The bridge to possible

2023 Global Networking Trends Report

Simplifying secure multicloud connectivity for the distributed workforce

The bridge to possible

2023 Global Networking Trends Report

Simplifying secure multicloud connectivity for the distributed workforce

Table of Contents

Welcome 3

Key Findings: The state of networking for connecting multiple clouds 4

Essential Guidance: Successful networking strategies for secure access to cloud-based applications 5

Introduction: Trends in Multicloud Access 7

Essential Guidance: Six Best Practices for Providing Secure Access to Multiple Clouds 9

Conclusion 21

The bridge to possible

Welcome

The annual Cisco Global Networking Trends Report highlights important strategies and technologies within the enterprise networking and cloud industry. The report combines findings from primary and industry research with executive perspectives and insights to identify the latest technology trends and provide guidance to help IT organizations evolve their networking models in support of dynamic business needs.

In the 2023 report, we explore how organizations are deploying and evolving their networks to support secure connectivity for distributed applications, people, places, and things. We surveyed more than 2,500 IT leaders in 13 countries across North America, Latin America, Asia Pacific, and Western Europe.

The bridge to possible

Key Findings: The state of networking for connecting multiple clouds

Hybrid work continues to pose secure connectivity challenges.

The era of hybrid work is driving the need for new approaches to securely connect remote workers to corporate data and assets distributed across multicloud environments.

- While employees are encouraged to return to the office, more than 40% continue to work remotely either full time or a few days a week.
- The transition to applications deployed across multiple clouds and a highly distributed workforce makes traditional security models obsolete, creating a headache for IT professionals, with more than half (51%) identifying cloud security risks and 39% citing the increase in remote workers as major challenges.

The transition to cloud and multicloud is accelerating.

If business agility is the question, many continue to see cloud as the answer.

- Organizations continue to adopt cloud platforms, with 78% of survey respondents saying that their organizations are planning to host more than 40% of their workloads in the cloud by 2025, up from 63% of organizations today.
- Multicloud adoption is also on the rise, with 42% of cloud and networking professionals saying that more agile and scalable application development is a key motivation for using multiple clouds.

Securing user access to cloud applications tops the bill of 2023 networking challenges.

Maintaining end-to-end visibility across the digital service delivery chain (e.g., between user and cloud) to assure a consistent application experience is also a major concern among enterprise IT professionals.

- Providing secure access to applications distributed across multiple clouds is the top challenge cited by 41% of networking professionals.
- Gaining end-to-end visibility into network performance and security as more traffic originates or terminates beyond the boundaries of the corporate network is the second biggest challenge, cited by 37% of respondents.

The bridge to possible

Essential Guidance: Successful networking strategies for secure access to cloud-based applications

Pursue Networking and Security Convergence

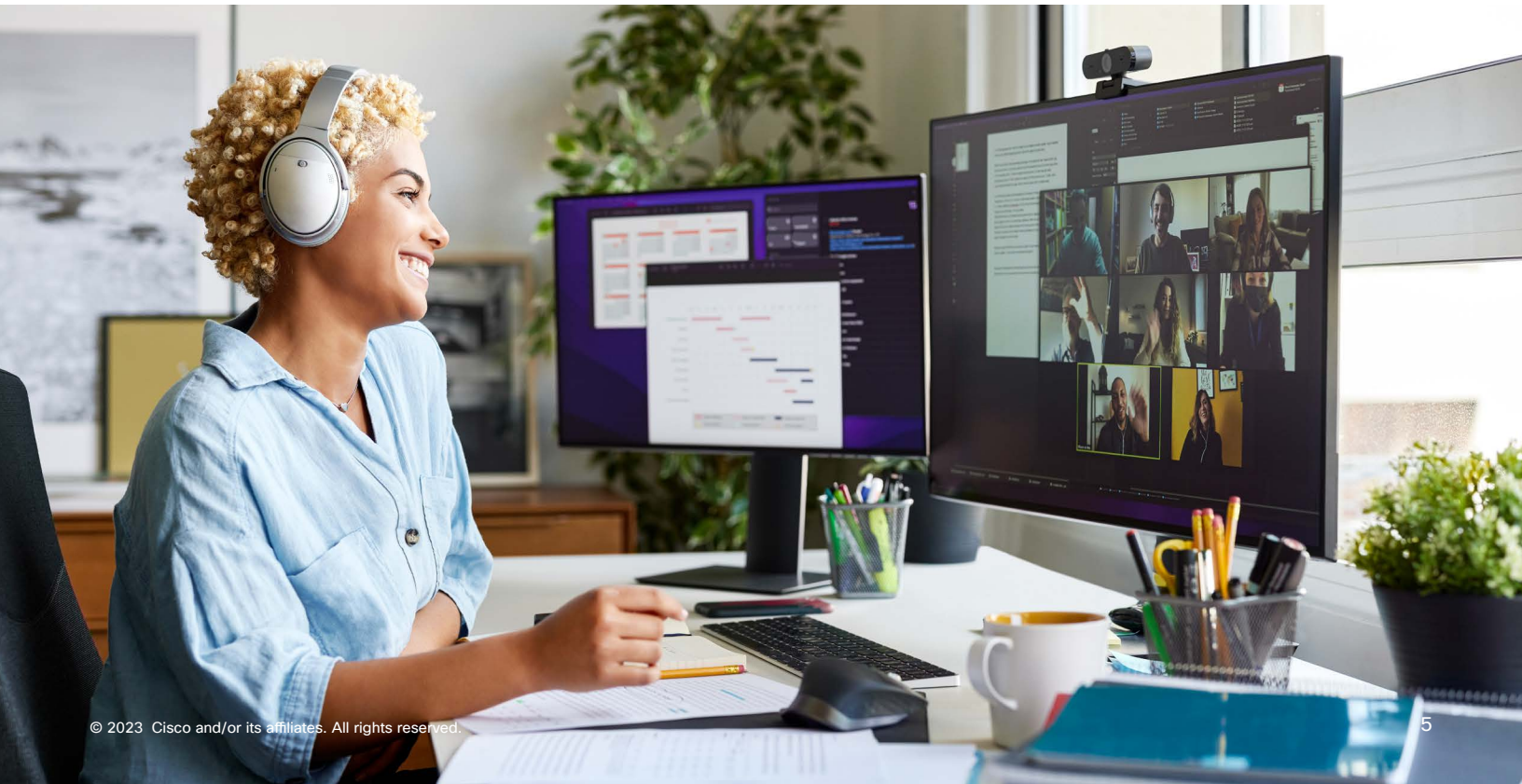
Increase collaboration between IT teams to simplify operations from access networking to the cloud.

Siloed organizations and traditional models for delivering connectivity can no longer meet the dynamic security needs of distributed applications, people, places, and things.

- Standardized policies, shared telemetry, and streamlined workflows across security, networking, and cloud operations deliver better and faster IT and business outcomes than environments that operate in technology silos.
- Siloed operations were cited by 40% of respondents as a key challenge when providing secure access from distributed locations to multiple cloud-based applications.
- Cloud professionals believe network operations need better alignment with cloud operations, with 38% wanting closer integration with networking teams and 34% citing operational consistency as a key goal.

