perimeter 81

2020 State of Network Security Report

How IT Managers Are Solving the Security Challenges of Remote Work

perimeter 81

Executive Summary

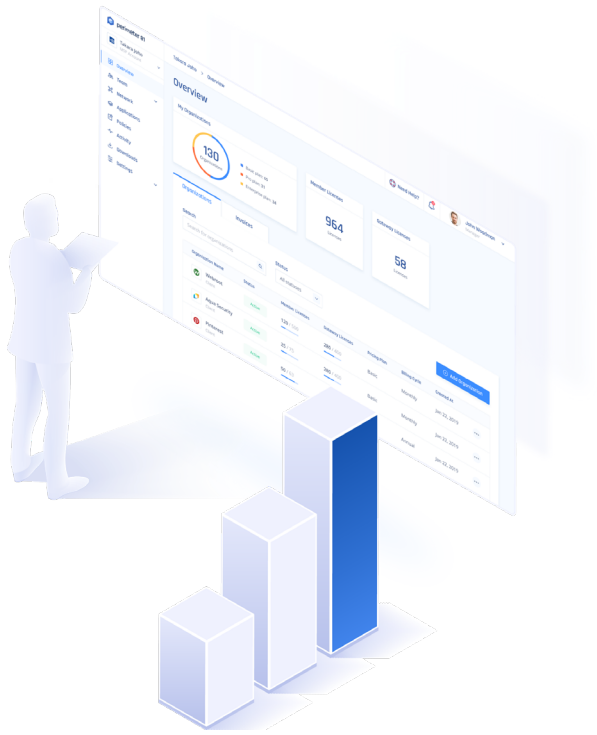
The purpose of this report is to provide tangible, actionable insights based on the survey responses of over 200 IT professionals, who were questioned about the security implications of remote work, COVID-19 and how their companies are making due.

In the first part of our report, we find that a 72% majority of organizations are moving towards cloud-based security solutions, and away from their dependence on legacy tools, primarily VPNs (66%), and their neglect of extra security layers such as 2FA and deeper monitoring. During the COVID-19 pandemic and transition to remote work - which respondents indicate will continue to be a trend - concerns about the security of their traditional approach was the biggest (73%) reason that security is moving to the cloud.

Besides security, a major concern for IT professionals is high latency. This productivity killer is sometimes experienced when using outdated remote security solutions, and more worryingly, is often or always experienced by nearly one fifth of respondents in the second part of our report. Cloud-based security may address latency, but managers identify other factors in their search for a fitting remote work solution as well.

Top challenges for security are covered in part three. Scaling ranks highly in their future cloud security solution, say 39% of IT managers, as remote work quickly reveals how inefficient it is to apply security policy to these disparate workforces. Scalable solutions will more capably solve IT's biggest security concerns during remote work: new devices (61%) and a lack of visibility across the entire network (56%).

As IT managers increasingly witness the onset of remote work and grapple with security, they are unquestionably moving toward cloud-based solutions. These pave over the security holes and inefficiencies that come with legacy technology applied to a modern environment: edge computing for high latency problems, and micro-segmentation for scalable remote access policy management. Budget is the only concern left, but this worry is quickly dissipating as unified network security solutions make their way into the SaaS market.



perimeter 81

The COVID-19 pandemic has forced the acceleration of the inevitable: remote work.

Driven by global health concerns, businesses were required to enforce company-wide work-from-home policies overnight. While the world has been moving in the direction of remote work and it was expected to become the norm within 5-10 years, few could have anticipated the shift would occur so quickly.

For many organizations, this new reality found entire teams working remotely for the first time ever. It was common for employers to focus the first two months of quarantine on ensuring that employees were healthy, devices were connected and projects continued to move forward, all while adjusting to the home becoming the new office. Now, with no real end in sight, businesses are facing the possibility that they will be managing their remote teams permanently, at least for some portion of the traditional workweek.

More than a likelihood, remote work is now considered a pillar of effective business operation due to results including greater agility, employee satisfaction and productivity, and reduced costs. This incoming shift has created an unprecedented set of challenges for IT managers, however, who may not have experience leading their businesses' networking and security remotely. Best practices that worked in the office do not directly translate when employees work from home.

