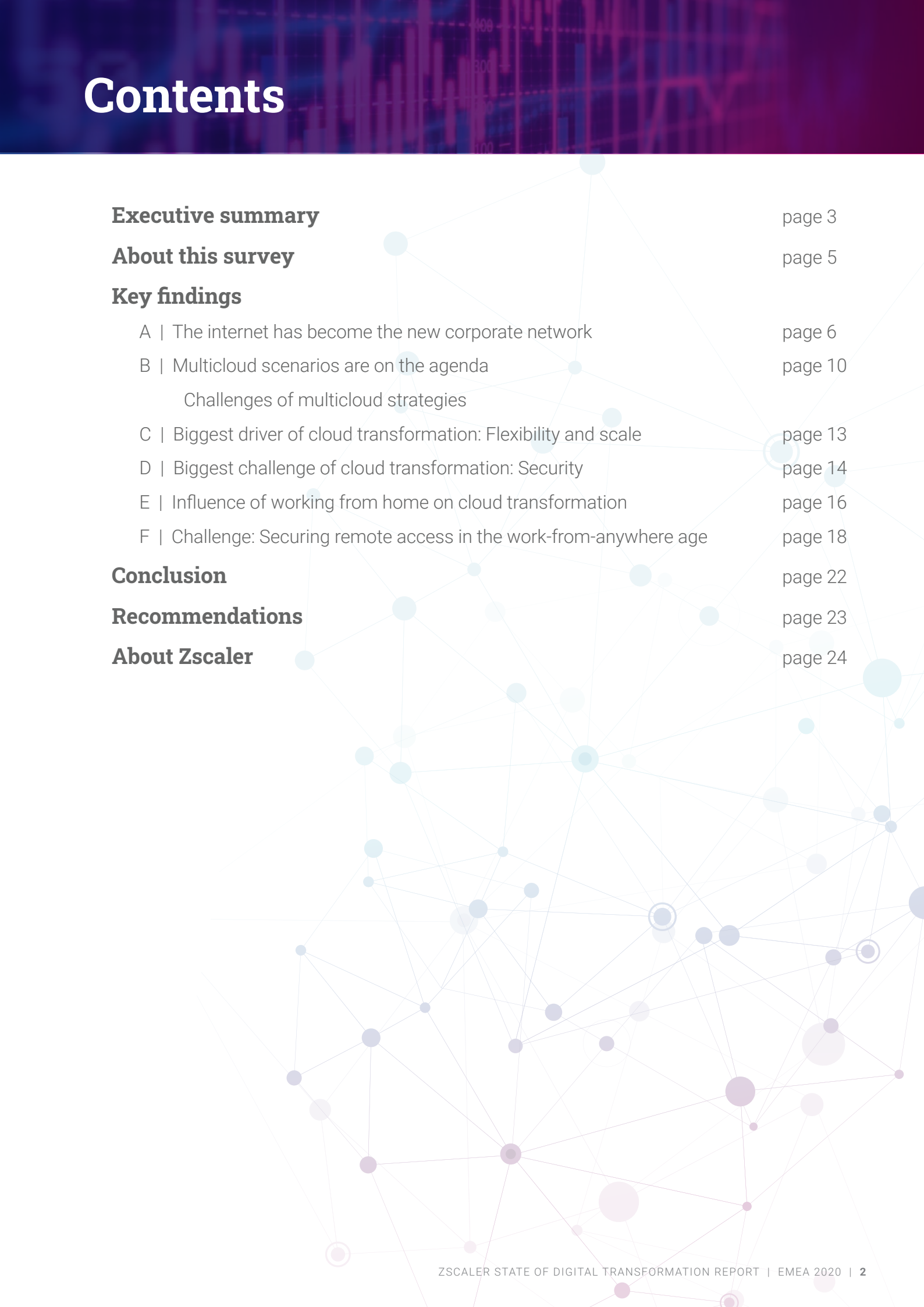# ⊘zscaler™

Report:

Zscaler™ State of Digital Transformation

EMEA 2020

The internet has become the new corporate
network, enabling work-from-anywhere

Contents

Executive summary

Prior to the pandemic, enterprises were actively migrating private applications to public clouds as well as enabling some users to access applications from any location and from any device. In response to the global crisis, employees and enterprises quickly embraced this new flexible style of working to an even greater extent. This has created a proliferation of security perimeters around users, devices, and applications, with corporations evaluating emerging security concepts to cope with these new requirements.

Working remotely means employees have the freedom to access data from practically anywhere, but this freedom also presents challenges related to mitigating business risk, as legacy infrastructures weren't designed to handle an increasingly mobile workforce. IT teams must quickly and securely enable employees to work from anywhere without disruption to the business. This might seem like a daunting task, but the solution is in the cloud: The cloud is what enterprises need when location no longer matters.

