2021

Cybersecurity INSIDERS

VPN RISK REPORT

TABLE OF CONTENTS

OVERVIEW

For nearly 30 years, VPNs (Virtual Private Networks) have been central to providing remote users with access to the corporate network. Now the digitally transformed world, where zero trust is a must and applications have moved outside the traditional perimeter, has changed that reality.

"Corporate VPN is an aging technology as organizations shift to more cloud-based services...However, in the wake of the global coronavirus pandemic, companies are realizing they have to fundamentally change the way they work."

- Rob Smith, Senior Director Analyst, Gartner

VPN technologies that were the heart of remote access have become a source of risk, leading organizations to reassess their long-term access strategy and use of VPN. The worldwide surge in remote work due to the COVID-19 pandemic has led to an increase in use of VPN, and thus, expanding the enterprises' attack surface. Threat actors are targeting VPNs as made evident by the countless new articles about VPN exploits and almost 500 known VPN vulnerabilities listed on the CVE database.

This 2021 VPN Risk Report surveyed 357 cybersecurity professionals, providing insight into the current remote access environment, the state of VPN within the enterprise, the rise in VPN vulnerabilities, and the role that zero trust will play in enabling access to apps going forward.

KEY FINDINGS:

- **93%** of companies are leveraging VPN services, yet 94% are aware that cybercriminals are targeting VPNs to gain access to network resources.
- **72%** of organizations are concerned that VPN may jeopardize IT's ability to keep their environments secure.
- **67%** of enterprises are considering a remote access alternative to a traditional VPN.
- Today, **72%** of companies are prioritizing the adoption of a zero trust model, while 59% have accelerated their efforts due to the focus on remote work.

Many thanks to Zscaler for supporting this important research project.

We hope you find this report informative and helpful as you continue your efforts in protecting your IT environments.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

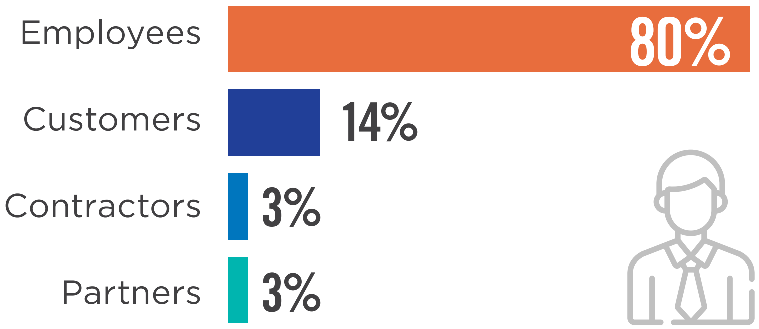
REMOTE ACCESS ENVIRONMENT

SECURE ACCESS FOR WHO, WHAT...

To build a plan to support remote work in a modern world, IT security teams must consider: who is accessing their applications, from what devices, and from where? Below is what our survey uncovered.

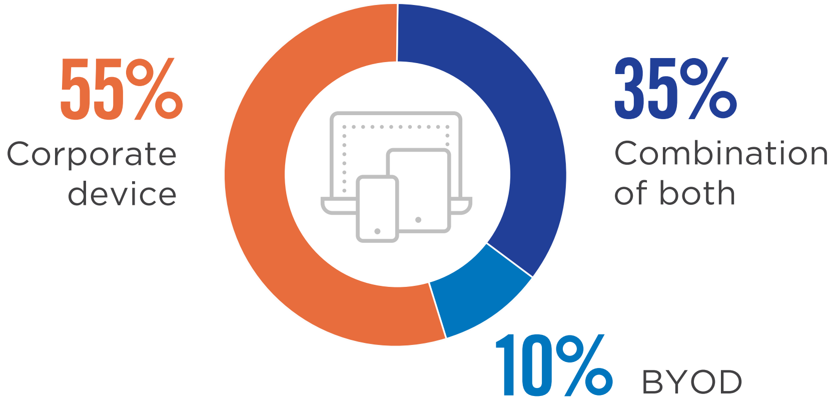
WHO: When it comes to requiring secure access to business apps, employees take priority, unsurprisingly. **Eighty percent of organizations are making employee access their first priority**, followed by customers (14%), partners, and contractors (3% each).

When requiring secure access to business applications, which group takes priority?



WHAT: When asked about what type of devices remote workers are using to connect to business resources and apps, **45% of organizations report the allowed use of BYOD/personal devices.** Being unable to enforce security measures on those BYOD devices makes device security and access control more challenging, especially in remote work scenarios.