With more employee devices and endpoints, IT teams are experiencing the challenge of lower visibility and potential exposure, as their inadequate legacy systems can't cover an increasingly dispersed and cloud-reliant workforce. With each passing month, IT and security teams are implementing more cloud-based SaaS vendor solutions on top of their network. While this may help businesses gain agility and boost the bottom line, it comes with security and networking challenges that must be addressed sooner rather than later.

To get a better understanding of the different secure network access challenges, we surveyed over 200 IT managers from companies of all sizes and industries.

We sought to determine the key IT and security insights they encountered since experiencing the shift to remote, and the result provides an interesting picture of the IT landscape and how its leaders think during these transformative times.

perimeter 81

72% of Organizations Very or Completely Likely to Adopt Cloud-Based Security Solutions

As technology advances by the day so do business networks. Thanks to the cloud, networks are now faster and more accessible than ever. However, as more devices connect and transfer large amounts of data between off-premises resources, it puts a massive obstacle in front of IT and security teams.

How do you securely connect to the internal networks when working away from your main office?

66%
VPN (Virtual Private Network)

58%
Cloud service through the web browser

48%
Remote access solution

34%
Firewall

9%
Dialup

IT managers overwhelmingly prefer the traditional VPN for securing employees' connections to company resources.

These obstacles exist because until now, IT secured remote workforces with legacy technology, which creates bottlenecks and limits network visibility in situations where workers exclusively connect from home. Legacy solutions like VPNs - currently in use by 66% of IT managers - and firewalls make security difficult, because they are unable to scale to many different connections, each with various characteristics and risks.

perimeter 81

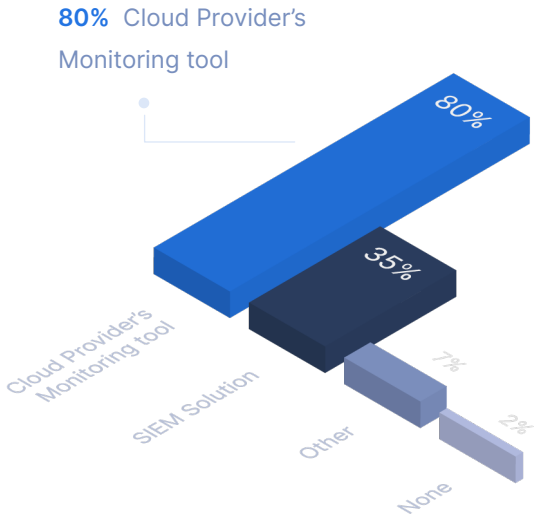
When working remotely how do you authenticate to get access to your systems?

2FA is accessible and common enough to be in use by 53% of respondents, though a good portion of IT teams don't authenticate users beyond the password level.

Besides a reliance on legacy tools, there is still a worrisome fraction of IT managers who do not augment their security with additional password or monitoring tools. Network authentication among 53% of IT managers is supported with the use of 2FA, but it is significant that the second most common response (33%) was that users authenticate with nothing but a password.

What kind of monitoring tool, if any, are you using to see who is accessing your network remotely?

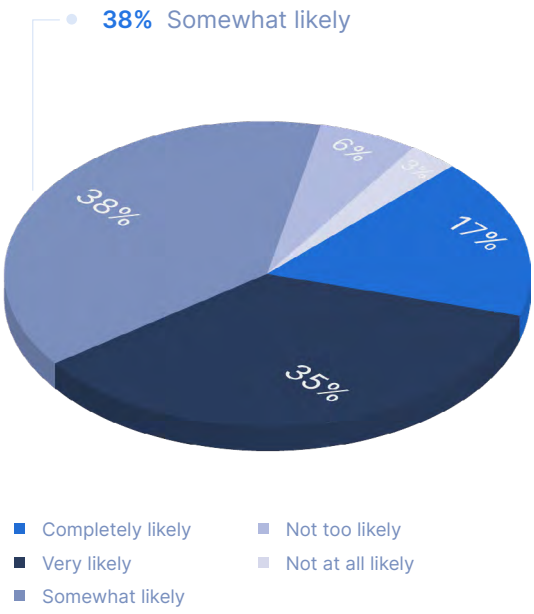
The vast majority (80%) of IT managers use the monitoring utility offered by their cloud provider, while some (35%) rely on more holistic Security Information and Event Management tools.



