paloalto® NETWORKS | PRISMA™ ACCESS BY PALO ALTO NETWORKS

The State of Hybrid Workforce Security 2021

Table of Contents

Presented by:

paloalto NETWORKS | PRISMA ACCESS BY PALO ALTO NETWORKS

Prisma Access by Palo Alto Networks offers the industry's most complete cloud-delivered security platform that consolidates more point products into a single converged service than any competing solution. As part of our secure access service edge (SASE) solution, Prisma Access transforms network security and allows organizations to enable secure hybrid workforces. Unlike competing platforms, only Prisma Access protects all application traffic with complete, best-in-class security while ensuring an exceptional user experience with industry-leading SLAs.

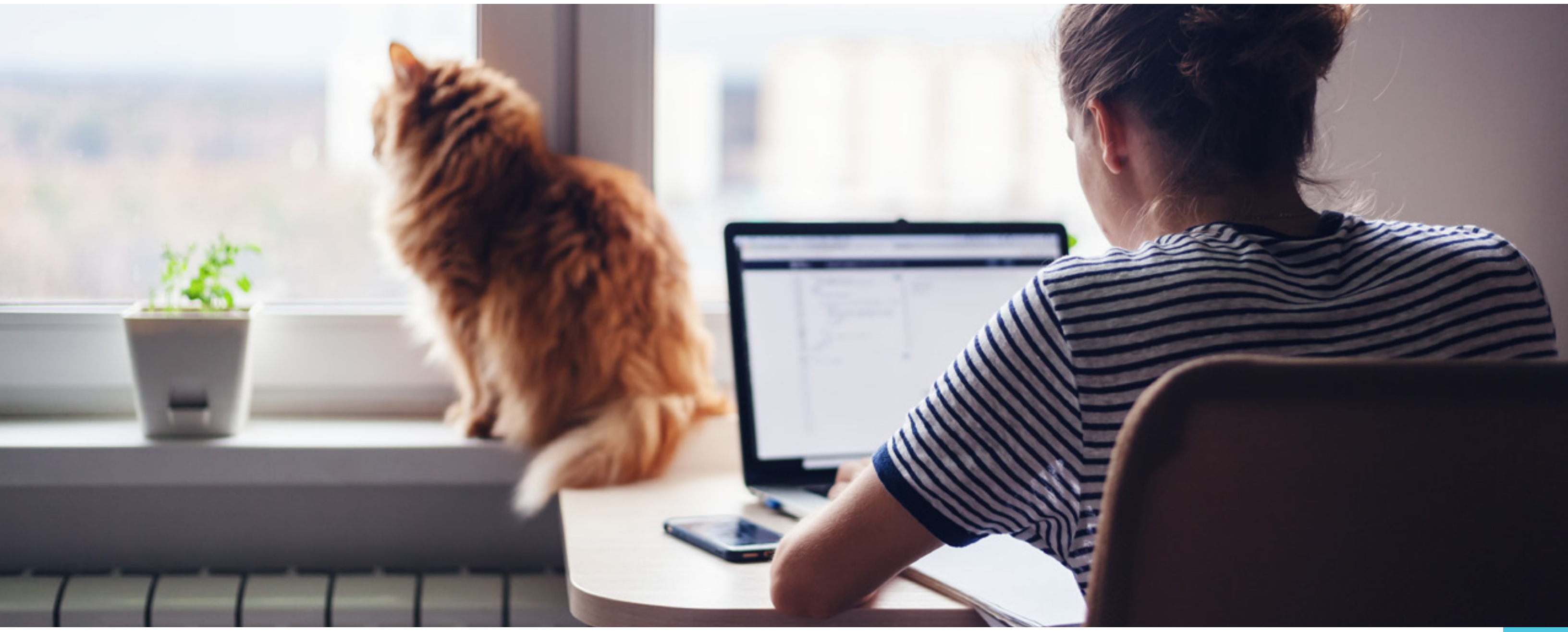
Follow us @PrismaAccess on Twitter to learn more or at https://www.paloaltonetworks.com/prisma/access

Introduction: A Hybrid Workforce Is Taking Shape

Nearly overnight, COVID-19 forced a quantum shift in how people work, with most organizations globally requiring employees to work from home where feasible. Organizations had to quickly adapt to meet the immediate need, utilizing their existing technologies or implementing new technologies to make their remote workforce productive.

With health safety restrictions currently changing across different regions around the world, it has become apparent that a long-term hybrid work model is taking shape. In fact, according to the "Global Work-from-Home Experience Survey," users are demanding it – 76% of global workers want the option to continue working remotely for at least part of the time.[1] Gartner further corroborates this trend: "By 2022, 25% of the global knowledge workforce will choose their home as the primary workplace, and 45% of the workforce will be working from home two to three days per week."[2]

Organizations are now thinking about how to evolve their networking and security architectures to maintain the productivity benefits of hybrid work – today and in the future – while reducing the risk of security breaches. In the rush to support significant increases in remote work during the pandemic, they became aware of considerable limitations in their legacy systems, which were never designed for rapid scale or for delivering consistent security everywhere. As they develop their long-term strategy to accommodate a hybrid workforce, businesses are transforming their networking and security infrastructures to make corporate resources available 24/7 and to deliver a secure, streamlined user experience.



About the Survey

Objectives

To gain deeper insight into how organizations are making the shift to a hybrid workforce arising from the global pandemic, Palo Alto Networks conducted one of largest and most complete studies on the state of hybrid work security for the enterprise in the world, the “State of Hybrid Work Security 2021.” The goal of the research was to:

- Establish the types of technologies and tools used to enable an organization’s remote workforce
- Determine how remote security has impacted an organization’s efforts to enable the remote workforce
- Show the value of investments in network and security architecture in providing a secure and efficient remote work environment

Methodology

Researchers surveyed and interviewed 3,000 enterprise information technology participants involved in information security, network operations, and application development. The survey was conducted by ONR, an independent third party, on behalf of Palo Alto Networks.

The breakdown was as follows:

1,250
from the Americas

1,000
from Europe
(including the U.K.)

750
from Asia Pacific

This population consisted of technology executives (C-level and vice presidents) and practitioners in networking and security and operations teams – all knowledgeable about their organization’s network and security architecture.