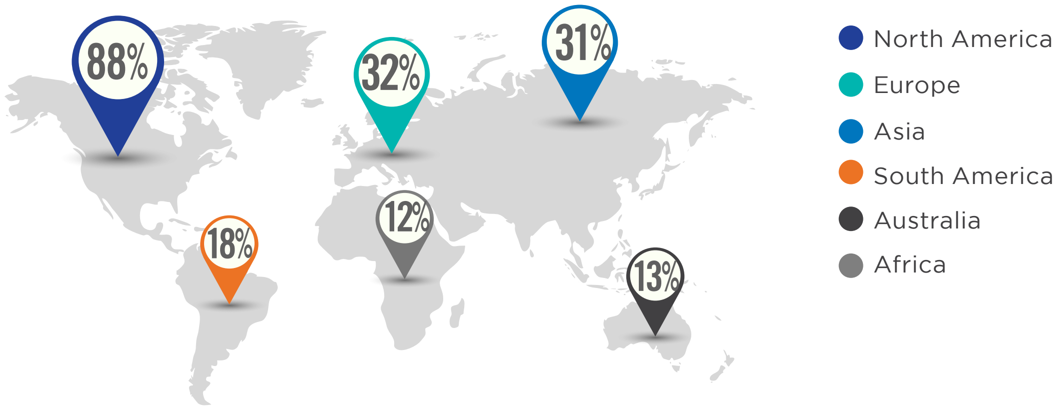
What devices are workers using to connect to business resources and applications?



… AND WHERE

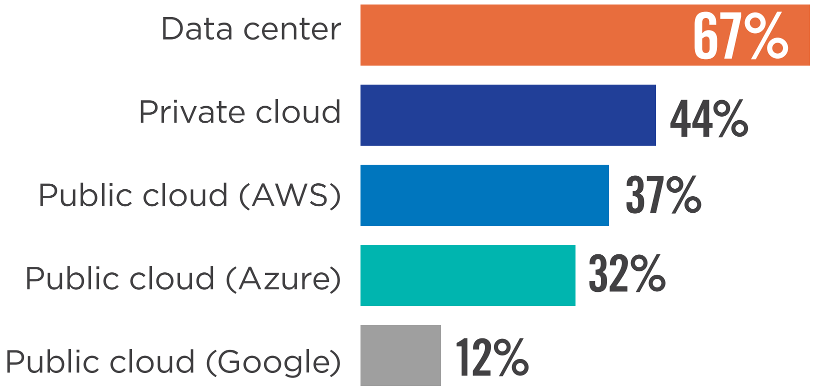
WHERE: Organizations in our survey report that **88% have remote workers connecting from North America, 32% with remote workers from Europe, and 31% from Asia.** With users distributed across geographies, supporting secure remote work can become a greater challenge as different regions have varying security standards, availability, compliance policies, etc.

From where are your remote workers connecting?



Additionally, this survey found that **enterprises' private applications are most typically running in data centers (67%), followed by the private cloud (44%), and then public clouds (37% AWS/32% Azure/12% Google Cloud Platforms)**. As organizations continue to adopt a multi-cloud strategy, ensuring consistent security across all environments becomes increasingly difficult.

Where are your private applications currently running?