Transition to a converged networking and security model with a SASE architecture.

Secure Access Service Edge (SASE) delivers the operational simplification and consistent security and performance that multicloud access and a hybrid workforce demands.



- Organizations are converging Software-Defined WAN (SD-WAN) and cloud security to deliver a SASE architecture.
- Within two years, 47% of respondents expect to connect their branches and remote clients by expanding their SD-WAN environments to a full SASE architecture.

Adopt Cloud-First Networking and Security

Extend SD-WAN connectivity consistently across multiple clouds for simple IT management and a better application experience.

Apply policy consistently across all clouds to automate cloud-agnostic connectivity to optimize and secure the application experience.

- Extending visibility, control, and zero trust access across cloud, SaaS, and middle-mile providers allows IT to deliver better and more secure user experiences.
- More than half of respondents (53%) say they are prioritizing integration with cloud service providers to improve connectivity to cloud-based applications from all locations over the next two years.

Evolve to cloud-centric security for consistent operations and policy.

Combining security functions in a cloud platform makes visibility, policy management, and control easier, more pervasive, and more effective.

- 59% of respondents said their top cloud access networking priority over the next two years is to centralize security in the cloud, in acknowledgment that consistent policy across users and devices located anywhere is a major requirement.

Transition to Proactive Operations

Seek a consistent user experience across the increasingly complex digital service delivery chain through end-to-end network visibility.

Without extending visibility beyond their own network to the Internet and cloud environments, IT teams cannot assure a consistent, high-quality user experience for cloud-based applications and services.

- 51% of respondents are prioritizing the use of end-to-end network telemetry and visibility for proactive detection and remediation of issues.
- Visibility into Internet and cloud traffic is especially important when the majority of user and device transactions transit beyond the corporate perimeter.

Move from reactive to predictive operations to improve uptime and performance levels.

Predictive analytics is gaining recognition as an important part of an Artificial Intelligence for IT Operations (AIOps) toolkit for simpler, faster, and more effective overall IT operations.

- Intent on preventing network degradation instead of reactively remediating outages, 47% of respondents prioritize adopting predictive network analytics over the next two years.

The bridge to possible

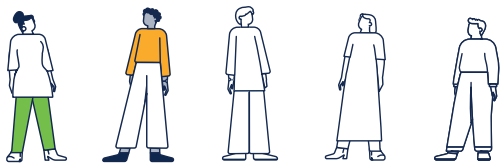
Introduction: Trends in Multicloud Access

"Computing may someday be organized as a public utility just as the telephone system is a public utility, each subscriber needing to pay only for the capacity he actually uses."[1] These were the prescient words delivered by Professor John McCarthy to an MIT audience in 1961.

More than six decades later, McCarthy's vision of a shared on-demand compute utility has not just come to fruition but is now one of the major enablers driving the global digital revolution.

The move to multicloud continues

Today, most organizations have adopted multiple clouds. The Cisco 2023 Global Networking Trends study finds that two-thirds of organizations already have more than 40% of their workloads in multiple clouds. What's more, most organizations are using more than two cloud providers, and a large majority are using more than five SaaS providers (see Figure 1).



Two out of every five people work remotely at least part of the week.

Hybrid work is here to stay

It is not only applications that have become highly distributed. The widespread adoption of hybrid work means people and things are also now more distributed than ever.

According to a recent study, even though 59% of people have returned to the office full time, a large proportion of people continue to work remotely, with 28% being in a hybrid arrangement and the remainder (13%) working fully remote.[2] These numbers vary considerably across industry and role.

At the same time, the rapid adoption of IoT technology

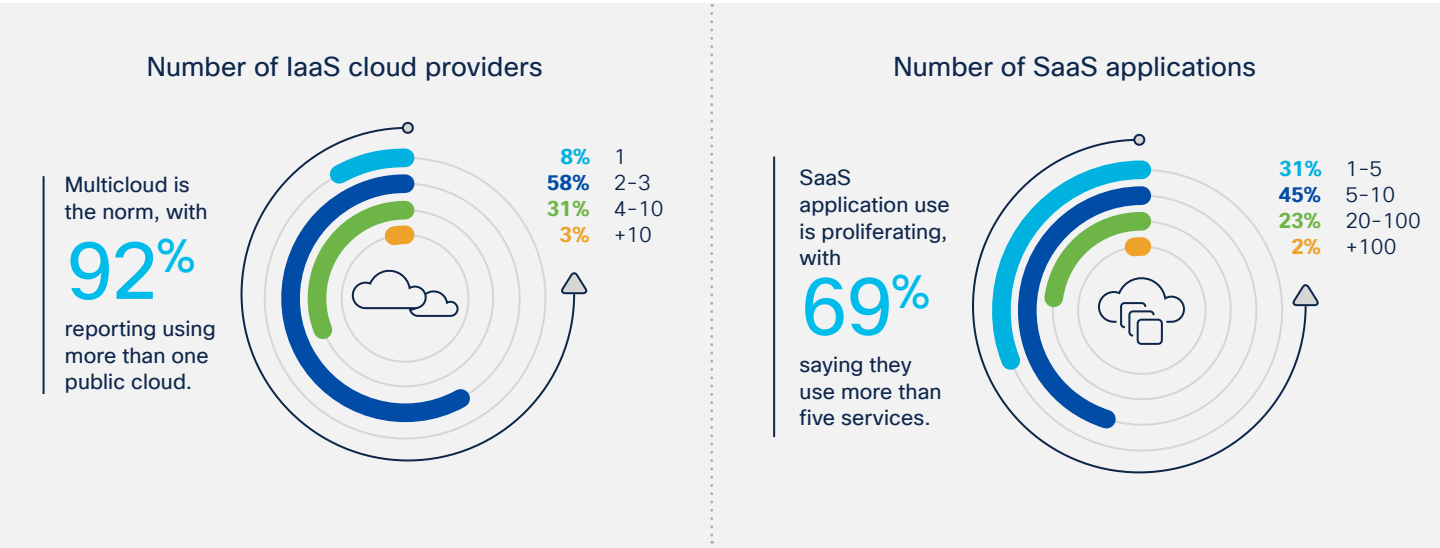


Figure 1. Use of multiple cloud and SaaS providers has become the norm.

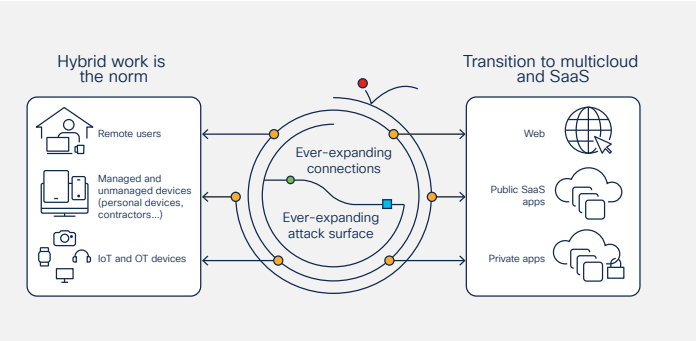


Figure 2. Hybrid work and the transition to cloud and SaaS mean the challenges of network security have surpassed human capacity.

and edge computing is adding to the ever-expanding number of connections and trillions of data flows that need to be managed and secured each day.

