in a NaaS model. Network resiliency (42%) and network monitoring and troubleshooting (38%) rounded out the top three. This reinforces the notion that managing an increasingly distributed and complex mix of locations, users, devices, applications, and cloud resources leaves too little time for value-added activities and innovation.



“The provider handles the day-to-day minutiae. The internal team can then focus on adding more value through the network by addressing new requirements coming alive. Our engineers and technicians don’t need to stop to solve problems. They can focus on new projects.”

– Senior network engineer, global consulting firm

Bottom line: Operational responsibilities are shared in a NaaS model. The burden of network lifecycle management moves to the provider, allowing the customer’s IT team to focus more on operational activities that contribute business value.



Roles, responsibilities, and skill sets

In shifting infrastructure maintenance and lifecycle management responsibilities to the provider, NaaS frees up a considerable amount of time. And it enables the customer's NetOps team to focus on desired network outcomes rather than the technological and operational aspects of maintaining the infrastructure.

In other words, network engineers shift from “flying the plane” to “calling the shots in the control tower.” But what types of shots do they anticipate calling?

According to our respondents, 27% believe their IT staff would leverage their technical expertise—and a NaaS dashboard—to translate business needs into network policies. A surprising 73% of respondents said they would prefer third-party providers to carry out this business-critical role, possibly indicating a perceived shortage or lack of confidence in internal skill sets.

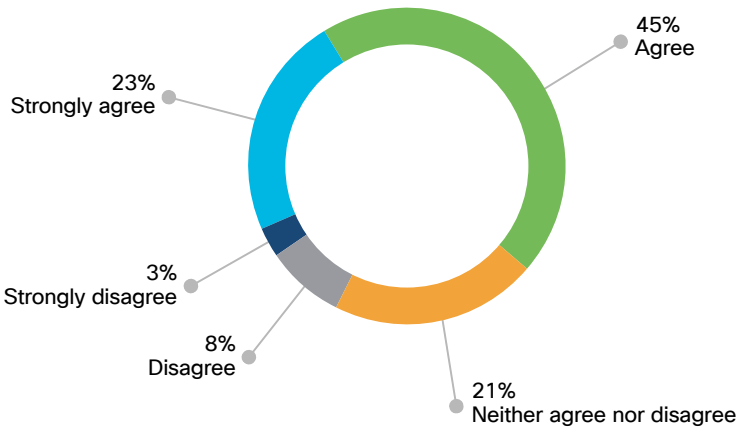
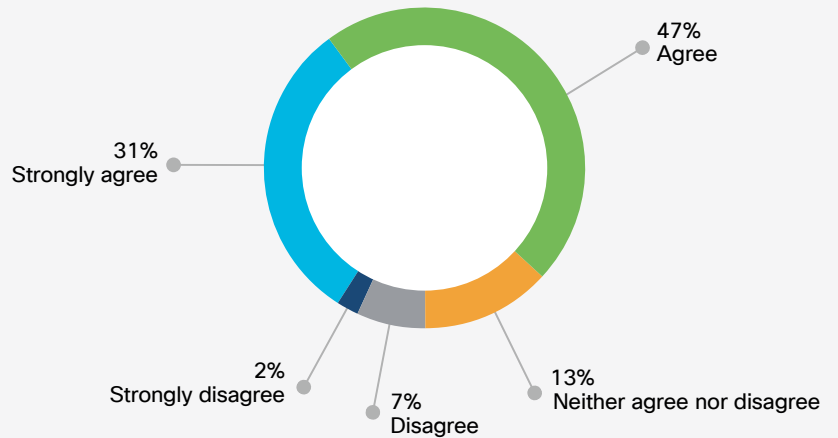


“With the lion’s share of the day-to-day work shifting to the NaaS provider, the customer’s NetOps team will likely gravitate toward general networking and network security skills, as well as design skills that translate business intent into high-level networking concepts. They will need to work closely with the NaaS provider to optimize network designs, policies, performance, and SLAs. And strong data science skills will be needed to identify and orchestrate these changes.”