Zscaler commissioned the **State of Digital Transformation** Research study of organisations in the UK, France, Germany, the Netherlands, Italy, and Sweden to discover:
- How far organizations have come on their transformation journeys
- Whether the internet has already become the new corporate network
- Whether the cloud is the new data center.

This report includes key research findings and recommendations to help organisations overcome common challenges in complex cloud deployments, and it addresses security concerns during a digital transformation.

Transforming an organization requires a fundamental overhaul of technology ecosystems. With apps moving to the cloud and users connecting from everywhere, the perimeter has become irrelevant and traditional hub-and-spoke networks are outdated. It's time to decouple security from the network and deploy policies that are enforced regardless of where apps reside or where users connect. The survey results show that the companies moving apps to the cloud without adapting their infrastructures and security tend to struggle with complexity and changing security requirements.

Executive summary

Key transformation priorities should include taking full advantage of modern technology and controlling risk. The needs of today's increasingly mobile workforce must be taken into consideration, including a positive and seamless experience. While securing users and applications is more important than ever, visibility across the entire enterprise network and connected device traffic has also become critical in defending corporate assets.

Three key focus areas for the mobile workforce

Supporting a handful of remote workers is one thing, but how do you enable a large workforce to securely access the internet, SaaS, and private applications when they could be anywhere in the world using any device? To start, you need to focus on three areas:

1 **Simplicity and scale:** Traditional network security is inflexible, making the ability to adapt to fluctuating capacity needs painfully slow, incredibly complex, or just plain impossible. Cloud-based solutions simplify deployment, scaling, and management to handle the inevitable changes to the business landscape.

2 **User experience:** Users should not be concerned with how they access an application, what device they're using, or where the app is running. In a work-from-anywhere world, a seamless user experience is critical to productivity. Enterprises need to consider access speed limitations when backhauling traffic through a central hub for the sake of security. The future of user connectivity means fast, local connections with service delivered at the edge in widely distributed, global points of presence to minimize latency.

3 **Security:** Allowing users to connect from anywhere is great, but if you connect them to the network, you face the risk of their infected devices introducing malware that can then move laterally, which leads to the possibility of denial-of-service (DoS) attacks. You must decouple application access from network access, and your attack surface must be as close to zero as possible. Cloud-delivered zero trust network access (ZTNA) services reduce this exposure.

About this survey

The goal of the Zscaler State of Cloud Transformation Research 2020 was to understand where companies are with their transformation efforts, and whether the internet has already become the primary transport network in these organisations. We also looked into the challenges and hurdles along this journey. Since this year's pandemic influenced cloud transformation projects and created a hunger for hybrid work environments beyond the crisis, we investigated these areas as well. We also wanted to find out how companies are coping with securing their multicloud environments.

Survey methodology

What

Atomik Research, on behalf of Zscaler, conducted an online survey of enterprise-level organisations, with 3,000 or more employees, based in the UK, Germany, France, the Netherlands, Sweden, and Italy.

Who

A total of 606 CIO, CISO, or heads of network architecture that are involved in cloud transformation projects were surveyed

WHAT IS THE STATUS OF MIGRATION OF YOUR APPLICATIONS/SERVICES TO THE CLOUD?

Total	Total N=606	UK N=101	Germany N=101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
We have completed 100% of the cloud migration	39%	38%	40%	49%	46%	23%	41%
We have migrated some applications/services to the cloud	61%	62%	60%	51%	54%	77%	59%

Survey demographics

RESPONDENTS BY JOB TITLE

Total	Total N=606	UK N=101	Germany N=101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
CIO	40%	52%	30%	47%	28%	23%	62%
CISO	37%	28%	43%	32%	32%	62%	26%
Head of network architecture	23%	20%	27%	21%	40%	15%	12%

RESPONSES BY COMPANY SIZE

Total	Total N=606	UK N=101	Germany N=101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
3,000 - 4,999 employees	53%	58%	47%	52%	51%	70%	41%
5,000 - 9,999 employees	33%	24%	45%	37%	39%	26%	31%
10,000 + employees	13%	18%	9%	11%	10%	4%	29%

Key findings

A | The internet has become the new corporate network

The overall goal of the report was to figure out how far advanced transformation projects of the responding companies are and how they are coping with the new world of cloud and mobility. Two-thirds of the responding enterprises had moved the majority of their business applications to the cloud, and close to one-fourth of enterprises (22 percent) were hosting more than three-quarters of their applications with a cloud provider. Italy led the way with 53 percent of companies having moved more than half of their applications to the cloud, closely followed by the UK (50 percent), Germany and France (both 45 percent), and Sweden (30 percent). The survey results indicate that the internet has reached the status of the new corporate network and the cloud has become the new data center.

What percentage of your enterprise business applications are running in the cloud?