Executive Summary

Many companies have struggled with their remote access as well as the security challenges that the pandemic and hybrid work have created.

61%

struggled to provide the necessary remote security to support work-from-home capabilities

Many leaders fear that shortcuts were taken that now put their organizations at higher risk.

48%

of organizations admitted to compromising security or increasing security risk through lax enforcement of security policies and allowing employees more leeway than what was normally acceptable

35%

of respondents agreed that their employees either circumvented or purposely disabled the remote security measures they implemented

53%

of organizations who prioritized remote access over security are now exposed to significant security risks from unchecked acceptable use policy violations and unsanctioned application usage

Organizations are looking to the future with secure hybrid solutions for their employees.

62%

of respondents are considering a hybrid workforce solution

71%

of organizations expect to have their security mostly or completely in the cloud over the next 24 months

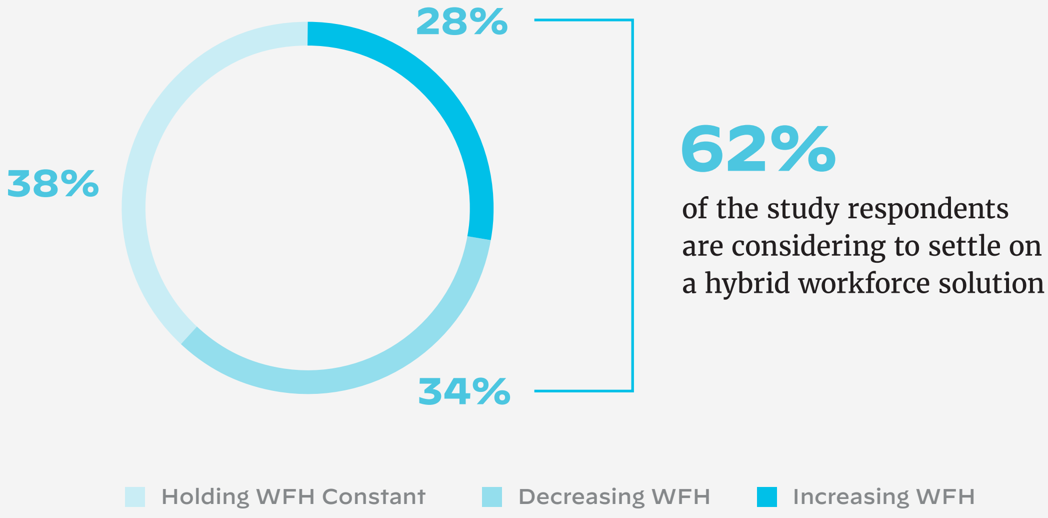
Organizations Fully Expect Hybrid Work to Continue

As organizations look to the post-pandemic future, they are preparing their hybrid workforce strategy, which needs to take into account operations, technology infrastructure, physical real estate, workforce productivity, workforce satisfaction, and culture.

At the time of the survey, over two-thirds of organizations indicated that between 25% to 75% of their workforce is working remotely – which is similar to the pattern seen during the peak of the pandemic. Organizations have moved some of their workforce back to the office, but the current work landscape remains generally similar to that during the height of the pandemic and is dominated by remote work.

While individual organizations are determining their specific optimal remote-to-onsite work ratio, looking across the world as a whole, organizations expect to continue remote work at a rate similar to the present rate. Forty-four percent expect to have over half of their employees working remotely in 12 months' time. With that in mind, as they fine-tune their specific remote capabilities, 62% of survey respondents are in the process of optimizing their hybrid workforce, with 94% considering some sort of hybrid workforce over the next 12 months.

Organizations' Work From Home (WFH) Plans for the Next 12 Months



62%

of the study respondents are considering to settle on a hybrid workforce solution

As one participant commented, "There's no way on earth that you can have zero home-office working in 2022. That would be just too extreme. It's just that all of the systems are there, and we kind of developed in that area. So, the planning will be that the home office will be utilized."

Pandemic Shifts the Focus of IT Transformation for Most

Before the pandemic, many organizations were in the throes of major digital transformation initiatives – which included migrating to the cloud and modernizing their infrastructure to better accommodate remote work. But the immediacy of the pandemic spurred a rapid acceleration in plans. Accommodating remote work became the main focus, as IT priorities pivoted rapidly. According to our survey, 67% of organizations simultaneously increased the capacity of their existing remote access architecture and implemented new technologies in an effort to evolve their infrastructure. Many simply increased the capacity of their current architecture at the time, but it wasn't a long-term solution, with 64% expected to change their remote access architecture over the next 24 months.

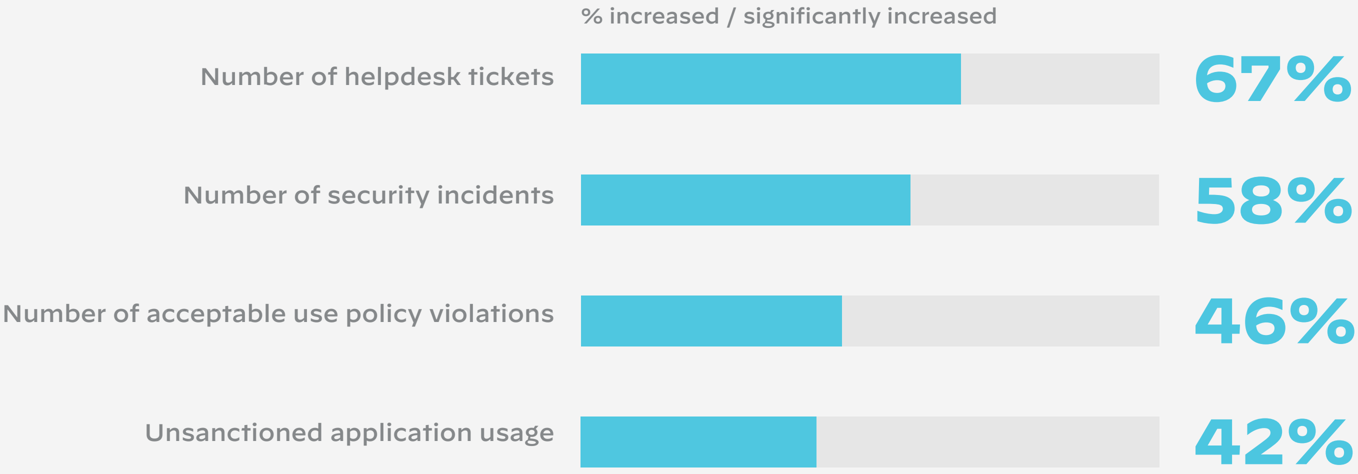
> "Our strategic plan (move to the cloud) is still a long-term strategic plan. Timing may have changed; we reallocated some investment to cover immediate remote access needs."

