Check Point®
SOFTWARE TECHNOLOGIES LTD

# REMOTE AND HYBRID WORK SECURITY REPORT

Survey uncovers the implications of remote work on organization's security and network architectures, and how IT Security Leaders and Professionals are addressing the evolving needs of the hybrid workplace.

# TABLE OF CONTENTS



# EXECUTIVE SUMMARY

## AN EXPLOSION IN REMOTE AND HYBRID WORK

The global events of the past year have had a profound impact on the way many of us work, meet, shop and study. Undoubtedly, the shift to remote and hybrid work is one of the most important changes to have taken place as a result of Covid-19.

As organizations raced to ensure business continuity starting in March of last year (2020), the demands placed on their remote access infrastructure exploded. For most organizations up to that point, network security infrastructure was designed to mainly support operations on-premises, in headquarters and branch offices, with only minor or marginal concessions made to support work-from-home and off-premises access.

## THE DISTRIBUTED ENTERPRISE AND SASE

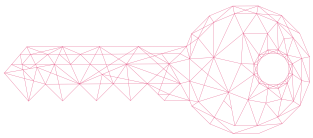
With so many working remotely, organizations quickly realized that relying on network architecture that routes all traffic to the on-prem data center for traffic inspection no longer provided the speed and performance required to support what has been dubbed the digital workforce transformation, leading IT security professionals and leaders to rethink their network security strategy.

# SURVEY OBJECTIVE

In this survey we sought to uncover the impact global events have had on organizations, particularly on IT and security strategies, including the extent to which remote work has affected organizations' security posture, operational overhead and its impact on users.

To uncover how IT and security professionals are dealing with these changes worldwide, we approached 450 IT security professionals, 50% of them in a senior leadership role (namely, director, VP or C-level executive).

# KEY SURVEY FINDINGS AT A GLANCE



### Not just hype: Remote work increases cyber risk

45% report an uptick in cyber attacks since the shift to remote work.

### Top breach and attack vectors since Covid-19 are data loss, phishing and account takeover

Data exfiltration and leakage (55%), phishing emails (51%) and account takeover (44%) saw highest increase since the move to remote work.

### Top challenges with current remote access solutions are scalability, privacy and BYOD

Scaling performance (46%), ensuring privacy (42%) and supporting BYOD (40%) were identified as the top administration challenges with remote access.

### Top remote worker complaints include performance, instability and VPN issues

Performance (latency) (67%), instability and crashes (66%) and VPN issues (62%) were identified as the most common reasons for help desk tickets.

### Cloud-delivered security considered critical for remote work

66% are using cloud-based security services to scale up remote access, and of those respondents, 61% consider cloud-delivered security to be highly strategic to that effort.

### Most are familiar with the SASE framework, but adoption is slow

Ninety four percent (94%) of respondents are familiar with SASE, and 30% have already implemented or are planning to implement the framework.

# CONCLUSION: SASE IS POISED TO SOLVE TODAY'S REMOTE WORK CHALLENGES

Driven by the hybrid workplace, organizations are seeking new methods to enforce consistent security policies, while maintaining the highest levels of threat prevention and a seamless experience for all.

Due to the long-term effects of remote and hybrid work on network and security architectures, the secure access service edge (SASE) framework is gaining interest. Representing a major transition in network security, SASE aims to bridge the security, management and performance gaps caused by today's distributed enterprise.

To support legacy systems, organizations are moving to cloud-based security where they can, and keeping on-premises network security where they must. Rather than ripping and replacing their entire infrastructure, organizations are likely to solve for one use case (e.g. implementing ZTNA for secure remote access) and adopt additional cloud services based on their needs and priorities.

# GLOSSARY

| | |
|---|---|
| SASE | Collectively known as the secure access service edge, the use cases listed below comprise the main services of this architectural blueprint. |
| Zero Trust Network Access (ZTNA) | Secures remote access to enterprise applications on-prem or in the cloud using zero trust principles and a security broker service through which all traffic is routed for security inspection. ZTNA is often deployed along slide VPN-as-a-service support for legacy applications and systems |
| Secure Web Gateway (SWG) | Protects remote workers' and branch offices' internet access to ensures that all internet connectivity is vetted using URL filtering, anti-malware and phishing protection and application control |
| Cloud Access Security Broker (CASB) | Secures SaaS applications through access control, encryption, threat prevention and granular permissions |
| Branch Firewall as a Service (FWaaS) | Secures branch offices as they connect directly to the internet and cloud over software-defined wide area networks (SD-WAN) |
| Networking-as-a-service | SD-WAN services that optimize enterprise traffic flow through best path selection factored for speed, QoS, cost and other variables |

# INCREASE IN REMOTE WORK

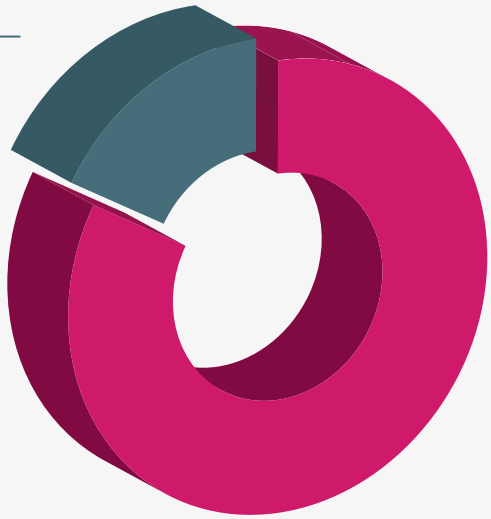
We first set out to check if organizations have in fact seen an uptick in remote work. The response was an overwhelming 'yes.' Eighty-three (83%) of respondents reported seeing an increase in remote work, with all industries survey being affected to a greater or lesser extent. Moreover, 63% say the number of users working remotely has increased by more than 50%.

***Have you seen an increase in remote work since Covid-19?***

More than **80%** of respondents have seen an increase in remote work since Covid-19

