RESEARCH
PAPER

Enterprise remote access and support: Is it time you deployed a modern secure connectivity solution?

CONTENTS

Introduction

Organisations today need scalable remote connectivity capabilities, without compromising on security. Whether working from home or on-the-go, employees, customers, and their partners rely on secure remote access to keep processes running effectively and efficiently.

At a time when Zero Trust cyber security strategies are increasingly the norm in this post cyber security perimeter era, VPNs no longer meet the dispersed workforce needs. Against an increasingly complex backdrop of attacks, outages, as well as resource and skills shortages, the pressure is on to deliver productive hybrid environments. How are IT decision-makers responding to this challenge?

This whitepaper explores the challenges facing 125 IT leaders when it comes to emerging trends such as new hybrid working models, reducing CO_2 emissions, global connectivity, and robotics and automation. Respondents included IT Directors, Heads of IT, CIOs, and CTOs from a range of industries such as banking, manufacturing, healthcare, and government.

Key findings

Organisations continue to have dispersed working environments, over 95 per cent of respondents operating hybrid or entirely remote.

Around 90 per cent of respondents agree that a modern connectivity platform is essential in today's increasingly hybrid digital economy.

Roughly a third of organisations have deployed a modern secure connectivity solution for remote access and support.

Interest in implementing a modern solution is extensive – over 95 per cent of organisations are at least interested.

Motivations for implementing a modern remote access solution include ensuring flexibility, security, and performance enhancements through reduced interruptions.

Less than 1 in 4 organisations say they are extremely confident in their current remote support and connectivity approaches for their employees and partners.

The greatest challenges facing organisations are end point security, resolving technical issues quickly using remote connectivity, and enabling work from home.

For those that have established a modern connectivity solution, 90 per cent rate its success as greater than 8 out of 10, 10 being extremely successful.

The new world of work

As the world of work becomes more dispersed, distributed and constantly on the move, the ability to access, connect, manage, monitor, and patch large diverse fleets of devices from afar, regardless of location or network, is now a must-have.

The pandemic saw a widespread shift to hybrid and remote work, a trend that is here to stay. Devices such as laptops, tablets, company mobile devices have proliferated and with it the need to protect and secure users with more stringent solutions that helps secure data, devices and people at rest and on the move.

This is evidenced in organisations' current working models, with 99 per cent of respondents reporting their employees are either entirely remote (2 per cent) or hybrid (97 per cent). Clearly, organisations are heavily dependent on better ways of connecting and providing support to these employees utilizing remote access and support capabilities.

Fig. 1 : Organisations' working models

On-premises full time (2%)

Entirely remote (2%)
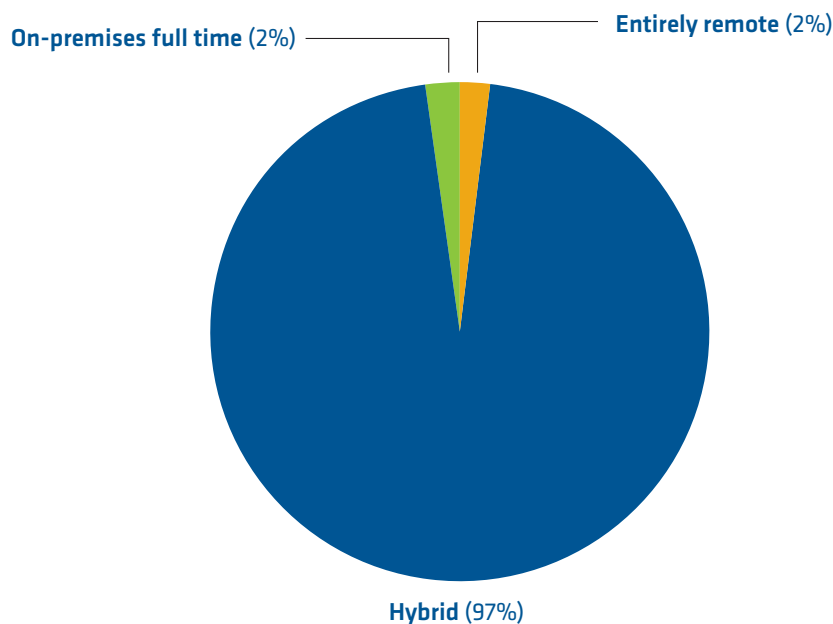
Hybrid (97%)

Newer ways of operating and working are the backbone of modern organisations, 90 per cent of respondents agree a sophisticated connectivity platform is essential in today's increasingly hybrid digital economy. Yet only a third of organisations have fully implemented such a solution.

