perimeter 81

The Decentralized Workplace & The Cyber Complexity Trap

The 2021 State of Cybersecurity Report

Table of Contents

Executive Summary

Perimeter 81's *Second Annual State of Cybersecurity Report* is based on our survey of more than 500 US IT professionals in firms with 50 or more employees. It covers how Covid-19 has changed the workforce, the top cybersecurity threats, and how IT professionals can overcome these new challenges.

Covid brought seismic shifts to the worldwide economy and the workforce. Work has become decentralized, cloud-based, and edge-less. Fancy offices or headquarters no longer define companies. Instead, they are now defined by their people—who work wherever, whenever, and however they please.

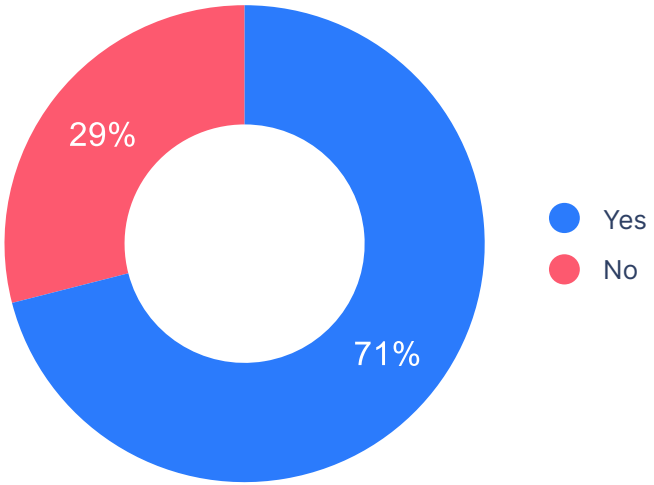
Just over six months ago, some of the leading Silicon Valley companies started planning their return to work, but employees would have none of it. They pushed back, and their companies listened. The bottom line is that hybrid and remote work is here to stay, and not just in Silicon Valley. A remarkable 87% of responding companies will have hybrid workers even after Covid—and more than half of them will work remotely 3-4 days a week.

In 2021, there have been tens of thousands of network breaches by cybercriminals, maybe even millions. We've read about many of the high-profile breaches, including the Colonial Pipeline, Volkswagen, Kaseya, T-Mobile, LinkedIn, and more. Nearly two-thirds (65%) of respondents had a serious cybersecurity incident in 2020-21, including 33% from ransomware.

Many vendors are trying to solve this ever-shifting problem with more solutions, more layers, more fences, more firewalls, and more brokers. This has led to the painful and complex reality in which the average CISO is forced to manage dozens of cybersecurity solutions, each with its own quirks, usability, and upkeep issues. Today's average enterprise has dozens of cybersecurity tools, and 71% of responding VPs/CIOs feel that the high number of cyber tools makes it more difficult to detect active attacks or defend against data breaches.

As IT professionals seek to mitigate an increasing number of cyber threats, a simpler, easier-to-use solution can be more effective in detecting and preventing the next cyber attack.

VP/CIOs: Do you find the number of different cybersecurity tools negatively impacts your organization's ability to detect and prevent threats?



5 Key Findings

87% of companies will be decentralized and have hybrid workers in 2021-2022, even after Covid.

30% of companies use more than 20 cybersecurity tools and solutions.

78% of hybrid employees will work from home two or more days a week.

71% of responding VPs/CIOs feel that the number of cyber tools negatively impacts their ability to detect and prevent threats.

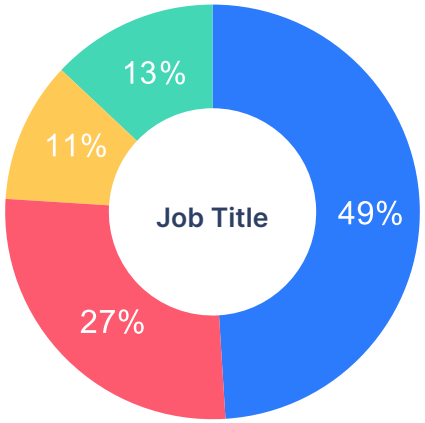
66% of companies had a serious cybersecurity incident in 2020-21.

