aryaka

The Report on

Enterprise Network Transformation

2023 Survey
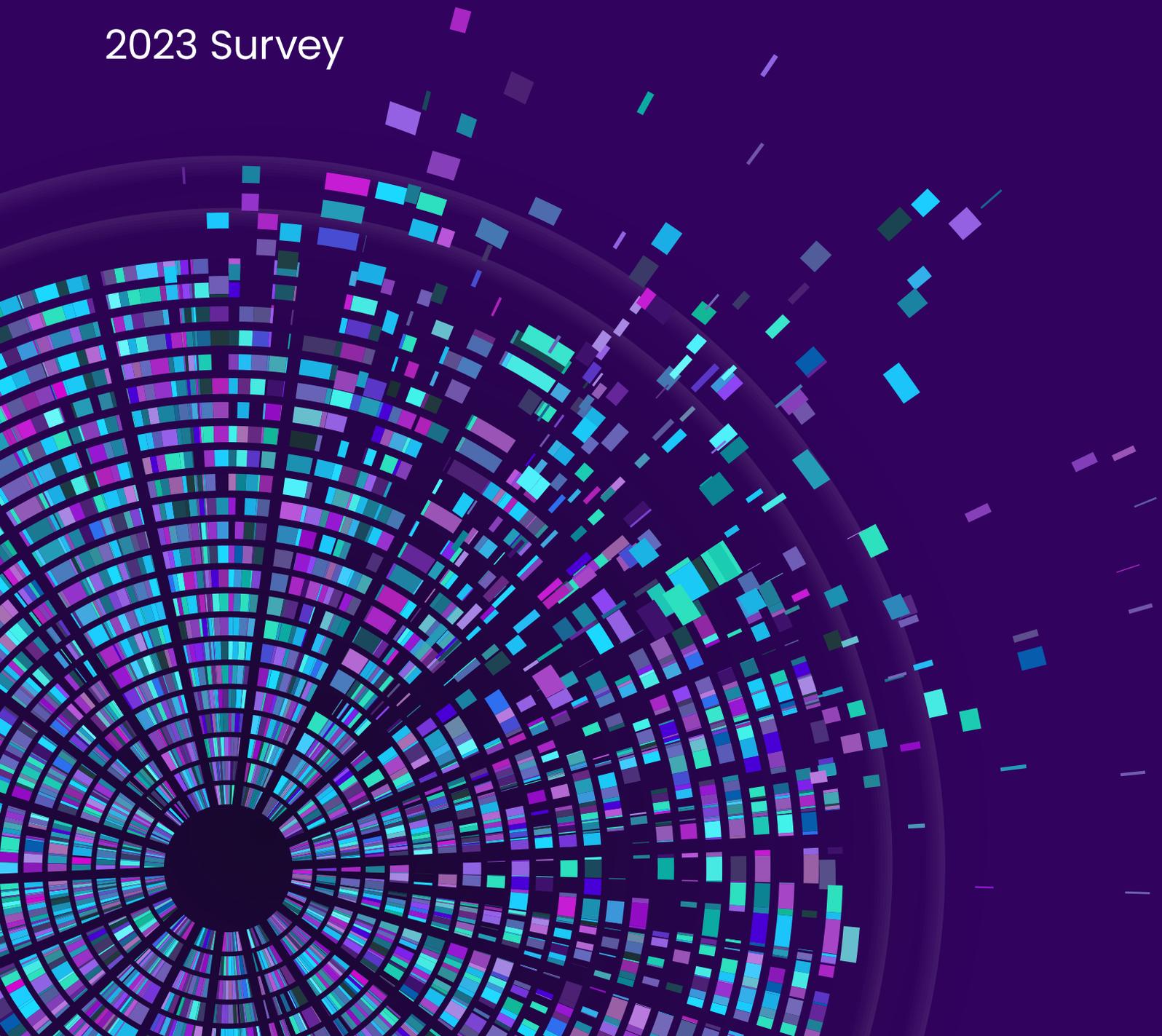
CONTENT

2023. Foundations for the future

01. Introduction

When Harvard Business School students analyze the transformation of the modern enterprise during the 'roaring' 2020s, what will stand out? The global pandemic? Its lingering impact on supply chains? The work-from-anywhere employee?

Or maybe it will be a story led by the economy. Record inflation. Rising interest rates and cost of capital? Banking woes? Or maybe the 'wars' will play a bigger part in the narrative. Russia and Ukraine. The currency wars. The Chip Wars. A new Cold War. An emerging war of artificial intelligence (AI).

It's in this macro chaos where CIOs, CISOs, and IT leaders are charged with building their technology capabilities and new businesses. They own the sometimes thankless mandate of not only operating, but reshaping their companies. In doing so they are preparing for the only certainty they have: uncertainty. Battle scarred and experienced, they now expect the unexpected. They are looking to build organizations that are flexible, adaptable, and ready for anything. In many cases, the architecture, policies, and technologies deployed today will determine how history sees these companies a decade from now.

2023 will prove to be a pivotal year -- the year where promises of converging disciplines like network and security become reality. The year that makes or breaks digital transformation strategies for the Global 2000 and more.

Whatever happens, we do know that networking infrastructure and services will be crucial to business success – as the network connects everything, from branch offices connecting to enterprise applications to AI in the cloud. To find out some of the answers to these questions and what it means for networking connectivity and services, we conducted a survey of 230 senior-level IT managers across the United States, U.K. Germany, and India. As you will see in the survey, global storylines have local effects. The goal of this study is to uncover them.

02. The Goal of This Report

The purpose of this report is to outline key trends in the evolving network and security market including the economic and technology decisions that leaders are making to thrive in a world of change. The research analyzes key themes across 230 C-level (50% of respondents), VP (16%), and director-level (34%) leaders at global enterprises in key roles in network and security.

