2022

Cybersecurity
INSIDERS

VPN RISK REPORT

zscaler™

TABLE OF CONTENTS

OVERVIEW

Organizations have relied on VPNs for decades to deliver secure remote access to employees. During the COVID-19 pandemic, companies were forced to rapidly shift to remote work to stay productive and profitable. However, using VPN for remote access puts those organizations at significant risk, as traditional VPN architectures often trust too readily and excessively. Bad actors can exploit the VPN attack surface to infiltrate the network and launch ransomware, phishing attacks, denial of service, and other means of exfiltrating critical business data. As reported by countless news articles about VPN exploits, almost 500 known VPN vulnerabilities are listed on the CVE database.

This 2022 VPN Risk Report surveyed 351 cybersecurity professionals to provide fresh insight into the state of remote access and VPN within the enterprise, the rise in VPN vulnerabilities, and the role that zero trust plays in enabling the next generation of secure access.

KEY FINDINGS INCLUDE:

- **78%** of organizations are concerned about ransomware attacks
- **44%** witnessed an increase in exploits targeting their VPN since adopting remote work
- **65%** of companies are considering adopting VPN alternatives
- **80%** of companies are in the process of adopting zero trust in 2022
- **68%** say their focus on remote work accelerated the priority of zero trust projects, up from 59% in 2021

Many thanks to Zscaler for supporting this important research project.

We hope this report is informative and helpful as you continue your efforts to protect your IT environments.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

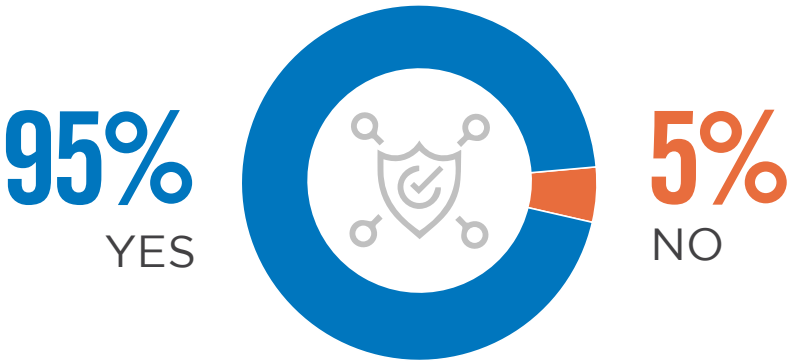
Cybersecurity
INSIDERS

REMOTE ACCESS ENVIRONMENT

SECURE ACCESS FOR WHO...

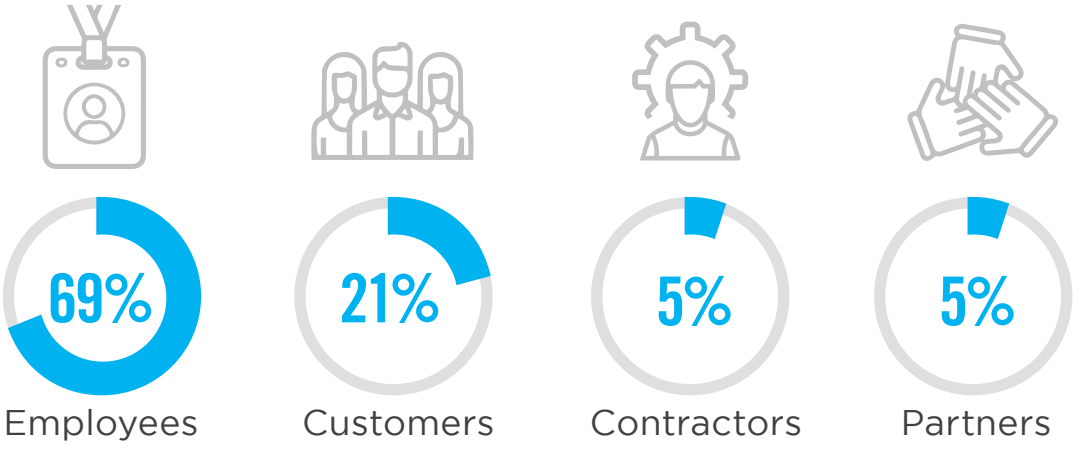
While the shift to remote work has already accelerated the adoption of remote access solutions, the latest survey found that this trend has only continued in 2021 and 2022. Now 95% of organizations are leveraging a VPN service for secure remote access (up from 93% last year). So let's dive into more detail about the current state of VPN and drivers for remote access.

Are you currently using a VPN service within your organization?



When it comes to requiring secure access to business apps, employees continue to take priority. Sixty-nine percent of organizations are making employee access their first priority. However, the relative priority has shifted compared to the previous year, as organizations are increasingly providing secure access to customers (21%, up seven percentage points compared to last year), along with partners, and contractors (5%, up two percentage points - each compared to last year).