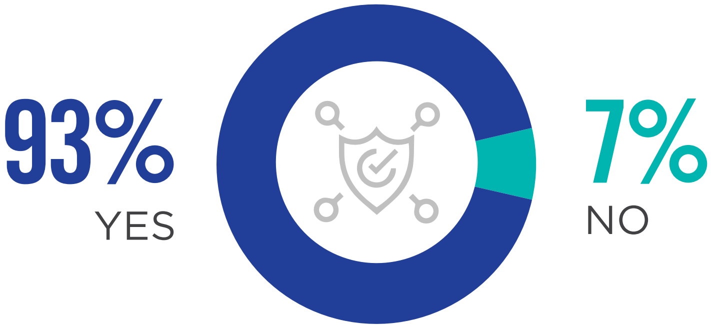
Other 4%

STATE OF VPN

VPN USAGE AND NUMBER OF GATEWAYS

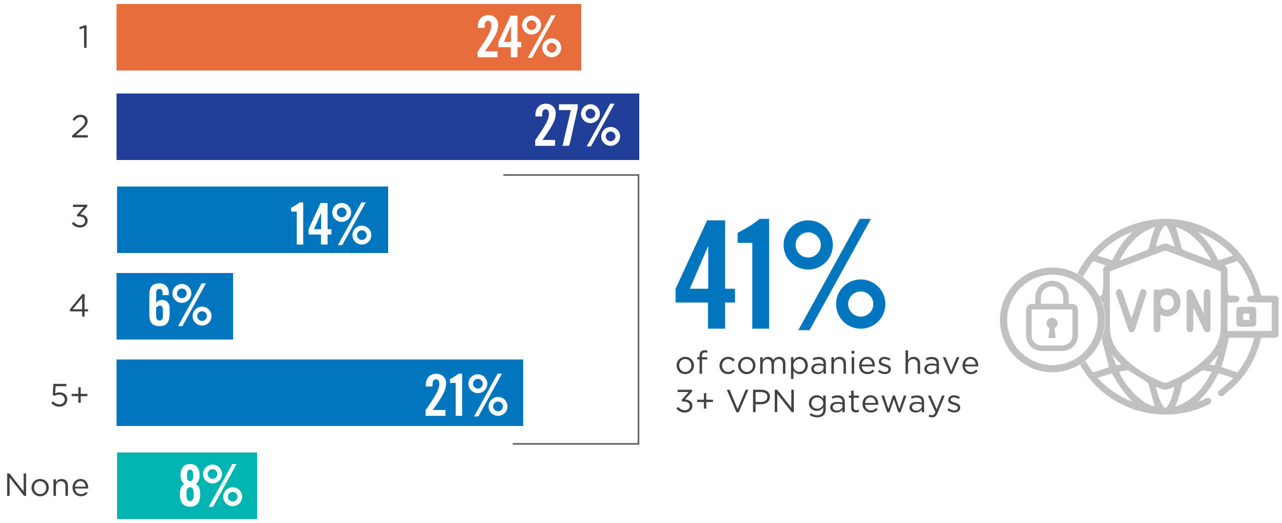
Remote access adoption has increased significantly due to the unforeseen events of 2020. While our survey found that **the vast majority of organizations are currently leveraging a VPN service for secure remote access (93%)**, we wanted to dive into more detail into the actual state of VPN and how 2020 affected your remote access.

Are you currently using a VPN service within your organization?



When asking respondents how many inbound VPN gateways they have globally, **41% of organizations state they have 3+ VPN gateways, with half of those companies reporting to have 5+ gateways.** Each gateway requires a stack of appliances, often including the VPN (RAS), Internal Firewall, Internal Load balancer, Global Load balancer, DDoS, External Firewall, etc. The more gateways an organization has, the more expensive secure remote access becomes and the more complicated it is for IT to administer and manage each inbound stack.

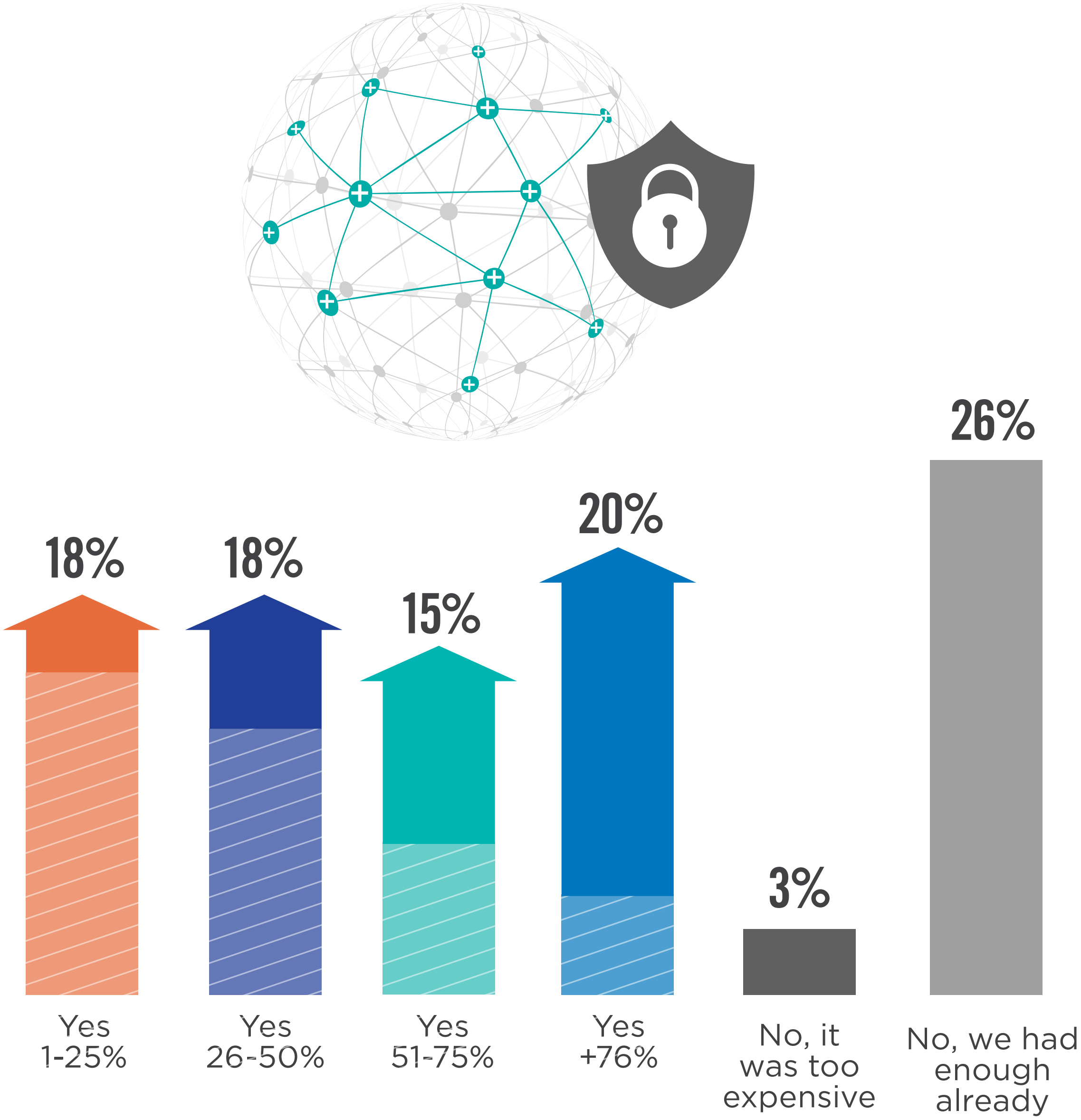
How many different inbound VPN gateways do you have globally?