What's New for 2021

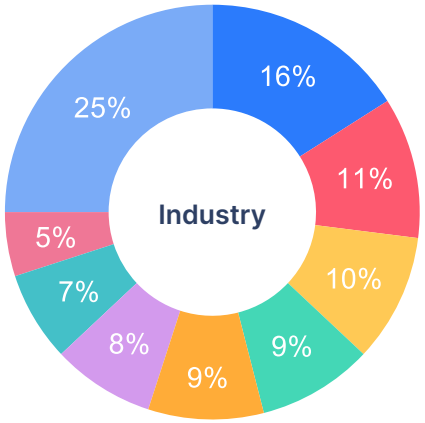
This report digs deeper into hybrid and remote work to understand whether it is really here to stay or just a passing fad. Is hybrid work just for big tech companies and the Fortune 1000, or is it really mainstream? We also examined whether the larger attack surface has resulted in more cyberattacks and where are the critical gaps or weaknesses in today's cyber solutions. Finally, we offer some new buyer's guidance and some predictions for 2022.

Survey Overview & Demographics

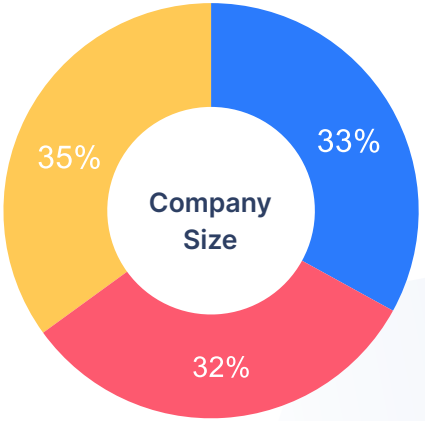
The results in this report are from an online survey of US IT professionals in firms with 50 or more employees conducted by Researchscape during Q3/2021. Six hundred twenty-nine respondents completed the survey, while 39 respondents gave partial results. Their responses were not weighted.



- IT Manager
- IT Director
- Cybersecurity Manager/ Director/Officer
- VP/CIO



- Software
- Manufacturing
- Finance, Insurance & Real Estate
- Professional Services
- Retail
- Internet
- Healthcare
- Telecommunications
- All Others



- 50 to 499
- 500 to 999
- More than 1000

Complete Findings

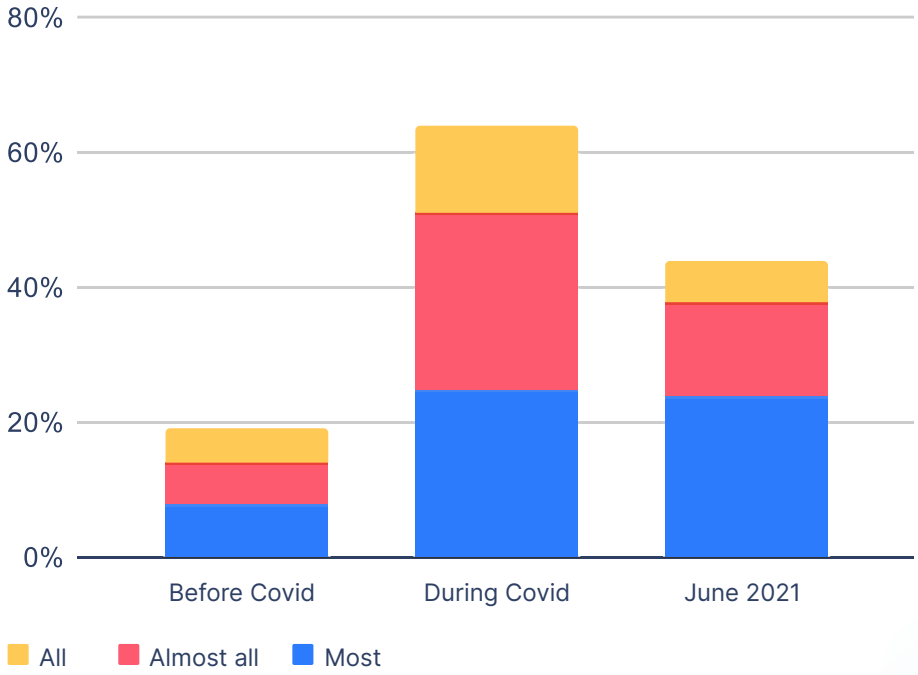
The Hybrid / Distributed Workforce is Here to Stay

In 2020, Covid put the world in a tailspin. More than 4.5 million people lost their lives in the largest pandemic since the Spanish Flu in 1918, and many more lost their jobs as businesses closed during government-mandated closures. Some companies, mainly in white-collar services and technology, made vast portions of their workforce remote, some within hours and others within days or a few weeks.