Fig. 2 : "A modern connectivity platform is essential in today's increasingly hybrid digital economy"
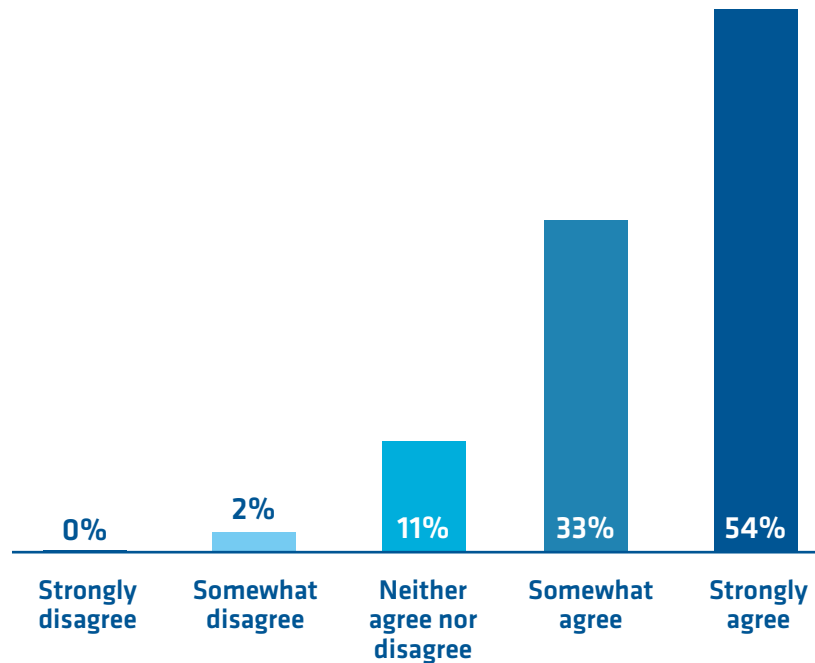
That's not to say interest is modest. Roughly 99 per cent of organisations are at least interested in adopting a modern connectivity platform that helps them stay agile and their employees productive in this hyper competitive marketplace.

IT leaders recognise the critical nature of supporting remote access and support as evidenced in figure 2, but a significant proportion are still considering, planning, or on the way to rolling out such solutions. Clearly, existing and legacy setups may be falling short. The need for modern secure connectivity solutions for remote access and support are therefore paramount.

Fig. 3 : Deployment of modern secure connectivity solutions for remote access and support

Category	Value
Fully implemented	34%
Currently rolling out	29%
Consideration stage	11%
Proof of concept	2%
Pilot	4%
Planning	15%
Migrating	1%
No plans, but interested	3%
No plans, and no interest	1%
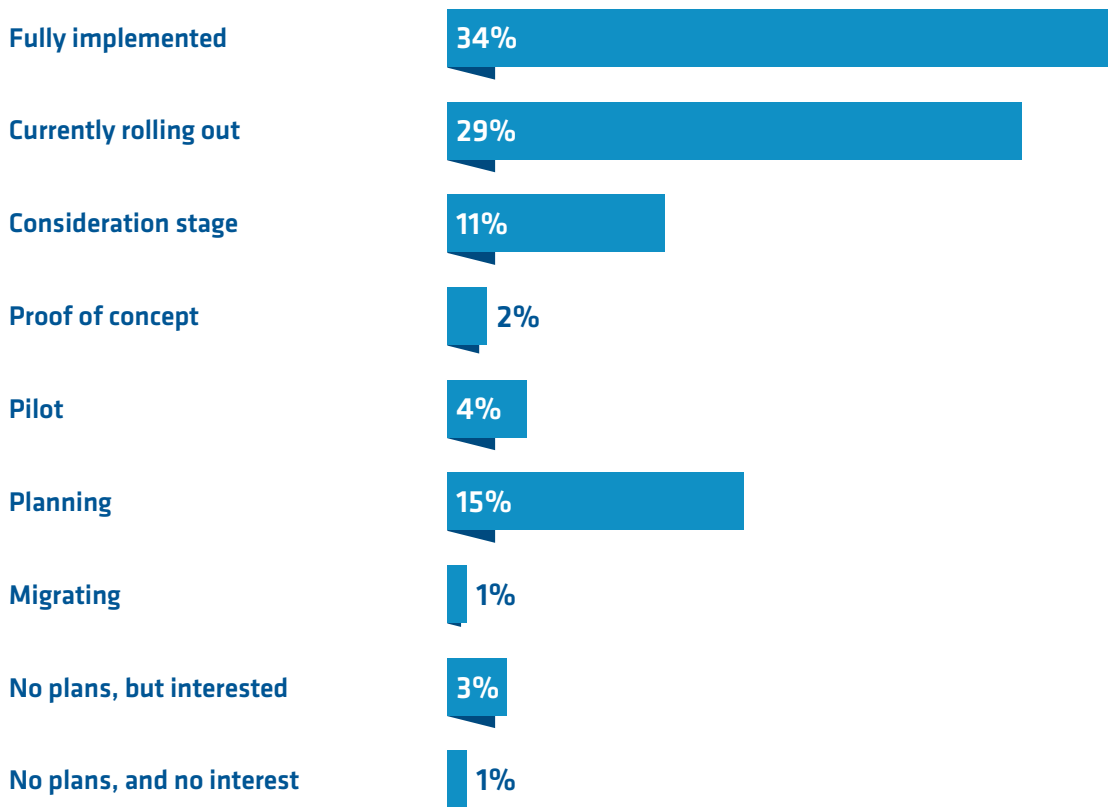
When asked for their motivations behind implementing a modern connectivity solution, respondents highlighted cost savings, security, and productivity as key drivers of adoption.