– Joe Clarke, Distinguished Engineer, Cisco



Adopting a NaaS model would provide our network team members with opportunities to upskill and deliver greater value to the organization.



NaaS will free up my networking team to focus on tasks that deliver IT innovation and business value rather than day-to-day network management.



Bottom line:

More than 75% of organizations agree or strongly agree that NaaS models will give their teams an opportunity to advance their skill sets and deliver more value.

Concerns and hesitations

NaaS impacts many areas of an IT organization, requiring new operating models, new integrations with existing processes and technologies, changing roles and skill sets, and a financial shift from CapEx to OpEx. With these wide-ranging implications in mind, the IT professionals we spoke with had mixed reactions to NaaS. And most were on opposite ends of the spectrum, being either hot or cold when it comes to NaaS adoption.

IT leaders' perspectives on NaaS seemed to reflect their overarching networking philosophy. And those philosophies were primarily divided into two camps: "control IT" and

"lean IT." The ones with the former philosophy have not only a highly skilled staff, but also a strong belief that their teams should own and fully control the networking stack. Conversely, the latter group is seeking to consolidate their IT, reassess routine versus value-added tasks, and find ways to offload infrastructure maintenance. Not surprisingly, the organizations with a "lean IT" mind-set that have already shifted some of their IT resources to the cloud are very open to NaaS solutions.

“We’re dragging our heels with NaaS because we feel the network wouldn’t get the care and prioritization it deserves, and it wouldn’t be a perfect match for our environment.”

– IT manager, networking, U.S. military agency

Some IT leaders with whom we spoke indicated that their networks and processes are highly unique, and they didn’t believe NaaS could address their one-of-a-kind complexities and challenges.

Others voiced a real concern that NaaS would cause upheaval within their IT organization.

While IT leaders share a broad set of concerns, a perceived loss of control is chief among them. Thirty percent of respondents questioned whether they will be able to meet future demands if they adopt NaaS. Other respondents were concerned about the loss of control for security (26%) and performance (20%). In actuality, NaaS is designed for greater on-demand scalability and faster support for the latest technologies. And security, performance, and other important control decisions still lie with the IT team, not the NaaS vendor.