The distributed workforce and the proliferation of IoT and edge computing are driving the need for scalable, secure connectivity and access to multicloud applications and globally hosted services across any network (Figure 2). This was identified by networking professionals as their top challenge for 2023.

Connectivity over the Internet is complicating this challenge, with infrastructure that lies outside of the visibility and control of networking and security professionals. Nevertheless, they are still responsible for the digital experience and protection of their employees, customers, and partners.

The increasing importance of speed and agility

Agility has become table stakes for most organizations today. Survey results show that the biggest motivator for the move to multiple clouds is not cost, as McCarthy originally predicted, but the need for business agility and innovation and the necessity to rapidly deploy new, high-quality applications and services. On the heels of a disruptive pandemic, geopolitical and economic disruptions, and supply chain challenges, the ability to pivot quickly to take advantage of market trends has become a top priority.

"People don't want to wait weeks or months for their business priorities. So, any sort of initiative that comes from a business, now they expect more instant gratification than the traditional bottlenecks that you had in the past."

– IT Director, Retail Industry

Organizations recognize that in today's environment, siloed technology and operations models are too limiting, no longer serve them well, and require new tools and processes. Connectivity and security challenges require a more holistic approach that can deliver a simpler, more secure, and more flexible network infrastructure and operations model.

The next part of this report addresses these challenges and provides best practice guidance on the journey toward achieving connectivity that is flexible yet secure. It also outlines how and why network and security teams must partner to deliver dependable, secure, robust, cloud-delivered experiences for employees, partners, and customers anywhere.

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

Essential Guidance: Six Best Practices for Providing Secure Access to Multiple Clouds

Essential Guidance #1: Increase collaboration between IT teams to simplify IT operations, from access to cloud.

Siloed organizations and the traditional models for delivering connectivity can no longer meet the dynamic security needs of distributed applications, people, places, and things.

Faced with the challenges of increased complexity and an expanding threat surface, IT leaders need to improve collaboration between teams so that they will be able to respond more quickly, efficiently, and securely to fast-changing business needs.

Four out of the top five challenges in providing user access from distributed locations to multiple cloud-based applications (e.g., Infrastructure as a Service [IaaS] and Software as a Service [SaaS]) are security related. Siloed cloud, network, and security operations were cited by 40% of respondents as a top challenge to providing secure access from distributed locations

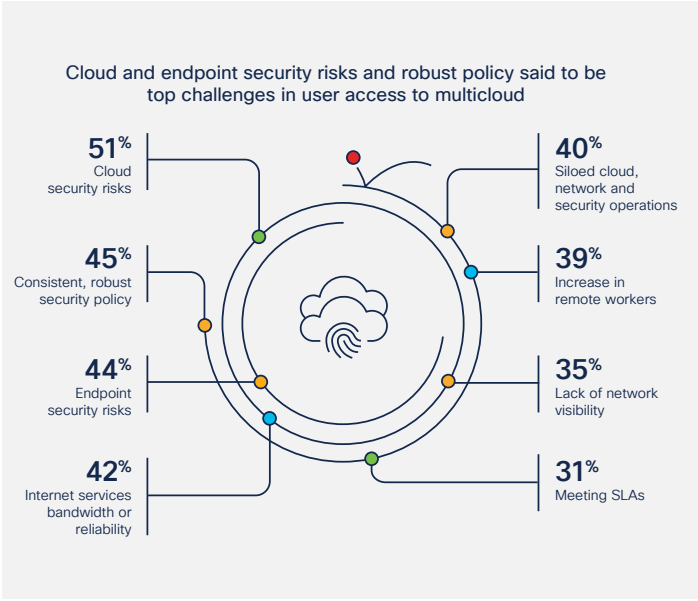


Figure 3. Challenges in providing secure access from remote locations to multiple cloud-based applications.

to multiple cloud-based applications.

Many IT organizations have network and security teams that plan and operate separately, but IT leaders can only address today's security challenges by eliminating technology and operations silos and reducing the number of point integrations systems.

Aligning teams, tools, and processes to streamline

The bridge to possible

38% of cloud professionals identify better integration with the network as a big operations challenge.

operations requires greater consistency in operating models. Research by Cisco has revealed that 86% of CIOs and IT leaders recognize the need to develop a more consistent operating model that spans on-premises, private cloud, public cloud, and SaaS systems.[3] It is widely recognized that the principles of the cloud operating model have proven successful with DevOps and CloudOps teams in simplifying operations and delivering agility. IT teams can gain similar benefits by adopting the principles of a cloud operating model. Survey data reinforce this thinking, with 38% of cloud professionals saying that their biggest operations challenge is better integration with the network, and another 34% stating their biggest challenge is maintaining operational consistency between the cloud and the network.

By bringing cloud operating model principles to the network and across the entire cloud/network IT stack, IT teams can accelerate innovation, improve security, and remove risk from cloud operations. They can reduce the complexity and fragmentation that can hamper collaboration between network, security, and cloud operations and ultimately support their organization's dynamic needs.

Bottom Line

Converging networking and security policies, technologies, tools, and operational workflows based on a cloud-centric model will allow organizations to work from a common set of tools, fostering consistently secure connectivity while increasing efficiencies and reducing risk.

3 https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/7/1

Expert View

Strong team alignment drives better security, simplicity, and performance.

"In the distant past, the operations team knew every layer and every system, from the cabling to the applications, and managed it all as a whole. We need to return to that model.

Even though networking in the cloud is not the same as networking on premises, and the organization no longer controls all the devices and software in the ecosystem, the need for security is the same. Importantly, securing people's access to cloud applications requires a consistent set of policies no matter where the user is or what they're currently using; this can be the north star for combining design, operations, and architecture.

In the future, we will see more networking and security teams collaborating on an end-to-end infrastructure, being driven by the principles of security and simplicity, not just operational performance, because they all lead to the same goal."

Wendy Nather
Head of Advisory, CISOs
Cisco

Essential Guidance #2: Transition to a converged networking and security model with a SASE architecture.

SASE delivers the operational simplification and consistent security and performance that multicloud access and a hybrid workforce demands.

It does this by bringing together network and security domains to provide a much-needed framework for securely and seamlessly connecting users to applications in complex and highly distributed environments.

SASE is fast becoming the convergence architecture of choice for secure multicloud access. Within two years, 47% of respondents expect to connect their branches and remote clients primarily using a SASE model.

However, many organizations are struggling to realize the full potential of SASE because their solutions lack certain capabilities or fail to deliver a fully converged network and security solution.

SASE convergence requires a strong SD-WAN foundation combined with a rich cloud security or Security Service Edge (SSE) solution (Figure 4). Only when these architectures are converged fully will IT organizations realize the full benefits of SASE. These benefits include a streamlined operational model to make the visibility, management, and control of securely connecting users anywhere as simple and as consistent as possible.