**17%**

No, we have not seen an increase in remote work

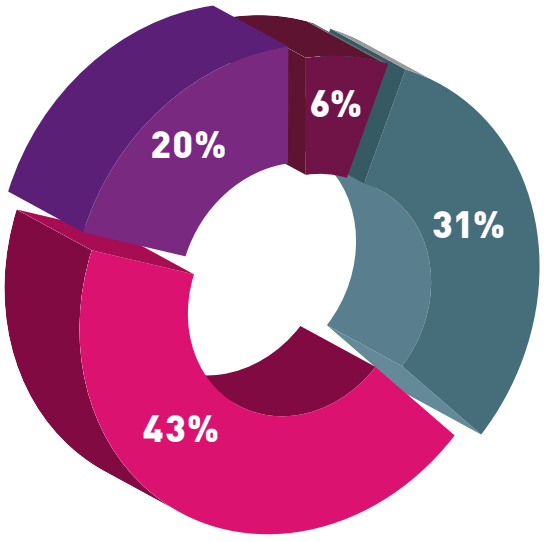


**83%**

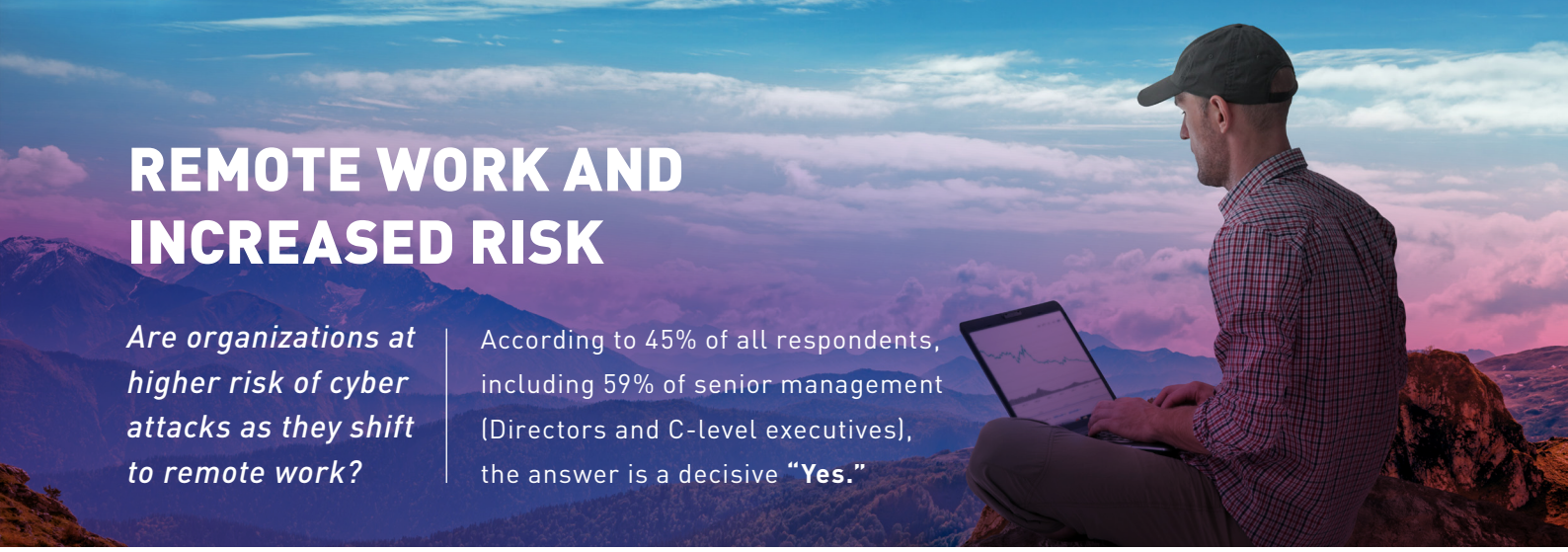
Yes, we have seen an increase in remote work

***In your estimation, by what percentage has the number of users working remotely increased in your organization?***

63% of respondents estimate the number of users working remotely has increased by more than **50%**




**Increase in number of users working remotely**

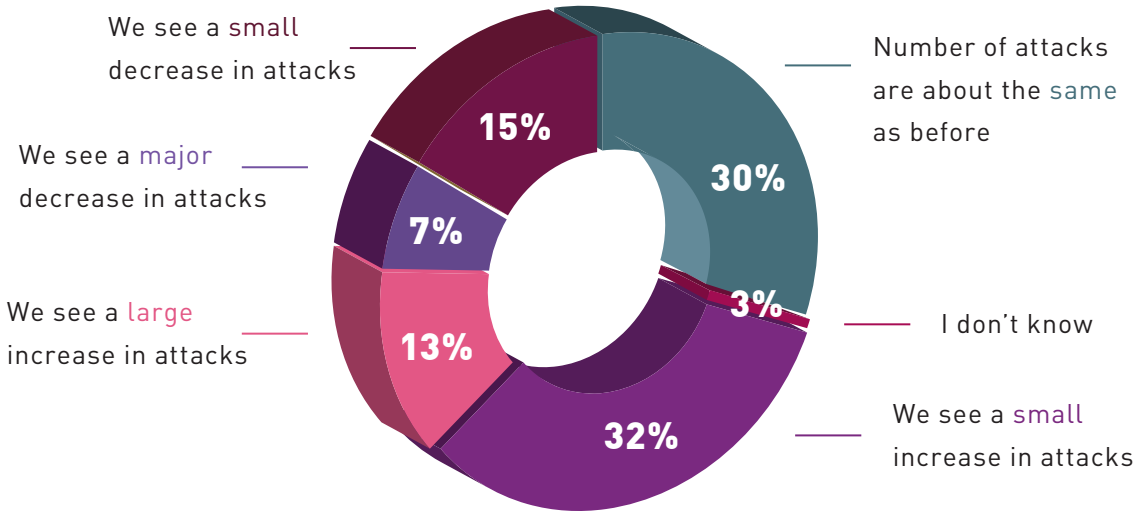


# REMOTE WORK AND INCREASED RISK

*Are organizations at higher risk of cyber attacks as they shift to remote work?*

According to 45% of all respondents, including 59% of senior management (Directors and C-level executives), the answer is a decisive **"Yes."**

***Has your organization encountered changes in cyber-attacks following Covid-19?***




**45%** of organizations report an increase in cyber attacks since Covid-19

## The industries who reported the highest level of cyber attacks

**54%** Finance

**52%** Utilities

**47%** Manufacturing

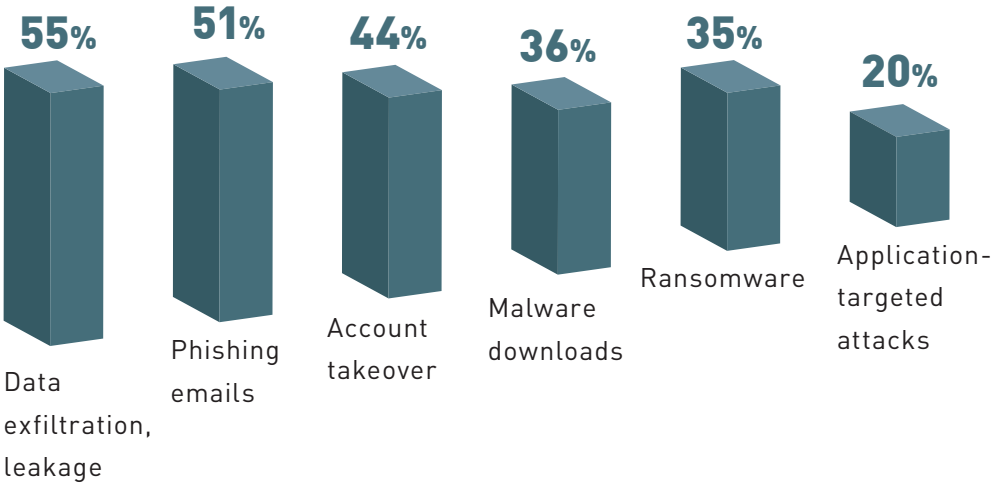
# REMOTE WORK AND BREACH & ATTACK VECTORS

The top cyber attack vectors reported by professionals who saw an increase in cyber attacks following Covid-19 are data exfiltration and leakage (55%), phishing emails (51%) and account takeover (44%).

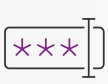
These figures speak to the need to implement data loss prevention (DLP) for internet and cloud access by remote users, so that the same level of data protection is deployed within and outside the office.

Intrusion Prevention Systems (IPS) and real-time anti-phishing engines are critical to preventing phishing attacks and account takeover, ensuring that all clicked links are inspected and that corporate credentials are not reused in non-work accounts.