Security Tops the List of Key Challenges

According to our survey, by mid-2021, most organizations felt comfortable with their network and addressed earlier user complaints about collaboration tool performance and efficacy. While most organizations have stabilized their network and remote access, one-fourth to one-third of respondents are still struggling to provide a positive, well-rounded user experience.

Organizations continue to tackle some significant issues, with security topping the list for 51% of respondents – and service quality and technical complexity following close behind at 48% and 47%, respectively. The move to remote work in the thick of COVID-19 has seen a dramatic increase in these areas, as cited by respondents: help desk tickets, security incidents, acceptable use policy violations, and unsanctioned application usage.

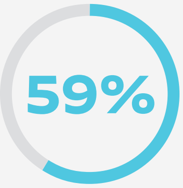
Impact of COVID-19 and the shift to WFH on your network



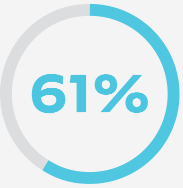
In addition, remote work has complicated issue resolution processes. As one participant points out, “users can’t walk up to another person and hand them their problem and have it returned to them fixed.”

Three Approaches to Network Access and Security Strategies

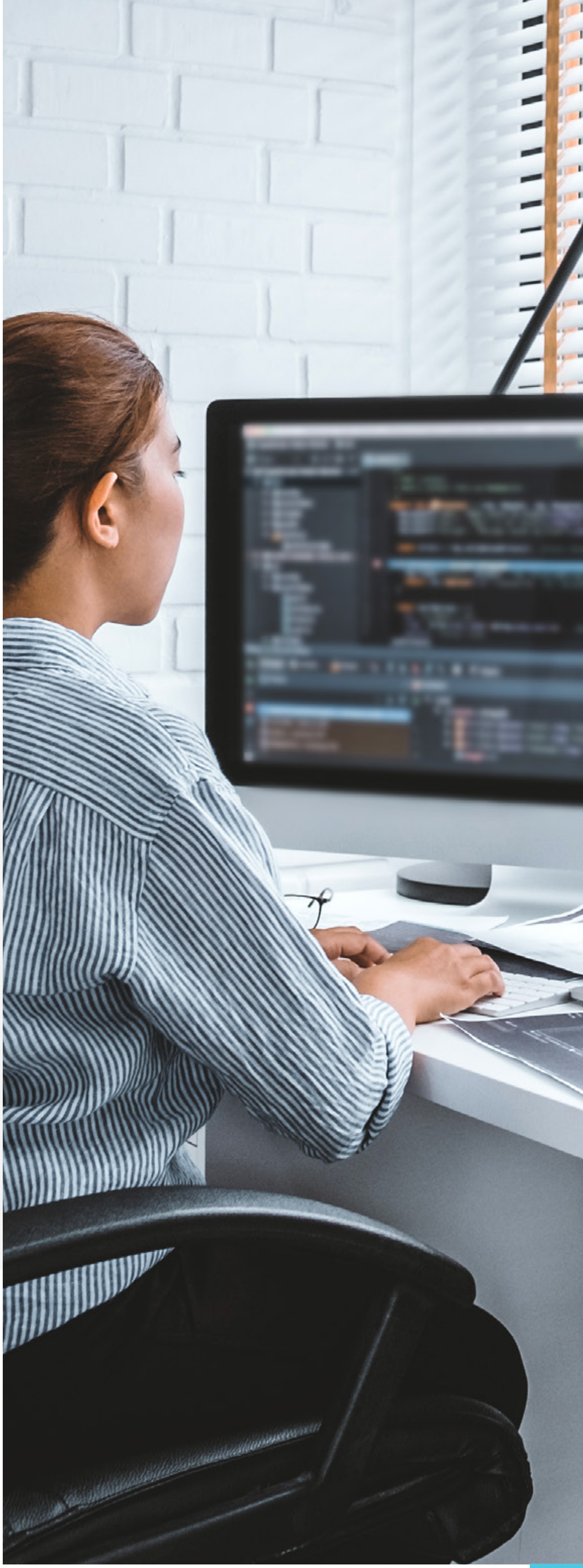
In a climate of extreme uncertainty about the future, along with severe budget constraints – especially at the outset of the pandemic – organizations were reluctant to invest in long-term solutions. Organizations broadly indicated that they struggled to provide both improved remote access and remote security (59% and 61%, respectively) and invested where they felt the need was greatest.



organization struggled to provide the necessary work-from-home capabilities in response to Covid-19

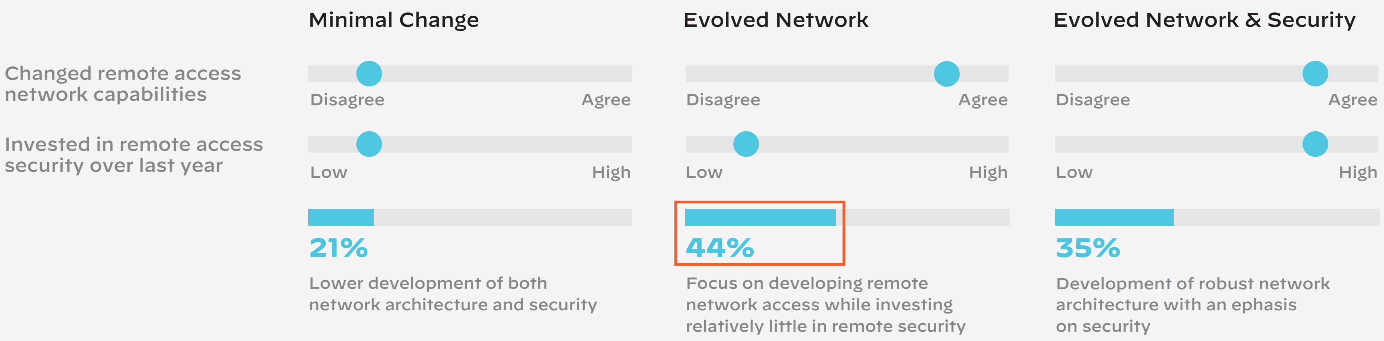


organization struggled to provide the necessary remote security for our work-from-home capabilities



This led to three broad approaches to developing network and security capabilities:

- **Minimal change:** 21% made very few changes in both their existing network architecture and security.
- **Evolved network:** 44% (the highest percentage) channeled their technology investments into improving remote network access while investing relatively little in remote security.
- **Evolved network and security:** 35% took a more balanced approach and developed more robust remote network access capabilities along with security.