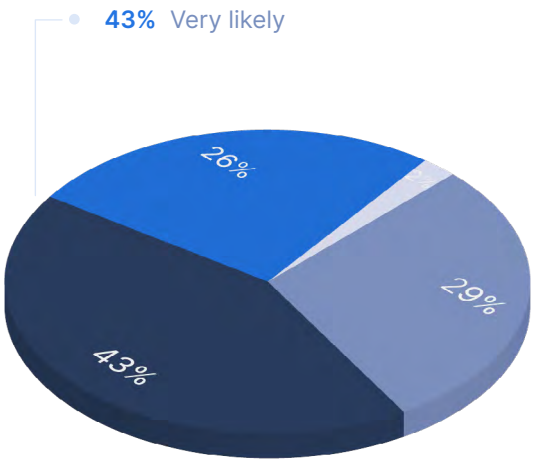
To ensure that their growing number of remote employees are connecting securely to their hybrid-cloud network, no matter where they work from, IT and security teams are overwhelmingly looking to adopt secure information access solutions to replace or complement their legacy tools. This has meant an embrace of cloud-friendly security for a multitude of reasons.

perimeter 81

Before COVID-19, how likely was your firm to adopt cloud-based security solutions?



Following COVID-19, how likely is your firm to adopt cloud-based security solutions?



The number of IT managers who are completely likely to adopt cloud security is up 70.58% from before to after COVID-19, while those who were very likely to adopt was up nearly 23%. The combined 72% who are at least very likely to adopt cloud security solutions now are up 38% from before the pandemic.

According to IT managers, their organizations are now more likely to invest in modern, secure information access solutions to support the remote workforce. With it they can complement their existing cloud infrastructure and replace old solutions that limit agility, security, and cost effectiveness.

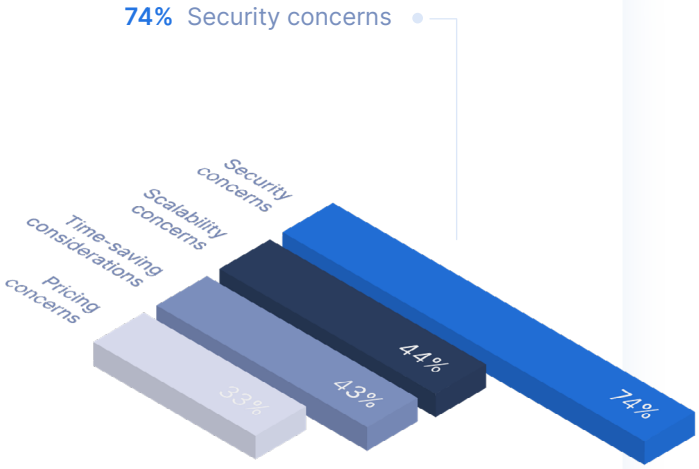
To further understand what is pushing organizations to the cloud, we asked the respondents about the reasons that prompted them to adopt cloud-based security solutions over hardware solutions. Lack of security figured prominently among their top concerns, followed by scalability and productivity.

Security and scalability and productivity are key benefits of cloud-based software services with ever-changing technology. Hardware and outmoded solutions meant to protect the traditional network on-premises network perimeter have forced IT teams supporting the cloud to try and fit a square peg into a round hole. They must work extra hard to achieve visibility across the network, manage permissions, configure settings, and more - and tolerate greater risks anyway.

perimeter 81

What are the drivers prompting you to adopt cloud-based security solutions (versus hardware)?

It's no surprise that over 73% of responding IT professionals choose to adopt cloud-based security because of security concerns, but they are also aware that the cloud saves their staff time and money when expanding security efforts as the organization grows.