The survey enabled us to extract trends that are emerging in this dynamic space. Those trends illustrated 5 key themes amongst IT leaders:

Theme 01.
An uncertain economy is impacting network and security budgets, but not in the way you would think as CIOs, CISOs, and IT leaders see the need to double-down on investment in the cloud.

Theme 02.
The rapid shift to cloud services and the complexity of a now hybrid workforce has changed how modern IT leaders view network and security, likely forever.

Theme 03.
Network and security leaders are no longer able to choose between investing in application performance or security; they are expected to deliver all of it and more.

Theme 04.
Network-as-a-Service, the continued decline of MPLS and a need to consolidate a sprawling vendor stack is forcing legacy telcos to lose their longtime stranglehold on the enterprise network.

Theme 05.
Network-as-a-Service is not only emerging, it is exploding as one of the only viable solutions for IT leaders to solve the growing complexity of an anytime, anywhere world.

We had an absolute blast learning from the world's smartest and most capable IT leaders. We hope that you enjoy reading it as much as we enjoyed creating it.

Cheers,

Team Aryaka

03. The Stat Sheet

98%
plan to increase their dependence and investment in cloud services

47%
will be accelerating their adoption of cloud and network services

90%
believe that ZTNA is a crucial component of SD-WAN and SASE services

28%
are selecting specific cloud and network services to save costs
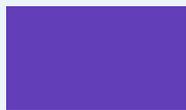
98%
said hybrid work has increased the need for new network and security solutions
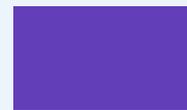
97%
need hybrid work plans immediately or within the next 12 months
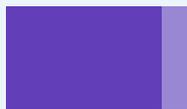
85%
feel that the complexity of networks is their biggest challenge
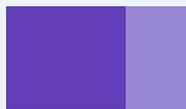
65%
feel that knowledge and expertise is their biggest challenge

35%
highlight network performance as their most critical area of investment
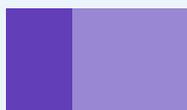
36%
highlight security as their most critical area of investment
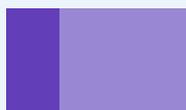
29%
highlight network monitoring as their most critical area of investment

94%
believe that SASE will play a larger role in their network and security plans
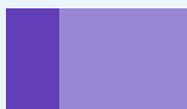
29%
of respondents rank ZTNA as either 1st or 2nd priority for integration for SASE
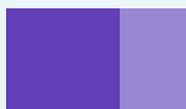
62%
will be phasing out MPLS

95%
of C-level leaders expect managed services and network-as-a-services to play a bigger role in 2023

The Economy Made Them Do It

Theme #1

An uncertain economy is impacting network and security team investment, but not in the way you would think as CIOs, CISOs, and IT leaders want to double down on investment in the cloud.

While headlines of Meta or Amazon layoffs dominate the news cycles, investment in critical enterprise technology, specifically cloud and advanced network services, is accelerating.

In one of the most remarkable findings of the survey, 98% of those surveyed said they will be increasing their investment and dependence on cloud, including cloud networking and security services. This runs counter to the narrative that you may have been hearing – that we are in a technology slowdown. What it does mean is that IT leaders are shifting from traditional IT to the cloud – which makes more sense. Regardless of any short-term macro-economic slowdown, it's clear that managers see cloud technology and infrastructure as a strategic investments for the future.

Some of the key elements in the survey targeted for investment include secure networking technology such as ZTNA, which has become crucial for remote and hybrid work. Leaders are positioning to invest in strategic initiatives such as hybrid work, cloud services, and digital transformation.

The explosion of the Internet, cloud infrastructure, and cloud services has made connectivity and access to the most advanced cloud services easy. It's also providing more competitive networking services than even before – allowing end users to pick and choose how to connect to the Internet or cloud with easily adopted, secure networking services.

Are you increasing your investment in cloud services?

*Did we say something?*
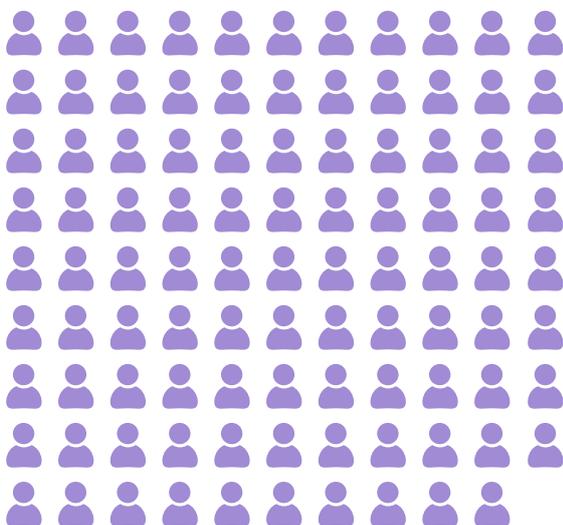
Yes 98%　　　　　　　**No 2%**

There continues to be a robust appetite for investment in new networking infrastructure. Driven by demand for expanding cloud services including software as a service (SaaS) and AI/ML. There is no shortage of need for networks to connect people, applications, and enterprises to datacenters, edge devices, and cloud infrastructure. So, it really is not a surprise to see that 47% of enterprises accelerating the adoption of cloud and network infrastructure, even when the economy threatens a recession.

How is the economy impacting Cloud Infrastructure and Services Adoption ?