Before Covid, only 11% of companies with 50 or more employees had almost all or all of their employees working remotely. This changed dramatically during the pandemic, with only 2% of companies having no remote workers at all and another 2% having almost no remote workers. In addition to business continuity and paid employment, remote work offered other significant benefits for both employers and employees, including increased work/life balance (68%), increased employee satisfaction (65%), and increased productivity (59%).

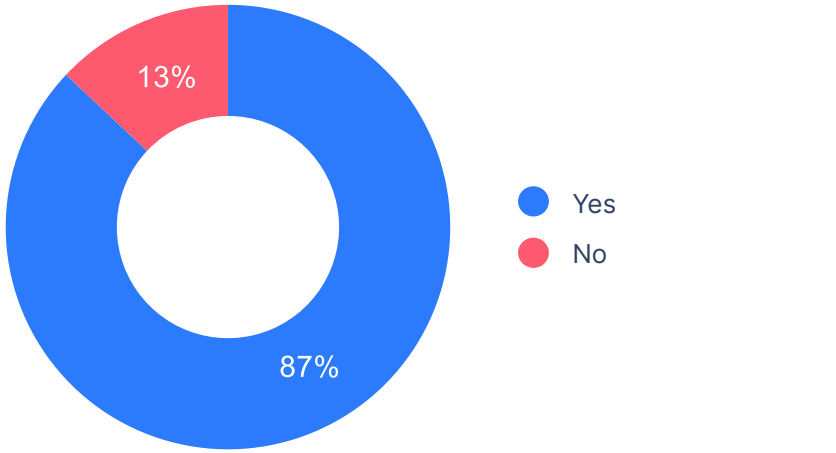
By June 2021, the percentage of companies with most, almost all, or all employees working remotely declined from 64% to 44%. Did this significant decline mean that companies were planning a return to “business as usual” after Covid in 2021-2022?

Remote Employees Before Covid, During Covid & June 2021

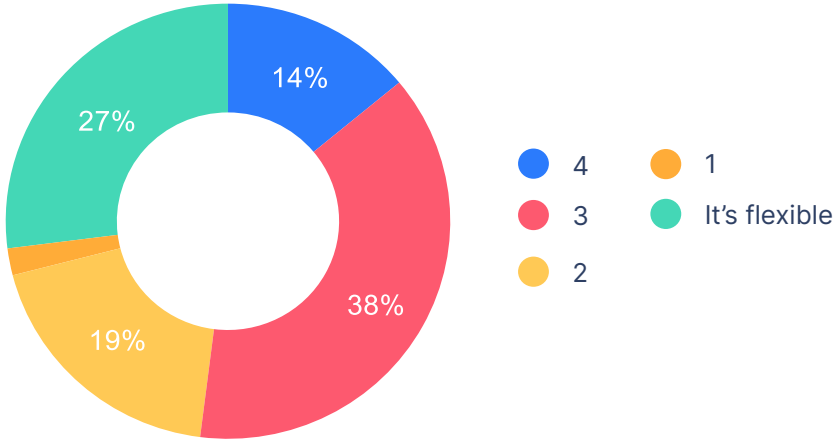


The good news for employers and employees is that hybrid work is unquestionably here to stay. This is equally true for small businesses, enterprises, and large enterprises. Eighty-seven percent of companies plan to have remote or hybrid work even after Covid in 2021-2022, with the overwhelming majority of remote employees working from home two or more days per week.

Does your company plan to have employees working remotely or hybrid post-Covid (2021-2022)?



How many days a week will employees work from home?