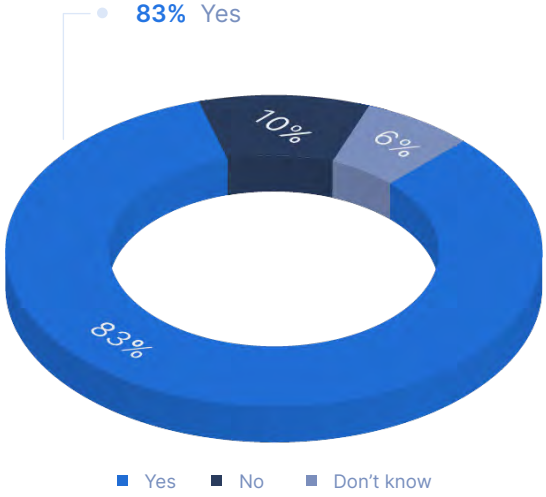


Providing fast remote access has quickly become a major concern for organizations in today's modern business environment, and the cloud helps with that. The introduction of remote or flexible work policies during COVID-19 has therefore run parallel with cloud adoption, but the amount of companies planning to move to remote full time may mean that cloud adoption hasn't yet hit its peak.

When asking respondents if their organizations will adopt remote work post-COVID-19, 83% of responders said their organization has already moved fully remote, or is already planning to.

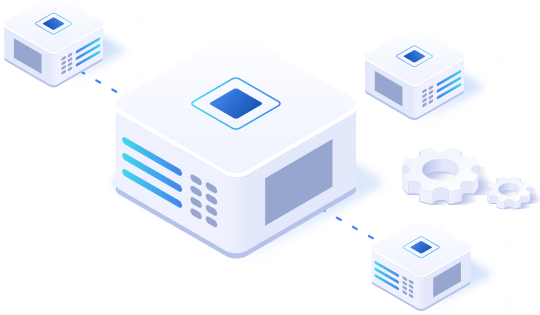
Do you anticipate your organization will adopt remote working post-COVID?

One thing we know to be true is that remote work is a key ingredient to building a high-performing and diverse company for the future. That's why remote work isn't just the past or the present, and the numbers reflect this.



perimeter 81

Network Performance Obstacles Disrupt Productivity and Revenue



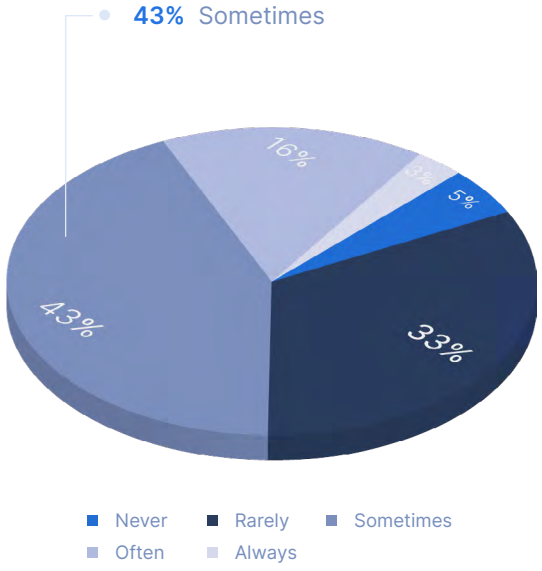
With remote work further ramping up investment in the cloud, companies are now concerned with making their hybrid-cloud networks as efficient as possible. The cloud is already beneficial in terms of reducing infrastructure costs and boosting accessibility for remote workers, but to maximize ROI, organizations want to help employees using the cloud perform as best as they can. For many, this has meant achieving the same low latency conditions that workers used to experience when they accessed resources that were hosted nearby.

In an on-premises work environment, legacy security solutions are hardly a barrier to productivity, both because the elements that characterize each connection are more predictable (IP address, location, device etc.) and because users are physically closer to the technology that protects their traffic. When workers go remote in large numbers, the same legacy technologies may offer some defense for the wider variety of connections, but accounting for their differences in origin has a noticeable effect on the speed of these connections.