MOTIVATIONS FOR IMPLEMENTING MODERN CONNECTIVITY SOLUTION

"We want to ensure a secure working environment"

"A change in working practices means our teams work at client sites, at home, while, traveling, and in the office. We need high level security with seamless user experiences"

"Our aim is to remove VPN and deliver unified access alongside Zero Trust strategies"

"To give equal support to remote and office workers"

"A shift in working culture means we need to tighten our security for remote access"

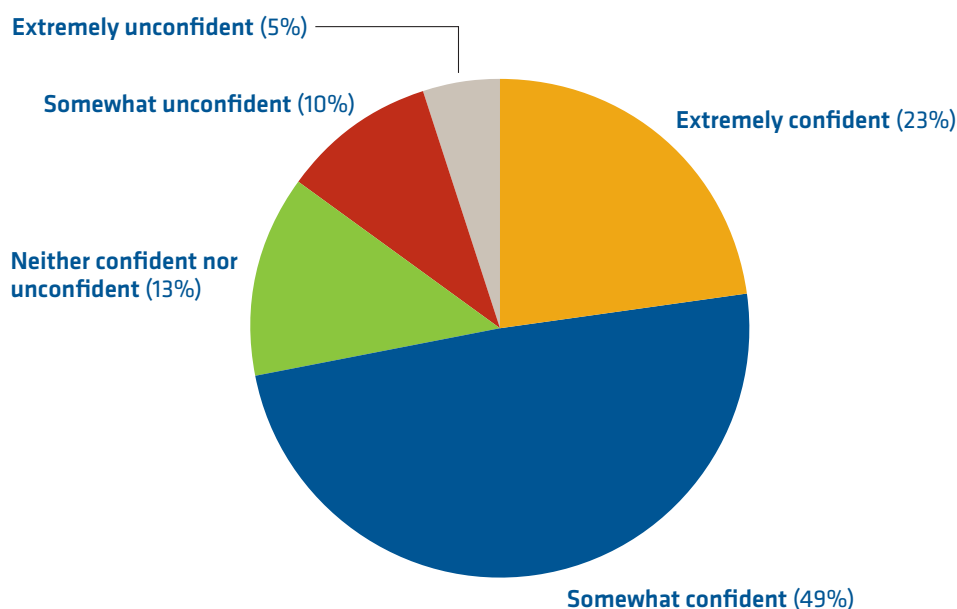"To provide an agile and safe working environment"

Modern solutions for modern problems

If organisations neglect to provide secure, managed connectivity that extends beyond the physical office, the likely outcomes are reduced productivity and a security posture that can be more easily compromised by third-party threat actors or externally orchestrated outages that can harm brand reputation and consumer confidence.

Cybercriminals are known to exploit ever-growing attack surfaces that are brought about by this proliferation of devices and people working remotely outside the bounds of secured, enterprise perimeters and networks. Without adopting modern solutions to combat this increasing danger, how can organisations trust they won't experience a detrimental or irrecoverable incident? How can they ensure downtime is kept to a minimum should an outage occur?

Fig. 4 : Confidence in current remote connectivity practices

Extremely unconfident (5%)
Somewhat unconfident (10%)
Extremely confident (23%)
Neither confident nor unconfident (13%)
Somewhat confident (49%)

Responses suggest confidence in current remote connectivity practices is minimal, with just 23 per cent of IT decision-makers claiming to be 'extremely confident' in their present solution. The greatest proportion, just under half, are 'somewhat confident', while 15 per cent are either somewhat or extremely lacking confidence in their existing practices.
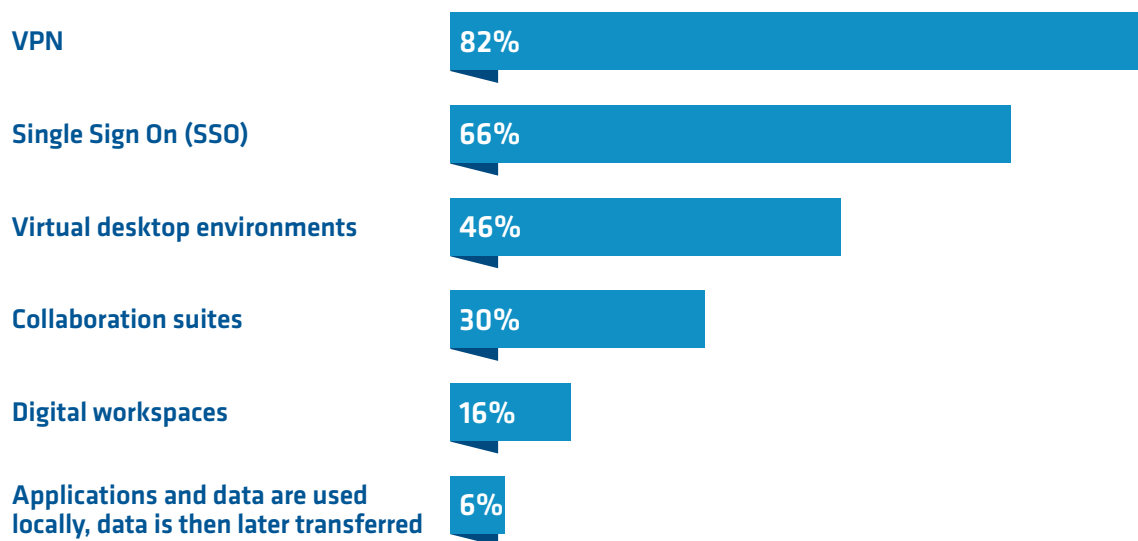
This also indicates that organisations are attempting to enable a modern workforce, one that prefers remote and hybrid working, without taking the necessary IT steps to secure such environments. This points towards vulnerabilities in security posture, and delays in resolving technical issues that negatively impact employee productivity in the short term.

