A Lynchpin Media BRAND

cxo priorities

Understanding the evolution of remote working and enterprise-level security.

A CXO Priorities' report in partnership with Palo Alto Networks

paloalto NETWORKS

Contents

Introduction

One of the most significant impacts of the pandemic was the rapid mobilisation of a remote workforce resulting in companies scrambling to fortify their IT infrastructures, devices and systems to make provisions to allow employees to work from home.

Around the world, the ability to work remotely has become crucially important for employment decisions. Companies have experienced significant reductions in the fixed costs of supporting a workplace environment, while upper management is starting to gain confidence in their employees' home office performance. A more flexible schedule and the ability to work from anywhere has made employees state that home office environments were preferable financially.

But remote working is increasingly becoming the new normal and organisations are beginning to build strong and solid systems that can survive attacks from hackers. In this report, we explore the major challenges organisations face with remote working and the security concerns around the work from home culture.

Survey overview

To get a better understanding, we surveyed CIOs, CTOs and IT directors at EMEA about their experiences and future plans around remote working and cybersecurity.

This report aimed to build an overview of the current evolution of remote working and enterprise-level security by exploring challenges with a remote workforce and how organisations plan to prioritise and invest in SASE solution providers.

Through this survey we aimed to discover:

- Challenges with managing a remote workforce
- Priorities and plans for future investment into a SASE solution provider

Summary of findings

- More than 75% of respondents say their company is currently experiencing challenges related to performance and security with a remote or hybrid workforce
- Nearly two-thirds of respondents state that lack of infrastructure is the biggest challenge when managing a remote workforce
- Ransomware is clearly the biggest security concern for organisations in recent years based on a 75% vote from respondents
- All respondents attest their organisation is considering an investment in a SASE solution in the next 6–12 months with a 100% vote
- VPN and SWG are the most important technology investment areas in the next 24 months
- Reduced overall costs (50%) and increased flexibility (48%) are the most important benefits when investing in a SASE solution provider
- App security (50%) and data protection (50%) are the most important factors when considering a SASE solution provider

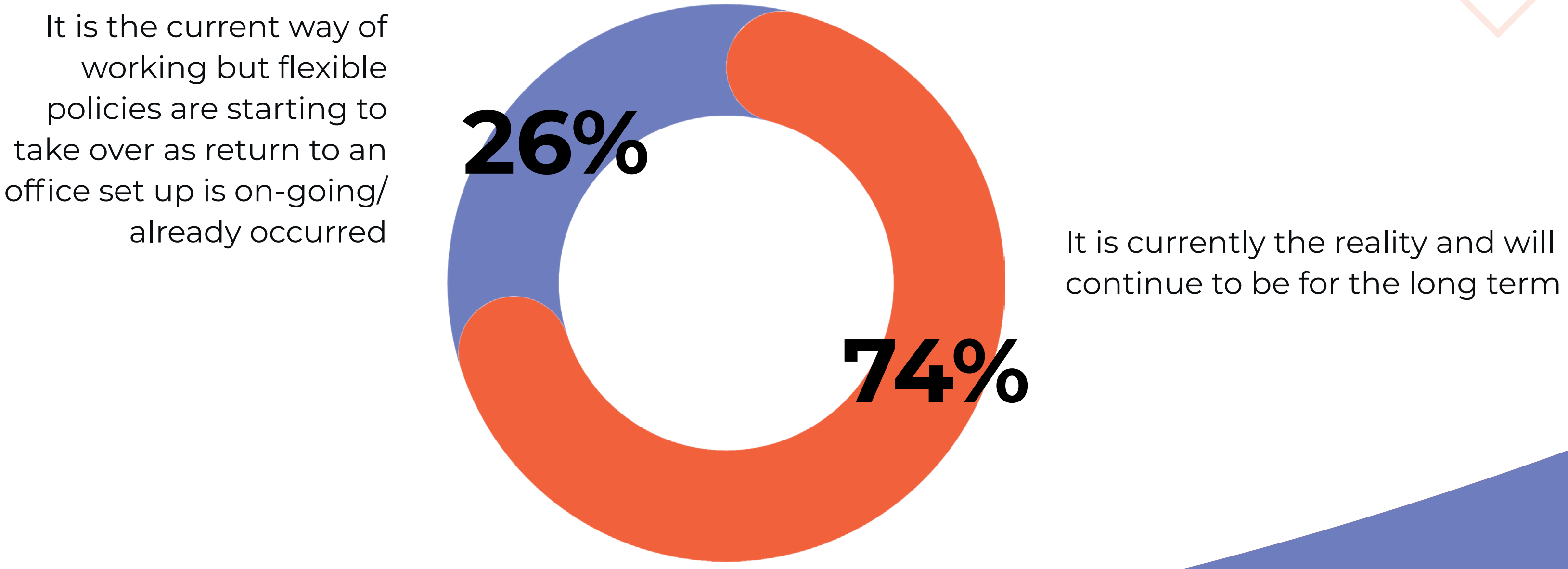
CHAPTER 1
Challenges with managing a remote workforce