47% Accelerating adoption of cloud and network solutions

28% Focusing on specific solutions to save costs

19% Slowing adoption

Outlined later in the report, we look at how and where these IT leaders are investing. We discuss the rise of Network-as-a-Service, and how it will likely follow the same S-curve that IaaS and SaaS demonstrated over the past 20 years.
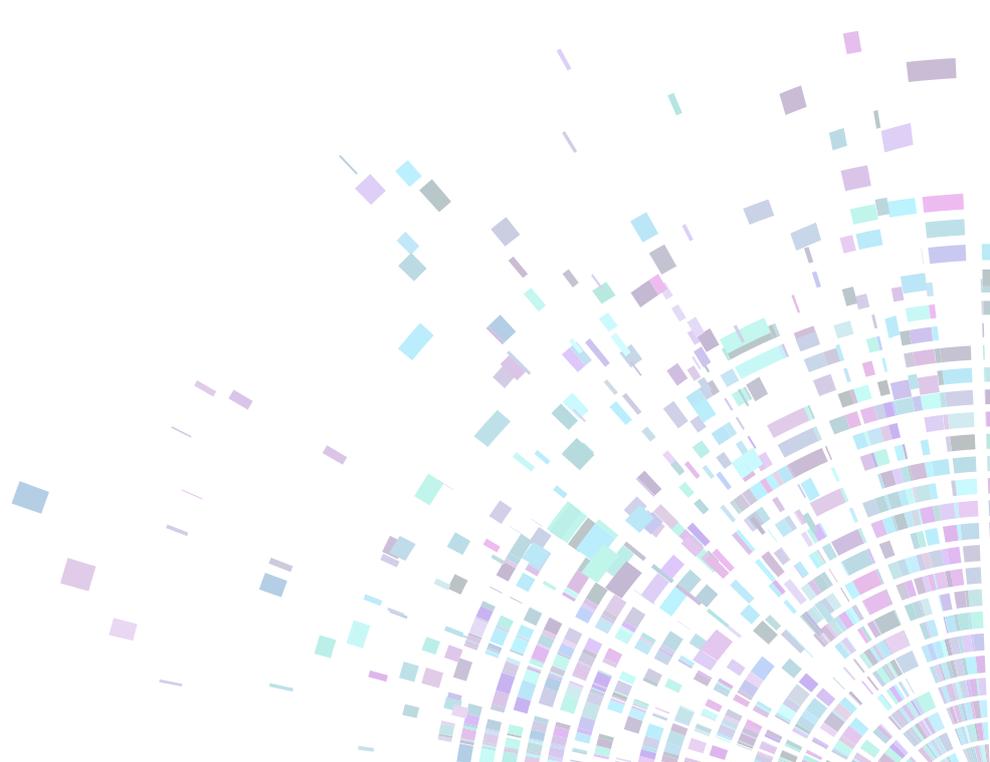
Work From Home Changed Everything

Theme #2

The rapid shift to cloud services and the complexity of a now hybrid workforce has changed how modern IT leaders view network and security, likely forever.

One of the less surprising storylines to emerge was that hybrid work is here to stay. That said, the impact of hybrid work on the transformational decisions that IT leaders are making is significantly under-reported.

One of the most punishing lessons that the pandemic taught IT leaders was that the old way of operating did not fit the way the world was working. The use of VPNs, data centers, and MPLS, were part of a legacy architecture that network and security teams 'got away with' for years. COVID changed all of that. Cloud services, remote work, and hybrid work changed all of that.

> Gartner forecasts 39% of global knowledge workers will work hybrid by the end of 2023
>
> *Source: Gartner Forecast Analysis 2023*

When we asked survey respondents if the advent of hybrid work and remote work has increased demand for technology such as SASE and zero-trust networking (ZTNA), the answer was a resounding yes, with 99% of respondents saying this was true.

Has hybrid work changed how you view managing networks and security ?


Yes 99%

Seriously? Again!?
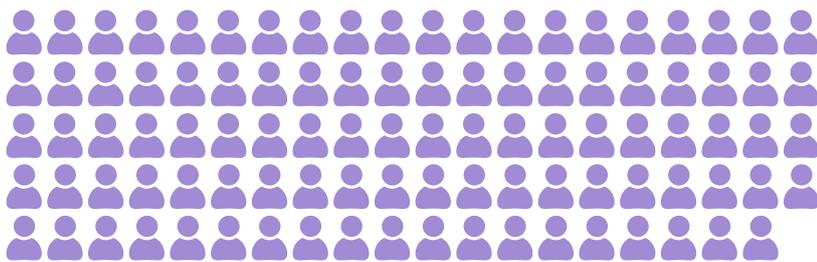
No 1%

There are several key trends behind the emerging need for new networking and cloud infrastructure. But one of the most pressing is to re-orient the digital workforce for a hybrid world in which they can connect to IT resources from anywhere.

The scale and breadth in cloud services and resources is expanding and changes brought about by hybrid work environments require a wholesale rethinking of how networks are delivered and managed. Most importantly, advancements in networking technology such as SD-WAN, SASE, wireless, and ZTNA means that workers can be securely connected in a more cost effective way.

When do you need plans for a hybrid workforce?

58% Immediately

39% Next 6-12 months

3% Greater than 12 months
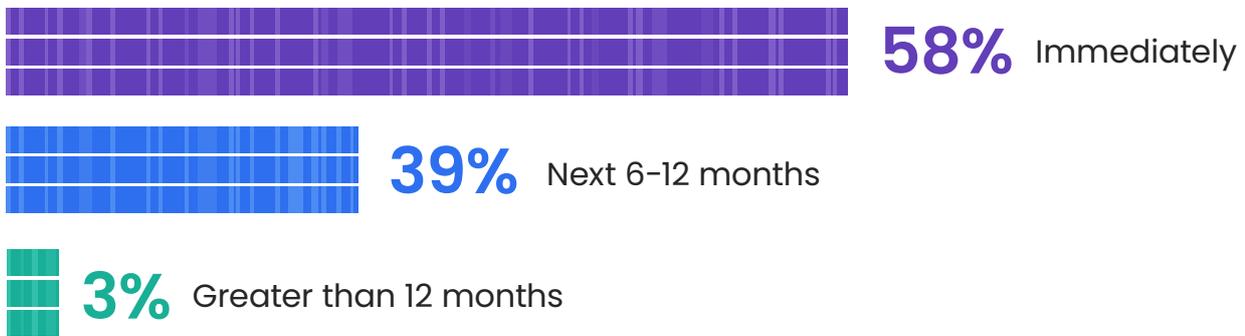
This new workforce, coupled with an expanding dependence on cloud and an enterprise that operates at the speed of Zoom, is dramatically increasing the complexity of networks (and the security that protects them). When asked what your biggest challenges were for managing enterprise connectivity, the top 2 responses were Complexity (83%) and Knowledge and Expertise (64%)

What are your biggest challenges managing your enterprise network connectivity ?