As hybrid work becomes the new normal, those who made minimal changes are now seeing the cracks in their network architecture. Forty-eight percent of those organizations with minimal upgrades to their network now believe that their network cannot support current remote work demands or that their remote network is not sustainable. In contrast, this sentiment is expressed by only 21% of those who evolved their network and 14% of those who evolved both their network and their remote security.

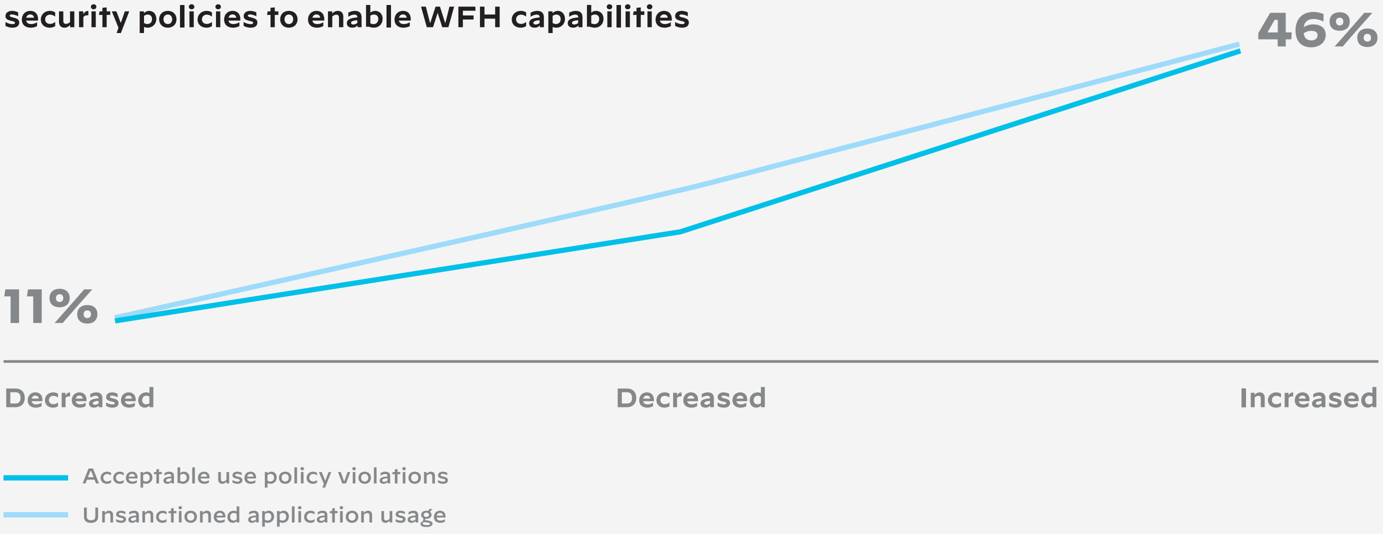
> "When we initially went to work from home, we didn't know if this was going to be a one-week thing, or if this is going to be a one-month thing. And it was difficult to make decisions that are sustainable over the long term, because you don't know if people are going to start running back to the office once this is over."

Security Took a Back Seat for Many

The data also shows that close to half of respondents focused on enabling remote access by evolving their network architecture, but they did not pay the necessary attention to making it more secure.

When it comes to security, expanding remote access for workers has had its consequences. As organizations enabled their remote employees, 48% of organizations admitted to compromising security or increasing security risk through lax enforcement of security policies and allowing employees more leeway than what was normally acceptable.

% of organizations who compromised their security policies to enable WFH capabilities



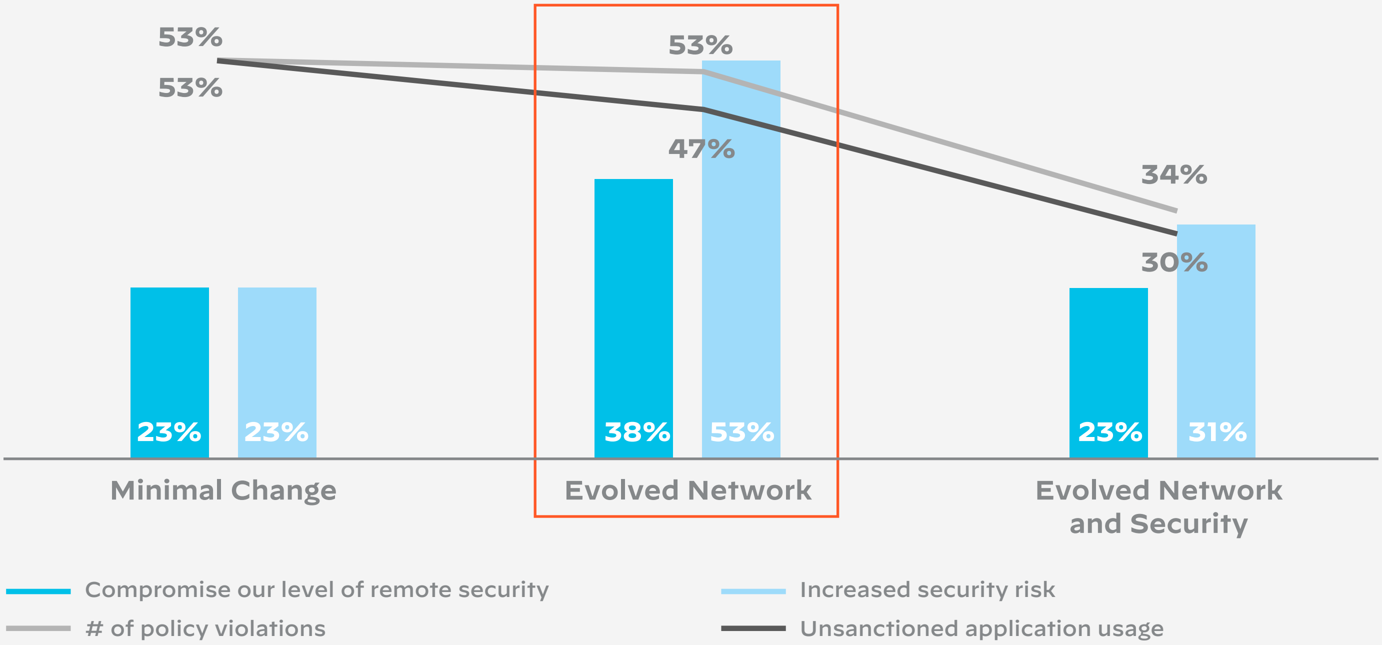
Remote Work Introduces New Security Challenges

