



eBook

Security and Network Transformation in the Age of SASE

As organizations around the world continue their digital transformations, more and more operational resources are being moved into the cloud. These operational resources span the entire IT estate, and success in these projects will require a rethink of both networking and security architectures.

The global network transformation market is expected to reach \$122.73 billion by 2026, at a compound annual growth rate (CAGR) of 39.7%.¹ Similarly, the global cloud security market is forecast to reach \$77.5 billion by the same year at a CAGR of 13.7%.²

Change is clearly underway, but there remains little consensus among organizations about how to approach their network and security projects with regards to budgets, change management, or technology rationalization.

This eBook identifies some of the key challenges that Netskope commissioned research from Censuwide and covering European companies revealed, augmented by third-party studies to provide a global picture. Our aim is to better understand how IT leaders are approaching transformation in the era of Secure Access Service Edge (SASE) architectures, and share insight into how organizations can rationalize teams, processes, and technology in pursuit of SASE success.



¹ "Global Network Transformation Market Research Report," Market Research Future, 2021.

² "Cloud Security Market Report," MarketsandMarkets, January 2022.

The Cost Savings of Moving Security to the Cloud

Research by Deloitte reveals that security and data protection is now a top driver for cloud adoption globally, with 58% of IT executives ranking it either number one or number two.³ A survey of U.S. executives meanwhile found that security is considered the top benefit of cloud computing by 60% of respondents.⁴

This is reflected in our own research. The vast majority of CIOs and CISOs (98%) we spoke to have moved at least some resources to the cloud, although fewer than one in five (18.5%) have transitioned more than three-quarters of their security infrastructure.

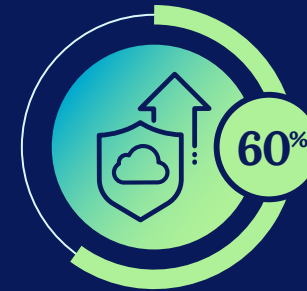
Most of those that are using cloud security have already reduced spending in some of the expected areas: 25% are saving on hardware and 23% on bandwidth. Meanwhile, 21% have reduced costs through vendor consolidation, and 21% have cut their spending on firewall appliances by deploying cloud alternatives instead. This is in line with global research studies. For instance, research by Secure Data suggests that a company with 500 workers will minimize its firewall expenses by 37% and save an average of \$139,000.⁵

However, because most companies are still in the process of digital transformation, it's fair to view these actual cost savings as preliminary—or, at least, worthy of regular re-analysis. For example, in our study, 30% of survey respondents expect to reduce costs through the introduction of Firewall-as-a-Service (FWaaS) technologies, but only 22% report having achieved these savings so far.

Section 1



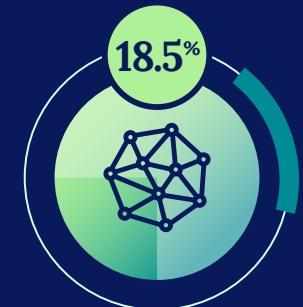
Security is considered the top benefit of cloud computing by 60% of C-level executives worldwide⁶



Security will account for 6% of cloud spending in 2023⁷




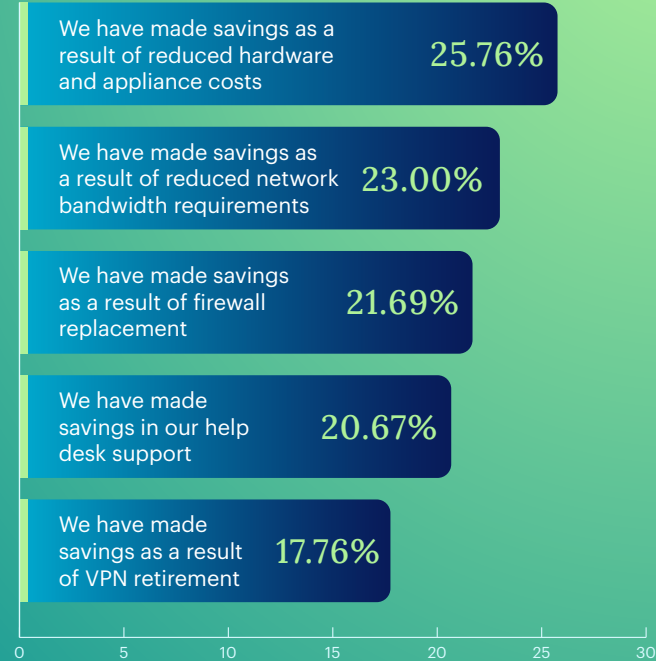
98% of European CIOs/CISOs have moved at least some resources to the cloud



Only 18.5% have transitioned more than three-quarters of their security infrastructure

Chart

Which of these statements, if any, is true for you and your organisation, as a result of moving security to the cloud? 