In a network that's accessible to remote workers, a wide array of different connections occur simultaneously across multiple resources. Unsurprisingly, for the majority (43%) of respondents, latency is sometimes experienced across these networks. More surprisingly, nearly one-fifth (19%) of respondents reported that this occurs often or always. Lag time when users connect and input data or commands into applications hampers productivity directly, and so reducing it is a central goal for networking professionals.

How often are your organization's staff experiencing network performance and latency issues when using a remote access solution?

It's not uncommon for companies embracing remote work to experience latency on their suddenly more complex networks. While 43% experience this, it's also significant that 16% of respondents suffer it often. This can have a drastic effect on productivity - and it does.



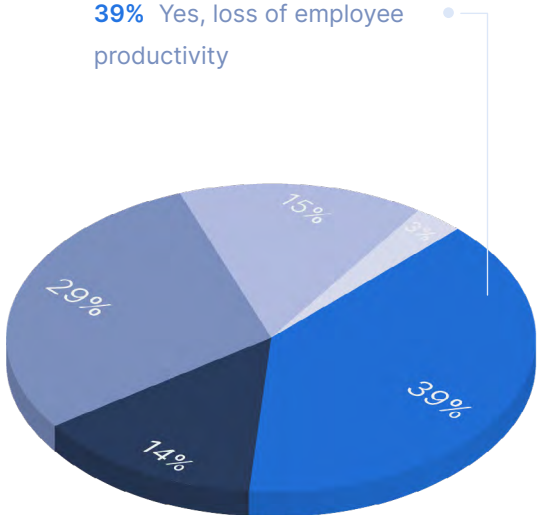
In terms of raw impact, higher latency means that workers experience a longer delay between the click on their mouse or keyboard, and the intended result inside whichever application or resource they're currently using. Everyone in the organization works more slowly in these conditions, which compound as remote work gets more popular and resources spread beyond the traditional network perimeter.

Unsurprisingly, of the organizations polled about how this affects their staff, 39% - the largest fraction of those participating - report that it has negatively affected worker productivity. Factoring in those who lost both productivity and revenues, and we see that 68% total lost productivity, 43% report losing revenue, and 29% report losing both due to performance/latency issues. It's therefore vital for organizations that want to keep their remote workers productive to determine how they can cut latency, and take steps to do so without disrupting operations across the board.

Do you believe these latency issues have resulted in any loss of employee productivity or business revenues?

Companies reporting on the IT impact of their remote work initiatives said that latency results in a direct loss of employee productivity, which is indirectly tied to the bottom line.

- Yes, loss of employee productivity
- Yes, loss of business revenues
- Yes, loss of both employee productivity and business revenues
- No
- Don't know



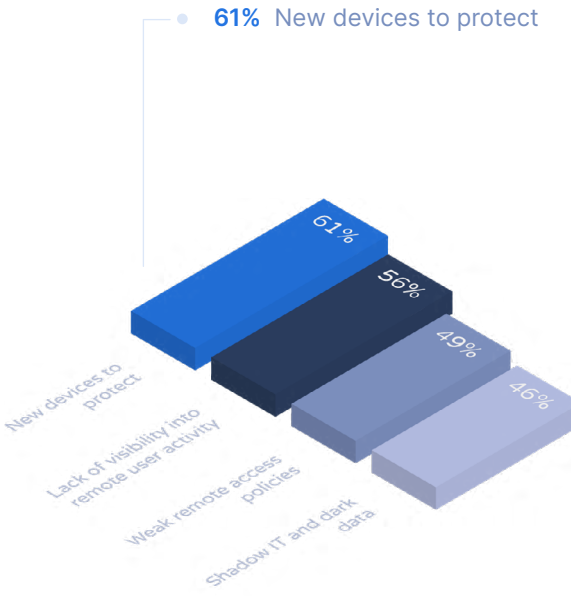
perimeter 81

Scalability, Budget Top Challenges for IT Leaders as Remote Work Becomes Permanent

A corporate network that is optimized for remote workers is crucial for satisfying operational goals and ensuring business continuity in the "new normal", but these aren't the only concerns for a growing company. The survey results reflect this idea well. Because new resources (such as SaaS applications) and users are added to the network as the organization matures, the scalability and visibility of user access enters the picture.