As these organizations evolved their remote access, many never established proper security controls, processes, and policies for remote work. This respondent sums it up succinctly: "We didn't really have a security posture for remote working. As it expanded, there was a significant security gap – because it's a whole different world operating remotely than it is operating inside a facility."

The reasons for this include tight budgets, lack of time and resources, the need to respond quickly to remote work demands brought on by the pandemic, and loosening security restrictions as a result. Over half (53%) of organizations that prioritized remote access over security are now exposed to a significant increase in security risks from unchecked acceptable use policy violations and unsanctioned application usage. Interestingly, those who made minimal changes to their remote access saw a 23% increase in security issues, so their security was also compromised, but not quite as much.

Impact of COVID-19 and the shift to WFH on different aspects of organization's network

% agree / strongly agree



As has been the case in the past, when security measures become a burden – slowing down systems or otherwise impeding productivity and impairing the user experience – employees will often find creative ways to evade them. Remote work and the rise of cloud-based applications has made that easier than ever before. The expansion of remote work has opened the door to both an increased burden of security and an increased opportunity to evade controls.

It's important to emphasize that most organizations were fully aware of the nature of the security risks they were taking on and that many were in a situation where it was difficult to procure the necessary investments to bolster their defenses. The lack of concrete security key performance indicators (KPIs) to justify return on investment (ROI) made it difficult to focus the appropriate investment in security.

Consequences of Compromised Security: Remote Security Evasion

Overall, 35% of respondents agreed that their employees either circumvented or purposely disabled the remote security measures they have implemented – and those evasions varied in severity.

What exactly has contributed to these risky behaviors by users? The pandemic prompted an urgent move to remote work and introduced risk factors that play into remote security evasion. These were not all necessarily new, but many of them were not properly understood or seen at scale prior to the pandemic.

Some of the contributing factors included increased complexity, relaxed enforcement of security policies, and an ad-hoc rather than a well-planned, more deliberate approach to security. On the user side, factors that contributed to evasion include unsanctioned application usage (known as "Shadow IT") and bring-your-own-device (BYOD), where employees use personal rather than corporate-issued devices for work.

Unfortunately, organizations that failed to prioritize security before the pandemic continue to bear the negative consequences of this oversight. The organizations that face high levels of remote security evasion today are the same organizations that deprioritized security when they expanded their existing remote access infrastructure to their much larger remote workforce. Factors that contributed heavily to high levels of security evasion included poor collaboration tools, increased BYOD usage without proper security controls or policies in place, and use of unsanctioned applications. Many organizations failed to foresee the results of their inattention to security as they quickly scrambled to enable remote work for their employees.

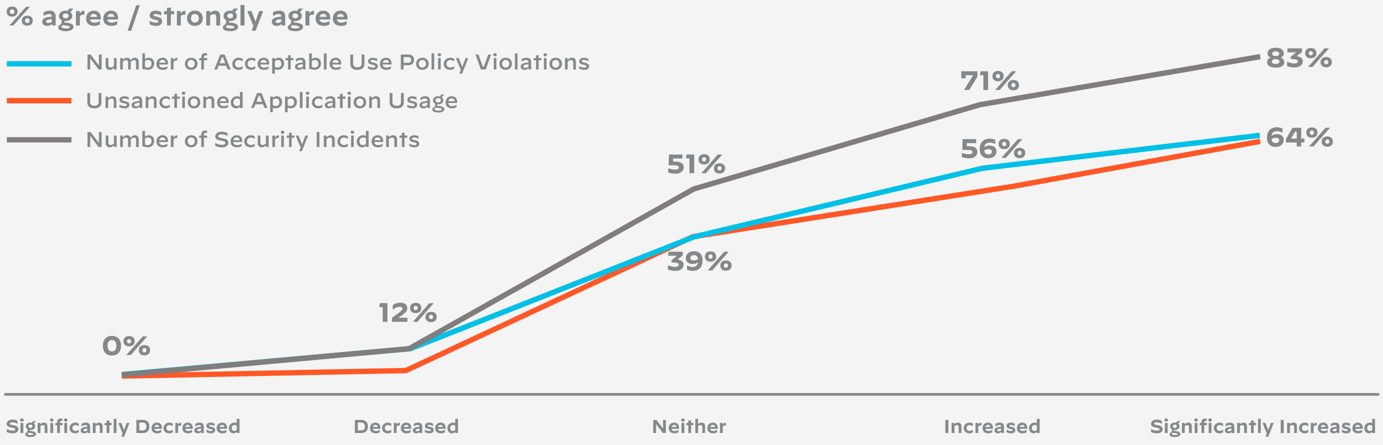
Risky Remote Worker Behaviors

- Using personal devices for work (BYOD)
- Uploading corporate data to unauthorized applications or cloud services
- Circumventing security controls
- Connecting to unsecured networks at home or when traveling
- Lacking cybersecurity awareness training
- Failing to report phishing and other threats
- Sharing confidential files via email
- Not updating security on devices

Findings from the survey corroborate this:

- Organizations that lack effective remote collaboration tools say that their users are **over eight times more likely** to report high levels of security evasion. Employees tend to find their own workarounds or use unauthorized applications to make collaboration more efficient – and this practice increases security risks.
- At the peak of the pandemic, many organizations relaxed their BYOD policies. Our survey shows that 60% of organizations expanded BYOD to enable their employees to work from home. But, as a result, organizations that allow increased BYOD usage have employees **who are over eight times more likely** to ignore, circumvent, or disable security than those who restricted BYOD.
- Increased BYOD usage also led to a spike in security issues – from unsanctioned application usage to acceptable use policy violations" and, especially, security incidents. Out of the organizations that saw a significant increase in BYOD, 83% saw an increase in both security incidents and unsanctioned application usage, while 64% experienced a surge in acceptable use policy violations. Perhaps earlier on in the pandemic, organizations likely had an inkling of the increased security challenges associated with BYOD, but did not expect the actual level of risk to rise so dramatically.