VPN CAPACITY AND SCALABILITY

The COVID-19 pandemic created a subsequent surge in remote employees where **71% of companies reported they were forced to increase their VPN capacity. Out of the companies that required additional bandwidth, a third of them increased VPN capacity by over 50%**. In contrast, 26% of companies reported no need to scale VPN during COVID-19. This could indicate that these organizations had unused capacity leading up to the outbreak and were overspending on their VPN.

▶ **Did you increase your VPN capacity during the COVID-19 pandemic? If so, by what percentage?**



TOP VPN CHALLENGES

While many organizations have relied on VPN for secure remote access with the increasingly mobile workforce, it's not without its pitfalls. **When asked to rank the most significant challenges organizations face with their remote access solution, lack of visibility into user activity takes the top spot, followed by the high cost of security infrastructure.**

What is your biggest challenge with your current remote access solution?

24%

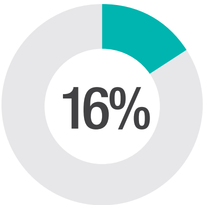
Lack of visibility into user activity taking place

23%

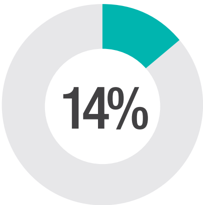
High costs of security appliances/ infrastructure

19%

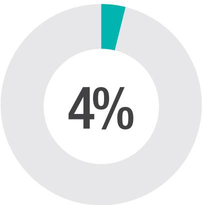
Requires giving employees and third-parties access to the corporate network



Poor user experience due to backhauls to VPN gateways



Complexity of managing existing remote access across public cloud environments



Inability to scale to meet user demand

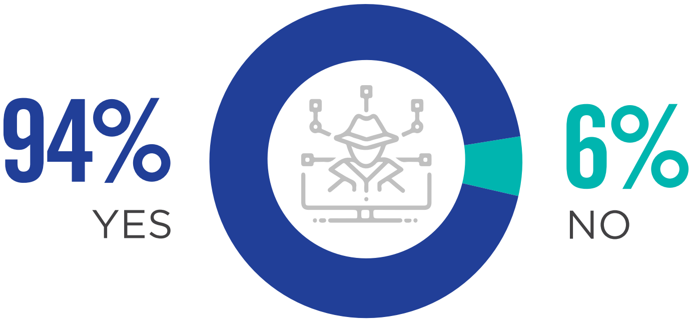
With users no longer connecting locally in the office, IT loses a significant amount of user activity, leaving many blind to what their users are accessing. Additionally, as companies have had to scale their VPN due to the rise in remote access, the high cost of appliances and infrastructure have eaten into many IT budgets.

VPN VULNERABILITIES AND RISK

INCREASE IN VPN THREATS

An increase in remote work has consequently resulted in a spike in popularity of VPN-targeted attacks amongst cybercriminals as they seek to gain unauthorized access to network resources exposed to the internet. In fact, **94% of companies know that their VPNs are vulnerable to cyberattacks and exploits** yet still leverage this technology while aware of the risk.

Are you aware that cybercriminals are targeting VPNs to gain access to network resources through exploits such as remote code exploits, Windows servers, ransomware, and social engineering attacks?