83%
Complexity
of Network

64%
Knowledge
and Expertise
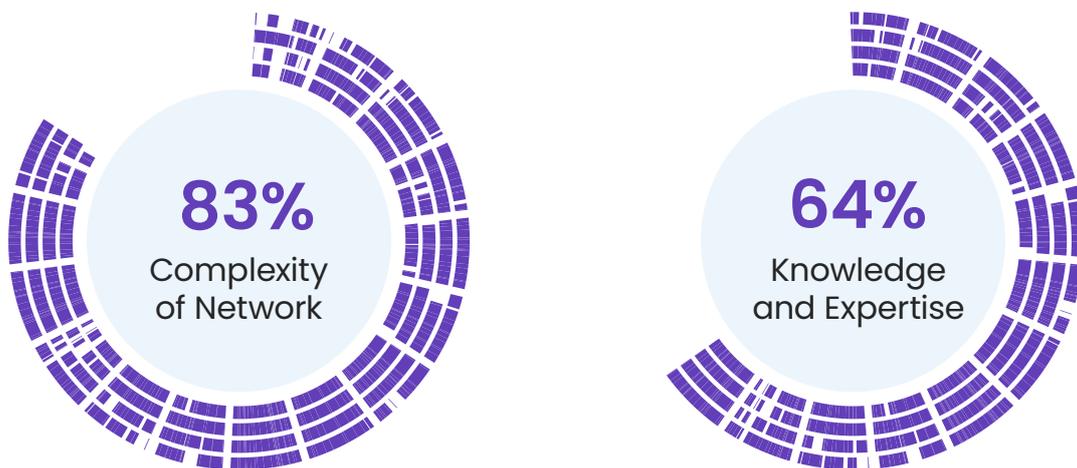
The numbers add up to more than 100%, because multiple responses were allowed. With 2/3rds of respondents acknowledging that they are struggling with the skills and talent to solve the issue, it highlights an emerging trend. This new network and security landscape is not one that you solve with just more headcount.

A new breed of security professionals is emerging, and they are in high demand. The network pro needs to understand cloud. The security person needs to care about application performance. The monitoring guru needs to do more than just monitor… they need to take action. This leads to the next key trend from the report, the days of picking between performance and security are behind us.

# Not This or That. This AND That

Theme #3

Network and security leaders are no longer able to choose between investing in application performance or security, they need it all.

In an always on, work from anywhere world, slow application performance is no longer an option for the enterprise network and security team. Everything needs to work as advertised, all the time. At the same time, the security of those services is non-negotiable. There is no longer a decision to make between performance or security, it's both. And what sits at the center of that balance, is the monitoring and visibility.

When IT leaders were asked where they intend to invest their network budget, the answers were an equal split between all three areas: performance, monitoring, and security. The reality is that it is becoming harder to separate this functionality. The leader was network security, at 36%, which should not come as a surprise. It is interesting to note that 35% of the respondents selected network performance as the next most critical area of investment in 2023, with a slight edge over monitoring and visibility, at 29%. This reflects the reality of earlier themes that the complexity of a hybrid workforce and cloud-first world is driving the demand for applications to perform as we expect them to. The good news is that network security and visibility go hand-in-hand, so you can solve both problems at once.

What is the most critical area of improvement for the 2023 networking budget?

36%
Network Security

35%
Network Performance

Network Monitoring
29%
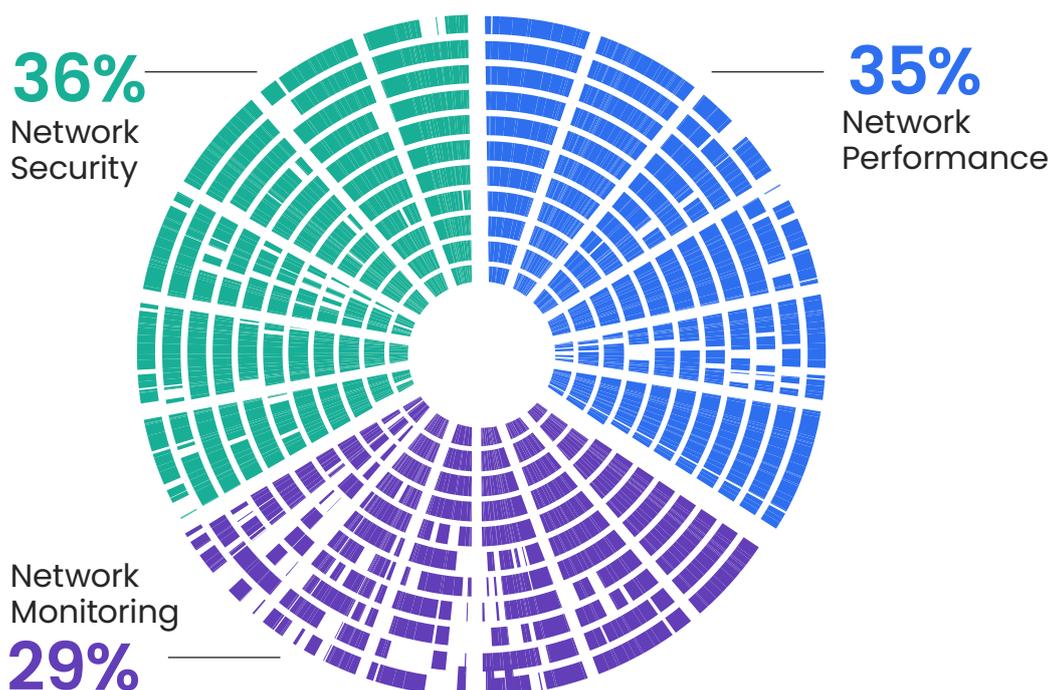
One thing that is sure is that global connectivity continues to be of critical importance. On a scale of 1 to 5 with a higher rating reflecting more importance, 61 % of respondents gave global connectivity the highest rating (5), and another 36% gave it the second highest rating (4). This not only reflects the growing global nature of the enterprise, but also a workforce that is growing increasingly beyond the traditional corporate footprint.