***If answered large or small increase in cyber attacks: Where do you see an increase in attacks and attack attempts?***

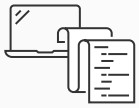



**Top Attack Vectors**



Account takeover

Phishing

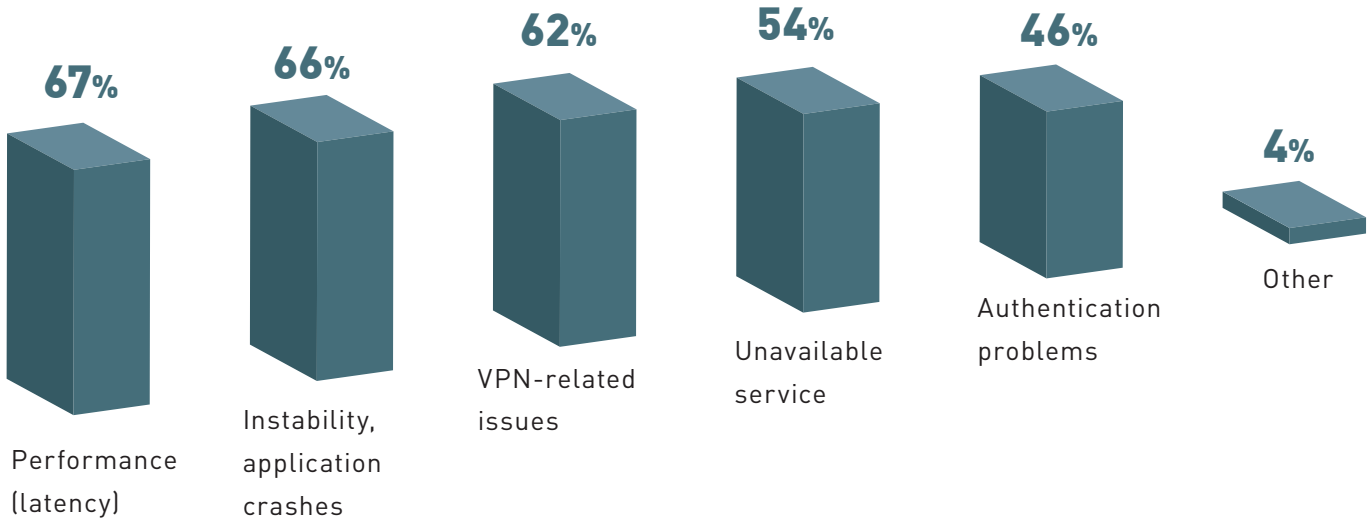


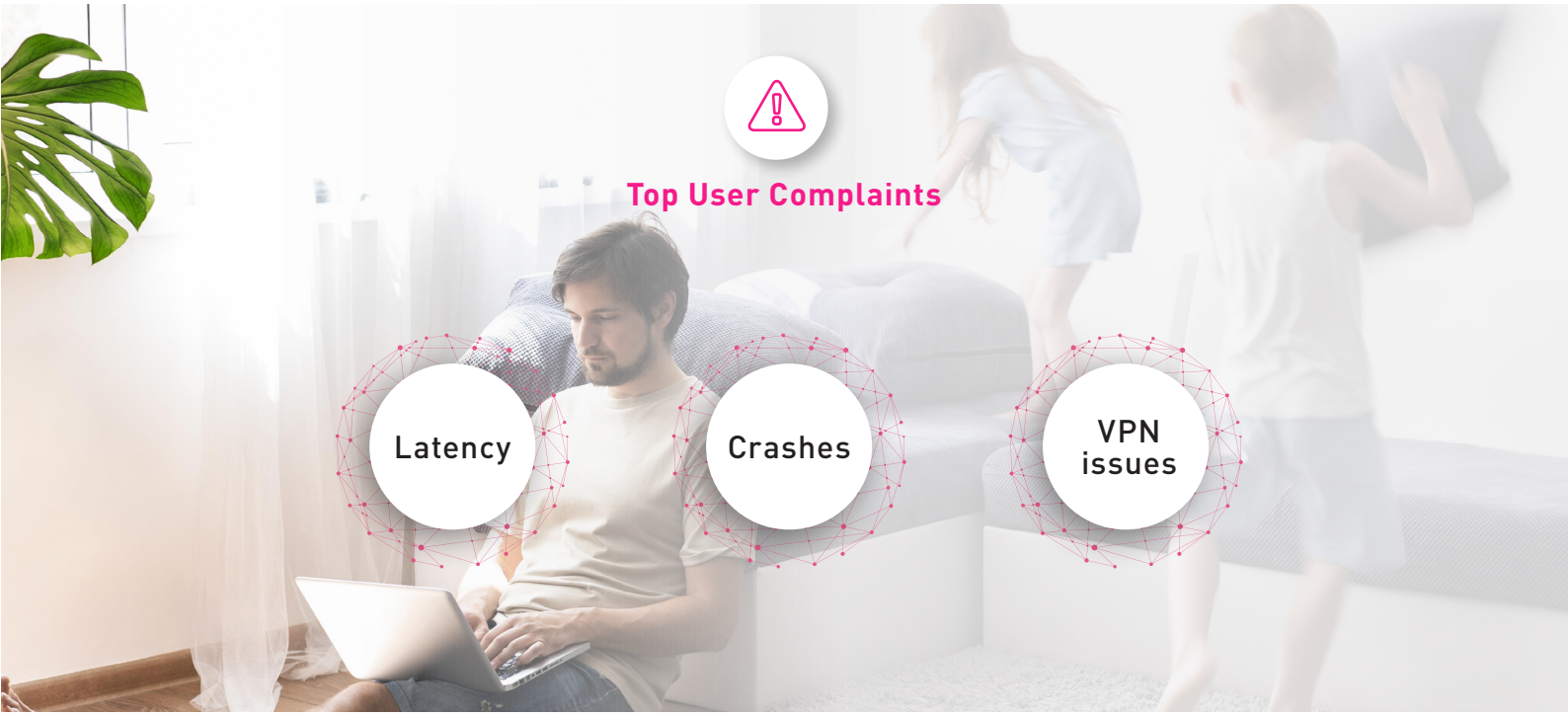
Data Leakage

# REMOTE WORK AND USER ISSUES

The move to remote work means all resources are accessed remotely. Performance issues / latency (67%), instability and application crashes (66%) and VPN-related issues (%62) were identified as the top three most common reasons for help desk calls and support tickets in regards to remote access.

Needless to say, security and networking infrastructure not adapted to remote work may lead to traffic congestion and a poor user experience. The traditional hub-and-spoke model of network architecture that routes all traffic to the on-prem data center for inspection is often difficult to scale, adversely impacting network performance and connection speed. Hence, the growing interest in cloud-based security service and SASE.