Question 1

Is remote working a continuing reality for your organisation?

Seventy-four percent of respondents confirm that remote working is the current and future reality for their organisations while 26% think it is the current reality but subject to a return to office soon. As work from home culture increases and will be around long-term, there is a need for strong security to protect organisations and their employees from malicious activities.

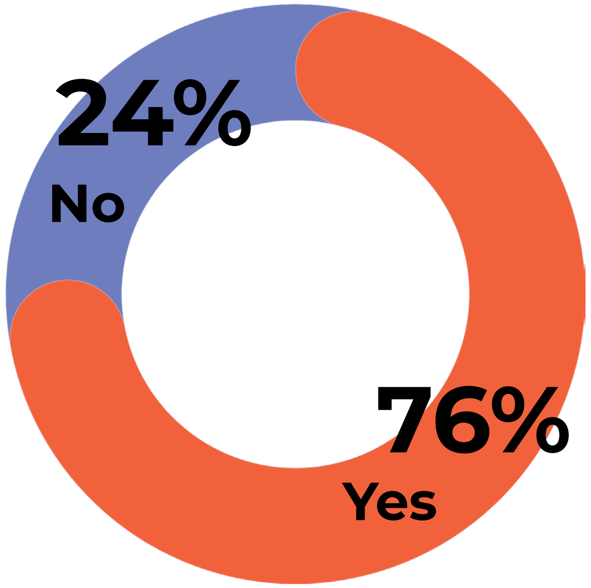
The challenge of managing a remote workforce has become a concern for many organisations since the pandemic. Dealing with rising costs, work equipment, workflow structure and for IT decision-makers, a more secure working space for employees, has become the new normal.



CHAPTER 1
Challenges with managing a remote workforce

Question 2

Is your organisation experiencing challenges related to the performance and security for your remote or hybrid workforce?