The Key Takeaway

The transition to the cloud is a work in progress, which means the savings cloud and SASE provide can be expected to increase over time. Organizations are focused on near-term projects such as VPN replacement and vendor consolidation, as the best sources of cost savings over the next one to two years.

³ Karthik Ramachandran and David Linthicum, [“Why organizations are moving to the cloud: Security, data modernization, and cost among top drivers for cloud migration,”](#) Deloitte, March 5, 2020.

⁴ [“55 Cloud Computing Statistics That Will Blow Your Mind,”](#) CloudZero, October 21, 2022.

⁵ Abdul Moiz, [“12 Reasons to Choose Firewall as a Service for your Business,”](#) ExterNetworks, December 8, 2022.

⁶ [“55 Cloud Computing Statistics That Will Blow Your Mind,”](#) CloudZero, October 21, 2022.

⁷ Matt Ashare, [“Security to take an outsized role in IT spending in 2023,”](#) CIO Dive, October 4, 2022.

Network and Security Convergence

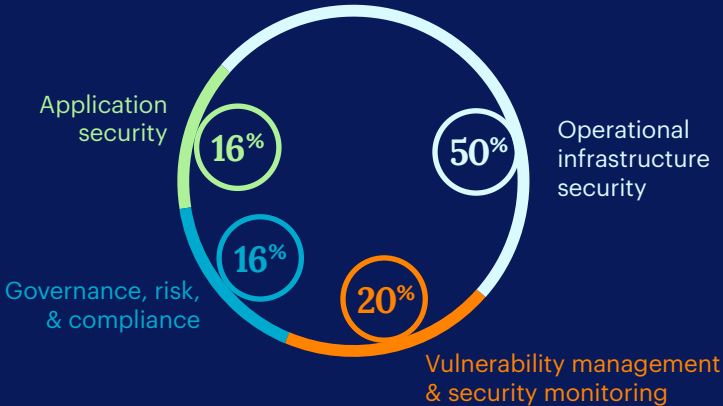
Unifying security and networking functions is a best practice for the corporate cloud journey. Moreover, the reason respondents gave to the Netskope survey for this convergence makes good sense: About a third of CIOs and CISOs think that separating the teams is unhelpful in management of cloud resources.

However, we found that a large majority of companies that are merging security and networking goals are maintaining separation of their budgets. Only 8% of survey respondents said they intend to blend security and networking budgets. Even if both teams report up through the CIO—about two-thirds of these IT teams will be reporting to both the CIO and CISO, either directly or through dotted line hierarchies—they might find themselves competing for resources and ownership of cloud technologies; 28% of respondents anticipate exactly this.

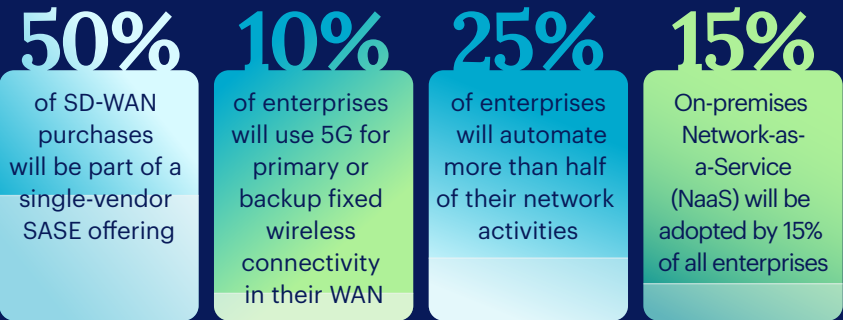
This uncertainty around the right approach to cloud strategy is reflected by broader uncertainty around how best to deal with security right at the top of the enterprise hierarchy. According to one global study by the Economist Intelligence Unit, almost 40% of executives believe that the corporate board should oversee cybersecurity, compared with 24% who felt it should be the role of a specialized cyber committee.⁸



Cybersecurity Budget Allocation in Enterprises⁹



Network Investment Planning Assumptions for 2025¹⁰





30%
of security and
networking teams have
already, or will, converge

but only
8%
are planning to blend
security & networking
budgets



The Key Takeaway

As cloud security best practices evolve, few companies are adopting an optimally efficient approach: converging the security and networking groups from both staffing and budget perspectives.