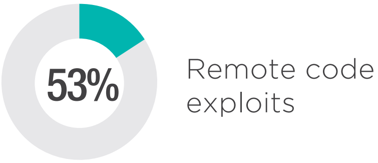
When asked about the most concerning internet-based attacks, **organizations agree that social engineering (75%), ransomware (74%), and malware (60%) are the most critical attack vectors**. As we have seen in the past, it only takes one infected device or stolen credential to put an entire network at risk, which is why cybercriminals are specifically exploiting users accessing VPN.

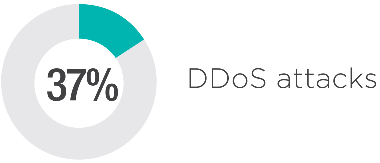
What type of internet-based attacks are you most concerned about?

75% Social engineered

74% Ransomware

60% Malware





Other 4%

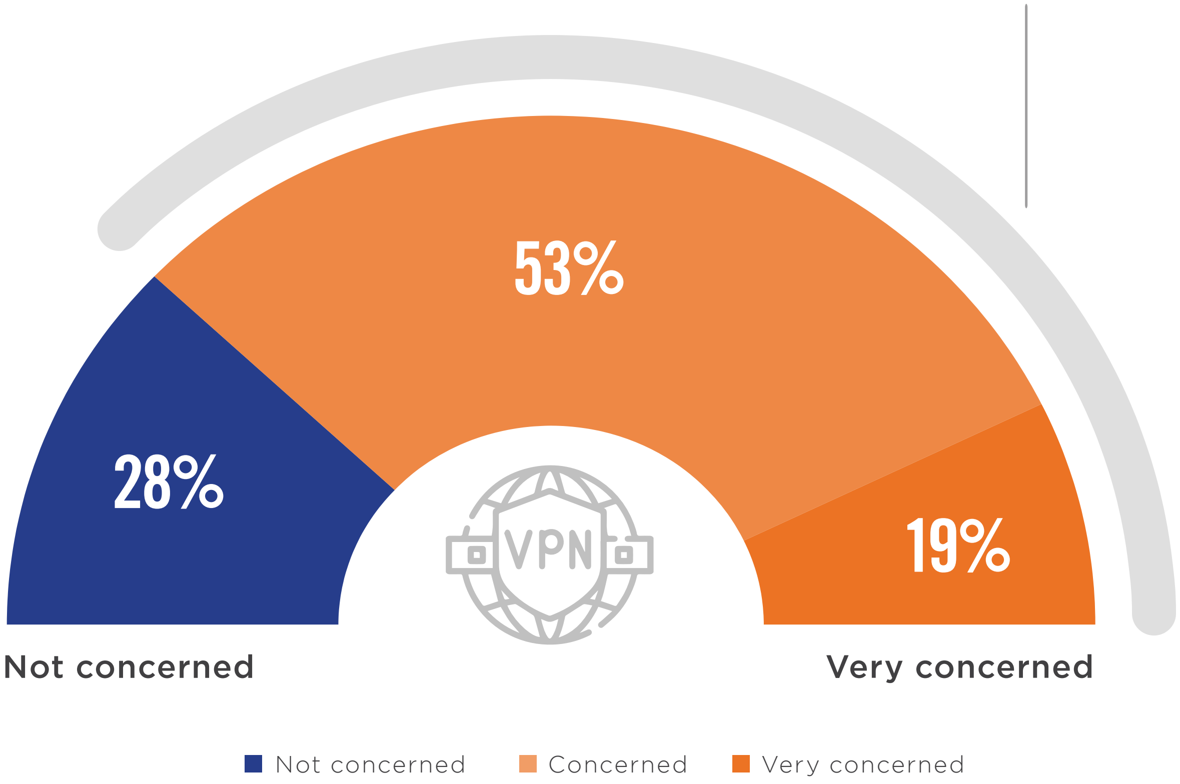
CONCERNS OVER VPN SECURITY

Seventy-two percent of companies said that they are concerned that VPN may jeopardize the ability to keep their IT environments secure. The question is raised to all IT, if your secure remote access solution doesn't deliver the level of security desired, does your remote access strategy need to be adjusted?

How concerned are you that VPN may jeopardize your ability to keep your environment secure?

72%

are concerned that VPN may jeopardize the ability to keep the environment secure.