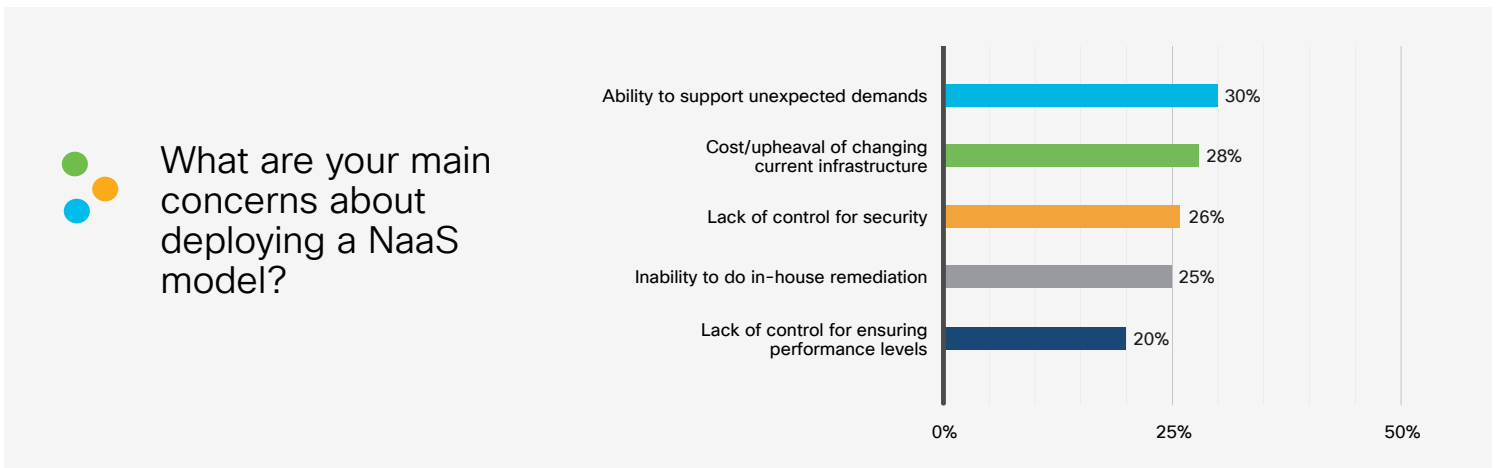




“A provider must adapt to our security guidelines and take directives from us. That’s a key differentiator for NaaS.”

– Lead architect, global technology firm

Twenty-eight percent of respondents said the cost and disruption associated with changing their existing infrastructure and operations were inhibitors. Understandably, organizations have a multitude of technologies and investments, many of which fall on different depreciation schedules. Other organizations have legacy technologies and applications that may not be a good fit for NaaS. And some simply don’t want to offload the day-to-day management of their infrastructure.



To address these concerns and hesitations, organizations can start small with one domain to test out the NaaS model. This would allow them to better understand NaaS capabilities and control points without significantly altering their network infrastructure or operations. They’d be able to experience and optimize the division of responsibility between the provider and their internal team, and learn how to work together to achieve the best outcomes. Once they have a full understanding of—and comfort with—the roles, responsibilities, and control points, they can scale and expand to other domains over time, leveraging the insights and best practices learned along the way.

Bottom line:
Concerns are to be expected with any transformational model. IT leaders can start small to evaluate the risks and rewards associated with NaaS to see if it’s right for their organization.



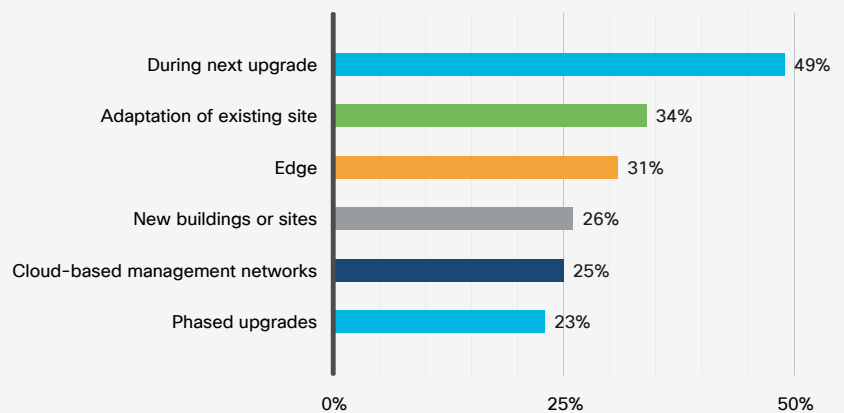
Adoption trends

Because of its impact on network operations and the diversity of ways it can be leveraged, NaaS adoption will be different for every organization. A NaaS readiness assessment and deployment roadmap can minimize complications and maximize success.

According to our respondents, 49% of IT leaders and 57% of network practitioners believe the best timing and circumstance for NaaS adoption is during a network infrastructure upgrade or refresh, when they are seeking to access new technology (automation, 100 Gigabit Ethernet, Wi-Fi 6, 5G, SD-WAN, SASE, etc.). Thirty-four percent of respondents said adapting an existing (brownfield) site where networking technology is already deployed is the ideal scenario for NaaS adoption. Interestingly, only 26% said a greenfield site would be the best fit for NaaS adoption. And only 23% said a phased approach, where domains are upgraded one by one with NaaS, would be the best scenario for their organization.



For which of the following scenarios do you believe NaaS would be the best fit for your organization?



Bottom line:

How, when, and why NaaS is deployed will be different for every organization.