⁸ Nick Ismail, "[Who is responsible for cyber security in the enterprise?](#)" Information Age, October 25, 2022.

⁹ Toby Shackleton, "[Cyber Security Budget Trends in 2022](#)," Six Degrees, August 17, 2021.

¹⁰ "[The top 5 trends in enterprise networking and why they matter: A Gartner® trend insight report](#)," DE-CIX Management GmbH, September 22, 2022.

A Question of Ownership

Transformational security technologies and frameworks—including SASE, SSE, ZTNA, and SWG—are on the radars of CIOs and CISOs around the world. For instance, global spending on SASE is expected to increase at a CAGR of 26.4% to \$4.1 billion by 2026.¹¹ Similarly, total worldwide spending on zero trust security software and solutions is forecast to grow from \$27.4 billion in 2022 to \$60.7 billion by 2027, at a CAGR of 17.3%.¹²

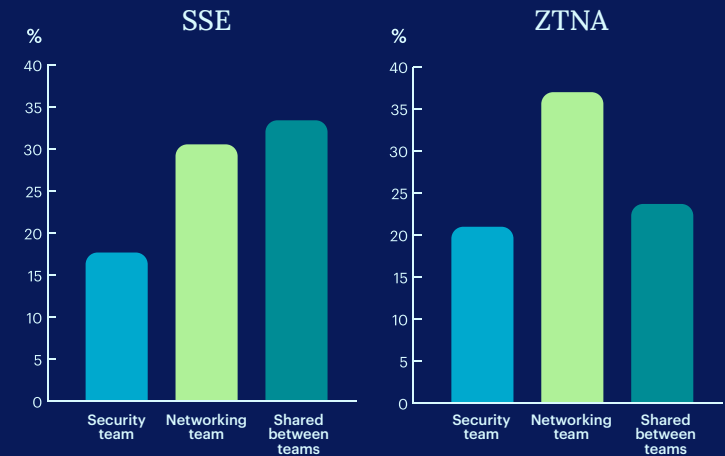
However, a common interest in these technologies does not translate to agreement on which group should have ownership of which products or transformation projects. Our survey found that 28% of companies give ownership of their SASE projects to their networking teams and 18% to their security organization. Meanwhile, in 31% of European companies, responsibility for SASE is shared between the two teams.