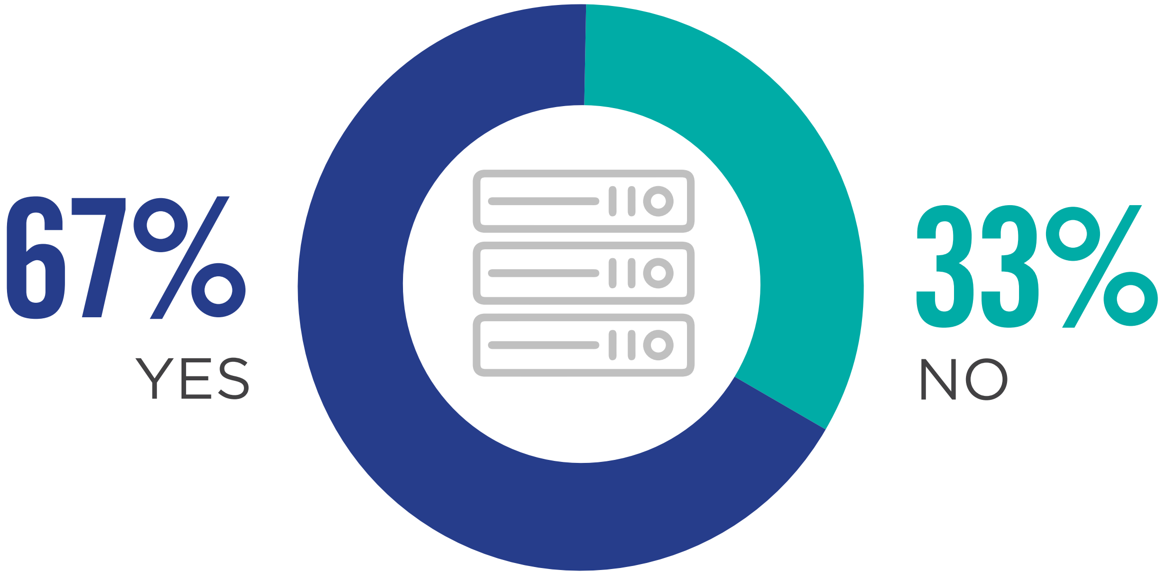


VPN ALTERNATIVES

With nearly three out of four businesses concerned with VPN security, **the majority of organizations (67%) are considering remote access alternatives to the traditional VPN.**

In light of VPNs' vulnerabilities and risks, 2021 appears to be the end of the VPN age and the beginning of a new era towards adopting a zero trust strategy.