Moving beyond VPN

The most common and popular approach to accessing work remotely is reliant on VPNs, with 82 per cent of organisations utilising them. However, VPNs regularly fall short when it comes to empowering remote work – often forcing organisations to compromise on security for convenience.

VPNs lack visibility, cause friction in the event of continuous use and bandwidth limitations, and often fall short in the hybrid working era. Still, organisations can be reluctant to move away from them, which is unsurprising given their widespread use and adoption.

Fig. 5 : How users typically access work remotely

VPN 82%

Single Sign On (SSO) 66%

Virtual desktop environments 46%

Collaboration suites 30%

Digital workspaces 16%

Applications and data are used locally, data is then later transferred 6%

The pandemic triggered a surge in VPN usage due to the need to quickly establish home working frameworks. For many, they enabled enterprises to rapidly get remote working initiatives going and to keep business running.
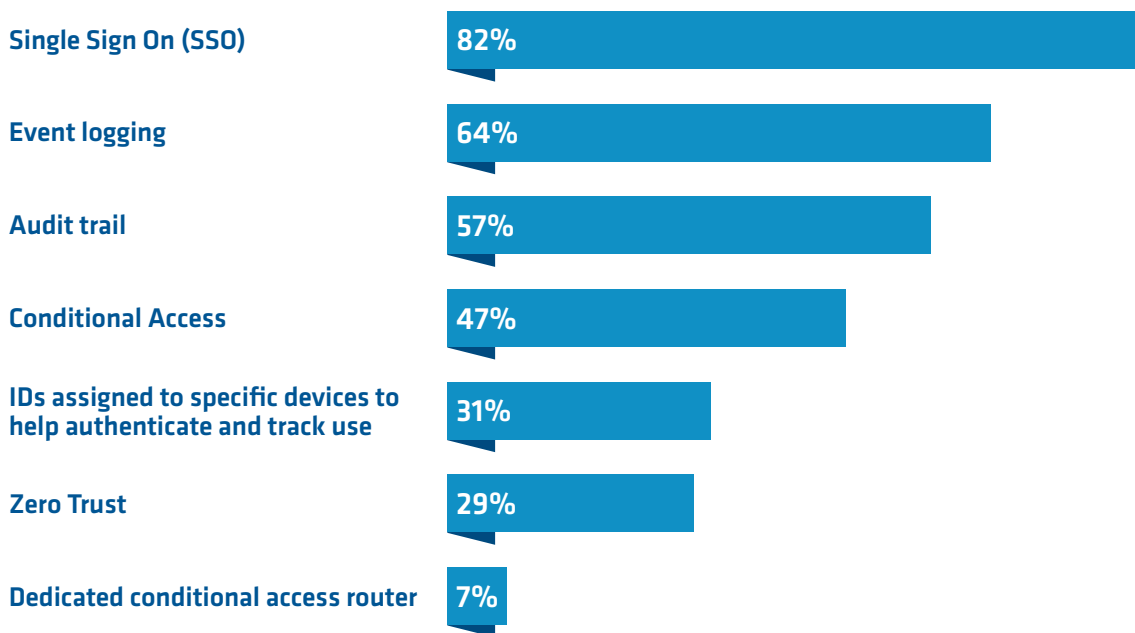
Adopting an alternative approach, one that utilises remote access software, provides users with direct connections to their files and resources on a separate device. Unlike VPNs, it does not require a complex configuration process nor constant maintenance to keep it running optimally, instead involving simple one-time installation that can be rolled out across multiple devices at once

Installing remote access software simply and intuitively saves on time and costs by removing the need to consult experts for troubleshooting

Features such as single-sign-on, end-to-end encryption, conditional access, and event-logging are crucial to achieving modern remote connectivity without compromise. Most organisations are utilising single sign-on features, event logging, and audit trails to secure their employees and processes

However, Zero Trust, a framework not a product enforcing "never trust, always verify", sees minor adoption. Zero Trust requires a holistic approach to security in which solutions are adopted that integrate with existing environments, enabling continuous verification without implicit trust. Many organisations aspire to a Zero Trust approach, however less than a third of survey respondents report they have such a security strategy. Given the rising threat of security incidents and an increasingly distributed workforce, organisations cannot afford to compromise on their endpoint management security.

Fig. 6 : Current remote connectivity approaches

Approach	Percentage
Single Sign On (SSO)	82%
Event logging	64%
Audit trail	57%
Conditional Access	47%
IDs assigned to specific devices to help authenticate and track use	31%
Zero Trust	29%
Dedicated conditional access router	7%

For those that have implemented a modern connectivity solution, the value is demonstrable. 1 in 3 rate the success of their solution as a perfect 10 out of 10, where 10 is 'extremely successful'. The remaining respondents, 60 per cent, assess the success as at least 8 out of 10. The average score awarded by respondents, was 8.5 out of 10, evidencing clear widespread success.