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

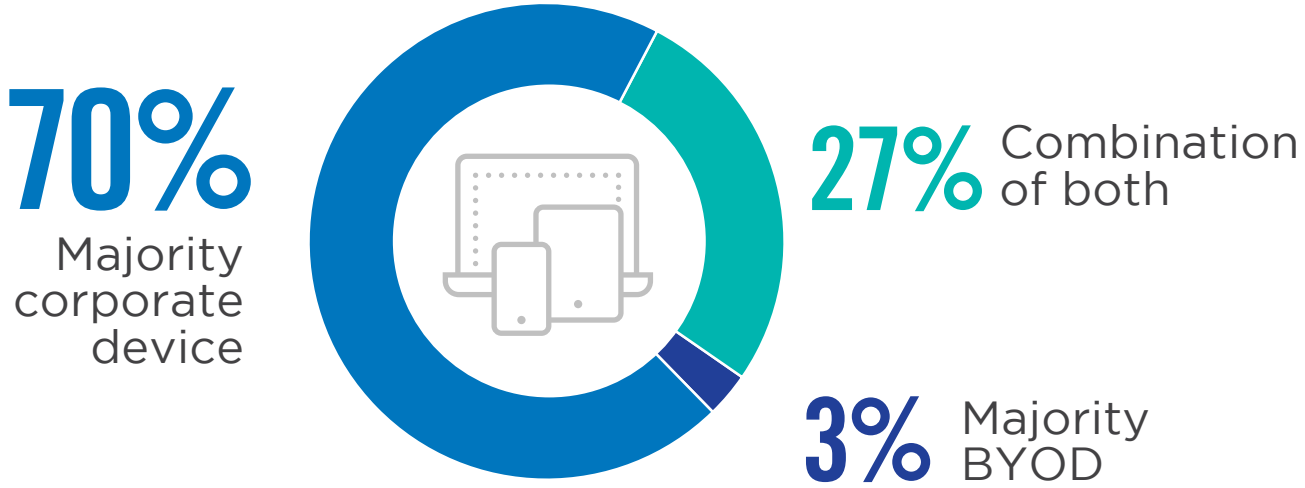


FOR WHAT...

Remote work in today's hybrid and highly distributed work environments includes more than employees. Other important stakeholders with varying needs of secure access include customers, partners and contractors - notably larger organizations with more than 2,000 employees are more likely to extend secure access to those groups. Security teams must consider: who is accessing their applications, from what devices, for what purpose and from where?

Organizations have a variety of device choices and policies when enabling secure access to remote employees. Seventy percent of organizations report they offer predominantly corporate devices. A small percentage have majority BYOD/personal devices (3%). Enforcing security measures on BYOD devices makes device security and access control more challenging, especially in remote work scenarios.

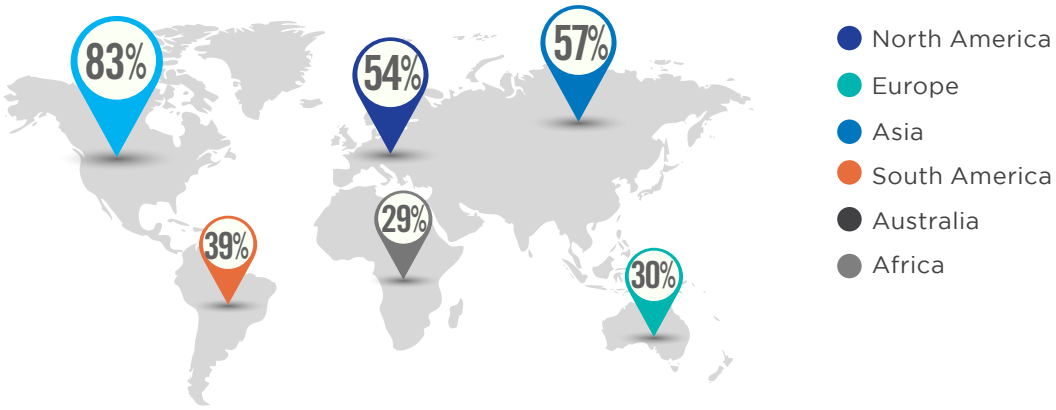
What devices are workers using to connect to business resources and applications?