Total	Total 100%	UK 100%	Germany 100%	France 100%	Netherlands 100%	Sweden 100%	Italy 100%
Less than 25%	1%	1%	4%	0%	4%	0%	0%
26 - 50%	33%	28%	35%	26%	32%	55%	20%
51 - 75%	44%	50%	45%	45%	44%	30%	53%
More than 75%	22%	22%	17%	30%	21%	15%	27%

Two-thirds of the enterprises have moved the majority of their business applications to the cloud.

Key findings

A more diversified picture is presented across the surveyed countries when we asked which applications had been implemented in the cloud. Overall, sales databases, data storage/file sharing, internet security, and B2B portals seem to be equally important, with finance apps being slightly in the lead. Sweden leads the crowd with close to two-thirds of respondents answering that they have sales databases (67 percent), finance (66 percent) and internet security (68 percent) in the cloud, whereas the UK leads with data storage/file sharing (58 percent), and France leads with internet security (55 percent) and B2B portals (56 percent). In Germany, ERP systems (49 percent) and B2B portals (44 percent) are commonly seen in the cloud.

Which applications are you running in the cloud already or are in the process of implementing in the cloud?

Total	Total N=606	UK N=101	Germany N=101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
Office suite	45%	39%	37%	50%	47%	52%	45%
Sales databases	50%	43%	42%	50%	44%	67%	51%
Data storage/file sharing	50%	58%	42%	50%	46%	60%	41%
Printing	31%	29%	40%	34%	37%	27%	19%
ERP	37%	46%	49%	45%	32%	23%	27%
Internet security	50%	42%	46%	55%	40%	68%	52%
People and culture	33%	35%	38%	40%	34%	31%	21%
Finance	51%	34%	43%	51%	61%	66%	50%
Development & eng. tools	37%	43%	33%	37%	36%	43%	34%
B2B portals	50%	50%	44%	56%	50%	58%	40%

(More than one answer was possible)

Swedish enterprises have made the greatest strides in cloud adoption, with two-thirds having moved sales databases, finance, and internet security to the cloud.

Key findings

One-third of German companies tend to keep the Office suite (34 percent) and internet security (29 percent) in house, whereas across Europe, printing (27 percent), people and culture (26 percent) and development and engineering tools (25 percent) are still kept in the corporate data center. Swedish companies are the most prudent, with 37 percent of companies having no plans to move printing services into the cloud, and about one-third of Italian companies plan to not only to keep their data storage/file sharing in house, but also the development and engineering tools.

Which apps are you planning to keep on your corporate network?

Total	Total N=606	UK N=101	Germany N=101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
Office suite	25%	30%	34%	25%	26%	21%	18%
Sales databases	22%	27%	22%	20%	26%	10%	28%
Data storage/file sharing	23%	15%	27%	19%	30%	14%	36%
Printing	27%	29%	25%	26%	25%	37%	22%
ERP	19%	18%	12%	21%	23%	23%	16%
Internet security	23%	29%	29%	19%	28%	14%	21%
People and culture	26%	20%	25%	25%	31%	29%	24%
Finance	21%	29%	27%	27%	13%	12%	27%
Development & eng. tools	25%	18%	22%	22%	28%	21%	33%
B2B portals	22%	22%	22%	22%	16%	21%	32%
Other	6%	4%	6%	4%	3%	4%	

Not only have business applications been migrated to the cloud, but the workforce is increasingly mobile. More than half of European businesses (53 percent) have more than half of their workforce working remotely. In one-third of organisations (36 percent), at least a quarter of the staff is remote. The Netherlands leads the way for remote workforces, with 44 percent of enterprises having more than half of their staff working remotely, and close to one-third of companies having at least 25 percent of their staff working from home. In Italy (35 percent) and the UK (33 percent), one-quarter of the workforce has no fixed office desk, whereas in Sweden (44 percent) and Germany (42 percent), close to half of the workforce is remote.

Key findings

With companies moving applications to cloud service providers and offering a flexible working model for a majority of their staff, the future workplace has already become a reality today. Those companies embracing this are at the forefront of becoming the borderless enterprise, where there is no longer a corporate perimeter that surrounds the workforce. Instead, everyone operates like they are their own branch office. This shift away from a 9-to-5 office culture has serious implications. How can staff be managed efficiently without face-to-face contact on a daily basis? How will teams collaborate effectively and how can productivity of the workforce be measured? Aside from HR and people management implications, the new corporate workstyle needs to be secured effectively. When data has left the data center and staff work outside the corporate perimeter, the organization becomes exposed.

What percentage of your workforce has no office desk (e.g., road warriors/home-based office)?

Total	Total 100%	UK 100%	Germany 100%	France 100%	Netherlands 100%	Sweden 100%	Italy 100%
25% or less	11%	20%	15%	10%	9%	5%	8%
26 - 50%	36%	34%	42%	31%	30%	44%	36%
51 - 75%	33%	29%	30%	31%	44%	31%	35%
76 - 100%	20%	18%	14%	29%	18%	21%	22%

In more than half of the European enterprises surveyed, the majority of employees have no fixed workspace in their companies' offices.