Fig. 7 : Success of fully implemented modern connectivity solutions

Average score =8.7

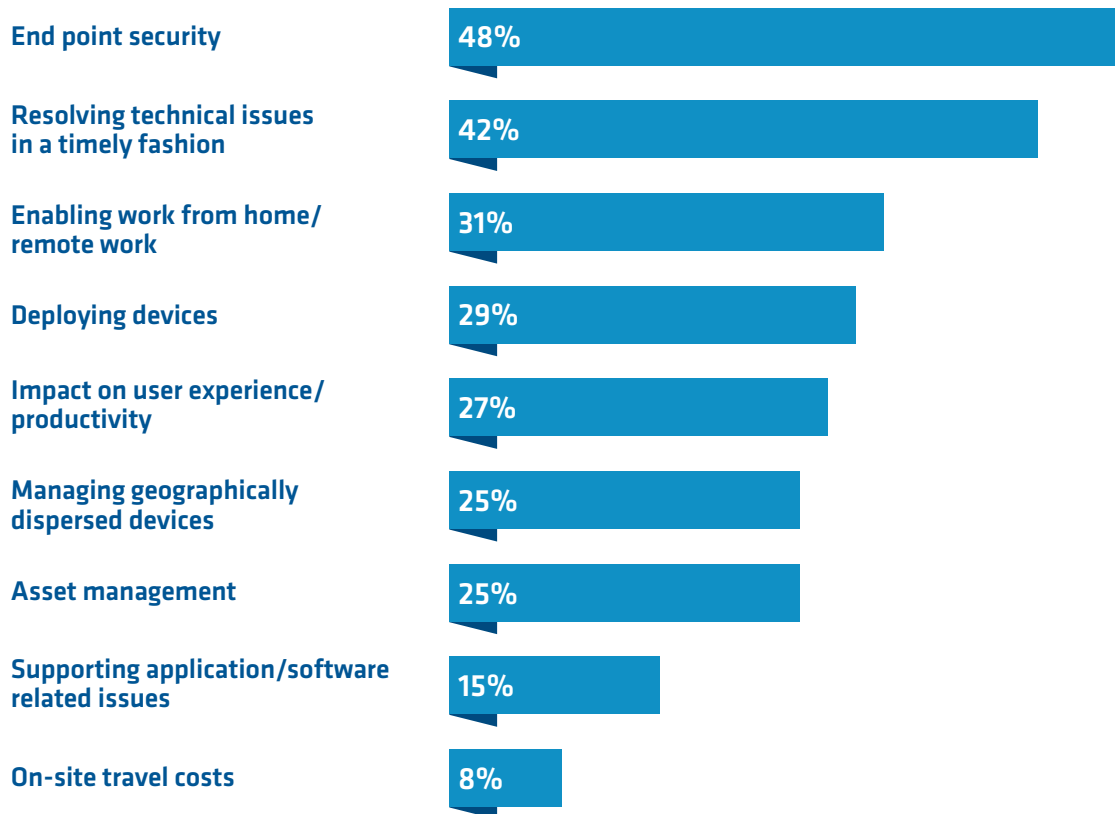| Score	Value
1 (not at all successful)	0%
2	0%
3	0%
4	0%
5	7%
6	0%
7	2%
8	30%
9	30%
10 (extremely successful)	30%
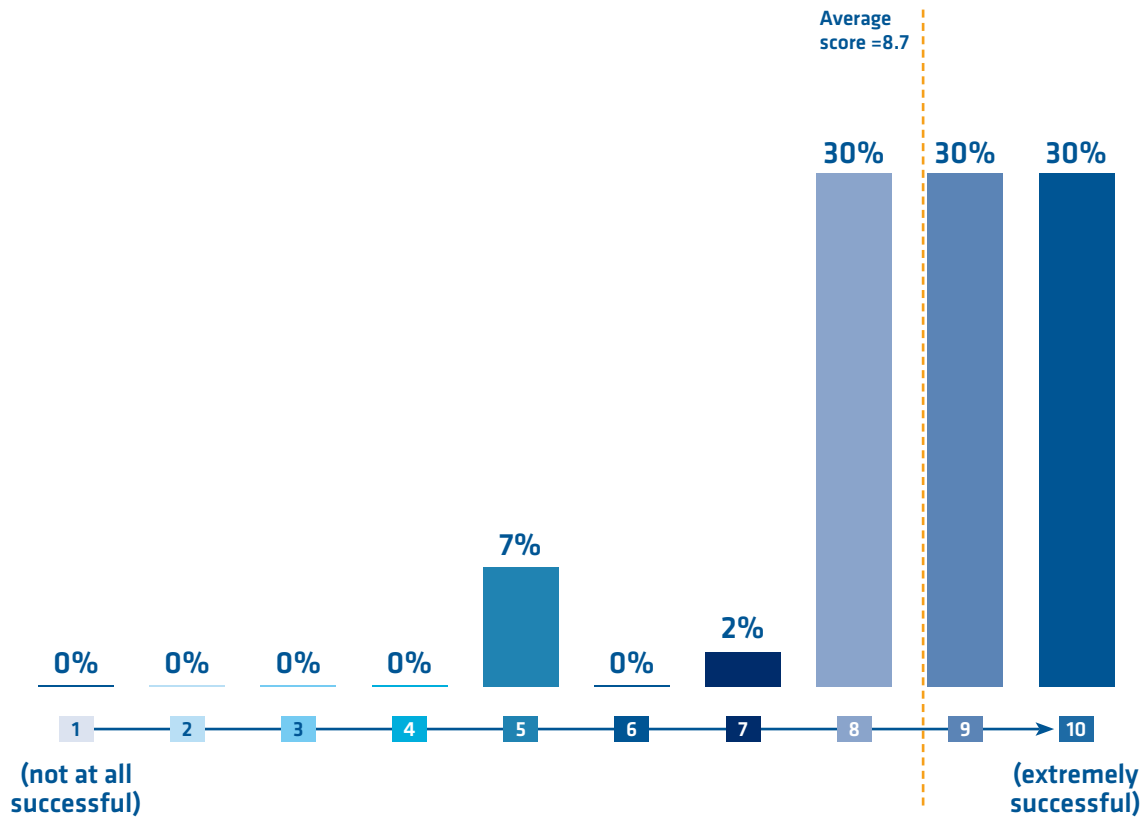
Overcoming hurdles