... AND WHERE

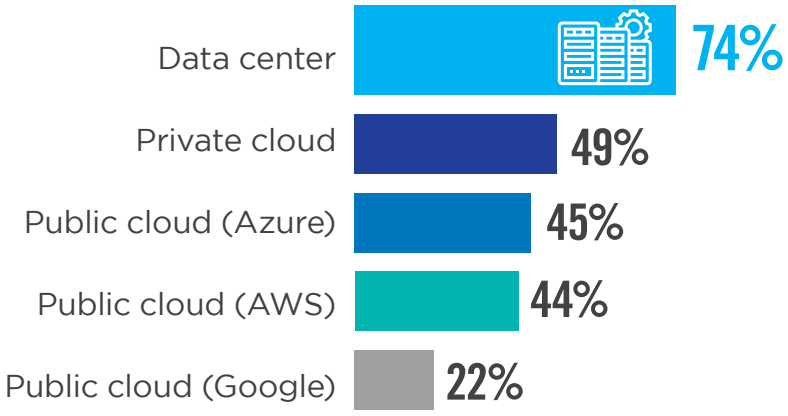
Organizations over 2,000 employees are more likely to have an international footprint. Eighty-three percent report that their remote workers are connecting from North America, 57% have remote workers accessing from Asia, and 54% from Europe. With users distributed across the globe, supporting secure 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?



Consistent enforcement of security policies is more challenging in heterogeneous environments. In our survey, organizations report that their applications are typically run in data centers (74%), followed by private clouds (49%), and public clouds (45% Azure/44% AWS/22% Google Cloud).

Where are your private applications currently running?



Other 1%

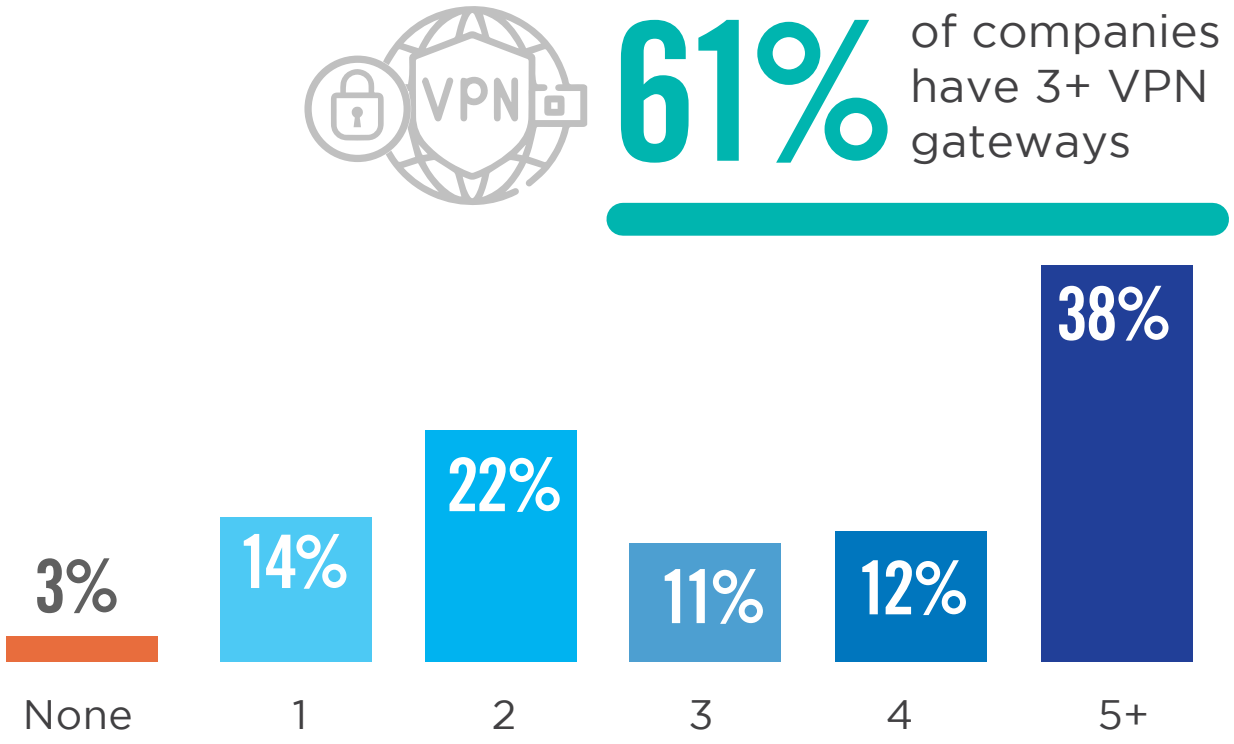
STATE OF VPN

VPN USAGE AND NUMBER OF GATEWAYS

The size and complexity of an organization typically drives the complexity of remote access infrastructure and management proportionally. A majority of companies in our survey (61%) have three or more VPN gateways – over a third of companies (38%) have even more than five.

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.