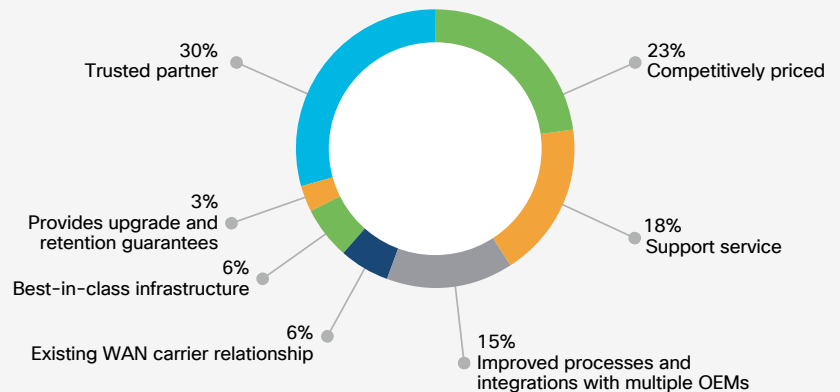
Choosing a NaaS provider

With the network being a critical enabler of employee productivity, customer engagement, and business operations, choosing the right NaaS provider is no trivial task. Some of the IT leaders with whom we spoke have a real fear of losing control. And yet they are willing to give up a measure of control if—and only if—it is placed in the hands of a trusted partner. Whether that means working with a systems integrator, managed services provider, or value-added reseller, they're most comfortable with established partners that already have a deep understanding of their network environment, business goals, and support needs.

For NaaS deployments, nearly a third of IT professionals in our survey viewed systems integrators as more trustworthy and competitively priced compared to network vendors. They also told us “trusted expertise” was much more important than “best-in-class infrastructure.”



What is the main reason you would prefer to work with a partner vs. directly with a network vendor for your NaaS deployment?

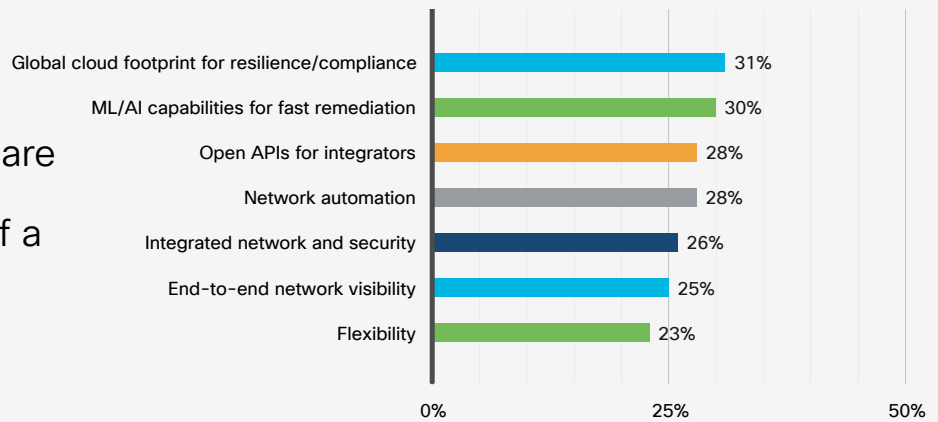


And when it comes to translating business needs into technical policies, IT professionals are two to three times more likely to trust a systems integrator or their internal IT staff than a NaaS vendor. This underscores the fact that organizations are looking not just for a solution when it comes to NaaS, but also for the guidance and assistance of a trusted advisor that knows them well.

When considering the technical attributes of NaaS providers and solutions, our respondents prioritized a global cloud footprint for reliability, performance, and regional compliance (31%), as well as machine learning (ML) and artificial intelligence capabilities that enable continuous optimization of the NaaS service (30%). APIs, automation, integrated security, network visibility, and network flexibility also rated highly.