“Bring your own device (BYOD) usage since COVID-19”



“Our security technologies were not tuned to provide visibility for such remote access, because the majority of the workforce was [previously] only in the office. Our security technologies were focused on providing visibility in that area and not for remote access.”

Insights Lead to New Security Priorities

Organizations are beginning to see the shortfalls of their remote security strategy, which, for 59% of those surveyed, consisted of ad-hoc point solutions. Forty-nine percent are seeing that this patchwork of unintegrated solutions results in blind spots that detract from their ability to prioritize risk and prevent threats.

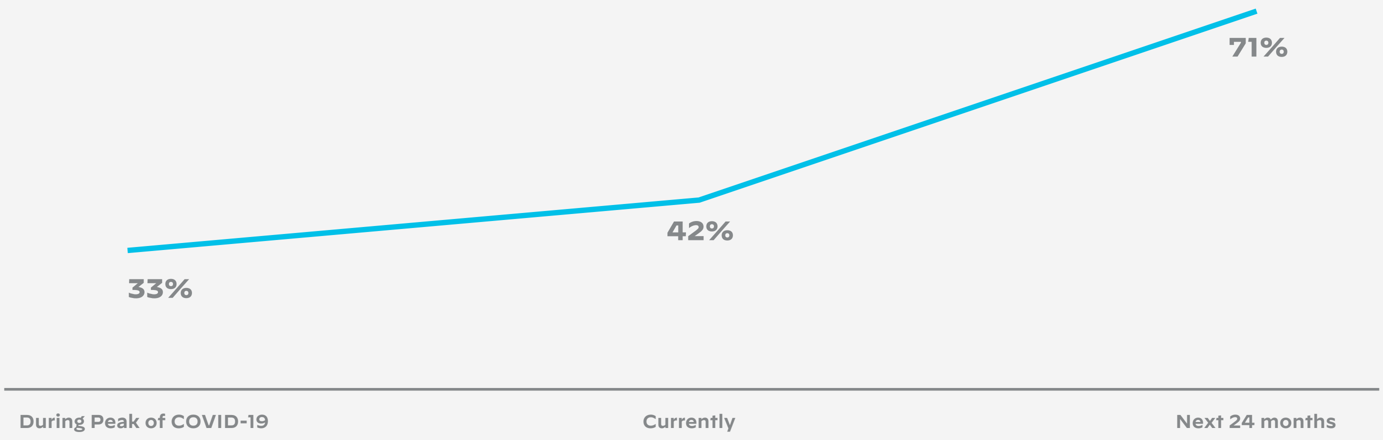
Now that the immediate fire-drill of shifting to remote work has passed in most regions of the world, organizations are changing their focus to develop the right long-term solution strategies for their hybrid workforce. Seventy-four percent believe a single end-to-end remote security solution would improve their posture. Additionally, cloud-based security has emerged as a key focus area for security leaders and decision-makers.

Moving security to the cloud

On a proactive note, 67% of organizations took action at the peak of the pandemic in order to better protect their remote workers – 41% moved some of their security to the cloud, and 26% boosted their existing on-premises security as a temporary fix.

However, the future outlook looks positive, with 71% of respondents planning to move their security mostly or fully to the cloud over the next 24 months. This significant trend supports the hybrid mobile workforce evolution. When people are mobile, cloud-centric security technologies are essential to enable collaboration, regardless of where users are.

% organizations with security mostly or completely in the cloud



The Impact of Security Evasion

Apart from the security issues discussed earlier, security evasion has also called into question the sustainability of organizations' network architectures and has caused poor hybrid work outcomes. Our survey demonstrates that this is a major concern for organizations with a high level of security evasion as compared to organizations with a medium level of security evasion. Organizations with high security evasion are:

- Nearly four times more likely to express concern that their existing network cannot support current demands when compared to their counterparts with mid- or low levels of evasion.
- Over four times more likely to feel that their remote access architecture is not sustainable compared with their counterparts with mid- or low levels of evasion.

Beyond the network and security consequences, organizations with high levels of evasion acknowledge that this has had negative remote work outcomes.

- They are more than twice as likely to believe that security evasion has hindered employee productivity.
- They show somewhat lower rates of perceived workforce satisfaction – 60% for this category compared to 80% at low-evasion organizations and 70% at medium-evasion companies.

Perspectives from Leadership and Practitioners

When it comes to hybrid work, leadership (C-suite and vice presidents) and networking or security practitioners (including lower-level management) are not completely aligned on the hybrid work challenges that their organizations face. Our survey indicated that both groups have positive views of the remote access user experience, despite the fact that users have raised flags about inadequate connectivity from home and lack of familiarity with and training on remote tools, technologies, and remote work security policies. Approximately 70% of leaders and practitioners believe that users have seamless access to all applications, regardless of where they work and that their organizations deliver uninterrupted, reliable connectivity.

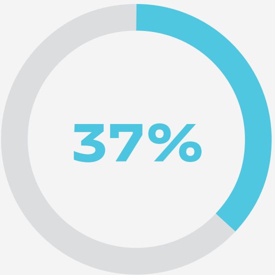
However, when it comes to the stability of their organization's remote networks, leadership is far more concerned about this issue than are practitioners. Forty-three percent of leaders compared to only 13% of practitioners agree that their existing remote access architecture cannot support current hybrid work demands and/or is not sustainable. More than half of leadership (53%) respondents lack confidence in their collaboration tools, while just under a third (30%) of practitioners feel the same way.