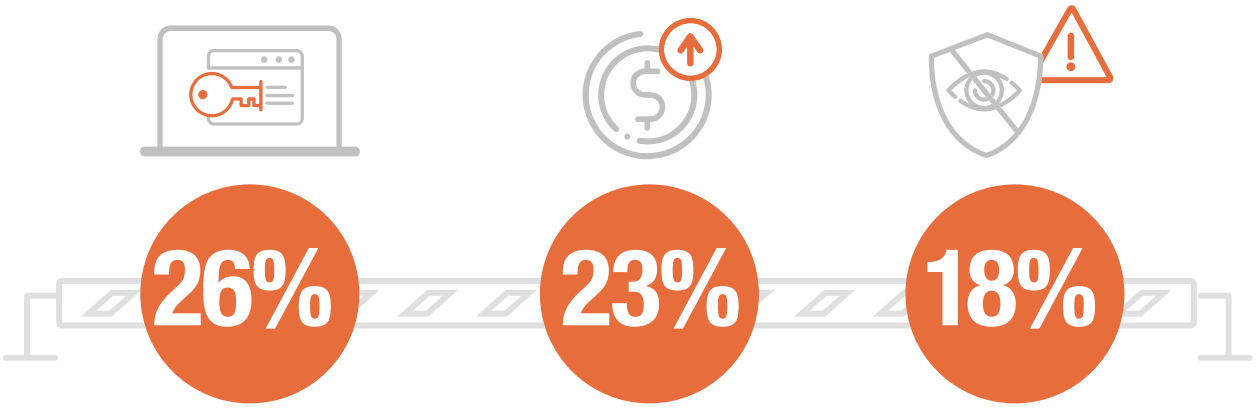
How many different inbound VPN gateways do you have globally?



TOP VPN CHALLENGES

Cybersecurity professionals in our survey confirm that remote access solutions are not without challenge, especially for larger organizations. Current VPN solutions require employee and third-party access to the corporate network (26%) is the biggest challenge as reported by organizations. This obstacle is followed by the high cost of security appliances and infrastructure (23%) and lack of visibility into user activity (18%).

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



26%

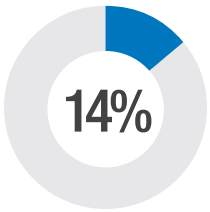
Requires giving employees and third-parties access to the corporate network

23%

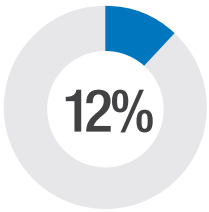
High costs of security appliances/ infrastructure