The greatest challenges facing organisations when it comes to remote access, support, and control concern security and fixing technical issues. Protecting and patching users from afar are critical in defending your organisation and maintaining productivity.

Employees expect seamless access from any device anywhere, which simultaneously increases attack surfaces. The increasing sophistication and frequency of cyberattacks demands organisations protect digital environments by patching vulnerabilities and mitigating risks from afar.

Fig. 8 : Greatest challenges for access, support, and control (3 maximum)

Challenge	Percentage
End point security	48%
Resolving technical issues in a timely fashion	42%
Enabling work from home/ remote work	31%
Deploying devices	29%
Impact on user experience/ productivity	27%
Managing geographically dispersed devices	25%
Asset management	25%
Supporting application/software related issues	15%
On-site travel costs	8%

Having greater visibility to see information and manage dispersed assets from, ideally, a single dashboard, should be top of mind for IT decision-makers. Monitoring and managing endpoints, kiosks, and assets in the field with optimal visibility minimises the time taken to identify issues. Already time-stressed IT personnel can resolve problems quickly and remotely, alleviating the pressure on teams and ensuring the right expertise is being leveraged at the right time. High stress, fast paced environments necessitate efficient and reliable technical support.
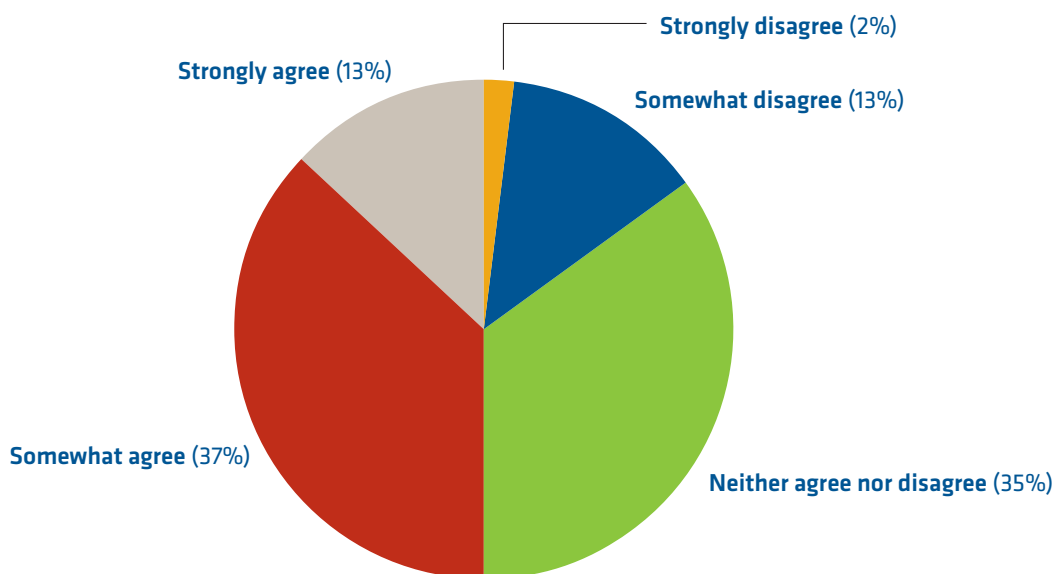
User-first initiatives

On-the-move employees or remote workers need consistent support capabilities. It no longer makes sense from a financial or productivity standpoint for employees to have to travel to a workplace to resolve IT issues, to be on-boarded, or to engage with their resources.

The savings on time, cost, and team effort that can be lost to solving issues through on-site visits, are huge. Whether that's IT workers traveling to troubleshoot systems or users having to journey into the office to get technical support.