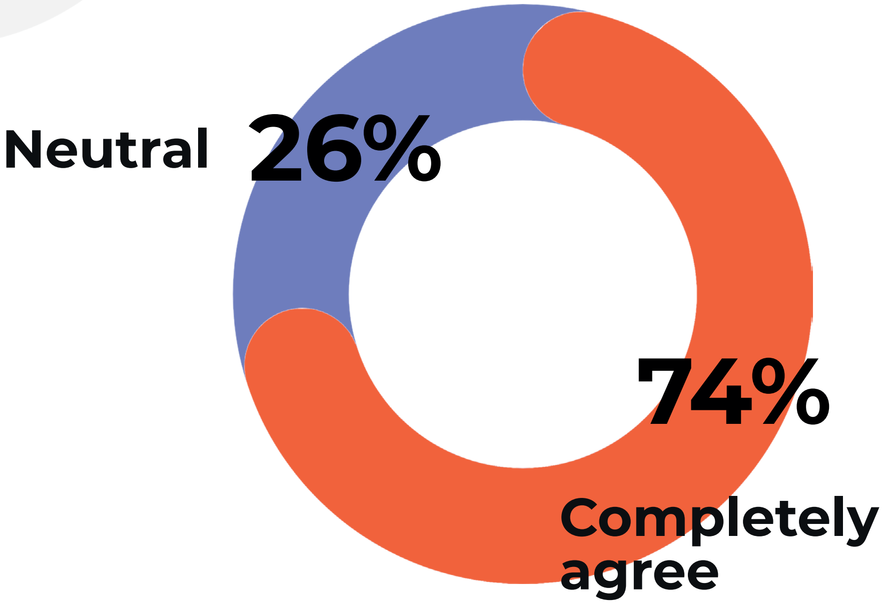


Over three-quarters of respondents (76%) indicate that their organisation faces challenges related to performance and security in a remote or hybrid workforce. This contrasts with 24% of respondents that do not currently experience similar challenges. This indicates organisations must develop the right tools to proactively audit network configuration and take data security seriously, whether for users at home or hybrid workers. There is a case here for a trusted 2.0 ZTNA provider which will protect application traffic, adding peace of mind to CIOs currently facing this challenge.

CHAPTER 1
Challenges with managing a remote workforce

Question 3

To what extent do you agree that current remote users or remote employees are protected and able to withstand remote attacks?



Respondents strongly agree (74%) that remote users or employees can be protected and able to withstand remote attacks. This is a call for organisations to protect employees who work from home using their personal devices as they visit random websites and install apps and software programs that might otherwise make them easy targets for malicious activities and hackers.

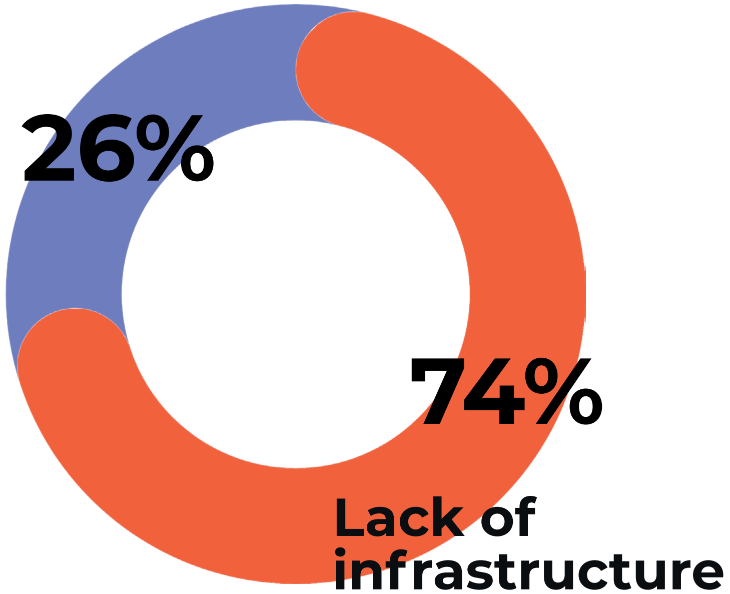
There were zero responses to the following options:

- Agree
- Disagree
- Completely disagree
- Don't know

CHAPTER 1
Challenges with managing a remote workforce

Question 4

Which of the following is the biggest challenge when managing a remote workforce?



Respondents say lack of infrastructure (74%) and lack of budget (26%) are the biggest challenges when managing a remote workforce. This infers that organisations need more pragmatism in developing security budgets and need to up the average annual security spending. The bottom line is that building a security budget is a win-win for both the CISO personnel as well as the organisation.