18%

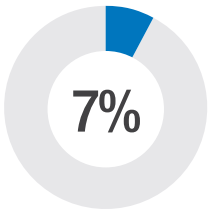
Lack of visibility into user activity



Complexity of managing existing remote access across public cloud environments



Poor user experience due to backhauls to VPN gateways



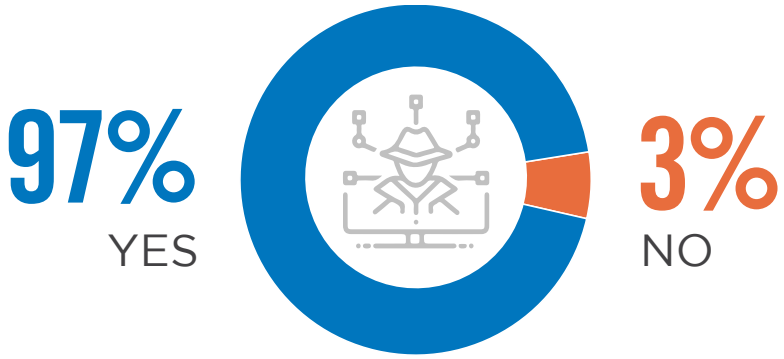
Inability to scale to meet user demand

VPN VULNERABILITIES AND RISK

INCREASE IN VPN THREATS

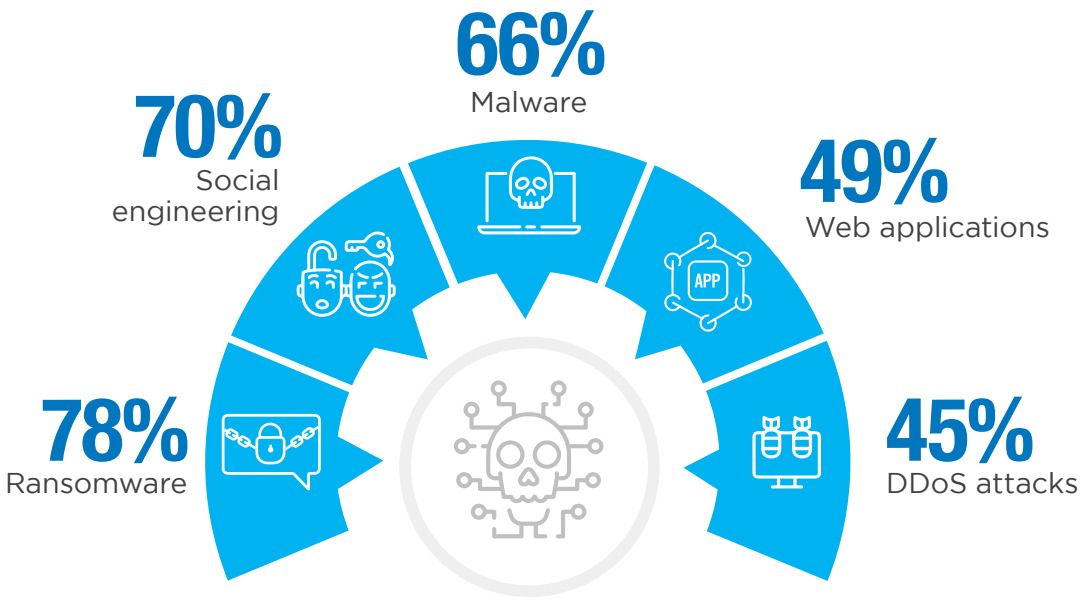
An increase in attacks and remote work has resulted in a sharp spike in the popularity of VPN-targeted attacks amongst cybercriminals as they seek to gain unauthorized access to network resources exposed to the internet. In fact, 97% of companies know that their VPNs are vulnerable to cyberattacks and 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 prioritize ransomware (78%), followed by social engineering (70%) and malware (66%) as the most critical attack vectors. Breaches show that it only takes one infected device or stolen credential to put an entire network at risk, which is why cybercriminals are targeting users by accessing though a VPN.

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

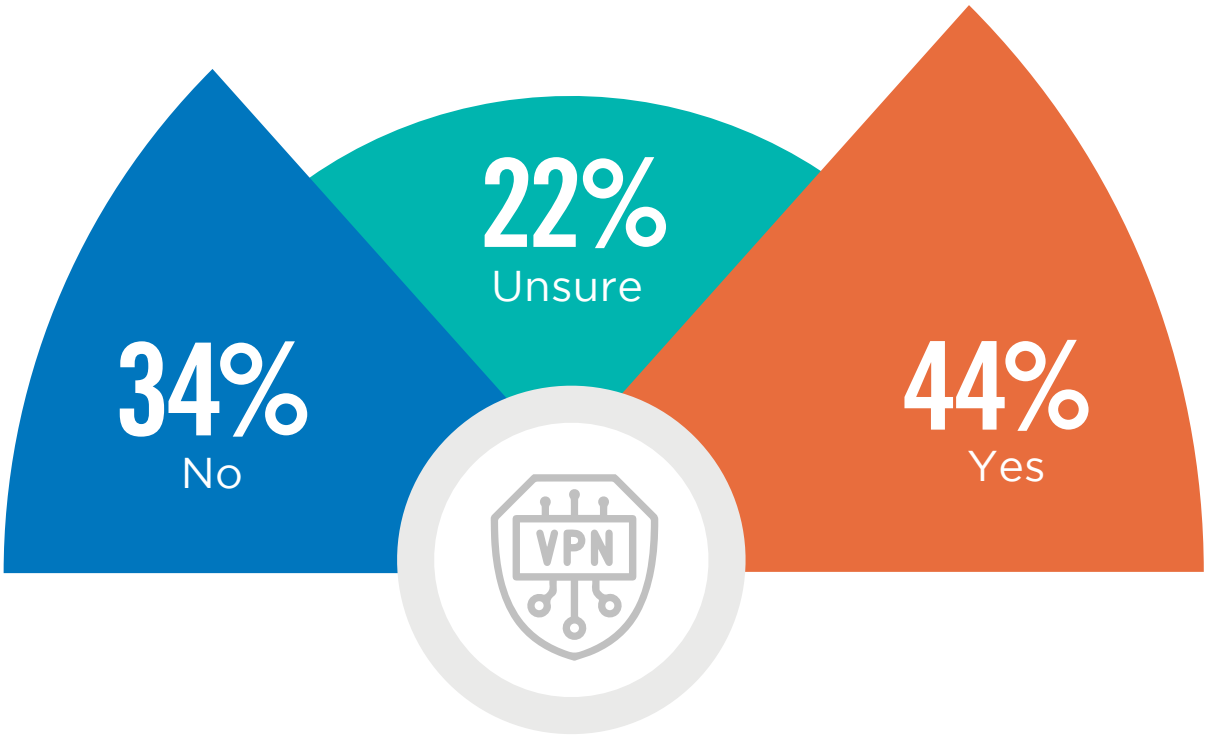


Other 3%

IMPACT OF REMOTE AND HYBRID WORK ON THREATS

Forty-four percent of cybersecurity professionals have witnessed an increase in exploits targeting their business's VPN since the shift to remote and hybrid work.

