netskope

Navigating Change: The Operational Impact of Network and Security Transformation

Budgets, staffing and division of responsibilities in a SASE era

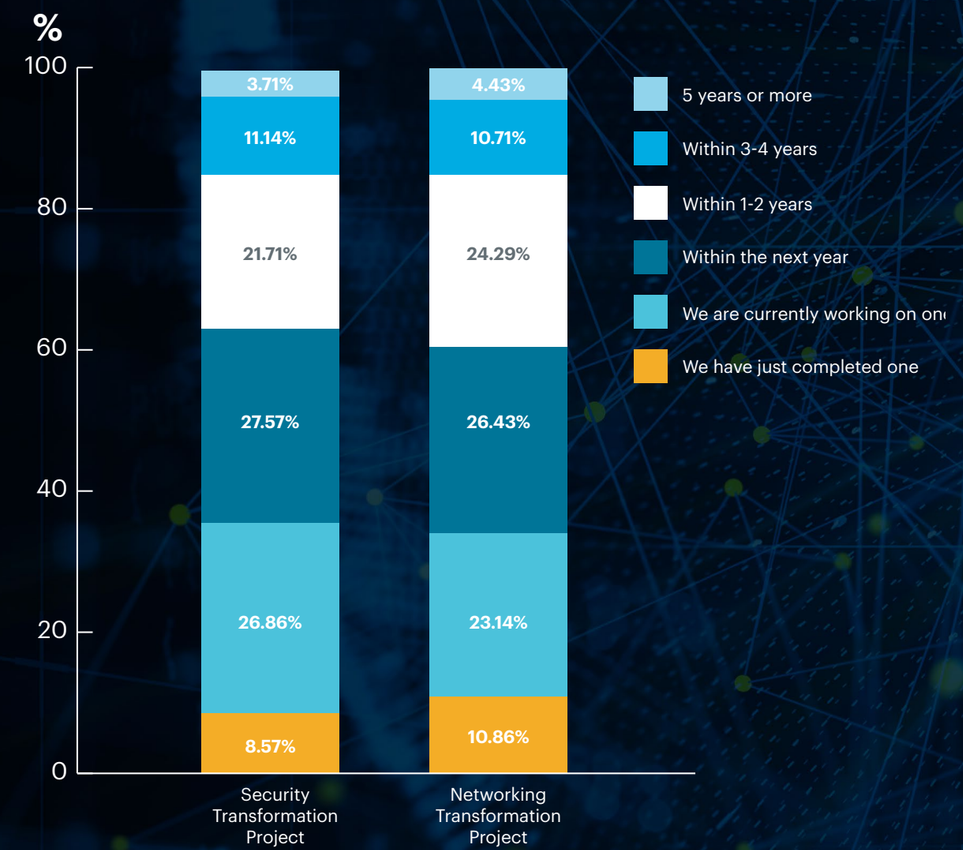
Like businesses in every corner of the world, European organizations are moving more and more operational resources into the cloud as they pursue digital transformation. Ultimate success requires a rethink of both networking and security approaches; and more than 99.5% of IT teams in Europe are either currently working on, or planning to launch, transformation projects in these areas. Currently, however, there's little consensus among organizations on how to approach those projects, whether in terms of budgets, change management, or technology rationalization.

To identify best practices among widely divergent transformation strategies, Netskope commissioned research by Censuswide to assess cloud-based networking and security strategies and understand how IT leaders for European enterprises are approaching transformation.

This is the era of Secure Access Service Edge (SASE) architectures, which converge networking and security across both teams and solutions. But our research shows that companies are taking diverse paths in efforts to navigate the transformation. In most organizations, security and networking teams maintain separate budgets and distinct responsibilities. And in many cases, it's unclear which team has ownership of significant cloud projects or strategies.

This eBook identifies some of the key challenges that our research revealed, suggesting opportunities to find a more collaborative and efficient approach to building secure cloud-based operations and to rationalize teams, processes, and technology in pursuit of SASE.

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



79% of CIOs and CISOs have already seen savings as a result of moving security to the cloud.

The vast majority of European CIOs and CISOs (98%) 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.

Because the vast majority of respondents 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, 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.