Talent searches now expand well beyond the corporate headquarters. Global teams are now the norm. And as we saw earlier, hybrid work is here to stay. Connecting those employees to the resources they need is the network and how that network operates is how well they can do their job.

How important is global connectivity in a SD-WAN managed service?

|		
Very Important	5	**61%**
	4	**36%**
	3	**3%**
	2	
Not Very Important	1	
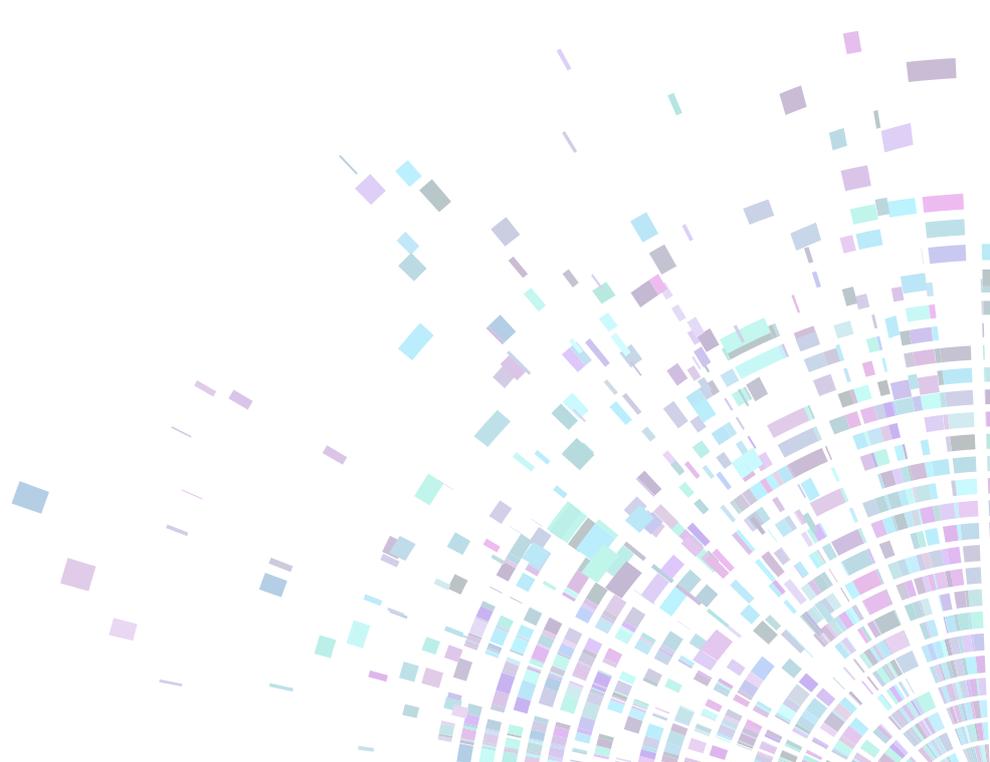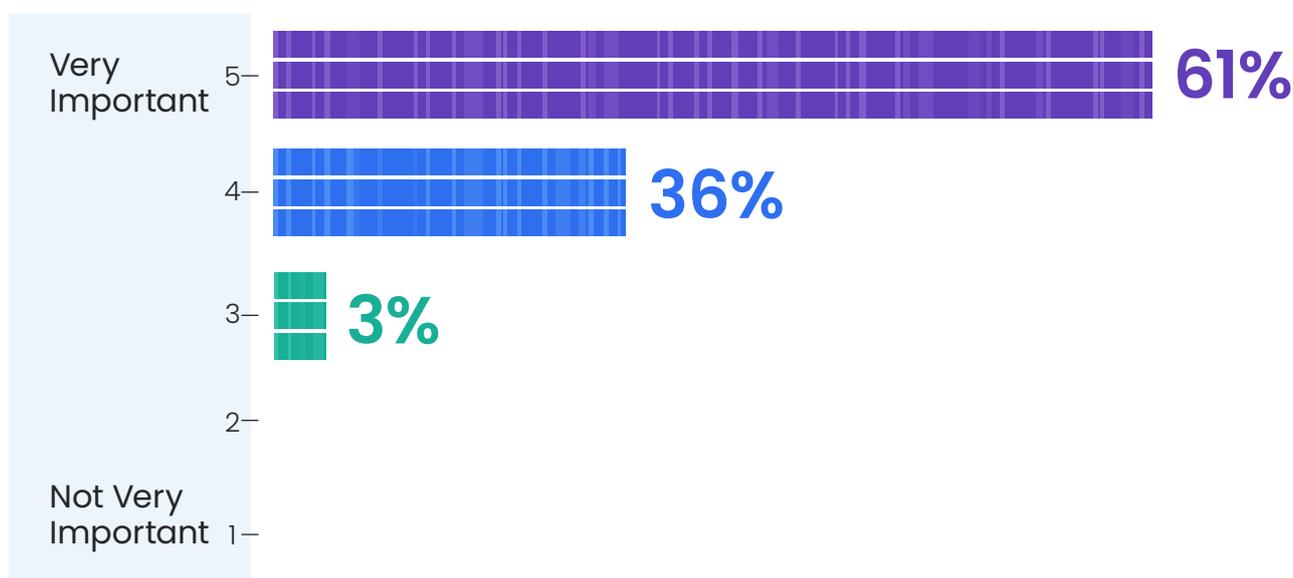
The Fall of Telco MPLS

Theme #4

Network as a Service, the continued decline of MPLS, and a need to consolidate a sprawling vendor stack is forcing legacy telcos to lose their longtime stranglehold on the enterprise network.