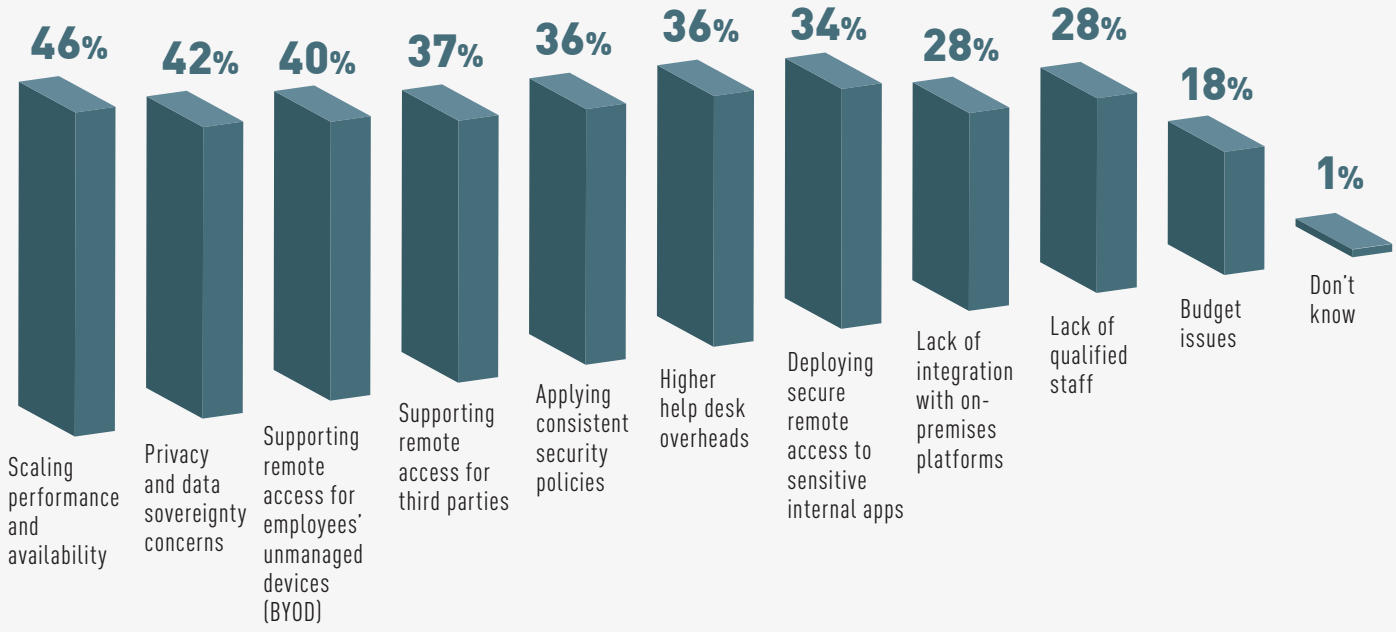



# REMOTE WORK AND ADMINISTRATION CHALLENGES

When it comes to managing remote access, the top three issues IT and security professionals contend with are scaling performance (46%), addressing privacy and data sovereignty concerns (42%) and supporting remote access for employees' unmanaged (BYOD) devices (40%).

Whereas cloud-based security and networking services can alleviate congestion and improve application speed and performance, privacy and compliance concerns can be addressed by using local points of presence (PoPs). With the emergence of service-initiated zero trust network access (ZTNA) from the cloud[1], organizations can support clientless remote access from unmanaged BYOD devices, including devices used by third parties (such as partners and consultants) without the need to install or manage an agent.

***What are the key issues you are experiencing internally with managing your current remote access set up? Check all that apply.***




**Top Admin Challenges**

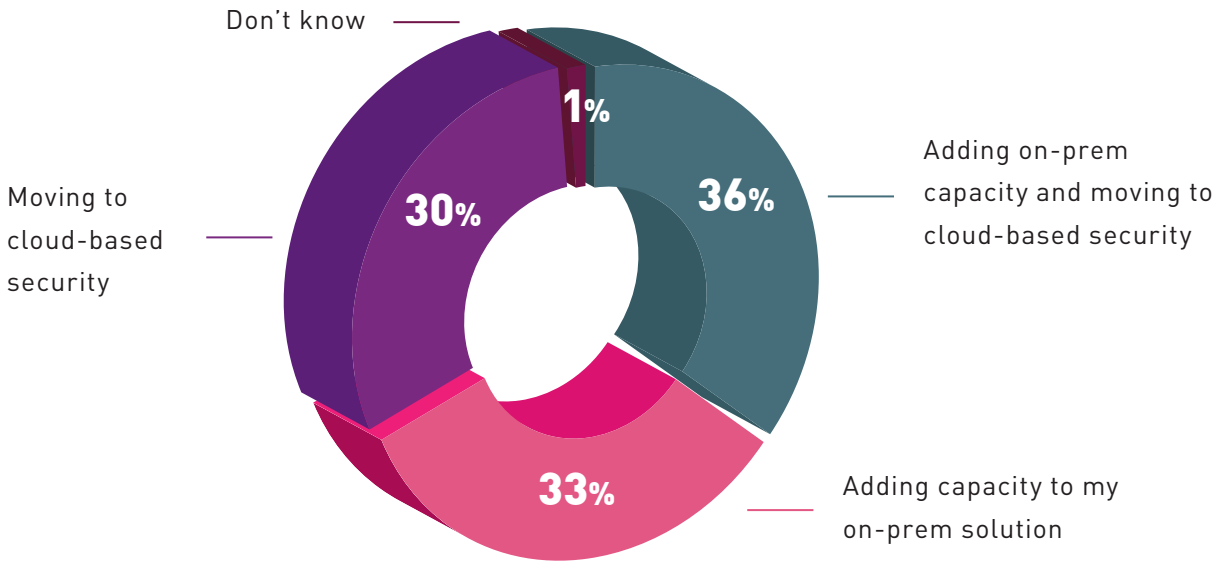

[1] For the full definition of service-initiated ZTNA, see *Gartner's Market Guide for Zero Trust Network Access* Published 8 June 2020, Steve Riley, Neil MacDonald, Lawrence Orans

# STRATEGIES FOR SCALING REMOTE ACCESS

When asked how they meet the hike in demand for remote work, 69% of respondents report they are adding on-prem capacity; 66% are moving to cloud-based security and surprisingly, 36% do both.

Why would organizations do both? For expediency, it may be easier to add capacity to current solutions, rather than rip and replace them with completely new ones. Alternatively, this may reflect a phased approach to adopting cloud-based services and SASE, or may be a result of data residency considerations, where organizations prefer to keep some inspection engines on-premises, rather than inspecting all web traffic in the cloud.