Have you witnessed an increase in exploits targeting your business's VPN since your employees have been working remotely?

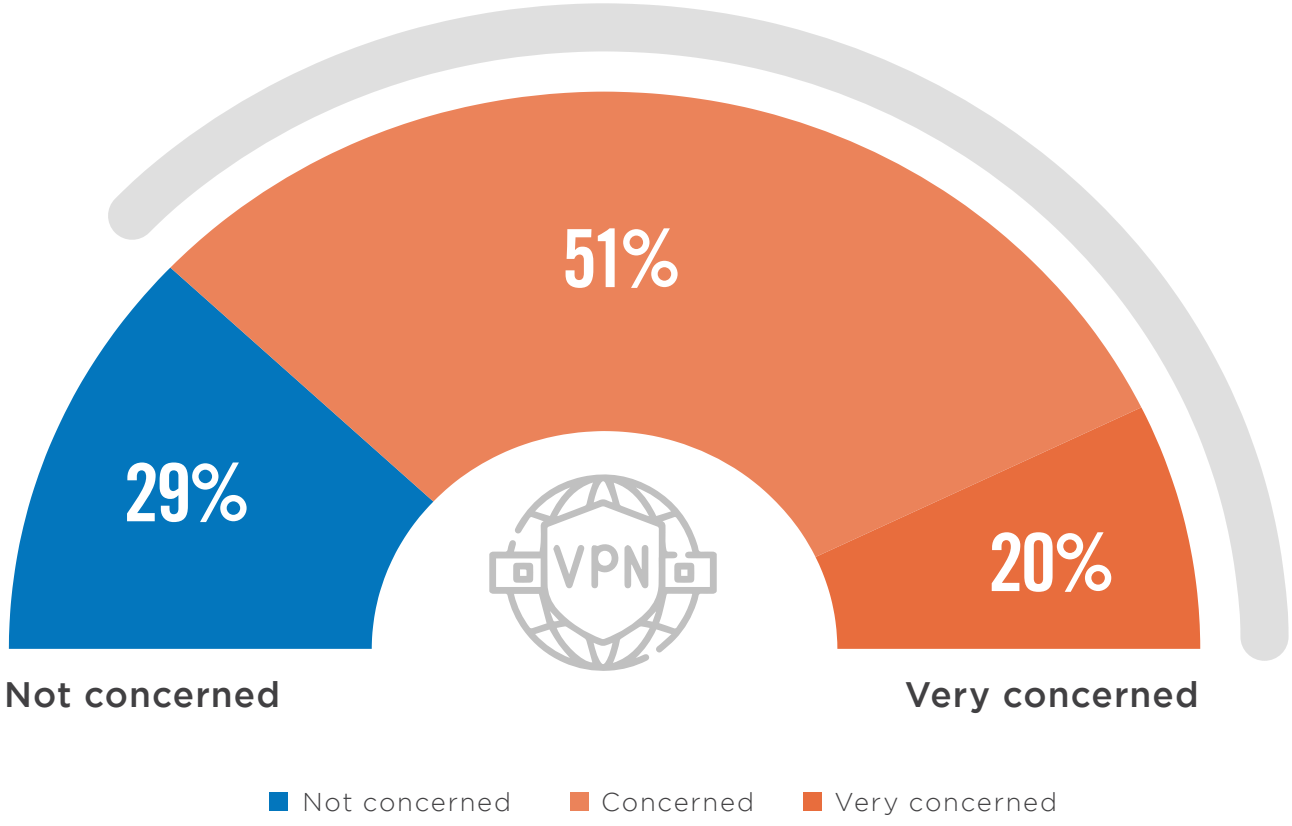


CONCERNS OVER VPN SECURITY

Seventy-one percent of companies are concerned that VPN may jeopardize the ability to keep their IT environments secure. This begs the question: if your secure remote access solution doesn't deliver the required level of security, should the remote access strategy be adjusted?

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

71% are concerned that VPN may jeopardize the ability to keep the environment secure.