With standardized policies, shared telemetry, and coordinated alerts across all security and networking components, a unified SASE solution enables NetOps and SecOps teams to improve IT efficiency, performance, and protection. A more efficient and consistent operating model and workflow across NetOps and SecOps teams invariably results in a better user experience.

Full-featured SASE implementations can deliver

"Secure Access Service Edge (SASE) delivers converged network and security as a service capability, including SD-WAN, SWG, CASB, NGFW, and Zero Trust Network Access (ZTNA). SASE supports branch office, remote worker, and on-premises secure access use cases. SASE is primarily delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies."

– Gartner IT Glossary, Secure Access Service Edge (SASE), as on 2nd May 2023.

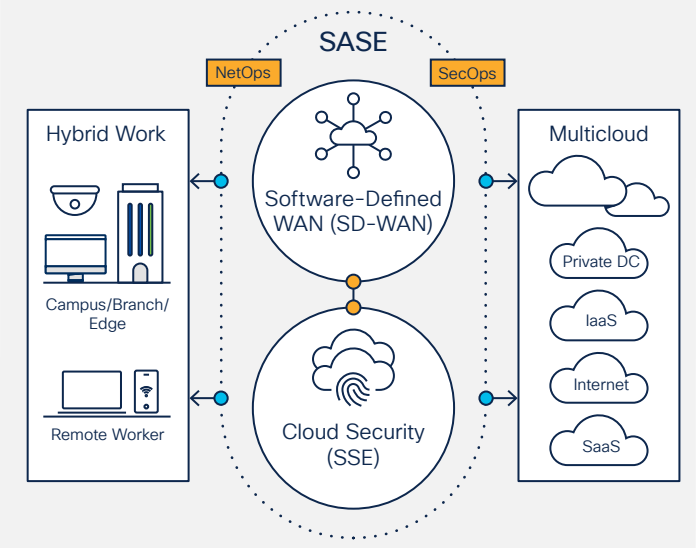


Figure 4. Network and security technology and operations convergence delivers a new secure connectivity model – Secure Access Service Edge.

The bridge to possible

Gartner® predicts that by 2025, 50% of SD-WAN purchases will be part of a single vendor SASE offering, up from less than 10% in 2021.[4]

improved operational efficiencies, better user experiences, and enhanced protection. Here are some examples of these benefits:

- Cisco's internal IT team reports a 40% reduction in OpEx using SASE
- Rigorous performance evaluation by an independent testing firm showed that Umbrella (a core component of Cisco SASE) with security policies in place performed as well as – often better than – accessing SaaS apps over the Internet with no security
- TechValidate Customer Research shows that 85% of Cisco customers cut malware infections by 50% with a SASE architecture in place

There are two basic approaches that can deliver these desired outcomes.

The first is composed of separate networking and security/SSE products, typically provided by a single vendor, or two vendors, which can be integrated into a complete SASE solution. This approach can be used by organizations that already have SSE or SD-WAN deployed and may need greater customization and flexibility.

The second is a unified approach that delivers all networking and security components as a single turnkey cloud service with unified management. A well-designed, unified SASE solution delivers speed, simplicity, and faster time-to-value.

4 Gartner, 2022 Strategic Roadmap for SASE Convergence, Neil MacDonald, Andrew Lerner, John Watts, June 2022, GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Expert View

When is a SASE solution not a SASE solution?

"Every organization has an installed technology base and there may be a temptation to simply add the missing SASE functionalities to whatever currently exists. However, it's important to note that SASE is a long-term strategic choice and simply deploying all the components of a SASE model without a high level of integration does not constitute a fully functional SASE solution and won't deliver the desired outcomes.

Depending on their priorities, networking and security leaders should opt for either a well-integrated SASE solution or a turnkey unified service.

By opting for a unified turnkey cloud service, NetOps and SecOps teams can benefit from centralized management with intelligent distributed enforcement, controls and visibility across endpoints, enterprise edge and the cloud edge to deliver a more secure end-to-end solution that further enhances the end-user experience.

"Whatever technology and architecture choices you make to better meet your needs, it is important to ensure there is an ongoing vendor commitment to combine all the components into a well-integrated or unified system."

Omri Guelfand
VP of Product Management, NaaS/SASE
Cisco Meraki

Bottom Line

In contrast to traditional security solutions, the unified, cloud-centric architecture of SASE pushes centrally managed security policies and enforcement closer to end users and applications, providing connectivity that is flexible, seamless, and secure.

Learn more about SASE

Essential Guidance #3: Extend SD-WAN connectivity consistently across multiple clouds for a simpler IT experience and better application experience.

Apply policy consistently across all clouds to automate cloud-agnostic connectivity to optimize and secure the application experience.

The cloud has become an extension of the enterprise network. For many, SD-WAN has become the stepping stone to a complete SASE implementation. By automating the extension of the SD-WAN fabric with major IaaS, SaaS, and middle-mile providers, IT gains more operational control to provide a better user experience.

Better control of the user experience is clearly top of mind with networking teams, with 53% of respondents saying they prioritize integration with cloud service providers to improve connectivity to cloud-based applications from distributed locations. Networking teams are taking action, with 49% of respondents saying they are prioritizing SD-WAN and multicloud integrations as a top initiative over the next 24 months.

SD-WAN multicloud integrations allow networking and cloud teams to accelerate and automate extensions from enterprise sites to the various cloud providers and other enterprise sites through Internet, interconnect, or colocation and cloud provider networks (Figure 5). These integrations allow administrators to optimize the application experience and achieve a more