▶ **Have you considered remote access alternatives to traditional VPN?**

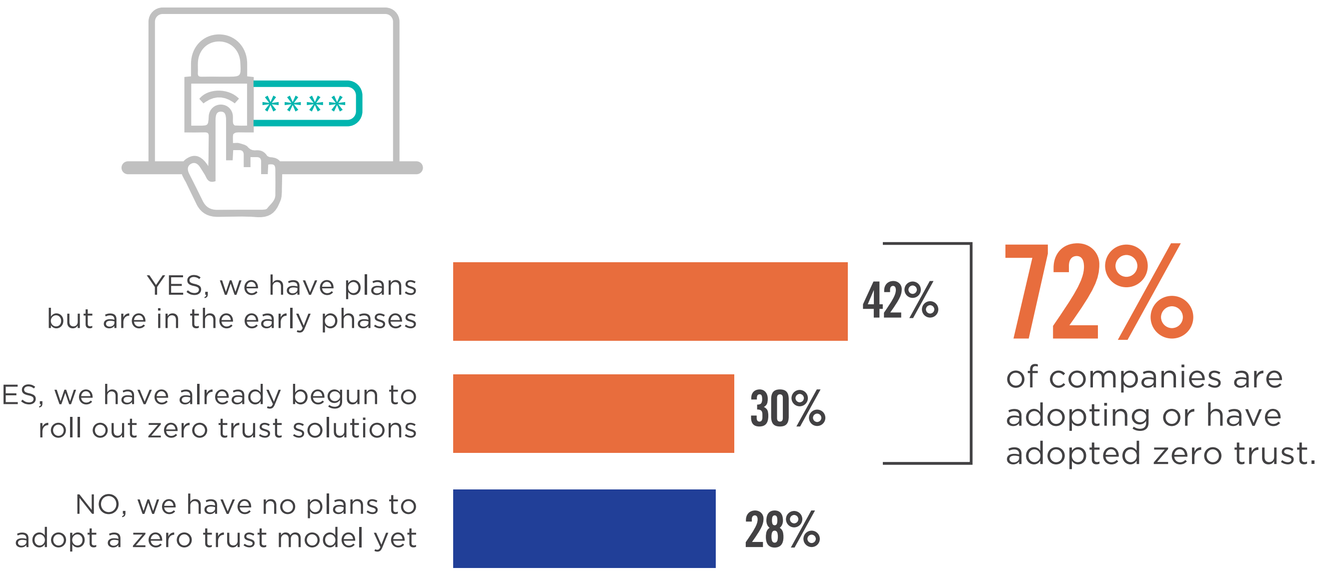


FUTURE OF REMOTE ACCESS

ACCELERATION OF ZERO TRUST ADOPTION

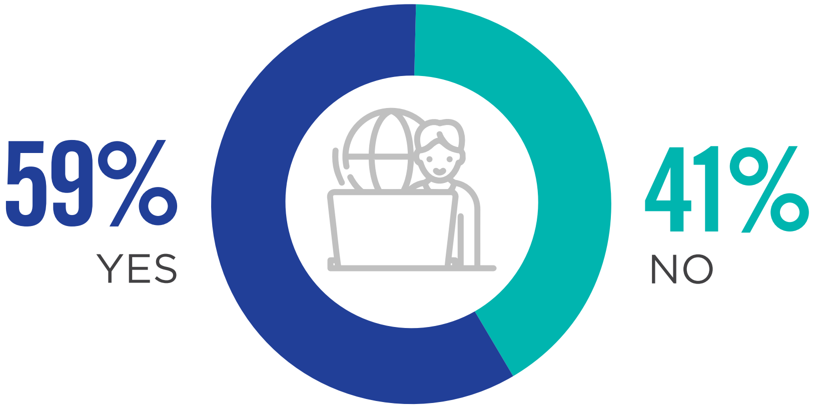
The adoption of a zero trust strategy through Zero Trust Network Access (ZTNA) and/or Zero Trust Architectures (ZTA) has/have rapidly gained traction in recent years. With the increase of mobile workers, **zero trust adoption has become a priority for many organizations, with 72% of companies confirming their plans to adopt a zero trust model.**

Is adopting a zero trust model a priority for your organization?



Not only are organizations making zero trust a priority, but **59% of companies are also accelerating their zero trust projects for faster implementation of the technology into their organization.**

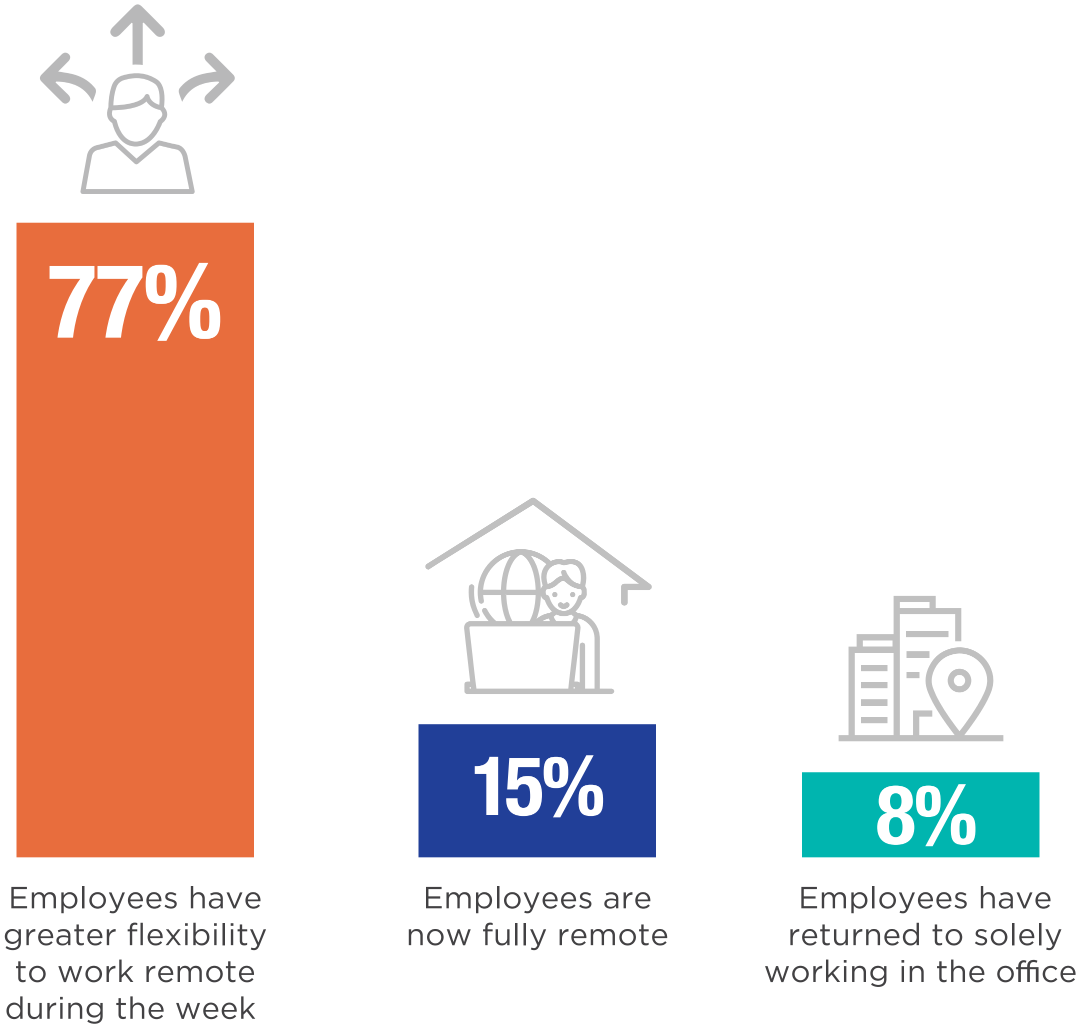
Has the focus on remote work accelerated the priority of zero trust projects at your organization?