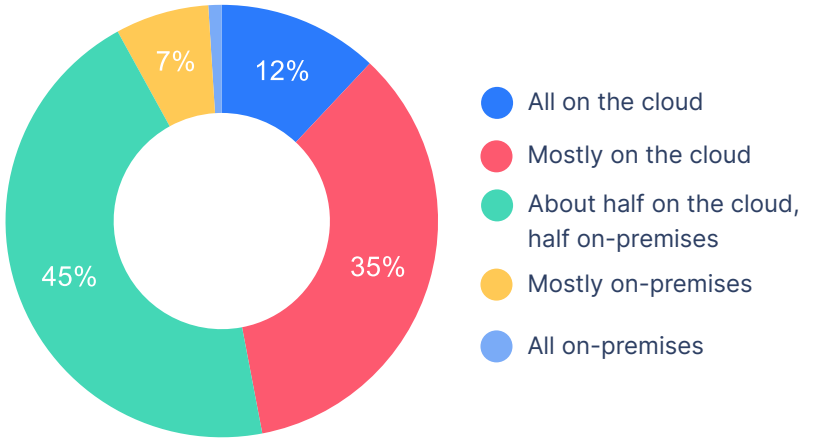
Networks Have Larger Attack Surfaces & Have Grown More Complex

When considering the distribution of employees and corporate networking resources, we can see that the attack surface in 2021 is significantly larger than the on-prem networks used by onsite employees a decade ago. In addition to the increase in remote and hybrid workers, the nature of “corporate networks” has dramatically changed. There are twelve times as many companies with all of their networking resources in the cloud than companies with all their resources on-prem.

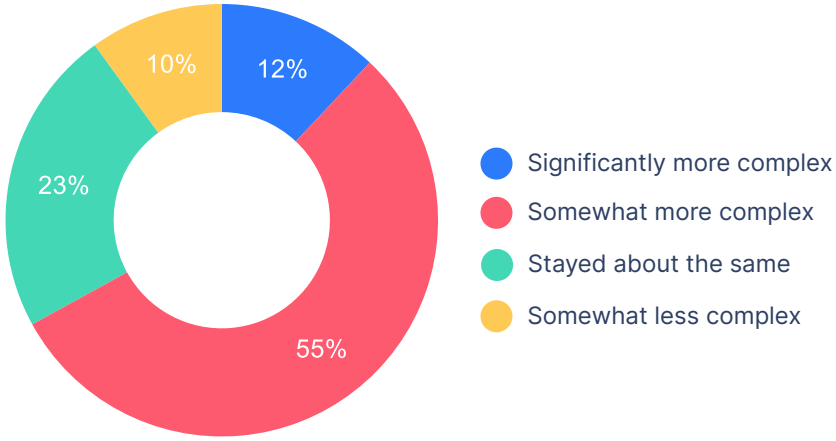
A mere 1% of respondents still have all of their networking resources on-prem, and 7% with resources mostly on-prem. A full 45% are about half on-cloud and half on-prem, while 35% have their resources mainly on the cloud, and 12% have all their resources there.

Cloud security is regarded as universally important, with 99% of respondents having some sort of cloud security in place. However, 58% feel that they face vulnerabilities or threats related to cloud misconfigurations, and 67% think that the distributed workforce has made cybersecurity more complex.

Where are your computing resources located?



How has the hybrid/distributed workforce affected the complexity of your cybersecurity?



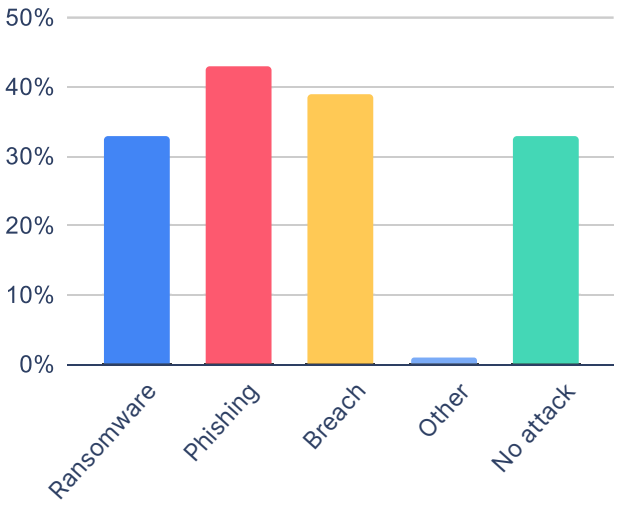
Ransomware is Pervasive, But Companies are Better Prepared Than Before

There were many high-profile breaches in 2020 and 2021, including Colonial Pipeline, Kaseya, T-Mobile, and Scripps Hospital. The ripple effects included panic-induced gasoline shortages, the postponing of non-essential medical procedures, and the shut-down of government agencies. In addition, personal data stolen from Guess, Volkswagen, and others could be sold on the Dark Web, used for identity theft, or spear phishing.