***How have you been scaling up your remote access solutions to manage the increase in demand?***



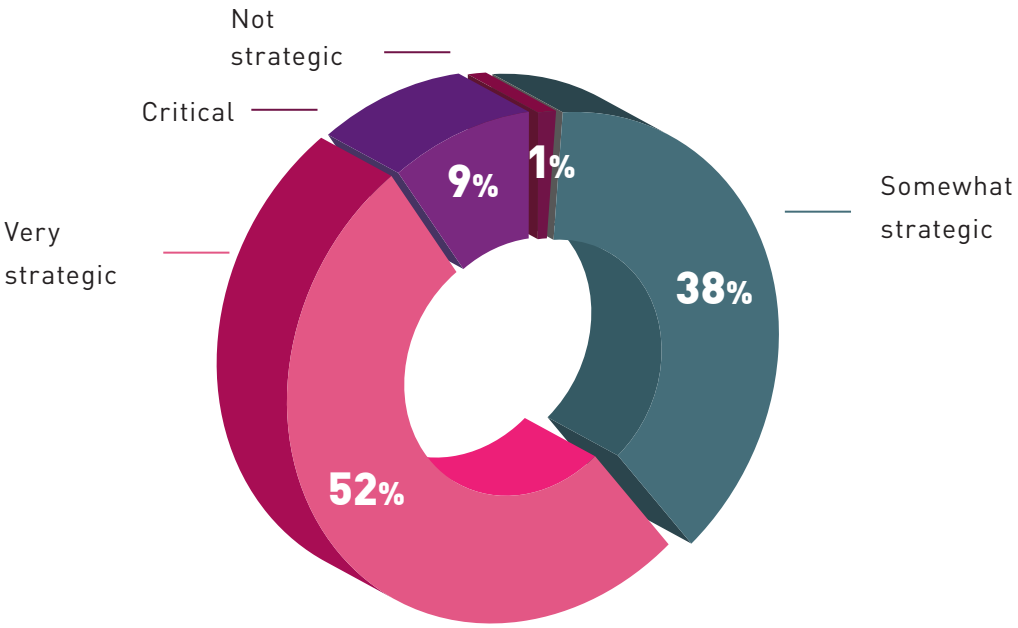

**66%** are scaling remote access with cloud-based services

# REMOTE ACCESS AND CLOUD-BASED SECURITY

When it comes to cloud-based security services, 61% of all respondents who moved to cloud-based security services consider them to be highly strategic to scaling remote access, as compared to 83% of VPs and C-level executives.

Now more than ever, cloud-based security services and SASE facilitate the transition to a hybrid remote-and-branch workplace. With users working anywhere, cloud-based services help organizations improve performance and availability on a global scale. And with applications themselves moving to the cloud, the need to secure them with on-premises engines is fast becoming obsolete. From reduced administration overhead to opex pricing, cloud services also offer numerous efficiencies from a management perspective.

***How strategic are cloud-based security services to your overall efforts to scaling secure remote user access?***



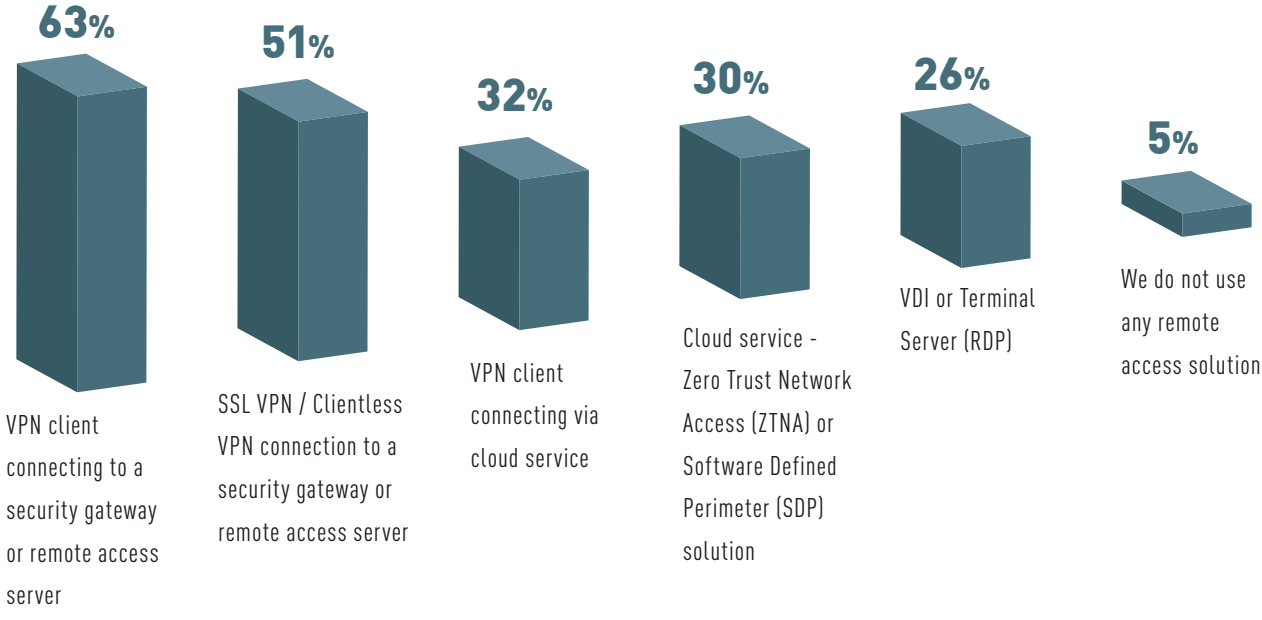

**~60%** who moved to cloud-based security consider it highly strategic for remote access

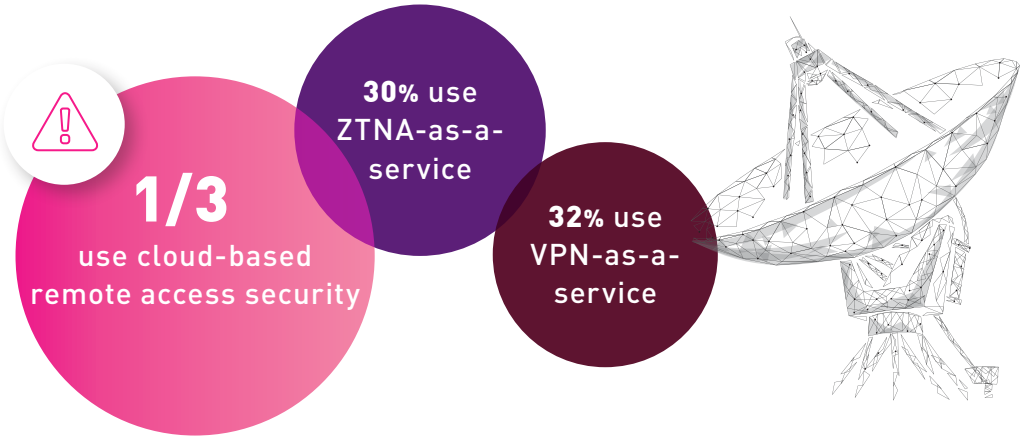
# SECURING REMOTE ACCESS TODAY

When it comes to securing remote access today, more than half of respondents report the use of traditional VPN clients (63%) or SSL VPNs (51%) connected to a security gateway or remote access server. Nonetheless, nearly one third (32%) currently consume VPN as a cloud service and a similar ratio (30%) use ZTNA cloud services.

Because the world of applications is distributed, different security mechanisms are needed to secure different types of remote access: Whereas VPN and SSL VPNs provide broad access to the target network, ZTNA architectures—a key component of SASE— are aimed at improving security by providing least privilege access, so users have the minimum privileges required to do their job.