There were zero responses to the following options:

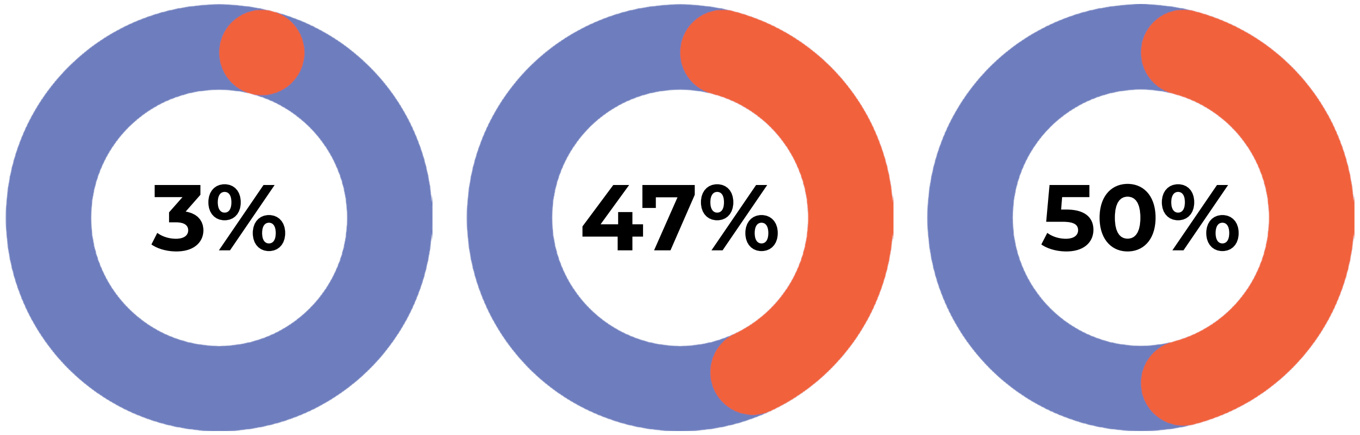
- Speed of roll out/implementations of remote infrastructure
- Lack of relevant security policies
- Lack of cyber awareness
- Wellbeing of security team (added pressure)
- Motivation and productivity

CHAPTER 1
Challenges with managing a remote workforce

Question 5

Which of the following represents the biggest challenge to your organisation when considering your hybrid workforce? (Please select 2)

Gaining visibility and control (50%) and securing access to the Internet and SaaS applications (47%) are considered the biggest challenges to organisations considering their hybrid workforce. Organisations wanting more visibility, control and access highlights the need for trusted security partners which can drive security improvements, increase security posture, identify vulnerabilities and constantly monitor multiple portals and alert systems.



Securing access to your private applications in your physical or cloud hosted data centres: 3%

Securing access to the Internet and your SaaS applications: 47%

Gaining visibility and control of your SaaS Applications: 50%

There were zero responses to the following option:

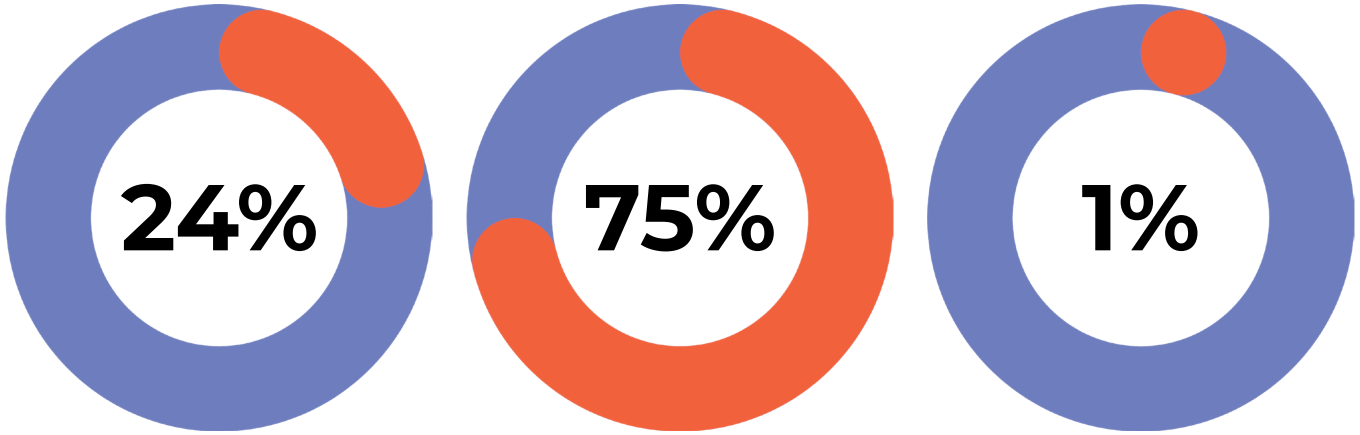
- None of the above

CHAPTER 1
Challenges with managing a remote workforce

Question 6

Which of the following issues has risen the most this year vs 2021?

Ransomware (75%) is evidently the biggest issue for organisations in recent years. Phishing and/or social engineering (24%) was also cited as an area of concern by the respondents. Securing and managing the various touchpoints has become more challenging with the increased adoption of remote and hybrid work cultures. As a result, organisations are realising the need to strengthen their cyber posture as ransomware is an ever-evolving threat, often rendering files and systems unusable. Therefore, successful SASE solution providers will need to make access to devices and data storage a priority with remote working the new normal.



There were zero responses to the following options:

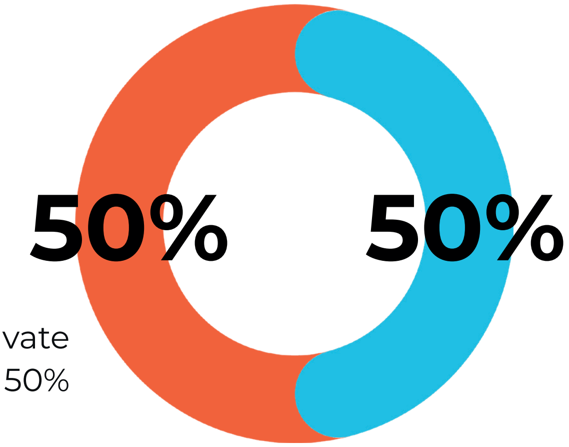
- Unintentional data leak (laptop sent to the wrong person etc)
- Credential theft and/or account compromise

CHAPTER 2 Priorities and planning ahead

Investment into solid and reliable SASE solution providers is critical, especially given the current rise in remote working. In this section, we look at the top investment areas for organisations in the coming year and the key benefits it can bring.

Question 7

Does your organisation plan to increase investment in any of the following technology areas within the next 24 months? (multiple choice)



Secure Web Gateways (SWG): 50%

Virtual Private Networks (VPNs): 50%

The top two priorities of investment areas for the next 12 months are Virtual Private Networks (VPNs) (50%) and Secure Web Gateways (SWG) (50%). With respondents selecting these two areas with equal merit, it is suggested they have had previous concerns or potential issues with managing traffic and security and are also leaning towards a hybrid business structure for the following year.

It is possible that respondents are seeking a SASE solution provider which values simplicity and flexibility. In that case, selecting providers which offer solutions with a single pane of glass would allow them to build a customised solution incorporating a mix of Zero Trust network access, secure web gateways, analytics, Unified Threat Management and policy management, for example.