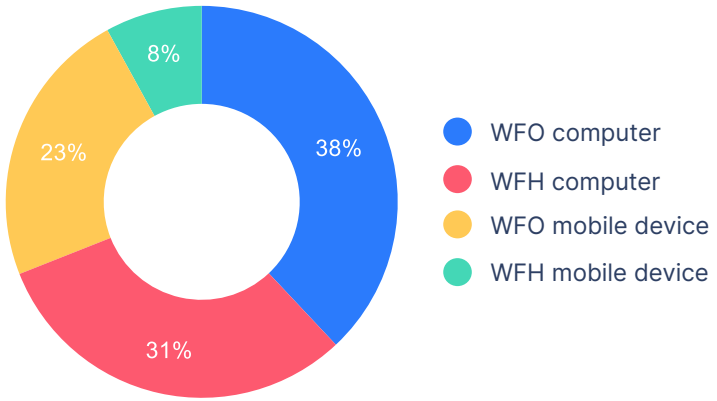
Although 51% of companies had already prioritized cybersecurity, the news of cyber incidents influenced an additional 34% of companies to make cybersecurity a part of their business plans and decisions. But news about ransomware wasn't the only factor driving their increased awareness. Sixty-four percent of respondents experienced a significant cybersecurity incident in 2020-2021, including ransomware (33%) and phishing (43%). A cybersecurity incident was slightly more likely to occur on a computer at the office (38%) than at home (31%), while a phone-based cyber incident was three times as likely to occur on a mobile device at the office (23% vs. 8%).

Companies are actively improving their cybersecurity posture and are increasingly better prepared to handle cyberattacks and ransomware. Nearly three out of four (74%) have created cybersecurity incident playbooks to assist them during a crisis, while 23% are working on one. Cybersecurity insurance is also a critical component for mitigating the business costs of a cyberattack, with 67% of companies having already purchased it while another 30% are considering it.

Has your company experienced any of the following serious cyber incidents in 2020-2021?



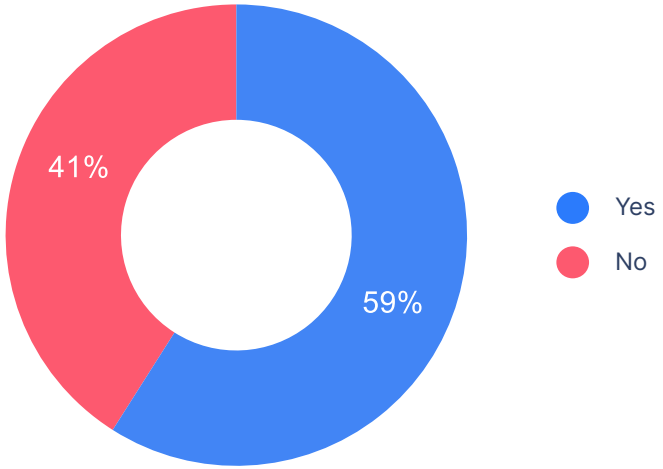
What was the attack surface of your most serious cybersecurity incident?



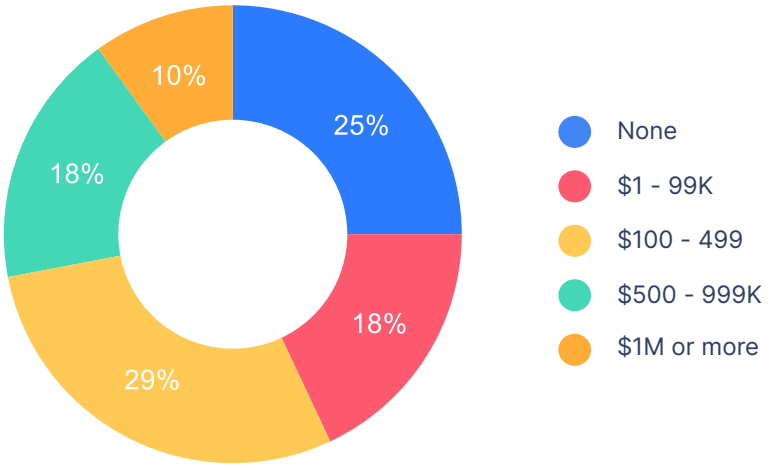
Eighty-seven percent of respondents said that they notified federal law enforcement during a ransomware attack. And although federal authorities strongly discourage paying the ransom to recover business data, 59% admitted that they did pay a ransom to cyber thieves. This is no surprise since it is faster, easier, and much less costly to pay the ransom than recover business data from backups. But as ransom prices rise, it is not clear how much longer companies or their insurers will continue to pay.