***What is your organization's current solution for remote access?***
***Check all that apply.***



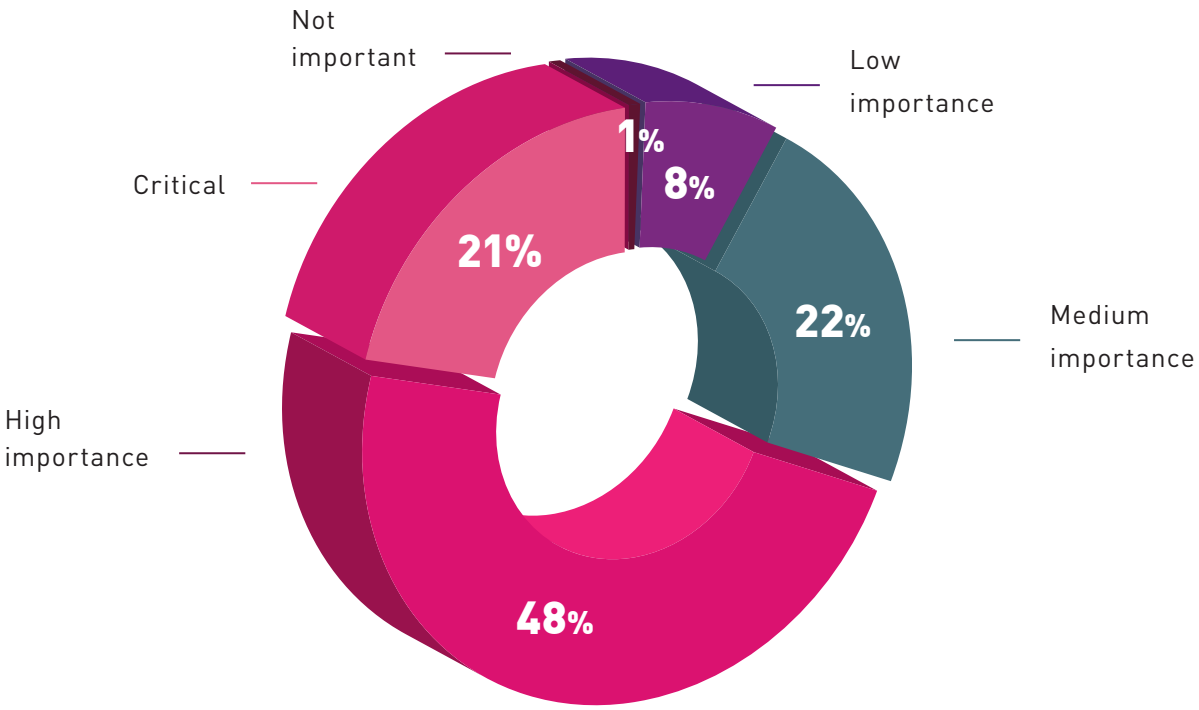



# PROTECTING APPLICATIONS ACCESSED REMOTELY

When enabling remote access to corporate apps, 70% of respondents consider the security of applications against cyber attacks and zero-day threats to be of high importance when enabling remote access (as compared to 77% among senior management).

Intrusion prevention systems (IPS) that perform deep packet inspection and virtually patch against vulnerabilities in servers, applications and protocols are an important component of preventing these types of attacks, as are web application firewalls (WAFs) and web application and API (WAAPI) protection solutions.

***When enabling remote access to corporate apps, how important do you think it is to protect your applications against cyber attacks and zero-day threats?***

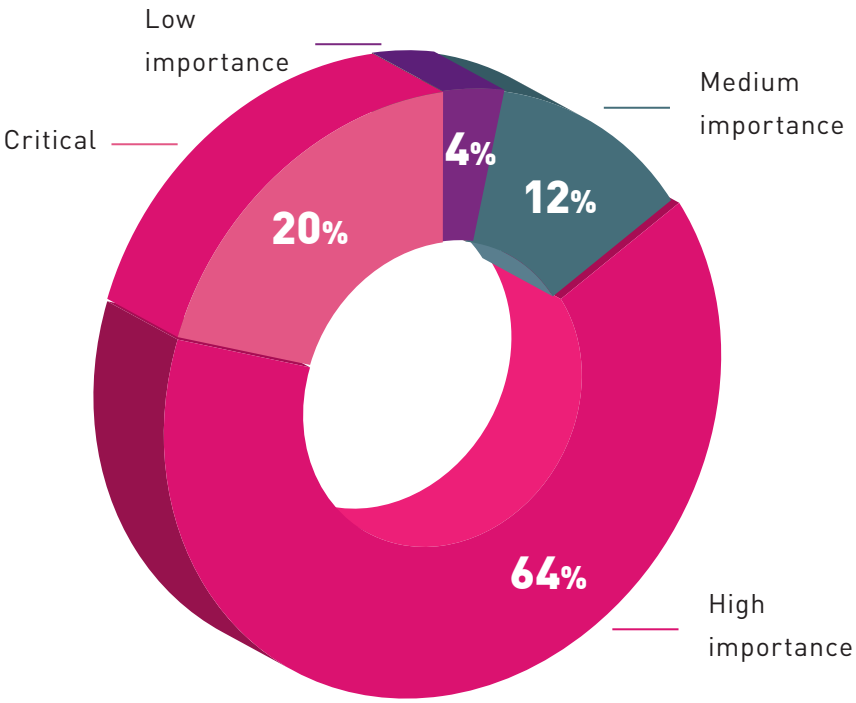


# PROTECTING USERS AGAINST PHISHING AND CYBER ATTACKS

When asked about this concern, over 80% of respondents consider the security of users to be of high importance when enabling remote access (as compared to 89% among senior management).

When working outside the enterprise firewall, users are more vulnerable to threats such as phishing sites, malware downloads and botnet-related communications. Preventing threats from ever reaching users' devices becomes critical, as retroactive detection and mitigation may be too little too late. As part of the SASE framework, Secure Web Gateways (SWGs) deliver secure internet access for remote users.

***When enabling remote work, how important do you think it is to protect your users against phishing and cyber attacks?***




**84%** consider the security of users to be of high importance when enabling remote access

Key to preventing user-targeted attacks are up-to-the minute threat intelligence and advanced sandboxing solutions that check each link accessed and each file downloaded, to block threats before they populate on users' devices. To prevent suspicious files and attachment from infecting users' devices, content disarm and reconstruction (CDR) solutions can be deployed to remove risky elements while delivering safe, visually identical sanitized files. Finally, by scanning online forms in real time—before users complete them—the very latest phishing sites can be blocked, completely eliminating the risk of account or data compromise.