B | Multicloud strategies are on the agenda

Before companies started their cloud transformation projects, corporate applications lived within the corporate network where they could be controlled and monitored. Nowadays, enterprises seize the opportunity to move applications to more cost-effective and more business-effective locations. If applications can reside anywhere, enterprises can decide whether or not to change the location of applications at any time without impacting the service for the end user. Multicloud strategies are on the rise as enterprises use the internet as the new corporate network and work with more than one cloud service provider.

On average, nearly half (49 percent) of the respondents said they operate in a multicloud set up of two cloud service providers, such as Amazon Web Services, Microsoft Azure, or Google. One-third of companies already have three providers. Sweden (52 percent) and the Netherlands (42 percent) are the most diversified, having already moved to three cloud service providers, followed by the UK with 30 percent. In Italy and Germany, most respondents operate with two cloud providers.

One reason for a multicloud scenario is that business units typically dictate the cloud provider based on the specific requirements of the applications being used. That means it is commonly the app that chooses the cloud, not vice versa. Enterprise business apps will find their requirements better suited to one cloud provider than industrial apps with their specific use cases for developers.

How many cloud service providers (such as AWS, Azure, Google, SAP, etc.) are you using in your enterprise?

Total	Total N=606	UK N=101	Germany N=101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
One	13%	22%	20%	11%	10%	7%	7%
Two	49%	49%	44%	60%	45%	34%	64%
Three	33%	27%	30%	23%	42%	52%	23%
More than three	5%	3%	7%	6%	4%	7%	6%

Key findings

Challenges of multicloud strategies

The cloud is supposed to simplify the infrastructure of an enterprise. However, with multicloud scenarios, IT decision makers face various challenges. The most common problems are securing access to multicloud networks (36 percent), setting up multicloud networks (35 percent) and, according to 32 percent of respondents, rising costs within MPLS networks. These challenges have one point in common: How can the architectural set up meet the demands of staff to seamlessly and securely access multicloud environments without driving up costs and complexity?

	TOTAL	
TOTAL	**529**	**100%**
Setting up multicloud networks	**183**	**35%**
Administration complexity	**156**	**29%**
Access for branch offices	**144**	**27%**
Bandwidth for branch offices	**155**	**29%**
Access for remote users	**145**	**27%**
Inconsistent user experience	**162**	**31%**
Loss of control over user access to applications	**125**	**24%**
Securing access to multicloud networks	**189**	**36%**
Performance of access to cloud applications	**148**	**28%**
Handling mergers and acquisitions	**129**	**24%**
Rising costs for MPLS networks	**169**	**32%**
Slow response to security events	**139**	**26%**

(Up to three answers were possible)

Enterprises are facing a common dilemma: How can the architectural setup meet the requirements of workers to seamlessly and securely access multicloud environments without driving up costs and complexity?

Key findings

On a country-by-country view, the challenges are more diversified. Set up remains one of the most common problems among 40 percent of respondents in Germany and 38 percent in the Netherlands and Sweden, while inconsistent user experience ranked higher at 41 percent in Germany and 40 percent in the Netherlands. Around one-third of enterprises struggle with bandwidth for branch offices, according to 35 percent of respondents in Germany, 33 percent in the Netherlands and Italy, followed by 31 percent in France. An equally important hurdle for one-third of enterprises seems to be remote access for end users, chosen by 32 percent in Germany and 35 percent in Italy, which is not surprising given the fact that inconsistent user experience was already ranking as one of the main overall challenges.

What challenges do you face in your multicloud network setup?

Total	Total N=529	UK N=79	Germany N=81	France N=90	Netherlands N=91	Sweden N=94	Italy N=94
Setting up multicloud networks	35%	33%	40%	23%	38%	38%	35%
Administration complexity	29%	29%	36%	21%	29%	33%	30%
Access for branch offices	27%	28%	31%	19%	32%	31%	23%
Bandwidth for branch offices	29%	22%	35%	31%	33%	22%	33%
Access for remote users	27%	29%	32%	21%	24%	23%	35%
Inconsistent user experience	31%	24%	41%	32%	40%	31%	17%
Loss of control over user access to applications	24%	23%	32%	23%	21%	28%	16%
Securing access to multicloud networks	36%	30%	35%	38%	26%	38%	46%

Where do the challenges come from?

Enterprises are likely to struggle with the complexity of multicloud setups and security concerns if they stick to their traditional hub-and-spoke network infrastructures when moving applications to the cloud. Application, network, and security transformation must go hand in hand to avoid common challenges. Enterprises must address these challenges by answering the following questions:

Challenge 1 | Complexity and Bandwidth | How can the network architecture be adapted to seamlessly and securely access multicloud environments without latency?

Challenge 2 | User Experience | How can security requirements be matched with an architectural network set-up, so that a user no longer needs to manually interact?