There were zero responses to the following options:

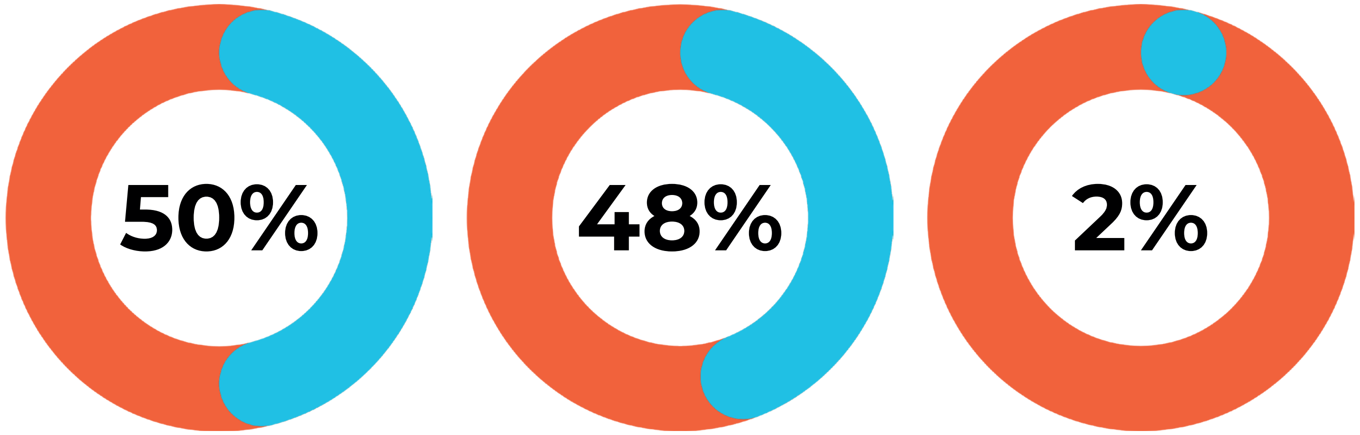
- Software-defined Wide Area Network (SD-WAN)
- Cloud Access Security Brokers (CASB)
- Digital Experience Management (DEM)
- Secure Access Service Edge (SASE)
- Zero Trust Network Access (ZTNA)
- Data Loss Prevention (DLP)
- Multiple solutions listed above
- No additional investment is expected
- Other

CHAPTER 2
Priorities and planning ahead

Question 8

In your evaluation of the benefits of a SASE solution, what are the two most important factors to commit to investment? (Please select two)

The ability to reduce overall costs (50%) is considered the most important when evaluating the benefits of a SASE solution. This is closely followed by organisations that place a heavy emphasis on increased flexibility (48%). As the needs of organisations vary, a one-size-fits-all approach is not ideal. Hence, organisations must consider SASE solutions that can tailor their service and price points to create bespoke security offerings.



Reduced overall costs: 50%

Increased flexibility: 48%

Faster innovation: 2%

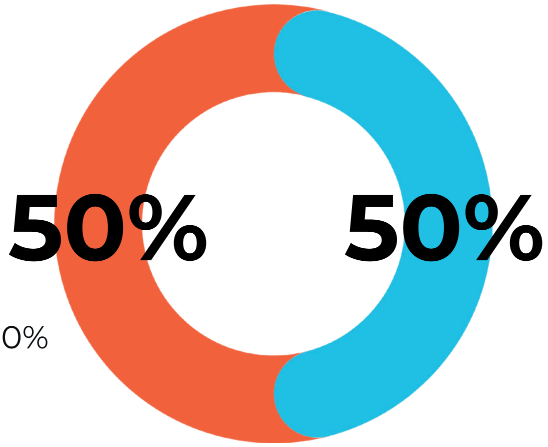
There were zero responses to the following options:

- A single vendor SASE solution with a single pane of glass management
- Efficiency gains
- Improved sustainability
- Scalability

CHAPTER 2
Priorities and planning ahead

Question 9

In your evaluation of a SASE solution provider, what are the top two factors you would consider? (Please select top two)



Data protection: 50%

App security: 50%

Respondents cite data protection (50%) and app security as the top factors while evaluating a SASE solution provider. This highlights how SASE solution providers must prioritise securing access and data to allow organisations to dramatically reduce the risk of data breaches.