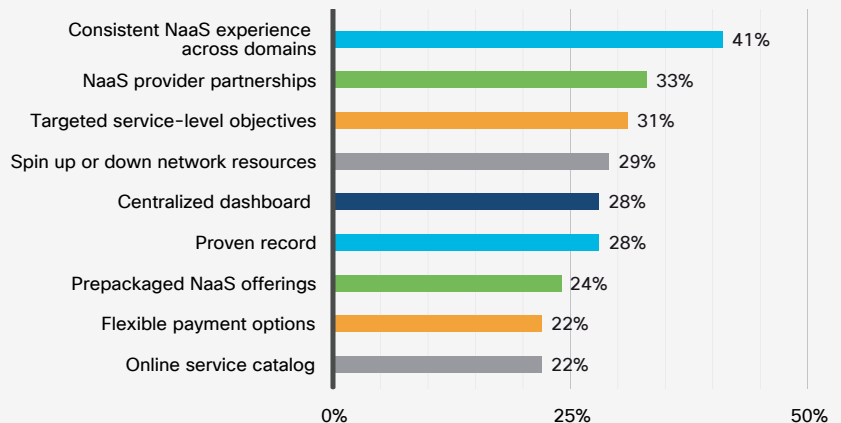
What do you believe are the 2 most important technical attributes of a NaaS offering?



Forty-one percent of respondents said it is important for a NaaS provider to offer a consistent NaaS platform across network domains (access, WAN, data center, cloud, etc.). With many IT teams struggling to manage multiple environments, tool sets, and operating models, NaaS provides an opportunity to consolidate network resources, policies, and operations.



Which of the following would be most important to have if you were to consider a NaaS provider's offering?



“What I’m really looking for is someone who can handle the routine management activities across our network and systems, like firmware updates, configurations, and changes. Then my team can focus on improvements, builds, and strategy implementations. And maybe it flexes. Maybe this month I’m doing some pretty heavy lifting on my own, and then I get some help for a couple months to expand that usage and assist with the work.”

– VP of technology and security, US\$100 M nonprofit



Bottom line:

Systems integrators are viewed as more trustworthy, competitively priced, and service oriented than NaaS vendors. Regardless of the provider, customers are looking for a service and operational experience that spans all network domains.

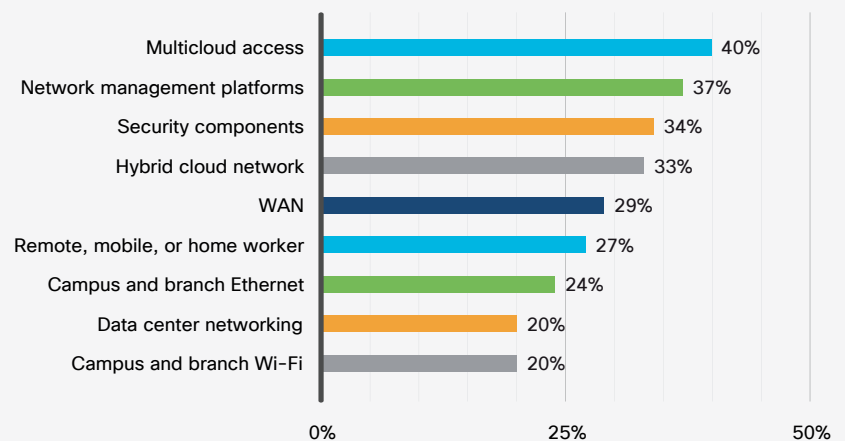


SASE and the different flavors of NaaS

There are a growing number of NaaS offerings, including wired and wireless LANs, VPNs, WANs, network security, remote or work-from-home access, data center networks, and cloud networks. According to our research, NaaS models that include multicloud access and security are the most desirable. This means that SASE, which provides secure multicloud access from anywhere, would be an in-demand as-a-service offering among many IT organizations.

Considering the challenges of connecting to multiple disparate clouds, it's not surprising that multicloud access was identified as the top priority (40%) for NaaS. By offering SD-WAN services, NaaS vendors can provide a consistent and optimized way to connect to a wide variety of cloud-based (IaaS and SaaS) applications.

Which aspects of your network equipment and management would be a good fit for NaaS?