Why this divergence? It’s possible that front-line practitioners have over-inflated or somewhat biased views about the quality and efficacy of the solutions they manage compared with decision makers and end users. Practitioners also have daily hands-on experience with the tools and the environment, giving them a better understanding of the remote access architecture and its limitations compared with business leaders and end users.

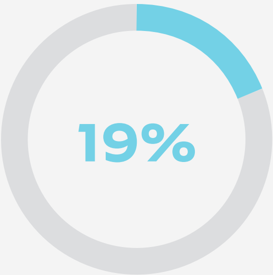
It’s also likely that leadership’s worries about their remote networks are driven by fears around security evasion. Upwards of 30% of leadership report that employees ignore, circumvent, or disable security measures, compared to 19% of practitioners. Practitioners may not appreciate the scale at which evasion of remote security is occurring across the organization.

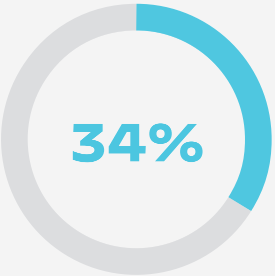
Leadership
Director titles and above
% agree / strongly agree

Individual Practitioners to Lower Management
% agree / strongly agree

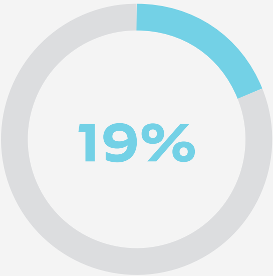


“Our remote security measures are **often ignored by employees**”





“Our remote security measures are often **purposefully disabled or circumvented by employees**”



Moving security to the cloud using a secure access service edge (SASE) approach is another area where there is some difference in comfort level between leadership and practitioners. A large majority of practitioners believe there is value in moving security to the cloud, while 27% of leadership are not comfortable with the idea yet.

Building an Optimal Workforce

As the world moves forward post-COVID, it's clear that most organizations worldwide are contemplating some form of a hybrid workforce. Survey results show that the majority of organizations that invested in evolving both their remote security and networks are aiming for an over 50% hybrid workforce, while those that instituted minimal changes or just focused on remote access are less confident about moving in this direction and are looking at a less than 50% hybrid workforce.

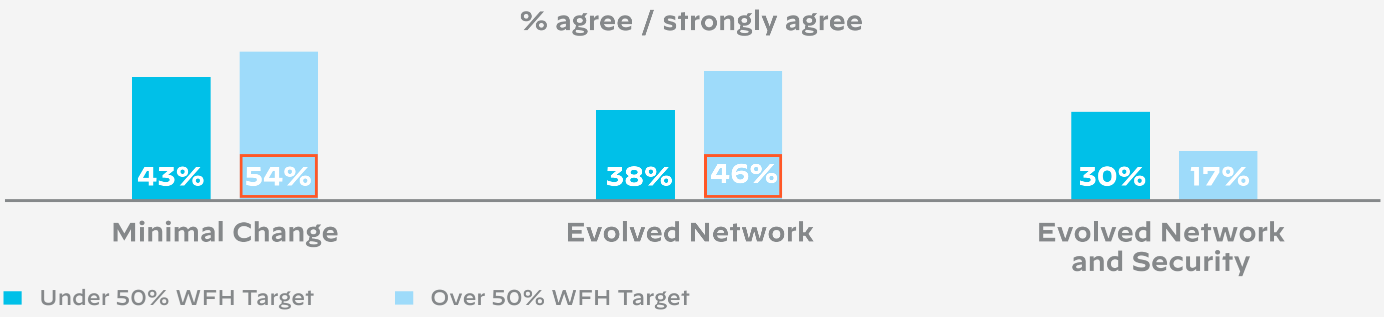
Clearly, the workforce seems to be enjoying remote work, with 71% of organizations reporting an increase in employee satisfaction since shifting to remote work. Given that, it is not surprising that the majority of organizations are looking to maintain a hybrid workforce model. Only 15% report that they will try to return to traditional in-office operations, and only 6% expect to be fully moved to the office within the next year. Instead, we see that 44% of organizations expect to keep over half of their workforce remote in the coming year, and almost everyone expects to support a hybrid environment.

A consistent theme that has emerged from the survey is that organizations targeting a higher hybrid workforce percentage (over 50%) need to prioritize their security evolution in order to control remote security evasion. Below are some results that affirm this, especially for those that made minimal changes or only focused on evolving their network:

- As mentioned earlier, almost half of leadership respondents lack confidence in their collaboration tools, while roughly one-fifth of practitioners feel the same way.
- Those organizations that made minimal changes or focused only on their network reported that they are struggling to enable effective and productive workforce collaboration – 54% and 46% respectively. By contrast, only 17% of the group that evolved both their network and their security are facing this issue.

Approaches to Building Network & Security

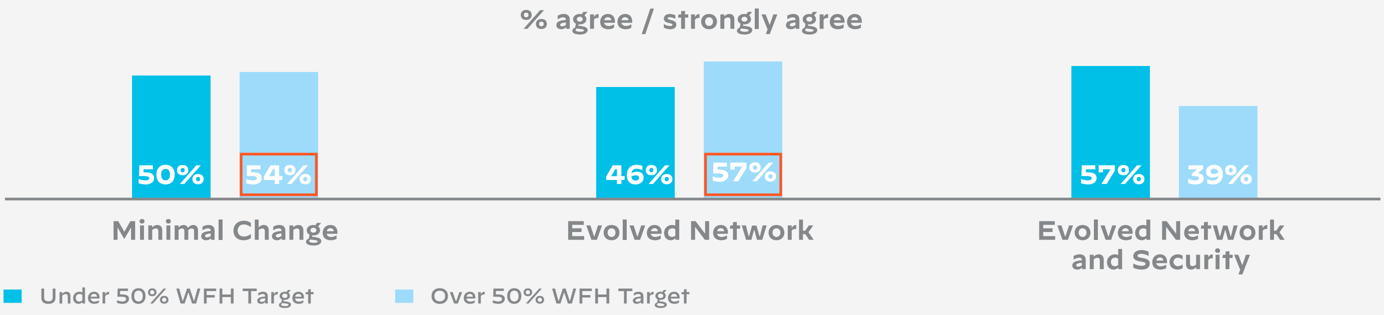
"My organization's collaboration tools do not enable our remote workforce to effectively engage and collaborate with their colleangues"



- Visibility concerns arising from the utilization of disparate point solutions emerged as a big concern for over 53% for the minimal-change respondents and 57% of the network-only respondents.