Furthermore, organisations can benefit from SASE solutions that offer cloud-scale solutions but also work hard to deliver an exceptional user experience.

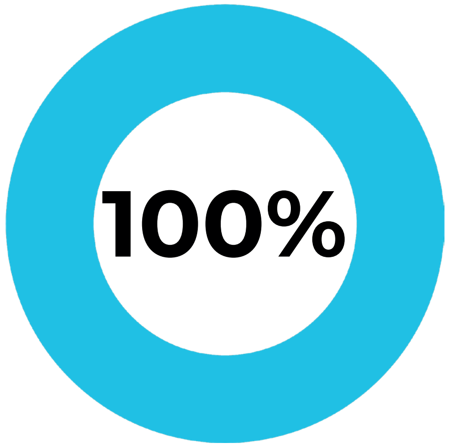
There were zero responses to the following options:

- Security inspection
- Adhering to principle of least privilege
- Ease of use
- Cost
- None of the above

CHAPTER 2
Priorities and planning ahead

Question 10

Is your organisation considering investment in a SASE solution?



Yes – within the next 6–12 months: 100%

All respondents are amplifying their plans to invest in a SASE solution for the next 6–12 months to tackle security threats. This suggests that respondents are preparing their current security budgets with a long-term view and serious investment. This could present an excellent opportunity for cybersecurity vendors which favour a ‘proactive’ and flexible approach and want to holistically fill the gap in a company’s security policy.

This suggests respondents value cybersecurity vendors’ expertise which can deliver a simplified and streamlined service to respect strict timelines. Providers which offer solutions combing security and networking into a single service could prove to have a time advantage (based on the flexibility that is valued in Q8 by respondents).

There were zero responses to the following options:

- Yes, within the next 3 months
- Yes, within the next 3–6 months
- Yes, but not for at least 12 months
- No, we have no plans to invest
- No, but we are looking into it

Conclusion

Nearly two-thirds of respondents cite that remote working is a continuing reality for their organisations, suggesting that a secure means of storing and protecting personal data remotely should be a major focus for IT leaders. Vendors must address ever-increasing security vulnerabilities and the downsides that come with remote working.

From a security standpoint, allowing employees to access company data from off-site locations raises concerns about data encryption, the security of wireless connections, the use of removable media and the potential loss or theft of devices and data. This is in addition to the use of insecure and weak passwords, the use of personal devices for professional purposes, weak software backup, poor recovery measures, lack of training and unencrypted file-sharing practices.

Reduced overall costs (50%) and increased flexibility (48%) were cited the most important benefits when investing in a SASE solution provider. With special attention on securing people who are on the move and eliminating the risk of vicious ransomware, there is scope for trusted providers to solve SWG and VPN conundrums for companies. As highlighted in the findings, ransomware was cited as the biggest security concern in recent years.

The future is bright for IT providers which focus on app development and increased flexibility. SASE solution providers which value flexibility that can create streamlined processes to combine networking and security into a single service can lead the pack here. Equally there is a strong case for providers with unified management and shared data lakes that lead to smoother collaboration.

When it comes to a stable and efficient future for remote work, companies need to be mindful of following a path which is both innovative and cost-effective for the end-users. The fact that 100% of respondents are considering investing in a SASE solution in the next 6-12 months indicates the pressing need for organisations to urgently protect their systems and employees from malicious activities in the long-term.

> With special attention on securing people who are on the move and eliminating the risk of vicious ransomware, there is scope for trusted providers to solve SWG and VPN conundrums for companies.

priorities

A Lynchpin Media

Sponsored by:

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054
info@paloaltonetworks.com

www.paloaltonetworks.com

priorities

CxO Priorities, a Lynchpin Media brand
63/66 Hatton Garden
London, EC1N 8LE

www.cxopriorities.com