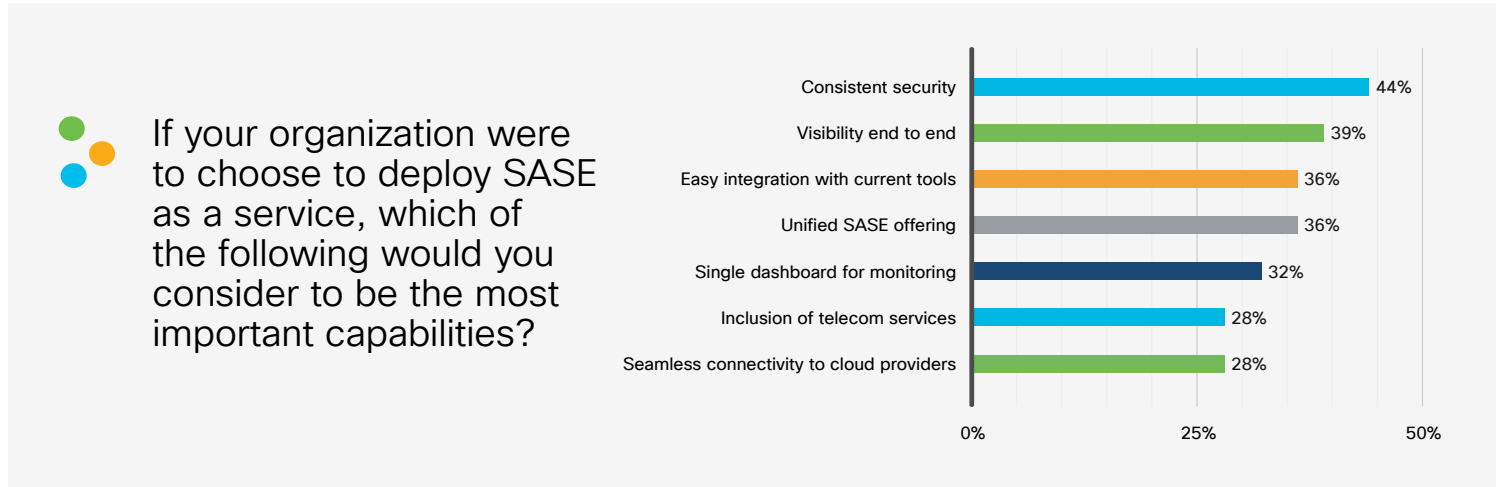


Thirty-four percent of respondents prioritized security-focused NaaS solutions, including VPN, security information and event management (SIEM), secure web gateway, firewalls, and intrusion prevention and detection services (IPS/IDS). These can help protect users, devices, and applications consistently across multiple clouds and computing environments.

NaaS vendors that offer a combination of multicloud access and security at the edge are well positioned to meet the growing demand for SASE solutions.



Nearly half (44%) of our respondents cited “consistent security, including threat detection and remediation, for all users and devices,” regardless of where they access from, as an important aspect of SASE. With increasing reliance on the internet for access to cloud-based applications, more than one in three (39%) are seeking “visibility and insights about network traffic across internet and cloud infrastructures.” And 36% are looking for SASE solutions that easily integrate with their current tools.



Bottom line: Multicloud access and security are top priorities for NaaS. Vendors that weave a SASE option into their NaaS portfolio can meet the growing demand to align and secure on-premises and cloud resources.



Conclusion

Countless IT organizations are struggling to manage network complexity, respond to disruptions, protect users and data, and keep up with the accelerating pace of business. To confront these challenges, many are investigating new networking models such as NaaS.

NaaS provides continuous access to the latest networking technologies through an on-demand or subscription-based model. It shifts the burden of day-to-day network management to a third-party provider. And in doing so, it allows IT teams to focus on value-added activities that deliver greater agility, resiliency, and innovation.

As with any transformational model, there are concerns and hesitations surrounding NaaS. But it is not an all-or-nothing proposition. IT teams can work with trusted partners to try NaaS on a small scale, evaluate the risks and rewards, and see whether it aligns with their overarching business and technology strategies.