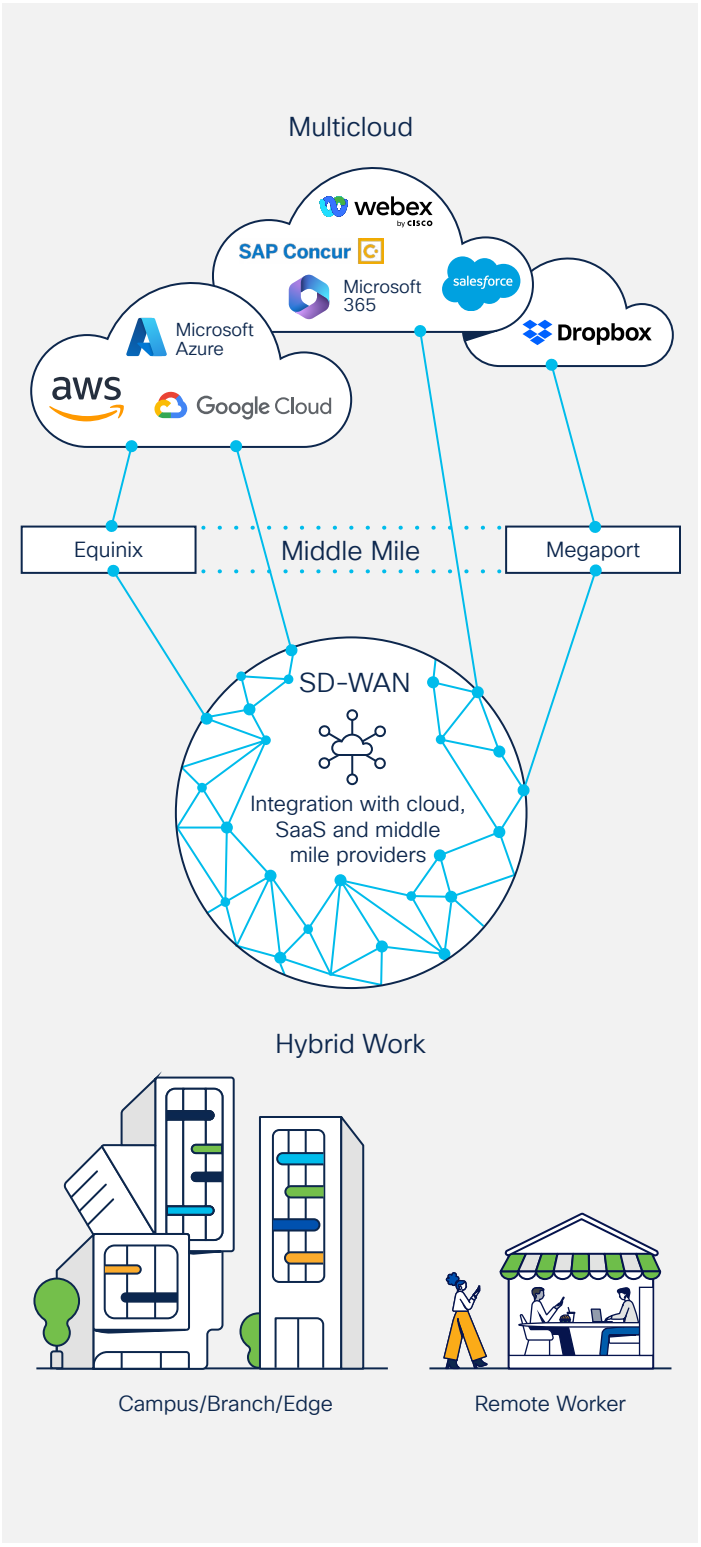


Figure 5. SD-WAN integrations with IaaS, SaaS, and middle-mile providers are vital for a better IT and user experience.

consistent operational experience across all cloud and on-premises locations. In addition, IT can deliver secure, scalable access to cloud applications and points of presence by integrating with global network interconnect providers such as Equinix and Megaport. These integrations allow IT to build a global network in a simplified, fully automated manner within minutes.

Bottom Line

SD-WAN multicloud integrations are critical to any IT team that needs to accelerate and simplify extensions from the enterprise to one or more clouds, optimize the user application experience, and better secure cloud applications with zero trust access.

Learn more about SD-WAN

Expert View

We can't ignore the complexities and risks of multicloud connectivity.

"In today's cloud-centric world, it is unimaginable to deliver an SD-WAN solution that does not have tight integrations with leading cloud, SaaS, and middle-mile providers. Customers can accelerate their cloud journey by automating the extension of the SD-WAN fabric between their global sites and cloud workloads and benefit from simplified network operations, assurance of end-to-end encryption, and flexibility for rapid business innovation.

Furthermore, with the increasing and constantly evolving threat landscape associated with the use of distributed cloud and SaaS applications, networks must adopt a 'zero-trust' approach and its core principles—'never assume trust, always verify and enforce least privilege.' By integrating SD-WAN with a zero trust approach, organizations can establish a security posture that controls who can access which cloud services, provide automated security control for admitted traffic, ensure continuous enforcement, and allow immediate adaptation to security posture changes."

JL Valente
VP, Product Management, Enterprise Routing, SD-WAN and Cloud Networking
Cisco

The bridge to possible

Essential Guidance #4: Evolve to cloud-centric security for consistent operations and policy.

Combining security functions in a cloud platform makes visibility, policy management, and control easier, more pervasive, and more effective.

With hybrid work now so prevalent, people are using both employer-owned and personal devices while consuming more and more applications from managed and unmanaged networks within and outside of the corporate network. Traditional perimeter security is no longer enough. It follows that IT is making it a top priority to ensure that all endpoints, applications, and data are secure.

Traditionally, the security policies used for remote workers have been different from those used on-premises. Remote security policies have different trust levels and are managed by separate security tools.

Supporting disparate policies increases IT overhead and may frustrate end users. Asked about security policy in the study, 45% of respondents identified consistent, robust security policy as a top challenge in providing secure multicloud access from distributed locations.

In addition to handling a relentless barrage of cyber threats, security teams are also required to update security policies regularly. The need for consistent application security policy updates across distributed workforces is a strong driver for centralizing security. It was cited by 59% of respondents, who say they prioritize centralizing cloud security as a top cloud access networking initiative over the next 24 months (Figure 6).