You might have gotten the memo – not everybody likes Multiprotocol Label Switching (MPLS). MPLS was a great technology for its time – the 1990s and early 2000s – when it was primarily used to securely connect enterprise offices to data centers or headquarters. And MPLS has become synonymous with services from the large telecom providers (telcos). But traffic patterns have changed, more connections to cloud services are needed, and alternatives such as Dedicated Internet Access (DIA) or private cloud connections can be just as secure and provide business-class performance. There are also a wider range of providers, including traditional telcos, independent managed service providers (MSPs), and cloud providers.

When we asked about the future of MPLS, respondents to the survey sent a clear message: They are moving away from it. As you can see from the responses, the largest group of respondents said they believe that alternatives such as SD-WAN are more effective and less costly than MPLS – and that they are looking to phase it out over time. Of the respondents, 29% believe SD-WAN, DIA, and MPLS serve different needs and will be used for the foreseeable future. A small group of just 7% plan to invest more in MPLS.

7%
Invest in
More MPLS

62%
Plans to
Eliminate MPLS

29%
Continue
Using MPLS
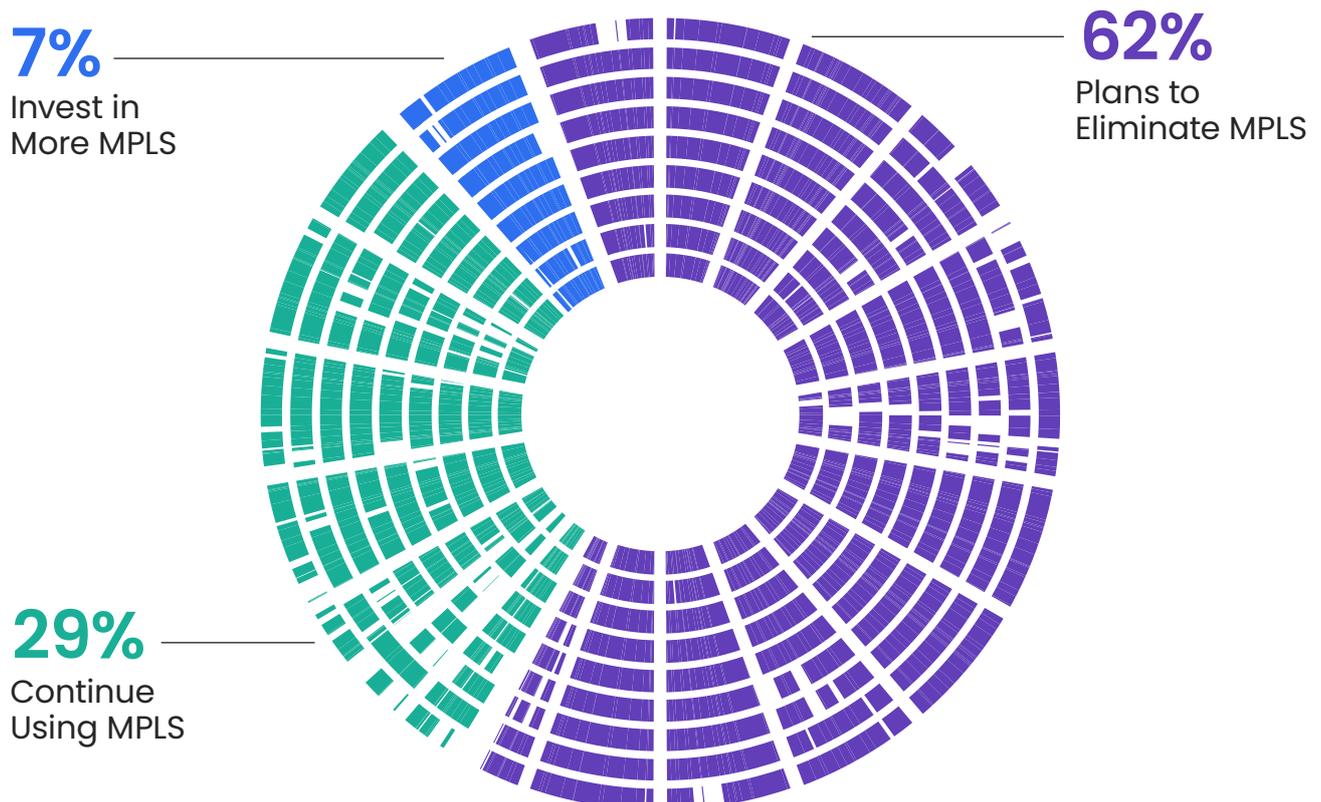
When looking specifically into who enterprises are looking to provide SD-WAN services to, there is a noticeable shift away from the traditional telco. 55% of respondents are looking for alternative providers or will leverage both. As we will discuss in the next section, much of this is in the Network-as-a-Service category.

The shift away from telcos has also been accelerated by the rise of the Secure Access Service Edge (SASE) as well as Network-as-a-Service (NaaS) – which we will cover in the next theme. SASE, a term coined by Gartner in 2019, describes the convergence of network and security into one platform. The prediction is that over time, the disparate vendors that provide tiny pieces of the security and connectivity puzzle – SD-WAN, Cloud Access Service Broker (CASB), Secure Web Gateway, Firewall as a Service (FWaaS), ZTNA – will consolidate into one or a few vendors.