Challenge 3 | Remote Access | How can a large distributed presence of staff be supported, that need secure access to multiple environments?

C | Biggest driver of cloud transformation: Flexibility and scale

We asked about drivers and challenges in our **State of Digital Transformation Report in 2019** and saw some changes in this year's feedback that might be due to the global pandemic. When asked for the top three drivers for transformation in 2019, the top responses were introducing more efficient processes (38 percent), allowing employees more flexibility (37 percent), being able to focus on core competencies (36 percent), improved profit margins (36 percent), and increased cost savings (35 percent).

In 2020, allowing employees more flexibility has risen to 42 percent (up 5 percentage points), followed by the ability to scale with demand, reduced on-premises administration complexity, and the business strategy to focus on core competencies (all at 40 percent). Increased cost savings rose to 38 percent and improved profit margins remained flat at 36 percent.

There are considerable differences on a country-by-country level. The UK and the Netherlands see the ability to scale with demand (41 percent and 42 percent, respectively) as more important this year, whereas financial aspects, such as increased cost savings (41 percent) or improved profit margin (42 percent in Benelux) were dominating in 2019. Most important for UK enterprises is, however, the business strategy to focus in core competency (43 percent). Flexibility for employees is most important for around half of the enterprises in Germany (51 percent), followed by the ability to scale with demand. For French IT decision makers, more-efficient processes (41 percent) and improved margins (40 percent) are the most important drivers, whereas more than half of the Dutch enterprises want to reduce on-premises administration complexity (54 percent).

What were the main drivers of moving your business applications to the cloud?

Total	Total	UK	Germany	France	Netherlands	Sweden	Italy
Introduce more efficient processes	38%	36%	30%	41%	31%	43%	49%
Allow employees more flexibility	42%	37%	51%	37%	37%	48%	44%
Ability to scale with demand	40%	41%	46%	37%	42%	45%	31%
Reduce on-premises administration complexity	40%	36%	42%	39%	54%	28%	34%
Business strategy to focus on core competency	40%	43%	39%	33%	42%	41%	43%
Improve profit margin	36%	37%	40%	40%	30%	43%	30%
Increase cost savings	38%	38%	43%	34%	31%	38%	44%

D | Biggest challenge of cloud transformation: Security

In last year's survey, security topped the list of biggest obstacles to transformation across all regions for nearly one-quarter of the decision-makers (23 percent), with the UK having the greatest concerns (28 percent), followed by Germany (26 percent). Complexity of transformation projects was next, mentioned by 13 percent of decision-makers, closely followed by lack of expertise (12 percent).

Not surprisingly, security still ranks first with even higher importance this year—42 percent of respondents across Europe reported challenges in this area. Costs and lack of in-house expertise were cited by more than one-third of respondents (36 percent), closely followed by complexity (35 percent). On a country-by-country level, Italy (50 percent) is most concerned about security, followed by the UK and Germany (46 percent), then Sweden (43 percent).

The biggest challenges in France are costs (47 percent) followed by company culture (35 percent). In the Netherlands, employee concerns around keeping their jobs (40 percent) is still dominating, similar to last year. Job insecurity has been raised as an issue as well by 43 percent of UK and 39 percent of Swedish respondents. This correlates with the challenges in both countries with regards to a lack of in-house expertise, as well as in Sweden (44 percent) and the Netherlands (37 percent). This issue also ranks high in Italy (42 percent) and Germany (41 percent). Cloud expertise seems to be less of an issue in France, only mentioned by 25 percent of companies in France and by 32 percent of UK respondents.

These findings show that while the cloud brings benefits to end users and enterprises alike, it also brings huge upheaval for the network architects tasked with overseeing this transformational shift. Understandably, this shift unsettles network architects, who are struggling to see a future for themselves in a cloud-first ecosystem.

In our 2019 survey, 23 percent of respondents said security was their greatest concern. In 2020, that number rose to 42 percent.

Key findings

The corporate network is the network architect's responsibility, but the cloud undermines its importance, which, in turn, diminishes the work of the network architects. However, one could be tempted to assume that the issue is not a lack of technical understanding around cloud, but a reluctance to change. Clinging to the old styles of working may preserve a feeling of relevance for network architects. More visionary architects might see opportunities to adapt their expertise to the new style of network architecture to revalidate their positions and bring enterprise knowledge to cloud deployments.

What were the main challenges of moving your business applications to the cloud?

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
Cost	36%	28%	37%	47%	39%	32%	38%
Complexity	35%	38%	43%	34%	34%	33%	32%
Security concerns	42%	46%	46%	32%	36%	43%	32%
Lack of in-house cloud expertise	36%	32%	41%	25%	37%	44%	42%
Existing commitment to on-premises solutions	32%	28%	39%	28%	38%	41%	22%
Employee concern around keeping their jobs	34%	43%	31%	30%	40%	39%	25%
Company culture	30%	32%	35%	35%	25%	27%	25%

E | Influence of working from home on cloud transformation

Before the coronavirus crisis, the "workplace of the future" was a widely discussed topic but often low on the list of priorities. Overnight, the pandemic has fundamentally changed the way companies work, forcing IT teams to rapidly relocate staff to home offices and switch to remote working solutions to ensure business continuity and preserve enterprise productivity.