What are the greatest security concerns for your organization in light of the new remote work environment?

The sheer number of new devices that must be protected when remote work is the status quo has IT teams concerned. In this environment, visibility and access policy management across these devices is obscured by legacy solutions' inability to easily scale.

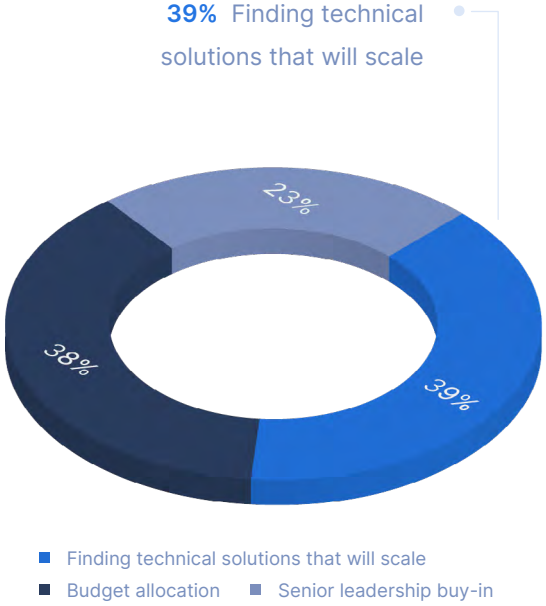


With time, it's possible for IT to make any remote access solution work well for a static number of apps or users. If they don't do it in a scalable manner, however, the team must invest similar effort every time the network changes slightly. Accordingly, when asked about obstacles in the way of a secure remote workforce, most companies agreed that difficulty finding a scalable technical solution will likely loom largest.

perimeter 81

What do you anticipate to be your greatest challenge in securing the remote workforce in the foreseeable future?

New solutions and strategies required for a secure remote work experience means scalability is the primary concern for companies implementing them. Companies do not want to reinvent the wheel every time a new user joins, or a new tool is added to the technology stack.



Another interesting takeaway is that scalability and budget availability are neck-and-neck regarding secure remote work challenges, at 39% and 38%, respectively. In many ways this makes sense: What's the point in finding a scalable remote access solution if there's no room in the budget for it, or alternatively, what's the use in a non-scalable yet affordable solution?

Ultimately, workforces everywhere are already embracing the remote work status quo, and organizations have added tools that help them do their jobs from anywhere. The issue has then become how to increase the efficiency of the remote work security apparatus now that it's in place.

perimeter 81

Embracing Remote Work: An All-Encompassing Endeavor

Remote work is here to stay, during and after COVID-19. The change it's had on the business world, or more specifically the information technology supporting the business world, has IT managers thinking differently than they once did. Data gathered on various topics posed to these managers, surrounding remote work and networking trends, gives us a glimpse into how decision makers in the industry see things moving forward.

Cloud Security Adoption is in Full Swing

While the proportion of companies using cloud-based security solutions is significant, there is a sizable representation of those that still use traditional firewalls and VPNs to secure networks in this new era. However, the numbers demonstrate that concerns about the security and scalability of these legacy tools are ushering in the wider adoption of cloud-based solutions, as organizations see the efficacy of remote work and overwhelmingly plan for its adoption to continue on the current trajectory.

Scaling and Latency Targets Becoming Easier to Hit

With momentum towards better security via cloud-based tools, IT managers are focused on making sure that scaling or efficiency obstacles don't resurface. Cloud-based network security solutions adequately protect network traffic and corporate data, but in many cases also encounter problems with orchestration, as IT must work harder to ensure multiple tools are applied to many different resources. Respondents also say remote access solutions increase latency, which negatively impacts the bottom line.

Edge networking is one idea that can help IT managers who have concerns about latency. Cloud-centric companies might consider edge networking tools as these products put resources closer to faraway employees (in geographically proximate data centers) and therefore reduce the latency they encounter when connecting remotely. To complement their more agile networks and boost scalability, organizations adopting these technologies can also explore software solutions that enable micro-segmentation.