For SD-WAN, Which type of provider would you prefer?

44% Telco

41% Not A Telco

14% Both
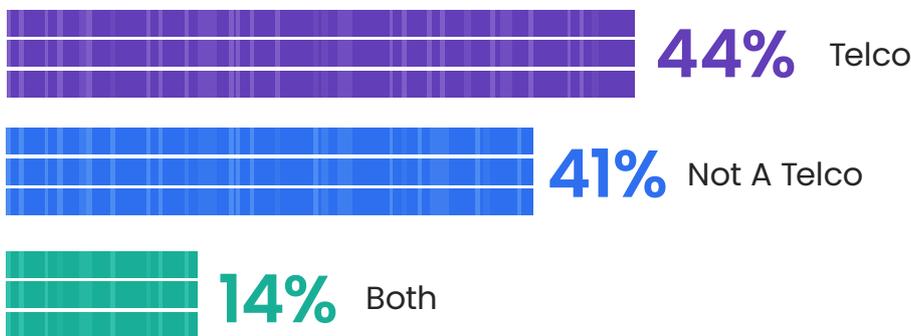
Gartner survey shows 75% of organizations are pursuing security vendor consolidation

Source: Infographic: Top Trends in Cybersecurity 2022 - Vendor Consolidation

This aligns with a host of research that shows that after years of vendor sprawl, IT teams are looking to consolidate, reduce, and simplify their network and security stacks. Aside from the headaches, the risk introduced by managing the handoffs across dozens of niche cloud, security, and network providers is tremendous.

Digging deeper here, we asked to rank order secure access service edge functionality. Cloud Access Service Broker (CASB) topped the list with 30% of respondent ranking it in their top 2 responses. Tied for second place with 25% in the top 2 was Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG) and Advanced Threat Protection (ATP).

Prioritization of SASE Functionality

	CASB	ZTNA	SWG	ATP
1st Preference	19%	15%	13%	13%
2nd Preference	11%	10%	12%	12%
	30%	25%	25%	25%

The Age of SASE and Network-as-a-Service is Upon Us

Theme #5

Network-as-a-Service is not only emerging, it is exploding on the scene as one of the only viable solutions for IT leaders to solve the growing complexity of an anytime, anywhere world.

While SaaS and IaaS exploded on the scene in early 2000s and 2010s, the network and security architectures connecting those services has been slow to catch-up. That changed with the pandemic, the overnight decentralization of the workforce, and an immediate need to modernize a network that was built for a different era.

As IT and networking groups look to serve a more diverse range of services and infrastructure, including hybrid work and cloud services, they need help. One possible solution is managed networking services and NaaS , which enables organizations to partner with managed service providers to provide their global network needs.

> **96% of C-level IT leaders expect managed services and network as a service to play a bigger role in 2023**
>
> *Source: Enterprise Network Transformation Report*

Managed services and NaaS have many benefits:

- NaaS enables organizations to be more agile by adapting networking services on demand

- For human resources, NaaS and managed services can enable internal network staff to focus on more strategic tasks

> **94% of respondents believe NaaS will play a larger role in their network security plans**
>
> *Source: Enterprise Network Transformation Report*

When we asked IT and network staff how they felt about the need for more managed services and NaaS offerings, it's clear that they expect these services to play a greater role in the future. Of the total respondents, 94% of respondents expect managed services and NaaS to play a bigger role, with 95% of C-level executives expecting it to play a larger role in 2023.

There are many considerations that go into building networks that may cause managers to weigh whether to build the networks themselves vs. using a managed service. Some of these considerations include cost, complexity, expertise and knowledge, and time. When our survey asked to choose which elements posed the largest challenges (multiple challenges allowed), the answers were balanced across the issues, with complexity representing the largest challenge by the largest majority (85%), followed by expertise (65%), and cost (58%).

All of these challenges – complexity, expertise, cost, and time – are issues that can be addressed by MSPs, which can build specialized networks at scale. Many organizations do not have the time, expertise, and resources to address these types of networks at scale.

04. Conclusion

2023 has brought about increased debate and uncertainty about the macro economy, and these questions have been exacerbated by the recent banking crisis. However, our survey data reflects the view that technology leaders see the ongoing need to make important strategic investments in technology and networking infrastructure to adapt to long-term changes in the way networks are used by enterprises.

Regardless of the short-term direction of the economy, the survey ratifies the belief in long-term themes -- technology leaders see a crucial need for cloud investment, hybrid work, the need for better applications performance, the need for better security, the decline of MPLS, and the the arrival of NaaS as key long-term investments.

These themes are likely to continue forward for the next decade, regardless of short-term hiccups in interest rates and the stock market. Network services are becoming more crucial than ever to connecting enterprises to applications and data delivered from the cloud. These network services need to be delivered in a secure fashion, and they should be delivered on demand in a dynamic NaaS model, rather than being nailed down in legacy circuits such as MPLS that require long time commitments with inflexible delivery models. The new NaaS model is also being embraced globally, with flexbile networking infrastructure that can be used to securely connect any worker from any location on the planet, to any application in the most efficient way.

The good news for technology leaders: Cloud-based network technology such as SASE, ZTNA, and NaaS are delivered with a more efficient business model that allows managers to scale and adapt their networks to rapidly changing conditions in the workforce or demand. The NaaS revolution is upon is, and it is inherently more flexible and adaptable to the modern cloud economy.

05. Survey Demographics

Aryaka has gleaned the insights from a global audience of network consumers, which included 230 professionals based in the United States, the United Kingdom, Germany, and India. These professionals were filtered by a number of screening questions assuring that they had director-level and above roles in cloud, private security, endpoint security, IT infrastructure, and networking services. All respondents were professionals at companies with more than 100 employees. Among those surveyed, 50% were C-level and 16% were vice president.