Remote work has required significant adjustments for organizations and employees. However, the introduction of social distancing measures has meant that flexible workplace models have become a reality much faster than many companies could ever have thought possible. Whether or not employees perceived their experiences of working from home as a positive or a negative often boils down to one thing: The status of the cloud transformation in their company. By relocating applications and data to the cloud, and switching to a cloud-capable infrastructure, companies were able to lay the foundations for agile working.

We wanted to know how companies reacted to the global pandemic with regard to their cloud transformation projects and found that close to one-quarter (22 percent) of companies across Europe had already transitioned to a 100 percent cloud strategy. While 33 percent said their cloud transformation was not affected, an equal number said the pandemic sent their cloud migration into high gear. In only 12 percent of the enterprises have cloud projects been slowed.

On a country-by-country basis, 61 percent of respondents in Italy said the pandemic did not affect their cloud roadmap, but German and Dutch enterprises reprioritized projects and moved them forward in 60 percent and 50 percent, respectively, of the surveyed companies. The UK (33 percent) and France (34 percent) reported that in roughly one-third of enterprises, COVID-19 has not affected their cloud roadmap, while one-quarter of companies sped up their projects (23 percent in the UK and 28 percent in France). In Sweden, a bit less than one-third decided to go ahead as planned and move projects forward (31 percent).

Key findings

How has the global pandemic situation influenced the pace of cloud transformation projects

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
We already had a 100% cloud strategy implemented before the pandemic situation	22%	26%	17%	29%	20%	23%	18%
COVID has not affected our cloud transformation roadmap	33%	33%	10%	34%	27%	31%	61%
Priorities of cloud projects have been moved forward	33%	23%	60%	28%	50%	31%	9%
Priorities of cloud projects have been slowed	12%	18%	13%	10%	4%	16%	11%
No answer	0%	1%	0%	0%	0%	0%	1%

We wanted to get an idea about how companies plan to adapt to remote working as the new normal. Nearly half (48 percent) of all respondents expect that, in the next 12 months, the number of people that will work remotely will grow between 25 percent and 50 percent. This is true for 27 percent of UK respondents and 49 percent of Germany's respondents.

How do you expect the percentage of workforce without office desk (road warriors/home-based office) in your enterprise will change during the next 12 months?

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
Remain stable	14%	8%	7%	8%	3%	36%	24%
Increase by up to 10%	19%	14%	6%	29%	16%	19%	33%
Increase by up to 25%	24%	27%	27%	24%	30%	17%	22%
Increase by up to 50%	23%	27%	49%	14%	32%	10%	10%
Increase by up to 75%	5%	7%	6%	5%	6%	0%	5%
We aim for 100-percent remote workforce	1%	1%	1%	2%	0%	1%	2%
Remote workforce will decrease	13%	17%	5%	19%	14%	18%	5%

F | Challenge: Securing remote access in the work-from-anywhere age

Security was listed as one of the biggest obstacles to cloud transformation, so we wanted to find out which security systems are used by enterprises to connect their mobile workers to corporate apps. Traditional solutions, such as Remote Desktop Protocol (RDP), were in use by one-third of enterprises (33 percent), closely followed by remote access VPN solutions (30 percent). Less than one-fifth of enterprises were using an identity and access management (IAM) solution (19 percent) and only 17 percent had adapted a zero trust-based concept.

How do your mobile and remote workers access their corporate applications on the network or in the cloud?

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
Via a remote access VPN solution	30%	36%	16%	52%	22%	18%	38%
Via Remote Desktop Protocol (RDP)	33%	45%	24%	37%	44%	18%	32%
Via a zero trust-based solution	17%	9%	35%	7%	32%	13%	9%
Via Identity and Access Management (IAM)	19%	11%	26%	4%	3%	51%	22%

Taking a more granular look, huge differences became apparent. While more than half of the IT decision-makers in France were still relying on remote access VPNs, 51 percent of Swedish experts had an IAM solution in place. In Germany and the Netherlands, around one-third of enterprises had deployed a zero trust model. In the UK, the dominant solution (at 45 percent) was RPD, followed by VPN at 36 percent. In Italy, VPN dominated at 38 percent.

Nearly half of enterprises in Italy (48 percent), France (46 percent), and the UK (45 percent) were confident in their secure remote access infrastructures, while the Netherlands (44 percent) and Sweden (41 percent) were less confident. Germany (43 percent), Sweden (38 percent), and the Netherlands (34 percent) were already evaluating new security solutions based on the requirements of a growing remote workforce. Across Europe, 34 percent of enterprises were following the same strategy, however only 4 percent had concrete plans to switch to a new solution in the next 12 to 24 months.