98%

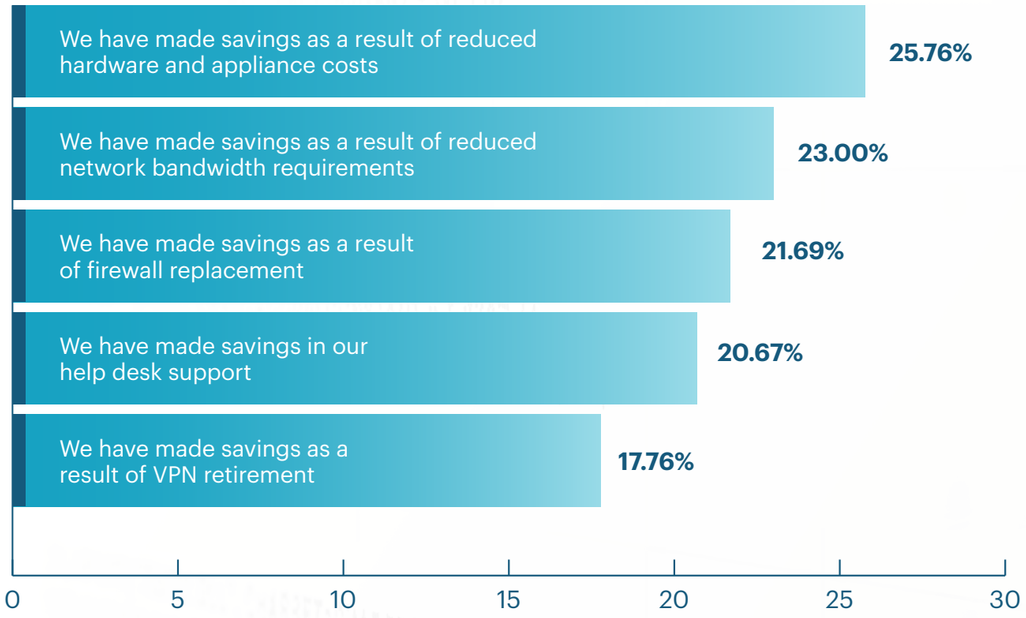
of European CIOs/CISOs have moved at least some resources to the cloud

but only

18.5%

have so far transitioned more than three-quarters of their security infrastructure

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. Businesses 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.

One in three CIOs/CISOs are planning to converge their networking and security teams, but very few are planning to blend security and networking budgets.

Bringing together the security and networking functions is a best practice for the corporate cloud journey. Moreover, the reason survey respondents gave for this convergence makes perfect 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 European companies that are merging security and networking personnel 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 European 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.

These concerns are heightened by a stark lack of consensus among survey respondents about the right cloud strategy. We found that 27% of organizations are moving responsibility and funding for network security to the security team, with the expectation that this additional budget will support transformation projects, including ZTNA and SASE. At the same time, another 27% are pushing security budgets to the network and infrastructure teams to fund a security-by-design approach.

30%

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

but only

8%

are planning to blend security and 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.

Wildly divergent views on who's responsible for key security technologies open the door to ownership battles.

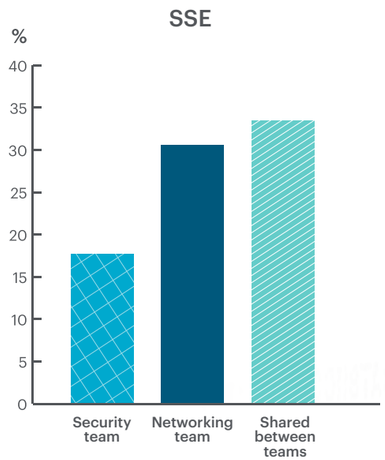
Transformational security technologies and frameworks—including SASE, SSE, ZTNA, and SWG—are on many European CIO/CISOs' radars. However, a common interest in these technologies does not translate to agreement on which group should have ownership of which products or transformation projects.

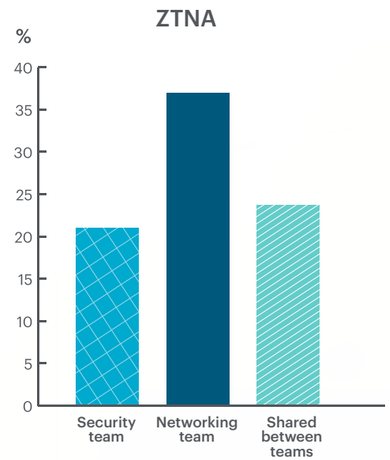
Our survey found that 28% of companies give ownership of their SASE projects to their networking teams and 18% to their security organization. Meanwhile, in 31% of European companies, responsibility for SASE is shared between the two teams.

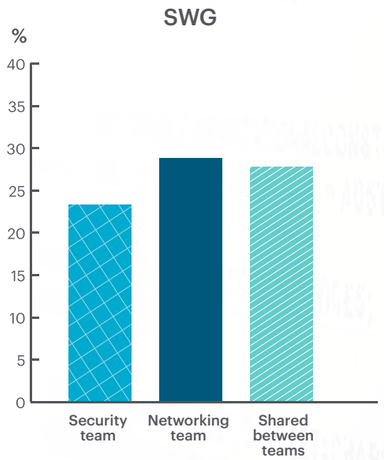
Although SSE is a relatively new term and is considered to comprise the security services that go into SASE, we found very similar divisions of ownership between the two. For SSE solutions, 30% are owned by the networking group, 18% are owned by security, and 33% are shared.