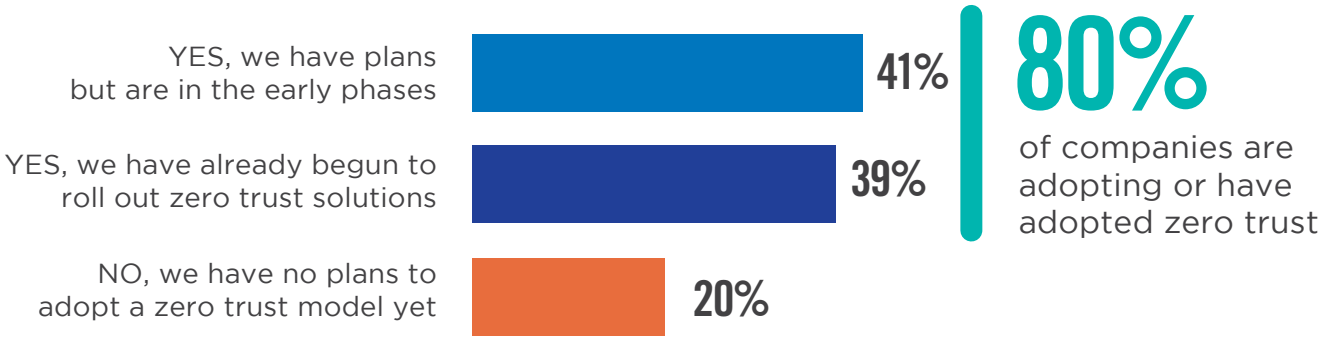


FUTURE OF REMOTE ACCESS

ACCELERATION OF ZERO TRUST ADOPTION

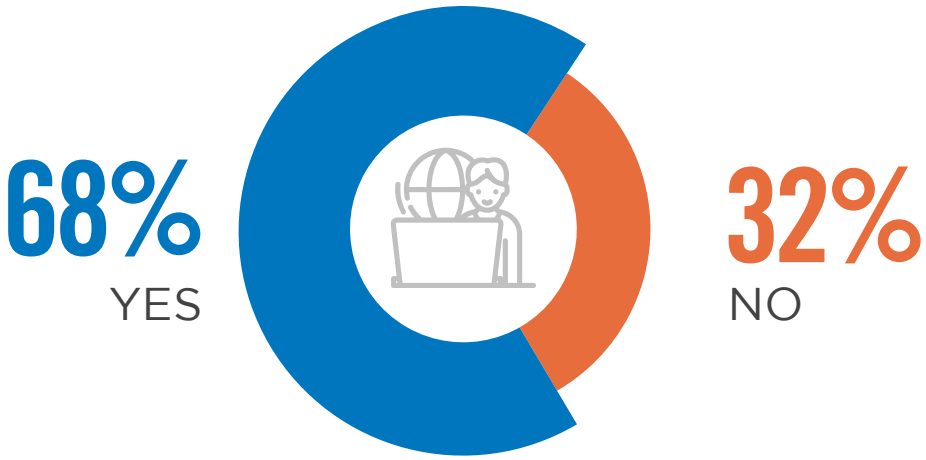
Zero Trust Network Access (ZTNA) and Zero Trust Architectures (ZTA) have rapidly gained traction in recent years. With the increase of mobile and remote workers, zero trust adoption has become a priority for many organizations, with 80% of companies actively planning or implementing a zero trust model.

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



The survey confirms that a majority (68%) of companies have been accelerating their zero trust projects since the recent shift to remote and hybrid work.