Key findings

How confident is your enterprise that the remote workforce can securely access applications in the corporate network and the cloud?

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
We are confident that we have a secure remote access infrastructure in place	33%	45%	22%	46%	22%	18%	48%
We are not confident that we have a secure remote access infrastructure in place	29%	18%	29%	28%	44%	41%	16%
We are evaluating new security solutions based on growing remote workforce needs	34%	34%	43%	24%	34%	38%	32%
We plan to implement a new security solution for the growing remote workforce in the next 12-24 months	4%	4%	7%	3%	1%	4%	5%

Since 34 percent of enterprises are evaluating new solutions, we wanted to know if enterprises are considering switching to a cloud-based secure access service edge (SASE) model, which dynamically allows or denies connections to the service based on an organization's defined business rules.

More than one-third of European companies (36 percent) were already familiar with the framework and had plans for a full, one-step transition, whereas slightly more than one-quarter (26 percent) had no plans yet, and close to one-fifth (19 percent) had plans to slowly transition to SASE. The most progressive fans of the concept were Germany and Sweden, with close to half of the enterprises in those countries having plans to adopt SASE (49 percent), followed by 41 percent of enterprises in the Netherlands. We also found that 11 percent of companies were already in the process of implementing the SASE approach. In France, about the same percentage of enterprises had plans to stay with their existing solution (28 percent) as those that were planning a slow move (27 percent). The same percentage had plans for a fast transition and only a small minority (4 percent) across Europe were not yet familiar with the concept.

> Nearly half of German and Swedish enterprises have plans to adopt the SASE framework, followed by the Netherlands at 41 percent.

Key findings

How would you describe your organization's awareness of and/or adoption of SASE?

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
We have not yet heard about/discussed SASE	4%	5%	2%	8%	6%	0%	5%
We have heard of SASE, but have no plans to adopt this approach	26%	18%	23%	28%	34%	35%	21%
We have heard of SASE, and we have plans to slowly transition to this approach (e.g., branch offices, followed by mobile entities, then headquarters, etc.)	19%	33%	11%	27%	14%	7%	26%
We have heard of SASE, and we have plans to transition all our entities at the same time	36%	27%	49%	27%	41%	49%	23%
We are in the process of transitioning to a SASE approach	11%	15%	14%	8%	6%	10%	13%
We have already transitioned to a SASE approach	3%	3%	2%	3%	0%	0%	13%

Digging deeper into the potential benefits of a SASE-based approach, half of all respondents across EMEA said that the main benefit is the reduced risk of security threats and data loss; 39 percent cited improved network visibility and control across all users and cloud platforms, and 38 percent said it enables the IT team to be a growth engine and contribute to the bottom line. More than one-third (36 percent) mentioned reduced complexity/increased agility of infrastructure.

Half of UK respondents said the main benefit is that it enables the IT team to be a growth engine and contribute to the bottom line, followed by reduced complexity/increased agility at 42 percent.

Key findings

Respondents from the rest of the five markets all said the main benefit was reduced risk of security threats and data loss across distributed data (48 percent in Germany, 47 percent in France, 54 percent in the Netherlands, 76 percent in Sweden, and 45 percent in Italy). Germany's IT decision-makers also said that improved network visibility and control across all users and cloud platforms was important for them, at 44 percent (in line with Sweden at 43 percent), as well as enabling IT to become a growth engine (43 percent).

Which of the following potential benefits of SASE are most appealing for your IT organization?

Total	Total N=606	UK N=101	Germany N-101	France N=101	Netherlands N=101	Sweden N=101	Italy N=101
Ability to scale globally and dynamically based on demand	31%	31%	33%	33%	34%	29%	29%
Reduced complexity/increased agility of infrastructure	36%	42%	37%	29%	38%	34%	40%
Superior user experience not harmed by latency	30%	25%	33%	25%	34%	34%	28%
Reduced risk of security threats and data loss across distributed data	50%	33%	48%	47%	54%	76%	45%
Enables IT team to be a growth engine and contribute to the bottom line	38%	50%	43%	34%	33%	34%	37%
Improved network visibility and control across all users and cloud platforms	39%	43%	44%	35%	37%	43%	32%
Reduced IT costs	32%	34%	42%	32%	23%	20%	41%
None	0%	0%	0%	1%	0%	0%	1%

Half of the UK enterprises said that SASE's main benefit is that it enables IT to be a growth engine and a contributor to the bottom line.

Conclusion

Traditionally, corporate applications lived within the corporate network where they could be controlled and monitored by the company. Cloud adoption has been on the rise and remote work is becoming the new normal. However, enterprises are likely to struggle with the complexity of multicloud setups and security concerns if they stick to their traditional hub-and-spoke network infrastructures.