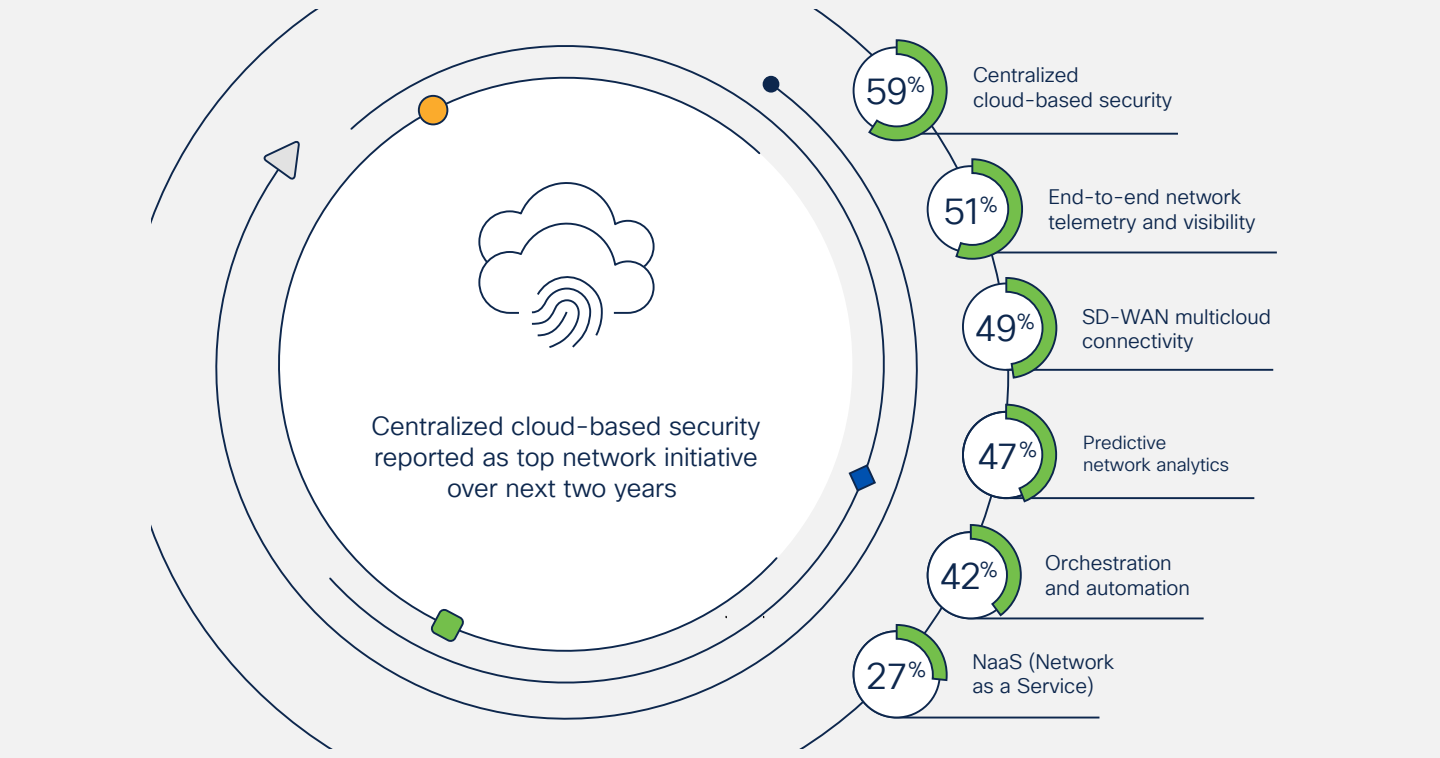


Figure 6. Top cloud access network initiatives over the next 24 months.

Traditional perimeter defenses are no longer effective on their own. A smarter way to secure access to applications and workloads at scale is needed as part of a centralized cloud security solution. This is where SSE, a central pillar of SASE, comes in.

Bottom Line

Work from anywhere, BYOD, and the proliferation of cloud services have made once clearly defined security perimeters obsolete. With many of the applications used daily residing in the cloud, it makes sense for organizations to design a comprehensive SSE strategy that consolidates multiple security capabilities and effectively delivers them from the cloud.

Expert View

Cloud security convergence is the key to a centralized and integrated model.

"For years, organizations went down the path of adding point security products to react to ever-expanding threats. That did improve security, but recently the extreme increase in operational complexity is outweighing the benefits. Moving to an SSE solution delivers a converged set of scalable, cloud-native security functions — Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access, and Firewall as a Service — to provide a better experience for end users, improved security outcomes, and reduce the burden on IT teams.

By choosing this type of integrated and centralized approach, you can ensure simplification of management tasks, easily scale performance, gain deep visibility, and achieve robust security across your organization. A converged SSE solution is essential to a complete SASE architecture."

Jeff Scheaffer
VP, Product Management, Security/SSE
Cisco

Essential Guidance #5: Seek consistent user experience across the increasingly complex digital service delivery chain through end-to-end network visibility.

Without extending visibility beyond their own network to the Internet and cloud environments, IT teams cannot assure a consistent, high-quality user experience for cloud-based applications and services.

Enhancing the user experience is an important objective for IT. To provide a great experience, networking teams are looking beyond traditional tools and adopting solutions that increase visibility into what's happening both within and beyond their own networks in real time. By correlating those expanded metrics with application performance, IT can use the resulting insights to optimize digital experiences for all their employees and customers.

As organizations accelerate their adoption of SaaS and cloud solutions and increase the use of public networks such as the Internet to provide access to these applications, and as these multi-hop networks become increasingly complex, it has become imperative to invest in advanced visibility solutions. Over half of respondents (51%) recognize this as a top priority by focusing on end-to-end network telemetry and visibility as a major network initiative.

Any application transaction can traverse multiple networks, network segments, and services (Figure 7). This makes it difficult to track the performance and availability of any specific application. Nearly half (48%) of respondents recognize the need to prioritize Internet visibility and insights to improve connectivity. This further emphasizes the need for tools that help IT see into and visualize the complete transaction path,

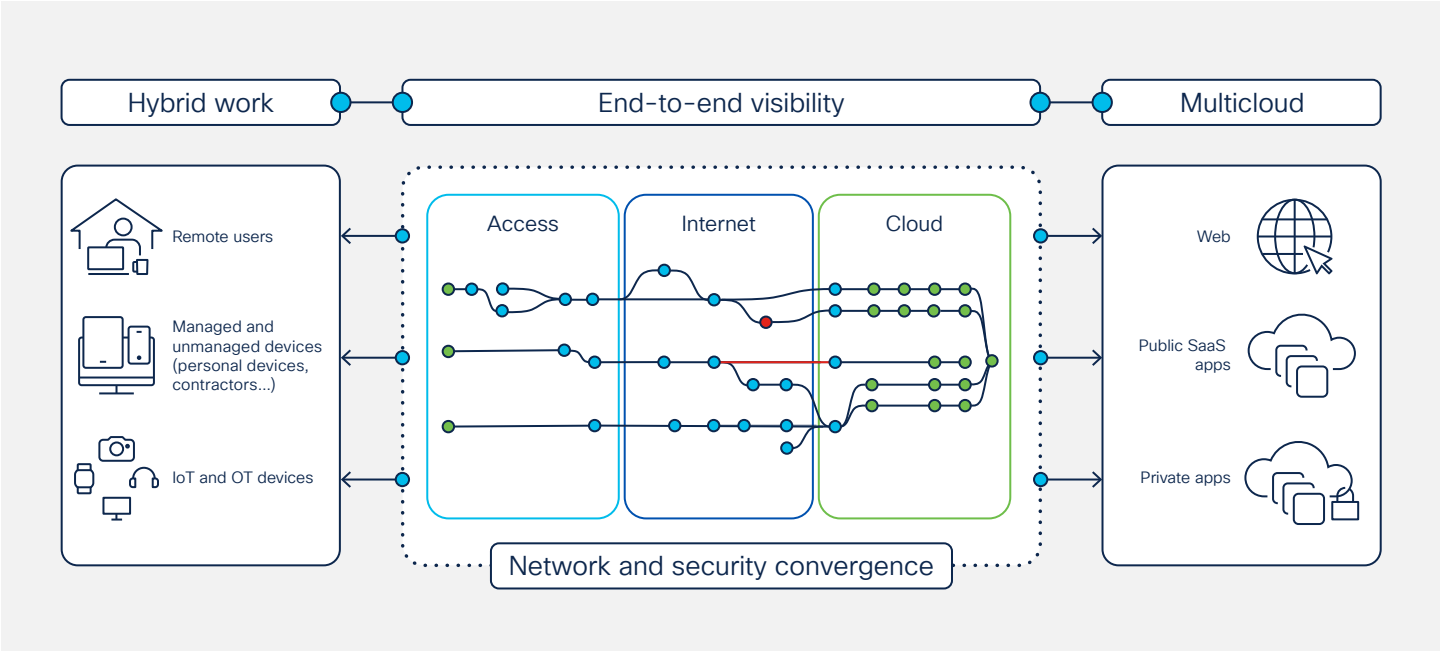


Figure 7. The spiraling complexity of connecting distributed environments over the Internet demands better end-to-end visibility.