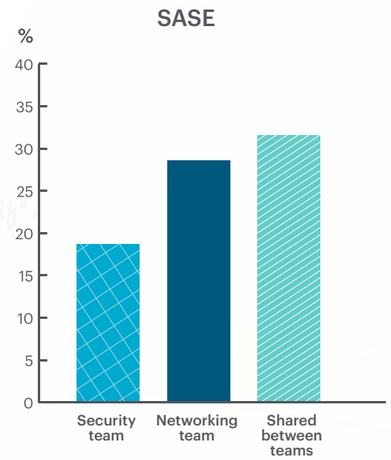
ZTNA is skewed toward networking ownership (37% networking, vs. 21% security and 23% shared). SWG is slightly more likely to be a security team responsibility than the other technologies (23% security, vs. 28% networking and 27% shared).

WHERE DOES THE TECHNOLOGY BUDGET SIT FOR THE FOLLOWING TECHNOLOGIES / INITIATIVES?









The Key Takeaway

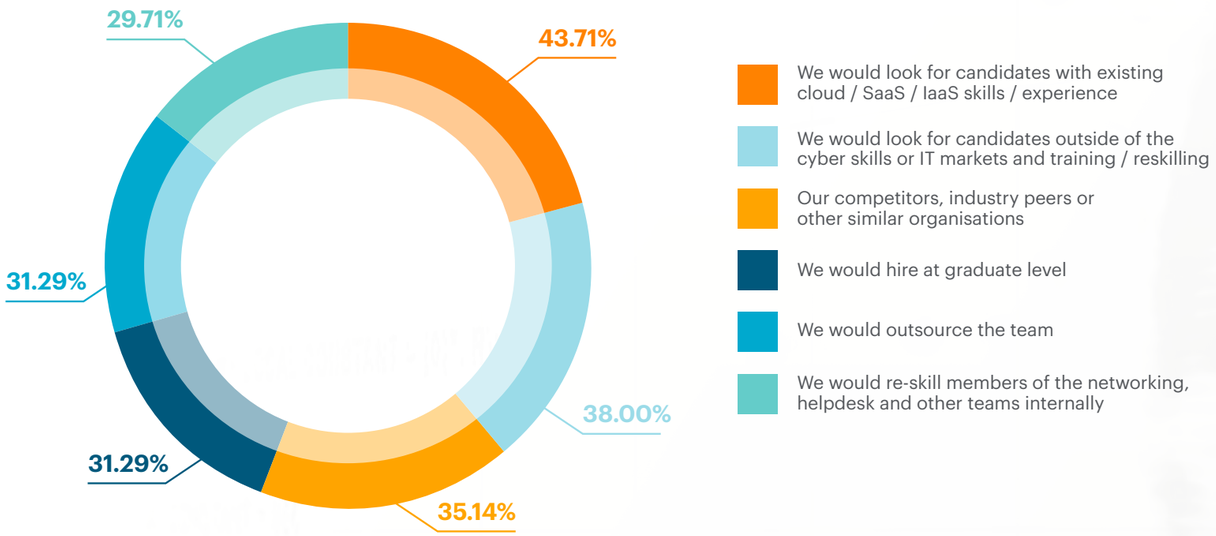
Ownership battles between networking and security staff could challenge outcomes and benefits. Since there is no broad external consensus on what teams own which initiatives, the CIO and CISO must decide and agree, and then be clear and consistent about which team has responsibility for each area of transformation.

46% of companies face staffing challenges as they look to hire additional security team members.

Among the European organizations that have moved some security activities to the cloud, 28% have already made changes to the structure or staffing of the networking team, and 26% have made changes to the security team. Nearly a third of survey respondents are either currently growing, or expect 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.

IF YOU DID NEED TO HIRE FOR YOUR SECURITY TEAM, WHERE WOULD YOU ANTICIPATE HIRING YOUR NEW SECURITY TEAM MEMBERS FROM?



28%

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

26%

have made changes to the **security team**.

The Key Takeaway

European 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: respondent percentages suggest more than two-thirds of teams struggle to find 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 non-traditional places—are much less likely to face a talent shortage.

What You Can Do Today

Moving corporate operations to the cloud represents a true, once-in-a-generation paradigm 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. More than half of our survey respondents expect to launch their planned digital transformation projects within the next two years.

CIOs and CISOs facing the same timeline for network and security transformation face an assortment of conflicting approaches on the best path forward. As our research indicates, most European businesses 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.

About Netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, Cloud Firewall, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere. Unlike others who force tradeoffs between security and networking, Netskope's global security private cloud provides full compute capabilities at the edge.

Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

netskope.com

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.