The SASE framework defined by Gartner seems to resonate with European enterprises for improving security and bringing back network visibility and control across all users and networks. SASE is based on the concept that reliance on the data center as the literal center of a company's network makes no sense in a world where more applications are moving to the cloud and users are accessing networks anywhere, at any time, from a multitude of devices.

The idea of the service edge pushes compute and services closer to users, which ensures minimal latency between the endpoint and the application. This model is in stark contrast to the delivery of services through network connectivity, as SASE is more simple, scalable, and flexible, with low latency and high security.

SASE will have dramatic repercussions within enterprise IT. Services will be at the edge, away from the network's internal workings or functionality. As such, users do not need to know where a network is or where an application is housed. Reliance on the physical network will diminish and there will be reduced demand on IT as an internal service within a company.

Based on the recommendation by Gartner that cloud-oriented and mobile companies must restructure access models to their services, we wanted to find out how far along companies are in their adoption of the SASE framework. As we have seen, a majority of companies already accept the cloud as their new network, and more than 66 percent of respondents have more than 50 percent of their applications in the cloud, so we wanted to know whether they are as progressive in adapting their security infrastructure to fit the requirements of the cloud age.

The mobile workforce isn't concerned where their applications are stored. They demand seamless access from wherever they are working, no matter where the applications live. Additionally, IT professionals must adapt to managing an increasingly mobile landscape in which the traditional perimeter no longer exists.

Technology decisions are critical to achieving business productivity and protection, as well as providing IT leaders with an opportunity to drive transformation. The traditional network-centric technologies that teams have relied on for more than 30 years, such as remote access VPNs, have frustrated users and are now being used as a conduit for cyberattacks. In the work-from-anywhere world, IT leaders must shift to a cloud-based access solution as they adapt to the evolving needs of the business.

Recommendations

Even before the COVID-19 crisis, the "workplace of the future" was a widely discussed topic, but often low on the list of priorities. However, the introduction of social distancing measures has meant that flexible workplace models have become a reality much faster than many companies could ever have thought possible. Whether or not employees perceive their experiences of working from home as a positive or a negative often boils down to one thing: The status of cloud transformation in their company.

By relocating applications and data to the cloud and switching to a cloud-capable infrastructure, companies were able to lay the foundations for agile working. Gartner's SASE framework outlines the security set-up for such a mobile working environment and describes ways to overcome challenges like bandwidth constrictions, inconsistent user experience and lack of visibility.

To empower a productive and secure remote workforce, enterprise should evaluate their infrastructure according to the following technology requirements:

- **User experience –** To provide the best user experience and avoid IT tickets, access solutions must support a variety of device types, and have a large, distributed presence. More points of presence will mean less latency, and a faster, more productive user experience for those working from home, as well as when they return to the office.

- **Identity-based policies –** Connect an authorized user to a specific application based on context (identity, device postures, etc.), and never to the network. This will provide a more granular means of connection, reduce lateral movement on the network, and minimize exposure of critical business resources to the internet.

- **Simplicity and scale –** Leverage cloud-delivered technologies that integrate well together to simplify management. For example, consider secure access service edge (SASE) platforms, which include zero trust network access (ZTNA) services, cloud access security broker (CASB), and more. SASE platforms integrate with modern identity providers, such as Okta, Azure Activity Directory, and Ping Identity, as well as user endpoint management software, such as CrowdStrike and Carbon Black. Since the platform is cloud-delivered, IT can easily scale up the number of remote users without having to worry about capacity.

- **Visibility –** Cloud access services that are inline provide rich information around who is accessing what applications, from what device, and from where. This includes inspection of data encrypted within SSL. Traffic logs can then be streamed to Splunk, Sumo Logic, or another syslog service to help minimize remediation time in the event of a breach and react quickly to anomalous activity.

About Zscaler

The world's largest security platform built for the cloud

The Zscaler platform was built from the ground up to enable customers to move securely to the modern world—the world in which the cloud is the new data center and the internet the new network where business takes place. It's also a world where employees can work securely from anywhere. The Zscaler platform was developed to ensure that business would be able to operate securely and productively as applications moved out of the data center and users moved off the network.

The Zscaler multitenant architecture is 100 percent cloud-delivered and provides fast, secure, and reliable access to the internet and cloud apps, as well as private apps in the data center or public and private clouds. Access is based on software-defined business policies that follow users no matter where they connect or what devices they're using. This zero trust access empowers organizations to limit access to specific apps and resources only to the users authorized to access them. Product integrations with companies like Microsoft, such as the one between Microsoft Azure Active Directory and Zscaler Private Access,™ embody this framework.

Zscaler has guided hundreds of companies through their secure digital transformations. **Contact** us for guidance on your journey.

More resources:

Watch the two-minute video to learn about the benefits of a cloud-based architecture.

Learn how Zscaler helped Siemens with its digital transformation.

zscaler.com