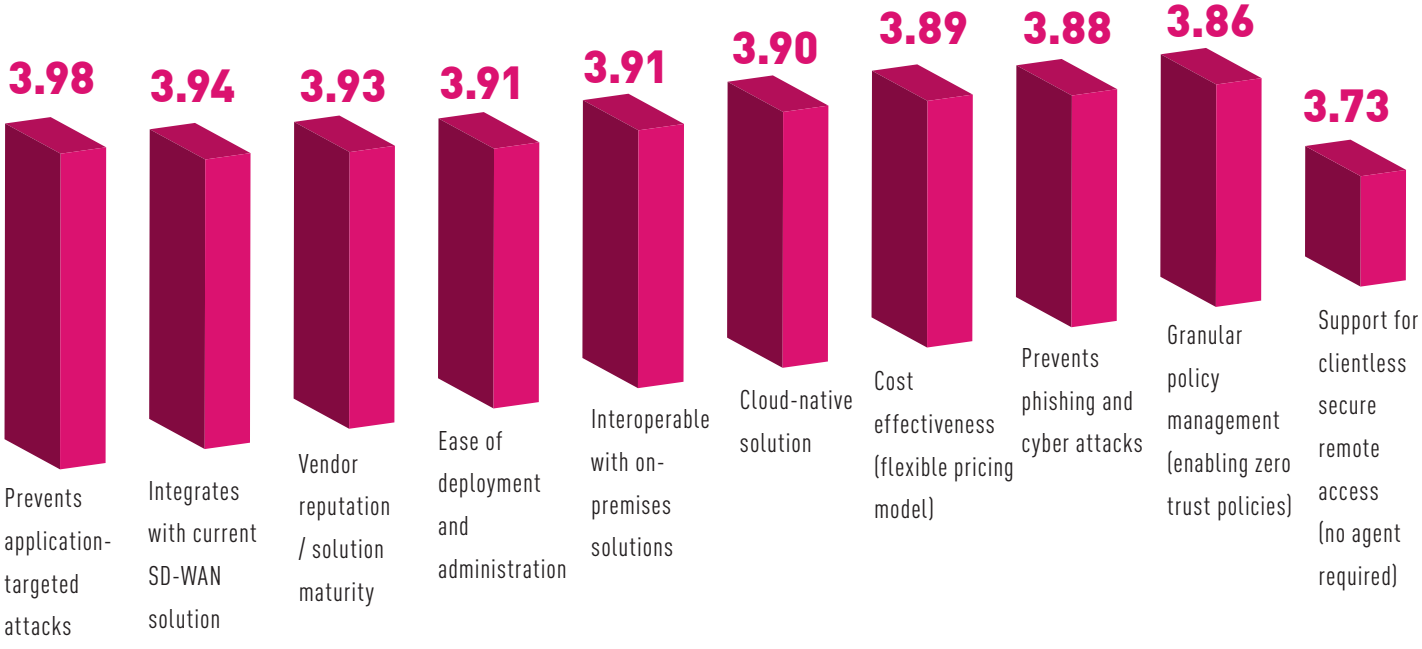
# CRITERIA FOR SELECTING A REMOTE ACCESS SOLUTION

On a scale of 1 to 5, with 5 being the most important, the top three criteria identified by respondents when shopping for a remote access solution were the prevention of application-targeted attacks (3.98), integration into current SD-WAN solutions (3.94) and vendor reputation (3.93).

Reaffirming the concern over app-related vulnerabilities and exploits, these numbers also reflect an awareness for the need to integrate advanced security services into the current networking (SD-WAN) infrastructure of branch offices connecting directly to the internet and cloud. SASE caters to this need with FWaaS for branch offices.

As the market is ripe with new and innovative services, professionals are also wary of the need to get support in the long term, leading them to consider solution maturity and vendor reputation.

***When selecting a solution to secure remote access, which criteria do you consider the most important?***



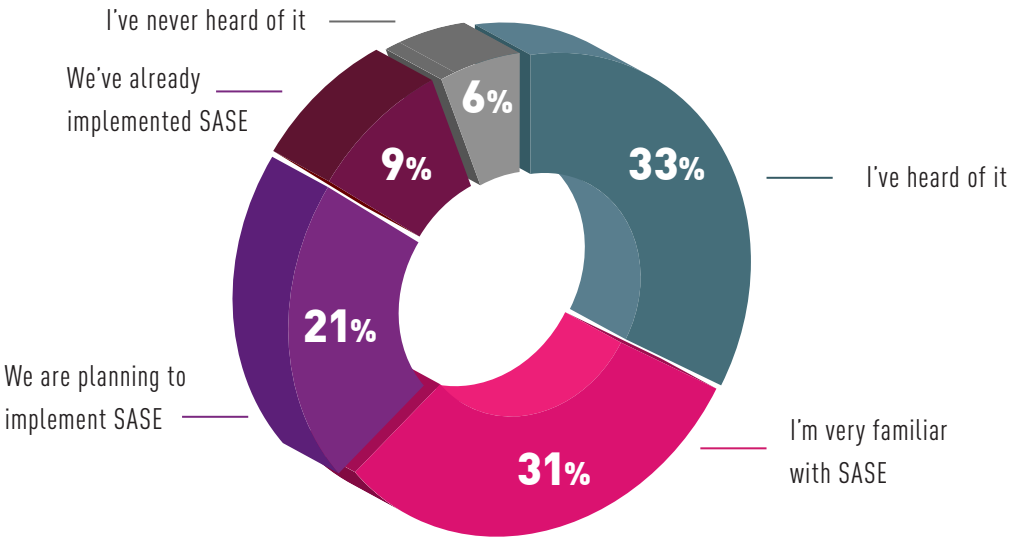

**Prevention of application-targeted attacks considered the most important criterion when selecting a remote access solution.**

# SASE ADOPTION

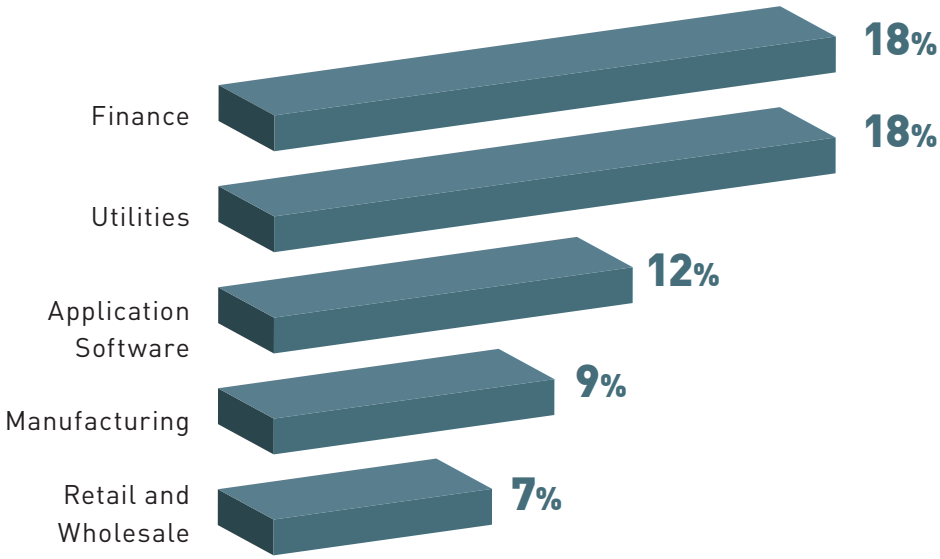
What is the adoption rate of SASE among IT and security professionals since its coining in 2019 by Gartner? Ninety four percent (94%) of respondents are familiar with SASE, but adoption is slow, with 9% who already implemented SASE and 21% who are planning to do so.

In the same vein, Gartner estimates that "By 2024, 30% of enterprises will adopt cloud-delivered SWG, CASB, ZTNA and branch office firewall as a service (FWaaS) capabilities from the same vendor, up from less than 5% in 2020."[2] These acronyms relate to key SASE use cases, namely securing internet access (secure web gateway or SWG), securing access to SaaS applications (cloud access and security broker, or CASB), providing secure remote access to corporate applications (ZTNA) and securing branch office connections (FWaaS).