Providing technicians with the ability to also remotely solve issues during events greatly reduces fatigue, redirects resources in a timely fashion, and minimises the upfront costs of travel. It also ensures the best talent is centralised within a company and allows organisations to scale their 'after sales' experiences.

The skills gap is growing, and organisations are feeling the pinch. They must leverage existing in-house expertise to have and hold a competitive edge in their marketplace.

Fig. 9 : "The IT skills gap at my organisation is growing"

Strongly disagree (2%)

Somewhat disagree (13%)

Strongly agree (13%)

Somewhat agree (37%)

Neither agree nor disagree (35%)

Additionally, supporting employee skills and development is imperative to attracting and retaining talent. Half of the organisations surveyed agree either somewhat or strongly that the skills gaps at their organisations are growing. Just 2 per cent of respondents could strongly disagree that this was the case for their workplace, suggesting talent shortages are fairly widespread.

Similarly, 73 per cent agree it is difficult to attract and retain IT talent today, making fostering in-house skills and development all the more important. Providing a user-friendly workplace in which issues are resolved in a timely fashion and access to resources is seamless is therefore paramount.
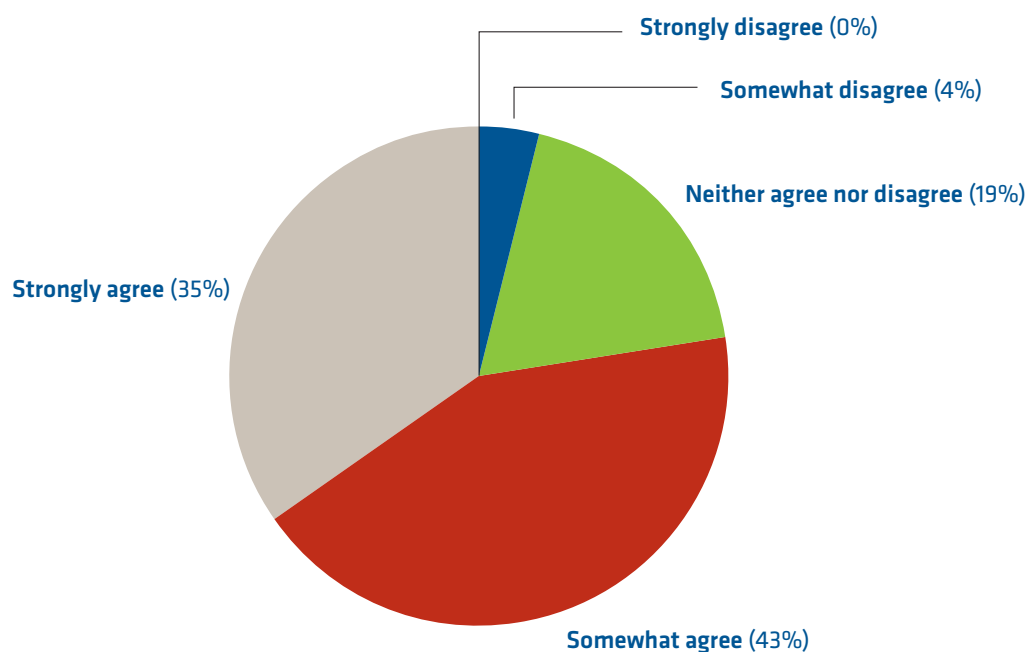
The impact of modern solutions

Modern platforms mean organisations don't have to compromise on user experience and security. Automating processes such as OS patch management and application updates significantly reduces the workload on IT teams that might have severe talent shortages, or limited budgets to reckon with. It also ensures updates and monitoring are timely and consistent, reducing downtime and supplementing visibility when it comes to understanding issues across all devices in a network.

With modern connectivity solutions that make use of robotics and automation, organisations can uphold stringent security measures from afar while ensuring productivity and interactions are not interrupted. Customer, employee, and partner experiences are more intuitive and seamless with modern solutions which will in turn create faster time to value.