Regarding the costs of a cyberattack, 25% of respondents reported no costs at all, while 18% reported costs less than $100,000. For 47% of cyberattack victims, the costs were between $100,000 and $1 million, and just 10% reported costs above $1 million.

Did you pay a ransom to cyberthieves?



What were the total costs/damages from cyberattacks on your business in 2020-2021?

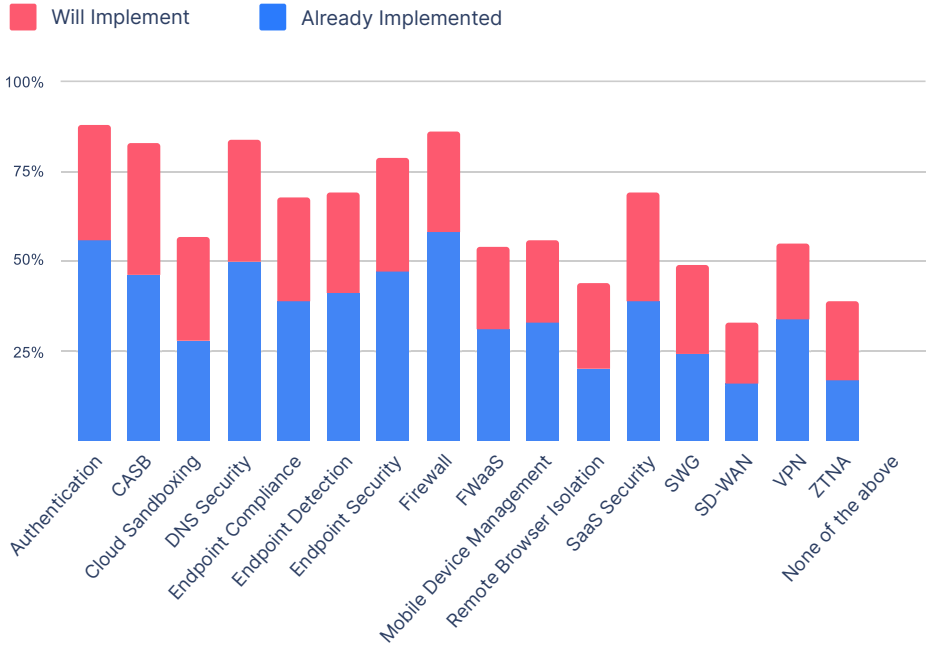


Cyber Complexity Negatively Impacts a Company's Ability to Respond to Threats

IT professionals face numerous risks, with respondents reporting a wide range of top threats, including data theft (19%), ransomware (14%), phishing (14%), supply chain attacks (13%), vishing (10%), and more.

To protect their networks, they are implementing a wide variety of solutions, including authentication, Cloud Access Security Broker (CASB), Cloud Sandboxing, DNS Security, Endpoint Security, Firewalls, Firewall as a Service, Mobile Device Management, Secure Web Gateways (SWG), SD-WAN, VPN, ZTNA and more.

Which cybersecurity solutions have you already implemented & which ones will you implement in 2021-2022?

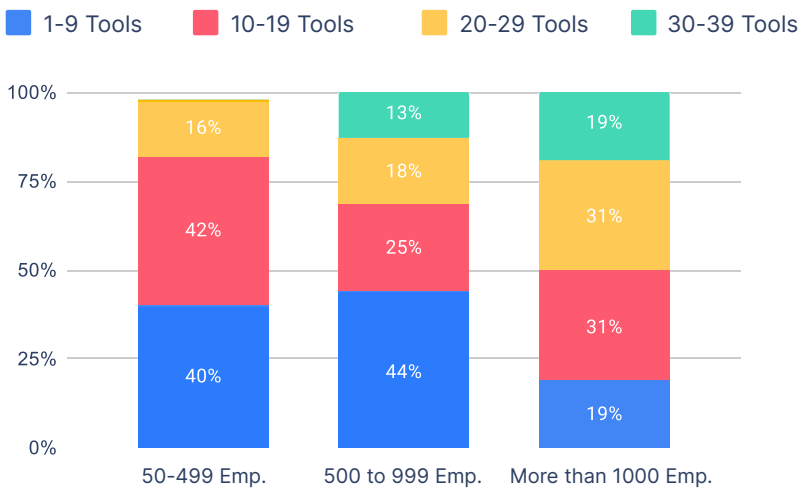


As the number of tools has multiplied, so has the cyber complexity. Thirty percent of all responding companies use more than 20 cyber and network security tools. As the size of the company grows, so does the number of tools. Exactly half of all companies with more than 1,000 employees use at least 20 cyber and network tools and 19% use more than 30 tools.