35%
Director (Group Director, Sr.Director, Director)

56%
C-Level (e.g. CEO,CFO), Owner, Partner, President

10%
Vice President (EVP, SVP, AVP, VP)
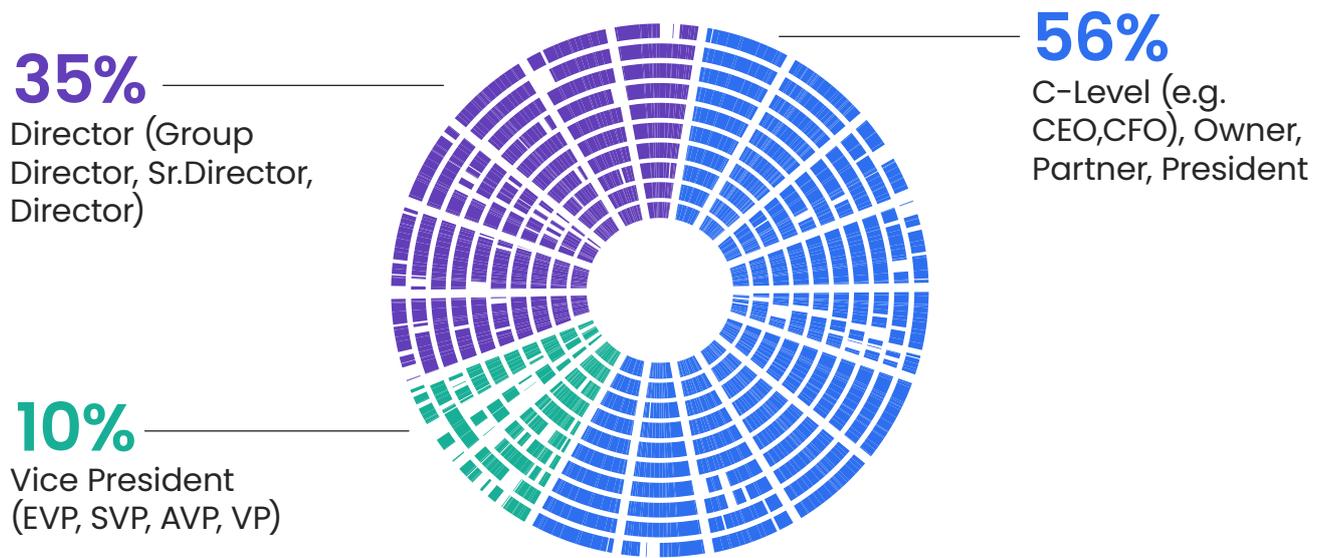
The survey base included 128 U.S. respondents and 102 total International respondents from the U.K., Germany, and India.

All respondents were screened with several filter questions to ensure they worked in an IT or networking role with budget authority.

No Country Recorded

India

Germany

United States

UK
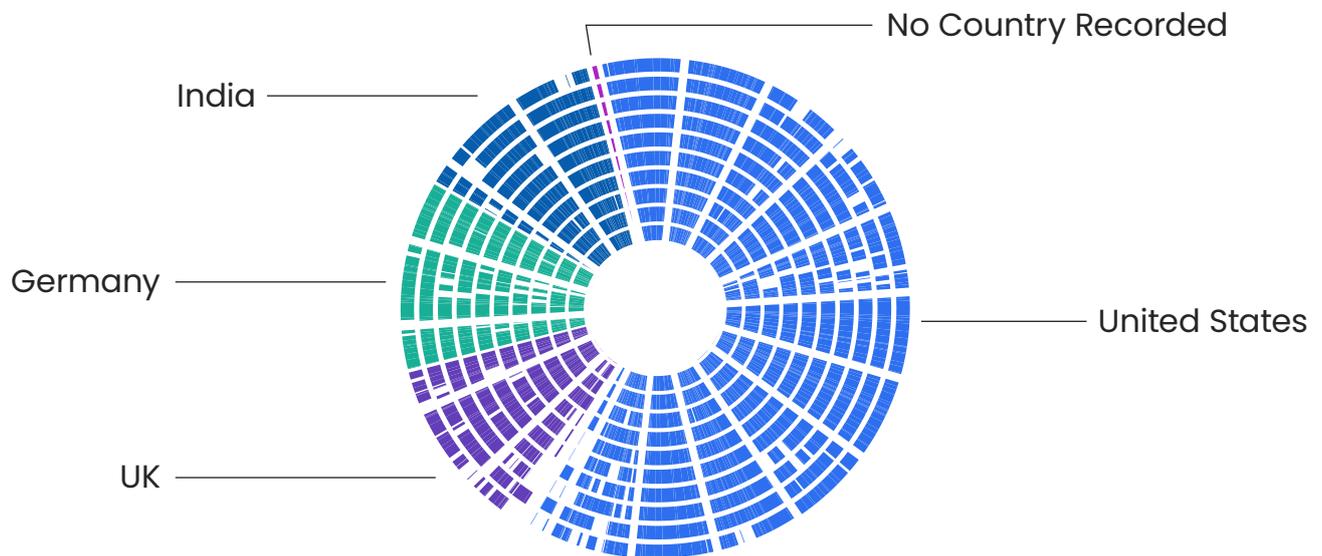
About Aryaka

Aryaka, the Cloud-First WAN and SASE company, and a Gartner "Voice of the Customer" leader, makes it easy for enterprises to consume network and network security solutions delivered as-a-service for a variety of modern deployments. Aryaka uniquely combines innovative SD-WAN and security technology with a global network and a managed service approach to offer the industry's best customer and application experience. The company's customers include hundreds of global enterprises including several in the Fortune 100.

info@aryaka.com | +1.888.692.7925

aryaka