***How familiar are you with the SASE (Secure Access Service Edge) concept and architecture?***




***Top industries reporting SASE implementation***
***(% of total implementations)***

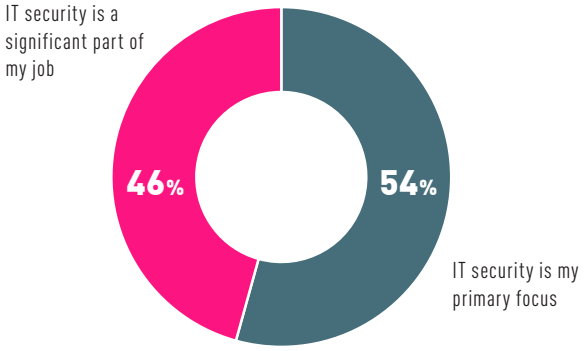



[2] Gartner 2021 Strategic Roadmap for SASE Convergence, 25 March 2021, Neil MacDonald, Nat Smith, Lawrence Orans, Joe Skorupa

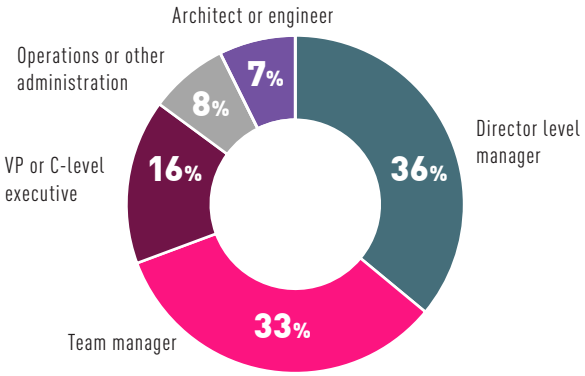
# SURVEY DEMOGRAPHICS

Results of this survey are based on 450 respondents from IT and security professionals, 50% of which are in managerial or senior management roles (directors, VPs or C-level executives). Respondent profiles are detailed below.

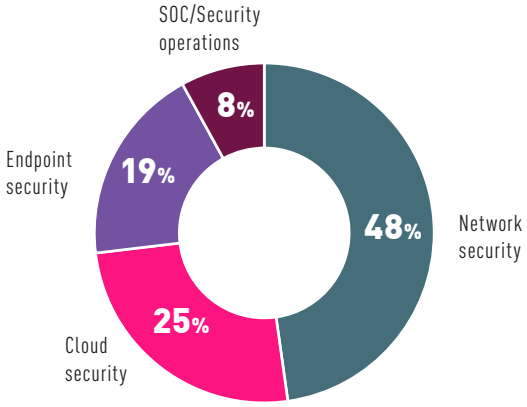
***How involved are you in your organization's IT security?***



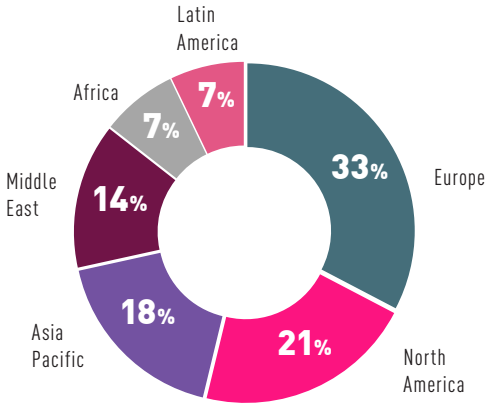

***Which of the following best describes your role?***




***What security area is your primary area of responsibility?***




***In which region are you based?***





All data is based on research completed in November 2020


Built to prevent the most advanced cyber attacks, Harmony Connect unifies multiple cloud-delivered network security services, such as **SWG, ZTNA, FWaaS and DLP**, and is deployed within minutes to apply Zero Trust policies with a seamless user experience.

**Secure internet access**
Protect remote users and offices with a SWG service that delivers the industry's best malware catch rate

**Clientless and client-based remote access**
Support access from BYOD or managed devices with ZTNA-as-a-service to enterprise apps on-prem and in the cloud

**Secure branch and retail connections**
Improve performance with FWaaS seamlessly integrated into your SD-WAN

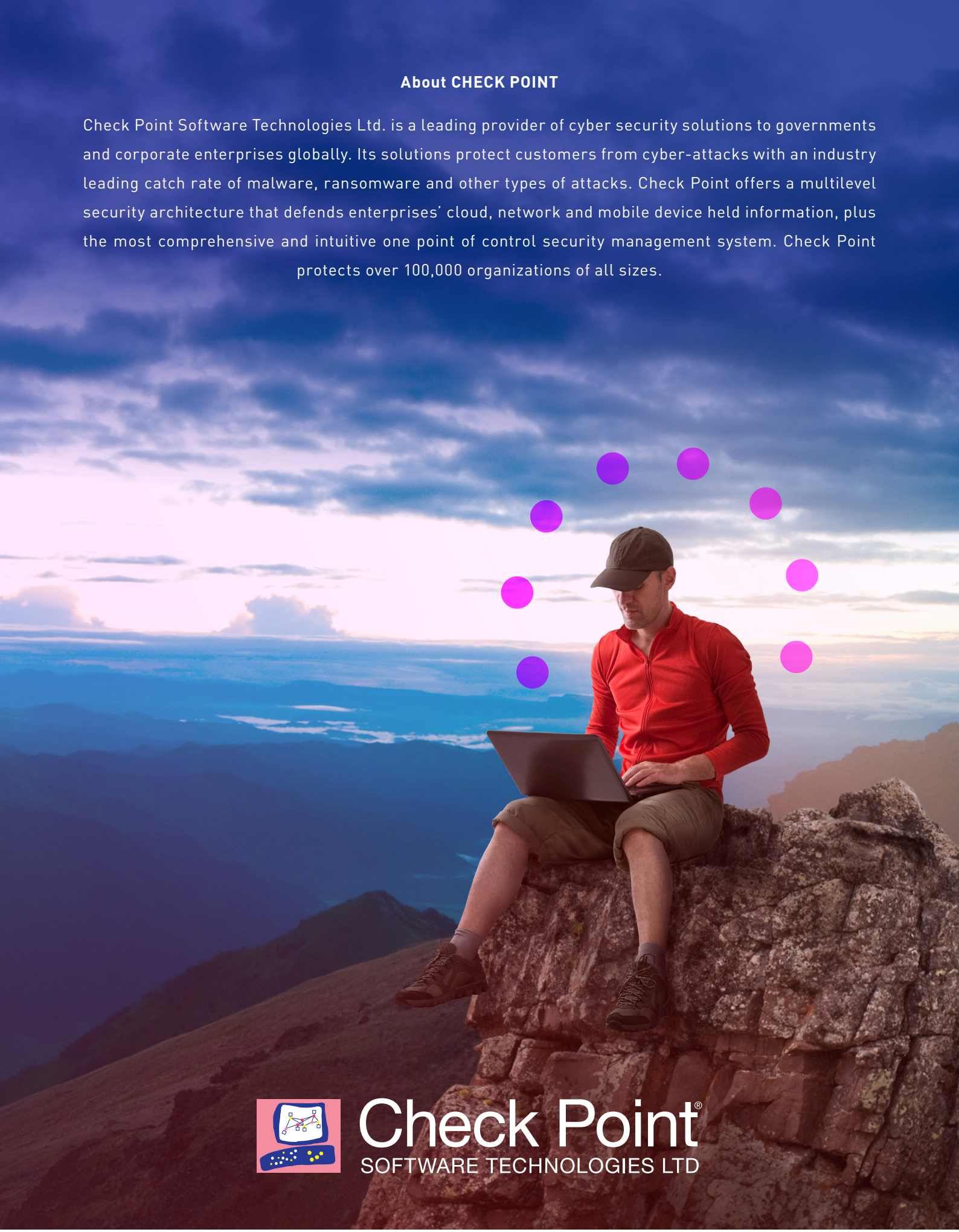
**Fast access, anywhere**
Get fast, secure connectivity from a global network of PoPs

**Privacy and Control**
Choice of availably zones to address privacy and data residency regulations

To learn more, visit us at:
**www.checkpoint.com/harmony/connect-sase**

## About CHECK POINT

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.



Check Point®
SOFTWARE TECHNOLOGIES LTD