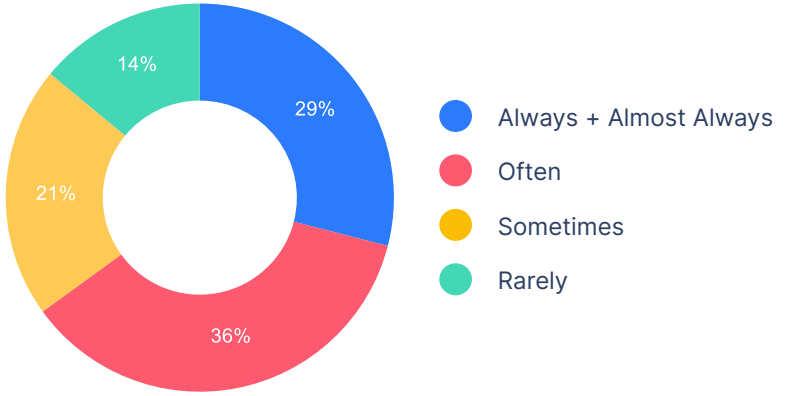
But the use of so many tools comes at a price. Forty-five percent of respondents feel that the number of cybersecurity tools negatively impacts their ability to detect and prevent threats. Among VPs and CIOs, 71% feel that the number of cyber tools negatively impacts their ability to detect and prevent threats.

Even more concerning, is the frequency at which cyber complexity negatively impacts the ability to detect and prevent threats. Some 29% of VPs and CIOs feel that cyber complexity from too many tools always or almost always occurs, while 36% feel that this occurs often. Only 14% of VPs/CIOs feel that this is rarely a problem.

By company size: How many cyber and network security tools organizations does your organization use?



VPs and CIOs: How often does cyber complexity negatively impact your ability to detect and prevent threats?



2022 Market Predictions

1. Staying agile is more important than ever.

Hopefully, Covid is really behind us, but our modern global world allows pathogens of all types to rapidly spread. The lesson learned is that businesses must be hybrid going forward. Not for employee work-life balance, and not for increased employee productivity, but because it's critical for business continuance. Agile businesses, especially those with a Cybersecurity Experience Platform like Perimeter 81 were able to continue working as the Covid Delta variant made its way across the world. One Perimeter 81 customer used the second wave to become fully officeless and saved millions of dollars in rent. Stay agile in 2022, and your employees, customers, and investors will thank you.

2. Green initiatives will explicitly or implicitly favor hybrid work.

When millions of people were sheltering in place or working from home during Covid, the improvement in air quality was beyond dispute (although there was some fake news about dolphins in the canals of Venice). There is a clear link between exposure to particulate matter in the air and various cancers as well as coronavirus death rates. Congestion pricing is soon coming to New York, Tel Aviv, and other cities. It will make commuting in private vehicles more expensive and give millions of workers another reason to work from home.

3. Ransomware and cyberattacks will continue unabated.

The multi-billion-dollar profits associated with cybercrime will ensure that it continues. We have already seen that coordinated action by governments and the private sector can bring results: multiple governments working together were able to disrupt the operation of the REvil ransomware gang that was responsible for the Colonial Pipeline cyberattack. Real success will only come from a sustained combination of cyber, legal and police actions that will result in the arrest and imprisonment of hackers and the seizure of their assets.

4. New cybersecurity regulations will benefit all of us.

While it's still early to pass judgment, the Biden Administration's Executive Order on Cybersecurity is a welcome first step to making the Internet a safer place. With this Executive Order, the federal government has recognized the reality that we are all part of one giant network. The Executive Order is the first step in creating a coordinated effort to make the Internet a safer place for all of us and confront cybercrime. In 2022, look for the Cybersecurity Safety Review Board to open for business. Their near-real-time analysis of attacks will improve response times, reduce the impact of cyberattacks, and help promote best practices, including Zero-Trust networking. Legislation prohibiting insurance companies or even businesses from paying ransoms could harm the profits of cybercriminals and take a real bite out of cybercrime.