With micro-segmentation possible via software-based networking products, IT can easily split the network into parts that are more or less sensitive in a few clicks. Many administrators use this technology to create user groups with custom access profiles, in order to define which resources specific employees, devices, roles, groups, departments, and even branch locations can access.

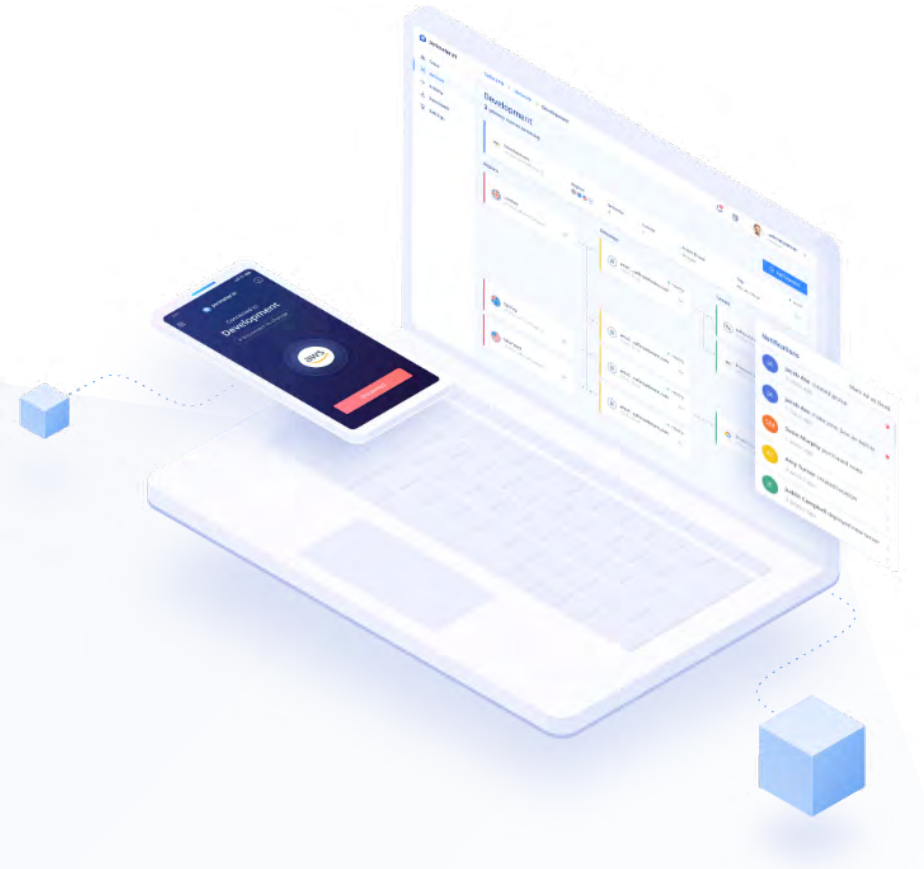
Budget is the Obstacle Left Standing

Those surveyed also noted that budgeting for the security of their remote workforces is a central challenge. However, advancements in cloud-based security would make any organization adept at keeping its remote workers as safe and productive as they are at their desks, and fully prepared for a future where the office is no longer the nucleus of the company. The barriers to achieving proper remote work security are coming down quickly, and organizations that work to build a solid security foundation now are also building momentum for future success.

perimeter 81

About Perimeter 81

Perimeter 81 has taken the outdated, complex and hardware-based traditional network security technologies, and transformed them into a user-friendly and easy-to-use software solution — simplifying network security for the modern and distributed workforce. Since its founding, Perimeter 81 has quickly gained traction in the Secure Access Service Edge (SASE) and Network as a Service market, and is revolutionizing the way companies consume cyber and network security. Our clients include Fortune 500 businesses and industry leaders across a wide range of sectors, and our partners are among the world's foremost integrators, managed service providers and channel resellers.



Contact Us

www.perimeter81.com

+1-646-518-1997

Request a Free Demo