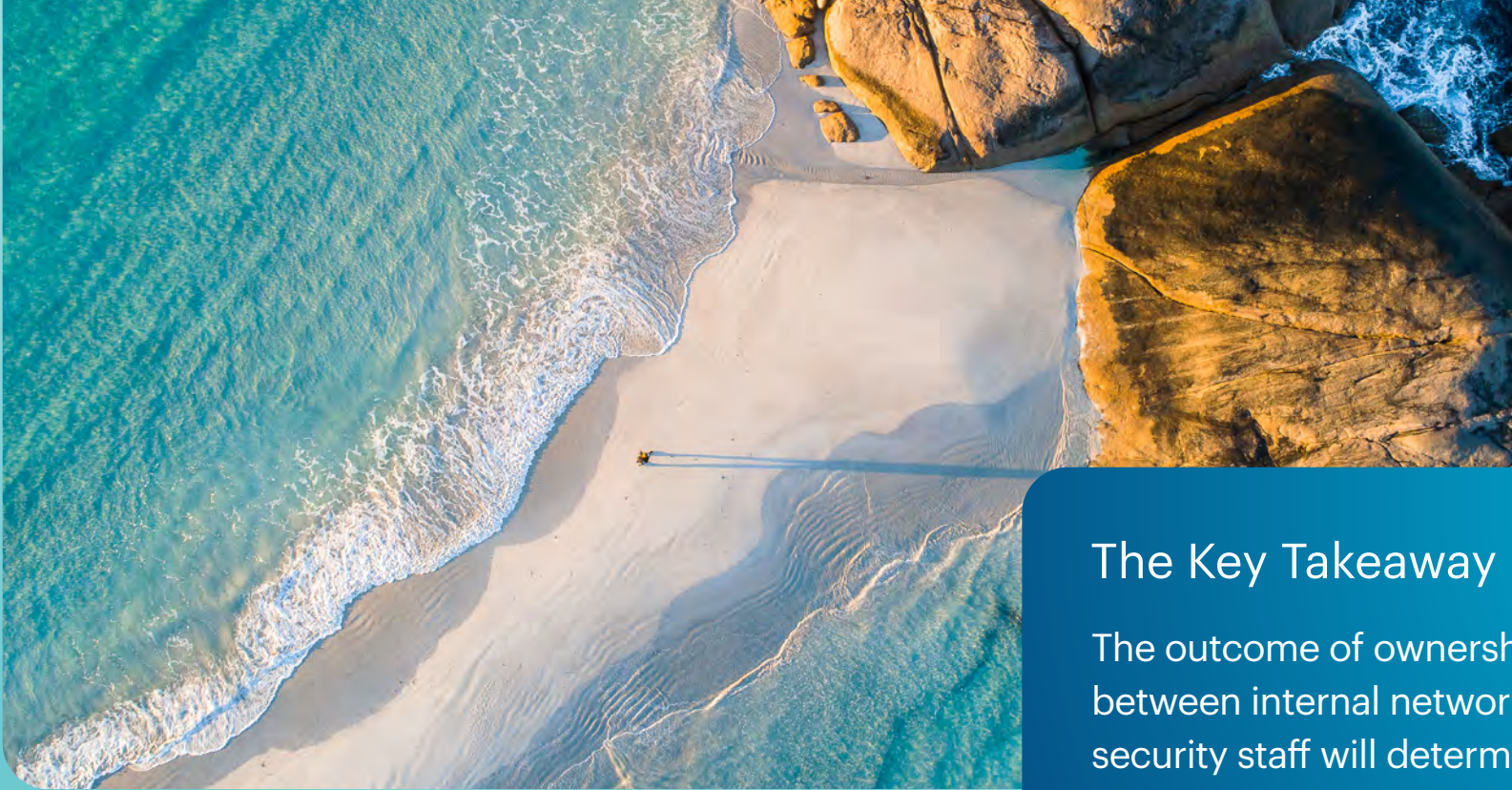
Although SSE is a relatively new term and is considered to comprise the security services that go into SASE, we found very similar divisions of ownership between the two. For SSE solutions, 30% are owned by the networking group, 18% are owned by security, and 33% are shared.

ZTNA is skewed toward networking ownership (37% networking vs. 21% security and 23% shared). SWG is slightly more likely to be a security team responsibility than the other technologies (23% security vs. 28% networking and 27% shared).



When is your organisation planning to undertake a security and/or networking transformation project?





The Key Takeaway



The outcome of ownership battles between internal networking and security staff will determine the organization's SASE direction.

Since there is no broad external consensus on what teams own which initiatives, the CIO and CISO must decide and agree, and then be clear and consistent about which team has responsibility for each area of transformation.

¹¹ ["Secure Access Service Edge Market Report,"](#) MarketsandMarkets, August 2021.

¹² ["Zero Trust Security Market Report,"](#) MarketsandMarkets, August 2021.

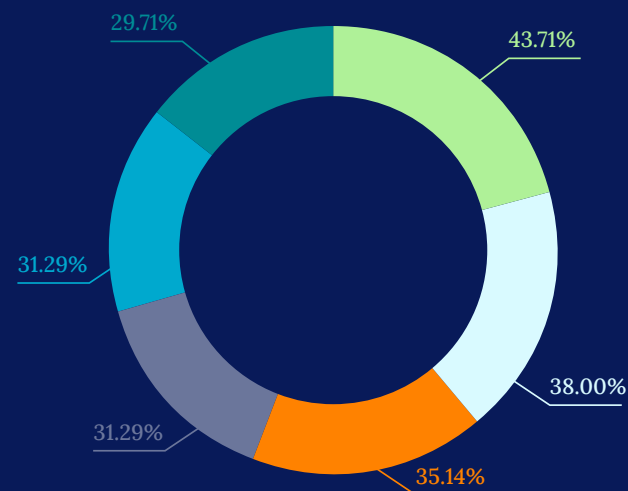
The Security Skills Gap

According to the Cost of a Data Breach Report 2022 by IBM and the Ponemon Institute, 62% of organizations believe that their security team is not sufficiently resourced.¹³ Our research shows that the move to the cloud will further impact the skills gap challenge, with nearly a third of survey respondents either currently growing, or expecting to grow, their security team to reflect the group's broader remit as the organization expands operations in the cloud.