REMOTE ACCESS MOVING FORWARD

The shift to zero trust and work from anywhere has been a catalyst to changing how organizations protect remote access. When asked about their outlook for remote access, **77% of organizations say their future workforce will be hybrid**, with greater flexibility for users to work remotely or in the office.

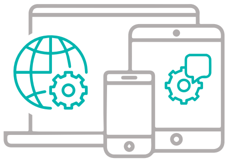
Fast forward to 2022, what does remote access look like at your company?



KEY TAKEAWAYS

While VPN has benefited from 30 years in the spotlight, the increase in VPN-targeted attacks, along with the continued shift towards mobility and cloud, has impressed on organizations the need for change in their secure remote access strategy, one built upon a foundation of zero trust principles.

In conclusion, here are the key takeaways:



With remote work expanding, users are everywhere, accessing apps from any device, and are accessing apps both in the data center and cloud.

VPNs are increasingly risky as socially-engineered, ransomware, and malware attacks continue to advance, exposing the business to greater risk.

Businesses are concerned about VPN's level of security and are looking to adopt a modern remote access approach, namely a zero trust model.

The majority of organizations have prioritized plans to adopt a zero trust strategy. With many businesses prepared to enable a hybrid workforce and workplace flexibility, adopting zero trust becomes critical.

Is VPN currently opening up your business to risk?

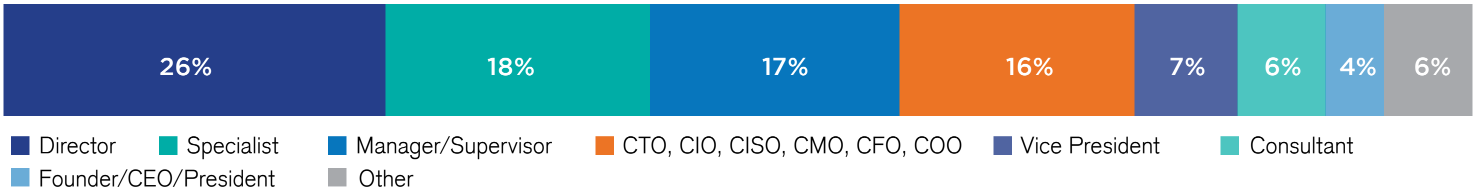
Get a free risk assessment and discover your network's attack surface before threat actors can.

UNCOVER YOUR ATTACK SURFACE

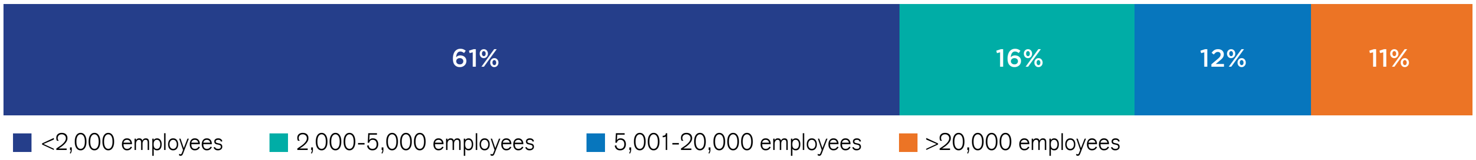
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 357 IT and cybersecurity professionals, conducted in January 2021 to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences related to VPN risk. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

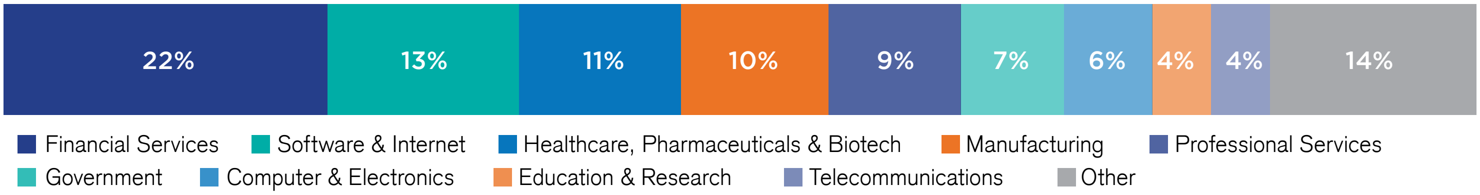
CAREER LEVEL



COMPANY SIZE



INDUSTRY



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

zscaler.com