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



VPN ALTERNATIVES

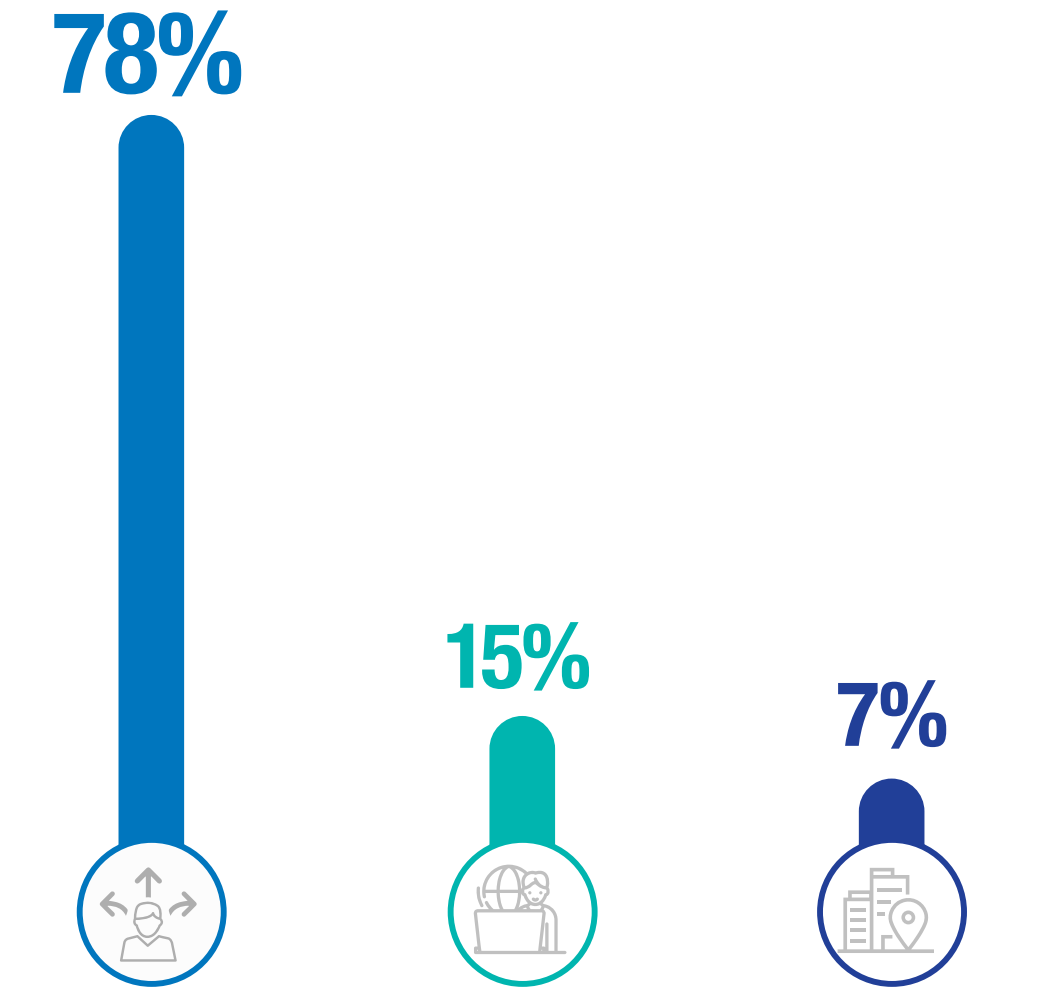
Not surprisingly, with nearly three out of four businesses concerned with VPN security, a majority of organizations (65%) are now considering remote access alternatives to the traditional VPN.

Have you considered remote access alternatives to traditional VPN?

REMOTE ACCESS MOVING FORWARD

The continued shift to zero trust and working from anywhere has been a catalyst to changing how organizations protect remote access. When asked about their outlook for remote access, 78% of organizations say their future workforce will be hybrid, providing greater flexibility for users to work remotely or in the office.

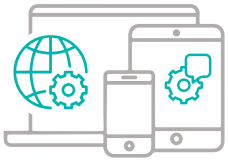
Fast forward to 2022, what does remote access look like at your company?



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 the 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 social engineering, 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?

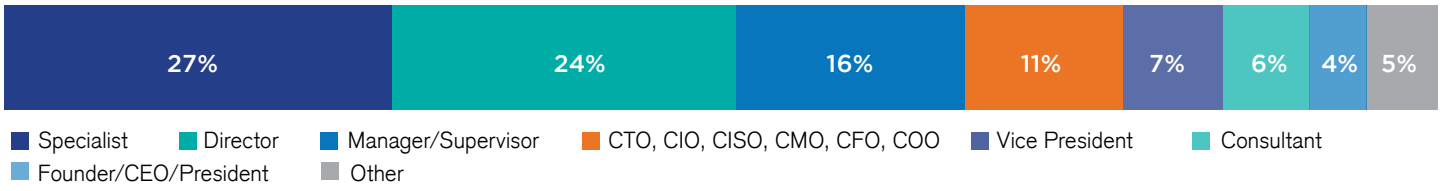
Get a free risk assessment and discover your network's attack surface before threat actors can.

UNCOVER YOUR ATTACK SURFACE

METHODOLOGY & DEMOGRAPHICS

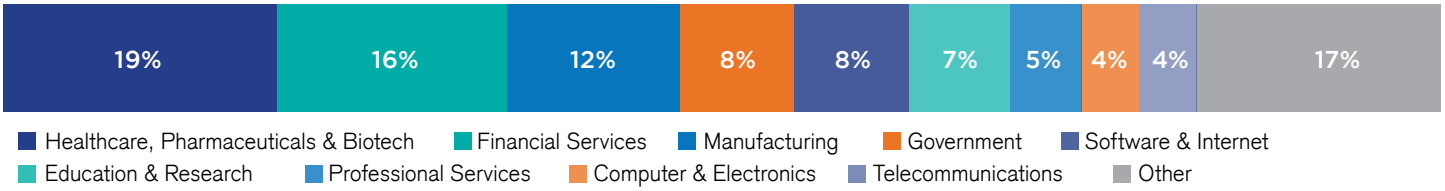
This report is based on the results of a comprehensive online survey of 351 IT and cybersecurity professionals, conducted in June 2022 to identify the latest enterprise adoption trends, challenges, gaps, and solution preferences related to VPN risk. The respondents range from technical executives to 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

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com