A significant proportion of CIO/CISO respondents (29%) said they have not experienced problems with finding qualified candidates for these security positions. However, an even larger group (46%) are either currently struggling to find suitable candidates or expect to have difficulty doing so in the future. Perhaps because of these concerns, 38% of all respondents plan to look for new security team members outside of cybersecurity or even IT.

Addressing the skills gap is mission critical because until it is solved, businesses are at greater risk of falling victim to an attack. According to the World Economic Forum, 59% of organizations worldwide would currently find it challenging to respond to a cybersecurity incident owing to the shortage of skills within their team.¹⁴ This is little wonder given that just 8% of global technologists have significant cloud-related skills and experience.¹⁵ Conversely, businesses with a sufficiently staffed security team report that the average cost of a data breach is lower than average.¹⁶

If you did need to hire for your security team, where would you anticipate hiring your new security team members from?



-  We would look for candidates with existing cloud/SaaS/IaaS skills/experience
-  We would look for candidates outside of the cyber skills or IT markets and training/reskilling
-  Our competitors, industry peers or other similar organisations
-  We would hire at graduate level
-  We would outsource the team
-  We would re-skill members of the networking, helpdesk and other teams internally



of global organizations agree that security is the top skills gap.¹⁷



have already made changes to the structure or staffing of the networking team.



have made changes to the security team.

The Key Takeaway

Companies' willingness to look for job candidates who don't yet have cloud security skills and experience demonstrates a reassuring level of creativity. But it's not only creative, it's also necessary given the difficulty organizations have in finding talent. CIOs and CISOs who are open to training new security team members—and who are willing to find skills matches or nurture-ready talent in nontraditional places—are much less likely to face a talent shortage.

¹³ ["Cost of a Data Breach Report 2022,"](#) Ponemon Institute and IBM Security, July 2022.

¹⁴ ["What you need to know about cybersecurity in 2022,"](#) World Economic Forum, January 18, 2022.

¹⁵ ["State of Cloud: The cloud skills vs. expectation gap,"](#) Pluralsight, 2022.

¹⁶ ["Cost of a Data Breach Report 2022,"](#) Ponemon Institute and IBM Security, July 2022.

¹⁷ ["State of Cloud: The cloud skills vs. expectation gap,"](#) Pluralsight, 2022.

Budgets, staffing, and division of responsibilities in a SASE era

Moving corporate operations to the cloud represents a true, once-in-a-generation shift for IT organizations and their CIOs and CISOs. Like any significant change, digital transformation is likely to be uncomfortable, but it's something organizations are prioritizing. As they do so, they are also transforming networking and security by moving key systems into the cloud.

Many organizations are still feeling their way toward best practices via trial and error. Some move into the cloud using the same management structures that worked well on-premises and are hoping for the best. This approach is risky. It doesn't make sense to expect legacy skill sets and budget strategies to work just as well in the cloud as in the corporate data center.

The leaders who are likely to be best prepared for digital transformation are gearing up for these projects by realigning budgets, rethinking team resources, and reconsidering recruitment practices. These organizations will be well-placed to leverage opportunities available in the emerging era of SASE-first enterprise.

About Netskope

Netskope is a leader in Secure Access Service Edge, redefining cloud, data, and network security and helping organizations apply zero trust principles. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and protects people, devices, and data no matter where they are. Netskope helps organizations reduce risk, increase effectiveness, and gain unparalleled visibility into all cloud, web, and personal application activity.

Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to mitigate threats and address technological, organizational, network, and regulatory changes.



Methodology



Research undertaken in October 2021 by Censuswide on behalf of Netskope, polling 700 IT professionals in Germany and the UK. Participants are all CIOs, CISOs, or IT Directors for organisations with more than 5,000 IT users.