5. Your IT friends will like you if you share this survey report with them.

If you've read this far, we hope that you've been inspired by the data revealed in this survey report and you'll share it with other IT professionals. Although change is inevitable, complexity is a choice. Go to www.perimeter81.com today, create your account, and start radically simplifying your cybersecurity.

Buyer's Guidance

Avoid Cyber Complexity with Perimeter 81

The best way to avoid cyber complexity is by using a Cybersecurity Experience Platform (CSX). A good CSX platform offers a single pane of glass for management, networking, and cybersecurity.

Perimeter 81 is the world's first Cybersecurity Experience (CSX) Platform and allows organizations of all industries and sizes to support the immediate desires of the nomads with a purpose—while granting IT teams the robust tools they need to safely manage it all. As a holistic, cloud-based solution, Perimeter 81 is designed around the four superpowers of Radically Simple Cybersecurity: Instant Deployment, Unified Management, Full Visibility, and Integrated Security.

Instant Deployment

In just a few clicks, purchase, provision, and enable secure zero-trust access on-prem, in the cloud, or anywhere in between. And if you have any questions, our hands-on, 24/7 support team is always available to help.

Integrated Security

Avoid the complexity of using dozens of cybersecurity solutions, with one intelligent and well-designed platform that makes it easy to configure your infrastructure, detect active attacks, and defend against data breaches.

Unified Management

Effortlessly onboard network users, instantly deploy secure cloud gateways, create multi-regional networks, and install cross-platform applications across all endpoints.

Full Visibility

Effectively monitor network health, view employee resource access, integrate with leading SIEM providers, and identify any suspicious activity—alll from a single pane of glass.

Perimeter 81 Core Features

Cloud Management Console

Easily define and manage your organization's network from a single location. All of your networks and their locations are displayed, giving you full visibility of all infrastructure including any connecting gateways for local users.

Zero Trust Network Access

Ensure policy enforcement and protection for all users, devices, applications, and data, regardless of where they're connecting. Integrate additional security on top of your corporate resources with a vast selection of complementary tools, including built-in 2FA and Single Sign-On.

Zero Trust Agentless Access

Quickly establish secure access to HTTP/S, SSH, RDP, and VNC applications without an agent. With just a click, employees can connect to any of the remote resources they need through their web browser. Establish highly effective trust boundaries by segmenting sensitive resource access with granular policies that include day, time, user group, and more.

Device Posture Check

Enhance network security by establishing trust in only those devices that comply with your organization's security policies. Provide continued monitoring and support for company-wide compliance with comprehensive reporting capabilities.

Firewall as a Service

Built for all layers, ports, and protocols, our cloud firewall ensures safe data transfer for IPs, users, and HTTP applications with a multilayer cloud approach. Define traffic policies with simple rules that offer unprecedented detail, enforce specific security posture and isolate sensitive dataflows.

About Perimeter 81

Perimeter 81 radically simplifies cybersecurity with the world's first Cybersecurity Experience (CSX) Platform designed around the four superpowers of Instant Deployment, Unified Management, Full Visibility, and Integrated Security. As a holistic, cloud-based solution, Perimeter 81 allows organizations of all industries and sizes to support the immediate desires of the nomads with a purpose—while still granting IT teams the ability to safely manage it all. The simplicity of Perimeter 81, from purchase to deployment and through day-to-day management, is a welcome alternative for the IT professionals and CISOs who struggle with the Cyber Complexity Trap™ caused by the 20 or more cybersecurity tools they use a daily basis to protect their networks.

The company was founded in 2018 by two IDF elite intelligence unit alumni, CEO Amit Bareket and CPO Sagi Gidali, and is based in Tel Aviv, the heart of the startup nation. Our clients include SMBs, Fortune 500 businesses, and industry leaders across a wide range of sectors. Our partners are among the world's leading integrators, managed service providers, and channel resellers. The company has raised more than $100 million to date in order to give both IT professionals and employees the freedom to fully and securely embrace the agility of the modern era—even during periods of rapid change and uncertainty.

Contact Us

Perimeter 81, LTD.
+1-929-575-9307
www.perimeter81.com

Request a Demo