The bridge to possible

including external networks and environments that they do not own or control.

Bottom Line

Cloud is the new data center, Internet is the new network, and cloud offerings dominate applications. By gaining a view of global Internet health and the performance of top SaaS applications, IT teams can proactively detect and remediate major unexpected network or application issues affecting them as soon as they happen.

Expert View

Consider the Internet the new infrastructure backbone.

"Digital experience supply chains have transformed from a single domain to multi-party, collaborative systems and networks. Users can exist anywhere. Applications are designed for agility, built on APIs and distributed micro services. Organizations must enable a seamless experience across many applications, services, clouds, and networks—all with less control than ever before.

Therefore, modern digital experiences require a different approach to visibility and assurance; an approach that empowers teams to quickly detect and diagnose disruptions and tie this to infrastructure and network problems regardless of the domain – home, office, cloud, or the Internet. This requires having access to the right data at the right time and being able to easily collect and correlate that data internally across application, network, and infrastructure operations and with third-party providers within the connected ecosystem."

Joe Vaccaro
VP, Product Management
ThousandEyes, Cisco

The bridge to possible

Essential Guidance #6: Move from reactive to predictive operations to improve uptime and performance levels.

Predictive analytics are gaining recognition as an important part of an Artificial Intelligence for IT Operations (AIOps) toolkit for simpler, faster, and more effective overall IT operations.

As the extended network is vital to how organizations conduct their business, any degradation in service or downtime is intolerable. IT leaders are looking to proactively identify and remediate issues before they occur and impact the user experience.

With the advent of cloud-based management platforms, enterprises have greater access to real-time and historical telemetry from more sources than ever before. New advances in predictive analytical models using artificial intelligence and machine learning (AI/ML) techniques can derive actionable intelligence based on all of this historical and real-time data. This helps organizations understand patterns around the data and accurately forecast and remediate issues before they impact the network. These models get smarter over time by learning from the data they receive through a continuous feedback loop.

47% of respondents say that they prioritize the adoption of predictive network analytics to improve cloud connectivity over the next two years.

Proactive IT operations are becoming especially important for providing consistent, high-performance services for distributed users accessing distributed cloud applications. Survey respondents see this as an important future direction, with 47% saying that they

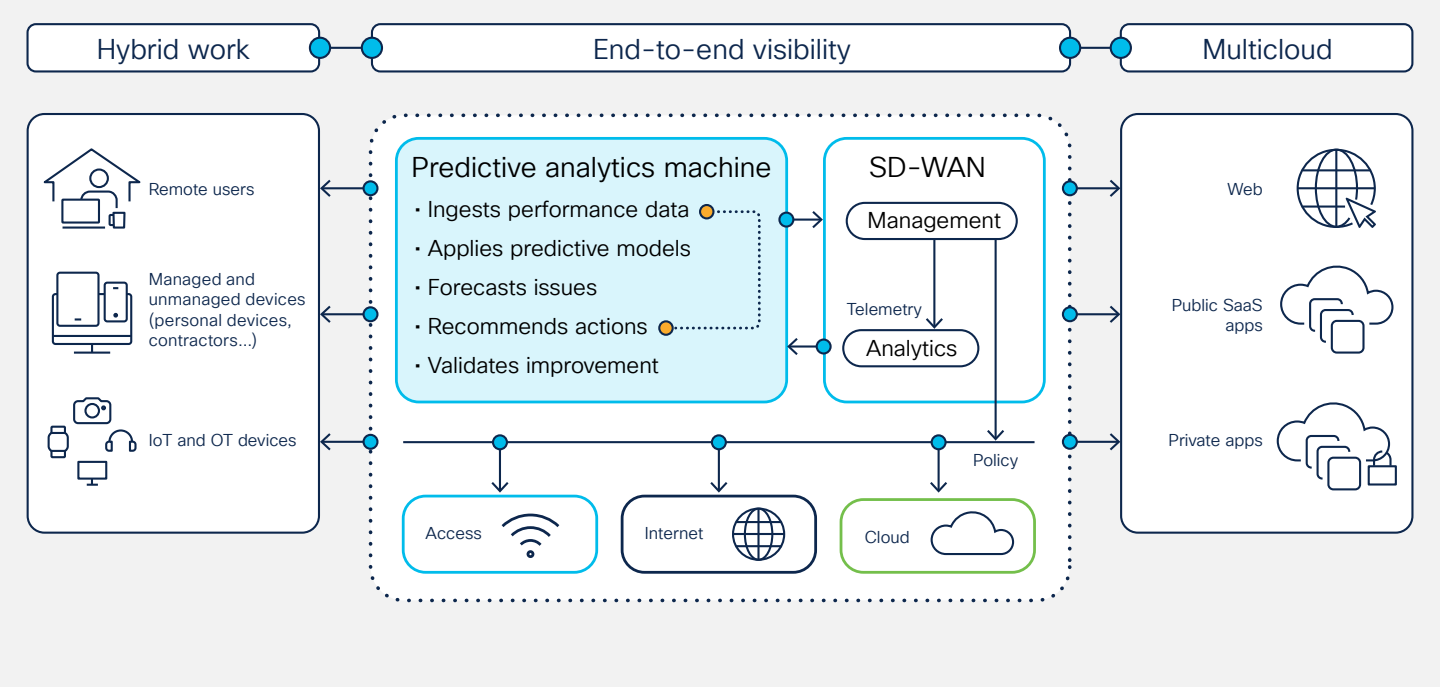


Figure 8. Integrate predictive analytics with SD-WAN management to identify and prevent network degradation before it impacts the user experience.

prioritize the adoption of predictive network analytics to improve cloud connectivity over the next two years.

Bottom Line

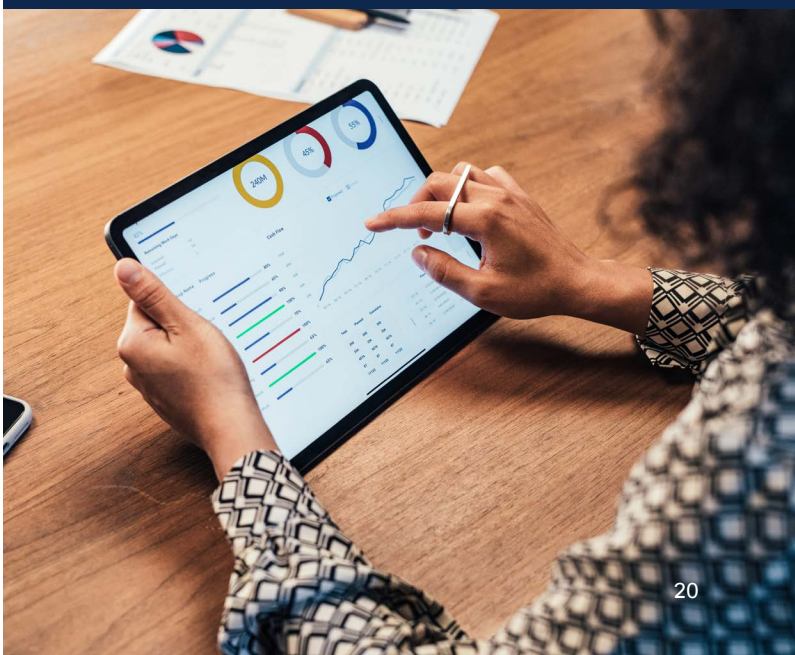
As the Internet shifts and evolves, the speed, cost, and quality of digital experiences hang in the balance. Organizations need to adopt predictive modes and proactive operational workflows that will optimize over time through continual data feedback loops-ensuring greater infrastructure elasticity and resilience.