Remote access further bridges skills gaps, by providing timely support to task workers operating in low-skilled environments from afar. Environments like retail, point of sale kiosks, and warehouses are subject to delays and end-user or operator experience is negatively impacted if hi-tech support is not readily available. This break in experience can cascade down and also create a negative customer experience if the supply chain is tightly knit and digitalised similar to ecommerce platforms of today that serve their customers at scale each day. A third of respondents strongly agree an affective remote connectivity platform would alleviate the pressure on supporting their employees, with 78 per cent agreeing at least somewhat with this statement.
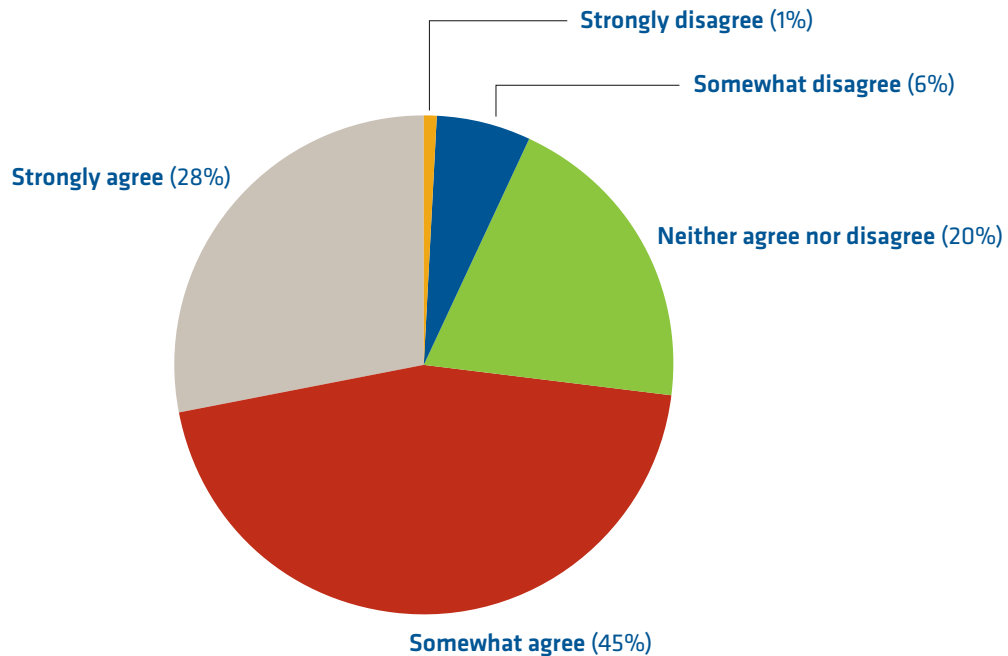
Fig. 10 : "An effective remote connectivity platform would alleviate the pressure on supporting our employees"

Strongly disagree (0%)

Somewhat disagree (4%)

Neither agree nor disagree (19%)

Strongly agree (35%)

Somewhat agree (43%)

With the world of work becoming increasingly digitised as enterprises are dependent on deploying screens and computing devices across the board, reliable support is crucial. Modern remote connectivity solutions overcome this, enabling devices to be managed easily in field scenarios and remote locations, without in-person technician assistance. This is integral to situations in which employees may not have the skill set or bandwidth to deal with technical issues when working in high stress, fast-paced environments.

IT leaders must provide an environment that is conducive for employees to do their best work. Centralising support enables organisations to operate at scale while providing support for a diverse and distributed workforce. This is heavily dependent on having the right technology in place. Frictionless, secure processes are the best way to facilitate a connected, productive, user-friendly working environment that permits global connectivity.

Fig. 11 : "It is difficult to attract and retain IT talent"

Strongly disagree (1%)

Somewhat disagree (6%)

Strongly agree (28%)

Neither agree nor disagree (20%)

Somewhat agree (45%)

Another key benefit of modern remote connectivity is the impact on an organisation's carbon footprint. As energy use and CO_2 emissions come under increasing scrutiny, organisations must endeavour to minimise their negative environmental impact. With remote connectivity technology, accessing, supporting and maintaining endpoint devices, and monitoring networks can all be carried out from afar. In most cases, it means travelling from one place to another becomes unnecessary and organisations can significantly reduce their carbon footprint. Utilising greener processes through digitisation ultimately creates a more sustainable future for us all.

Conclusion

Customer and employee experience depends on having fast, flexible, easy-to-use remote support technology. Solving technical problems as quickly and as smoothly as possible, without compromising data security, are key drivers of success and productivity for all organisations across industries.

Users must be connected irrespective of device platform, form factors, location, or bandwidth limitations. Faster issue resolution, higher customer and employee satisfaction, and stronger brand loyalty are all facilitated by reliable remote access capabilities. The right platform enables IT teams to solve technical issues for end-users swiftly wherever they are, whatever their device.

Managing and maintaining remote endpoints can see significant cost savings with remote connectivity software. In place of setting up onsite visits for routine maintenance, organisations can save precious time and budget by updating and viewing systems remotely.

The findings indicate organisations are not satisfied with their current solutions, as reported, confidence levels need improving. Unsurprisingly, VPNs are extensively used, however, IT leaders should endeavour to move beyond this approach and instead adopt more capable, robust, and secure platforms that enable remote access and support for a wide array of devices and endpoints.

For those that have established a modern connectivity solution, *Computing*'s research revealed emphatic success.

Crucially, remote access software removes the need for costly sites visits and allow teams to resolve issue quickly and reliably, without contributing to CO_2 emissions. Organisations wanting to remain competitive in a digitally mature marketplace must provide the tools to operate at scale with ease, without compromising data security.

About TeamViewer

TeamViewer is a leading global technology company that provides a connectivity platform to remotely access, control, manage, monitor, and support devices of any kind – from laptops and mobile phones to industrial machines and robots. TeamViewer continuously innovates in fields such as Augmented Reality, enabling companies from all industries to digitally transform their workforce and business-critical processes.

Through strategic acquisitions of Ubimax, Upskill, and Viscopic, TeamViewer has built a fully comprehensive, end-to-end AR solution on the market. TeamViewer Frontline optimizes processes along the entire industrial value chain, closing the loop to an entirely digital industrial workspace.

Founded in 2005, and headquartered in Göppingen, Germany, TeamViewer is a publicly held company with approximately 1,400 global employees. TeamViewer AG (TMV) is listed at Frankfurt Stock Exchange and belongs to the MDAX.

TeamViewer

October 2022