Additional resources and assistance

[What Is Network as a Service \(NaaS\)? >](#)

[Cisco+ Solutions >](#)

[Find a Cisco Partner >](#)

[Contact Cisco Sales >](#)



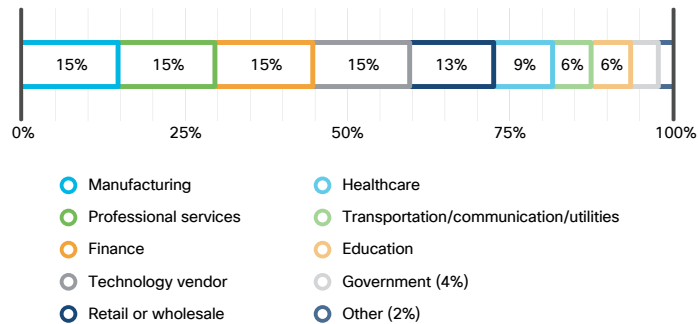
About this report

First published in 2019, the [Global Networking Trends Report](#) highlights the latest strategies and technologies within the enterprise networking and cloud industry. The report leverages industry research and provides perspectives, insights, and guidance to help IT organizations understand current technology trends, evolve their networking models, and support dynamic business needs.

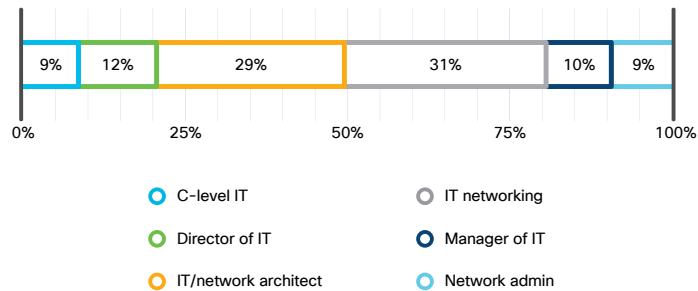
For the 2022 report, we conducted interviews with 20 IT leaders and received input from 1534 IT professionals in 13 countries about their views on NaaS and how they see it aligning with or augmenting their networking strategies over the next two years. Respondents were allowed to select up to three answers per question.



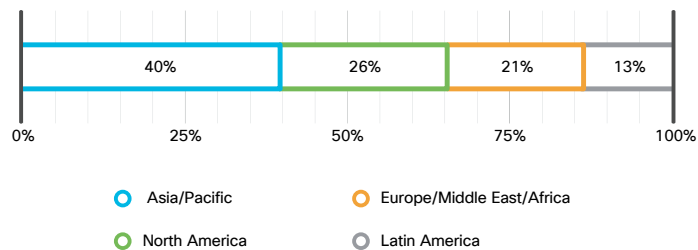
Respondent industry



Respondent role



Respondent location





Permissions for using this report

Cisco welcomes and encourages press, analysts, service providers, and other interested parties to use the information contained in this report. We do require proper attribution for any and all Cisco 2022 Global Networking Trends Report data that is published or shared—privately or publicly—in print or electronic forms (i.e., “Source: Cisco 2022 Global Networking Trends Report”). No further signatures and consent are required to refer to our publicly available white papers, reports, or web-based tools.

We are always interested in the context in which our content is used. We appreciate when parties using our content are able to share copies of their completed work containing Cisco 2022 Global Networking Trends Report insertions. You may forward documents containing Cisco 2022 Global Networking Trends Report references to networkingtrends-inquiries@cisco.com.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, see the [Trademarks page](#) on the Cisco website. Third-party trademarks mentioned are the property of their respective owners. The use of the word “partner” does not imply a partnership relationship between Cisco and any other company. (2205R)

2022 Global Networking Trends sources

1. Global Network-as-a-Service (NaaS) Market Industry Dynamics, Market Size, and Opportunity Forecast to 2027, Report Ocean, March 2021.