Expert View

Predictive analytics has arrived because IT teams need it, and the technology is now capable of delivering it.

"Traditional reactive operational modes reroute traffic to alternative paths–but only after detecting a problem (often caused by connectivity issues or degraded services). The exciting promise of predictive analytics is that it uses telemetry, statistical data, and AI/ML-based computing models to predict potential issues before they happen. Cloud-centric environments are inherently unpredictable. The ability to automatically recommend action or proactively redirect traffic will be key to optimizing performance and mitigating the risk of system downtime. This benefits organizations by improving user experience and empowering IT to focus on strategic initiatives rather than reactive triage."

Murtaza Doctor
VP, Engineering
ThousandEyes, Cisco



The bridge to possible

Conclusion

Both remote and hybrid work are here to stay. The adoption of multiple clouds is accelerating. But providing secure, consistent connectivity to highly distributed workers, devices, and applications remains a challenge due to an expanding threat landscape and the complexity of tools and techniques across networking, cloud, and security teams.

In isolation, these teams cannot address these connectivity and security challenges or deliver the digital experiences and agility organizations need to compete. Most IT leaders understand that. They are aggressively bringing together networking, cloud, and security technology, and testing innovative operating models to address these dynamically changing needs.

One clear approach is to move to SASE, with almost half of our survey respondents planning to deploy a well-integrated SASE architecture for connecting their branches and remote clients within two years. The promise of SASE is a simplified and more secure IT experience, thanks to a more effortless and flexible way to securely connect distributed employees and customers to cloud applications at scale. The combination of networking and security platforms that support cloud-driven automation and network insights enables more integrated workflows and better collaboration between NetOps and SecOps teams.

A cloud-centric SASE model harnesses the power of data to deliver capabilities like end-to-end visibility and predictive analytics, which are critical to ensuring a consistent user experience.

There are multiple ways to get started on your SASE journey based on your business and technology priorities.

Learn more about SASE and how Cisco can help you on your journey.

The bridge to possible

About this report

The Global Networking Trends Report was compiled in February 2023, and based on surveys conducted in 13 countries across North America, Latin America, Asia Pacific, and Western Europe.

This year's report included survey data from network operations professionals within organizations using cloud services. This report uses survey data to provide insights into how multicloud environments are influencing network technology and operations priorities, preferences, and choices.

The survey data referenced in this report was commissioned by Cisco, collected by 451 Research, part of S&P Global Market Intelligence, and analyzed by Cisco. It is part of an independent web survey of more than 2,500 global IT decision-makers and professionals in cloud computing, DevOps, and enterprise networking roles.

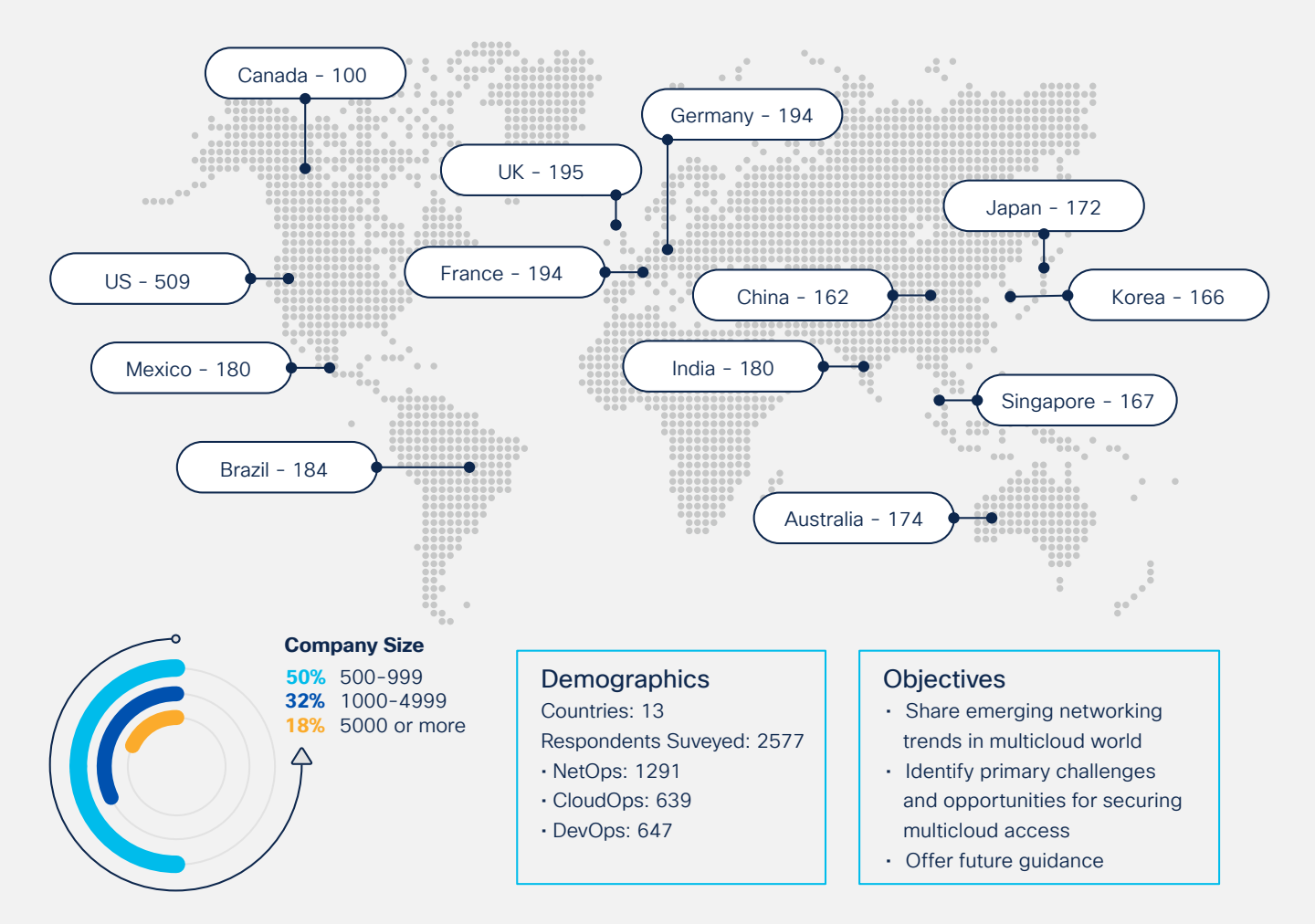


Figure 9. Cisco 2023 global networking trends survey research methodology and objectives.