Approaches to Building Network & Security

"I believe the number of point solutions that we use to secure our remote workforce creates blind spots that detract from our ability to prioritize risk and prevent threats"



Conclusion

In the post-pandemic world, the concept of a hybrid workforce is rapidly gaining acceptance. The question is: To what extent do organizations plan to support that work style going forward and how prepared are they?

The results of our survey show that organizations that are targeting a lower percentage of remote work are holding their own for now. On the other hand, those that aspire to expand their hybrid workforce capabilities face some key challenges – namely high security evasion, ineffective remote collaboration tools, and poor visibility across the entire corporate environment.

More than three-quarters of organizations recognize that network connectivity is critical to workplace happiness and are doubling down on their efforts to enable their networks. Eighty-one percent of leaders report that remote access architecture is a top priority, and they note that maintaining comprehensive security and service quality are both their greatest challenges and most critical goals. As a result, they are increasing their investment in remote security architectures and moving security to the cloud.

By moving conventional remote access infrastructures to cloud-delivered solutions, organizations can accommodate the current and emerging needs of their hybrid workforces while gaining significant advantages over legacy architectures, including:

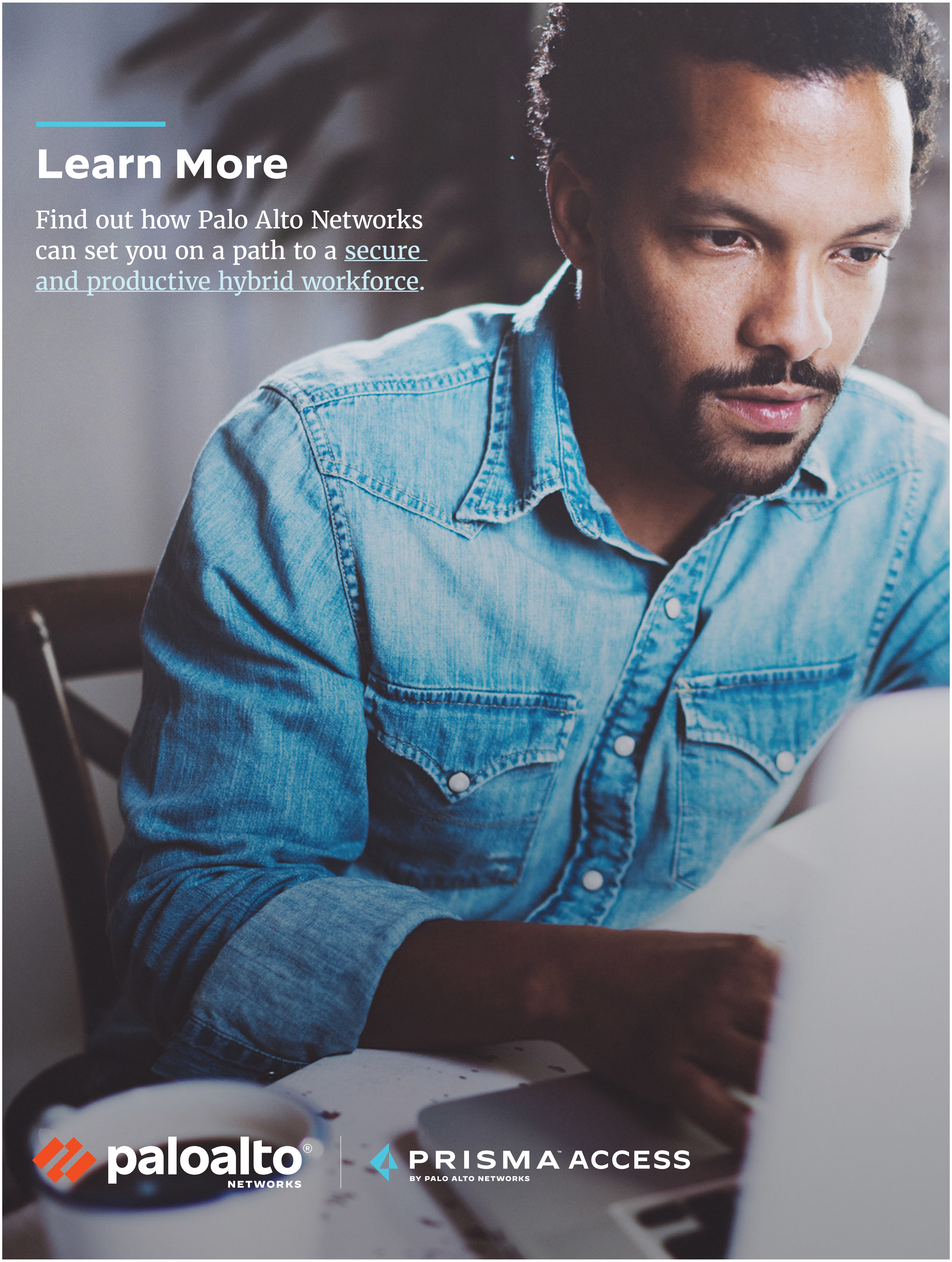
- Visibility into the network, applications, and user traffic, no matter where they are located: on premises, at home, or on the road.
- Control over what users and applications are accessing and sharing.
- Security across the entire network infrastructure, applications, services, and users to ensure that all threats and vulnerabilities are rapidly remediated.
- Simplified deployment to allow branch offices and home offices to be easily added to the network, without hardware or physical visits from IT.

Boosting investment in remote access security

Organizations plan to increase their investment in remote access security over the next 12 months, with 54% of those surveyed expecting to spend more than $5 million on their remote security, up from 31% over the previous year.

For more information about the research firm that conducted the fieldwork and provided the advanced analytics for this survey, visit: https://www.onrcx.com/.

1. https://globalworkplaceanalytics.com/global-work-from-home-experience-survey
2. https://www.gartner.com/smarterwithgartner/making-hybrid-work-more-permanent-set-some-ground-rules/



Learn More

Find out how Palo Alto Networks can set you on a path to a secure and productive hybrid workforce.

paloalto NETWORKS | PRISMA ACCESS BY PALO ALTO NETWORKS