Untethered: How CIOs & CISOs Are Paving the Way for the New Hybrid Workforce

In this in-depth research report, discover effective techniques to transition from exposed legacy infrastructure to an effective zero trust strategy

AN HMG STRATEGY RESEARCH REPORT POWERED BY ZSCALER

HMG STRATEGY

zscaler™

EXECUTIVE SUMMARY

As we move into a new phase of the global pandemic, many companies are grappling with how to bring their employees back after more than two years of being untethered from the office. Survey after survey shows that most people want hybrid work arrangements—a mix of in-person and remote—and are leaving for new opportunities when not provided the freedom to decide when and where they work.

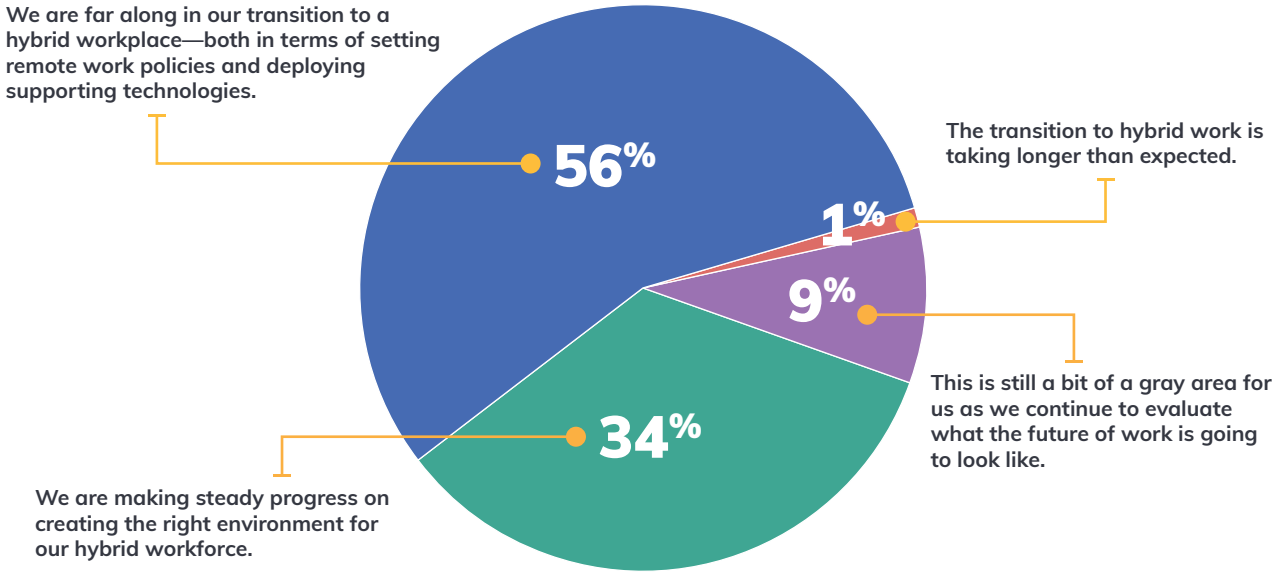
So, how do we successfully transition the business to the future of hybrid work? And how can CIOs and CISOs work in alignment with fellow members of the C-suite to deliver an agile and productive work environment while properly safeguarding the enterprise?

A recent survey of 138 CIOs, CISOs and corporate technology leaders conducted by HMG Strategy, sponsored by Zscaler, reveals that while 56% of respondents report that their organizations are "far along" in their transition to a hybrid workplace—both in terms of setting remote work policies and deploying supportive technologies—nearly half (44%) of executives characterize their organizations' transition to a hybrid workplace as a work in progress.

Indeed, among the 44%, nearly one in five surveyed say that the transition to a hybrid workplace "is still a bit of a gray area for us as we continue to evaluate what the future of work is going to look like."

Adapting to the Hybrid Workplace

How would you characterize your organization's transition from remote work to hybrid work?



Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

"Most organizations are surviving with their transitions from remote to hybrid work, but they aren't thriving," said **Bryan Green**, CISO Americas, Zscaler. For instance, since the start of the pandemic, most companies have made temporary, short-term investments to expand the use of VPN technologies or bypass sensitive high-bandwidth applications such as videoconferencing systems to address the pivot to remote work. "But they're not necessarily making the right long-term security decisions," Green added.

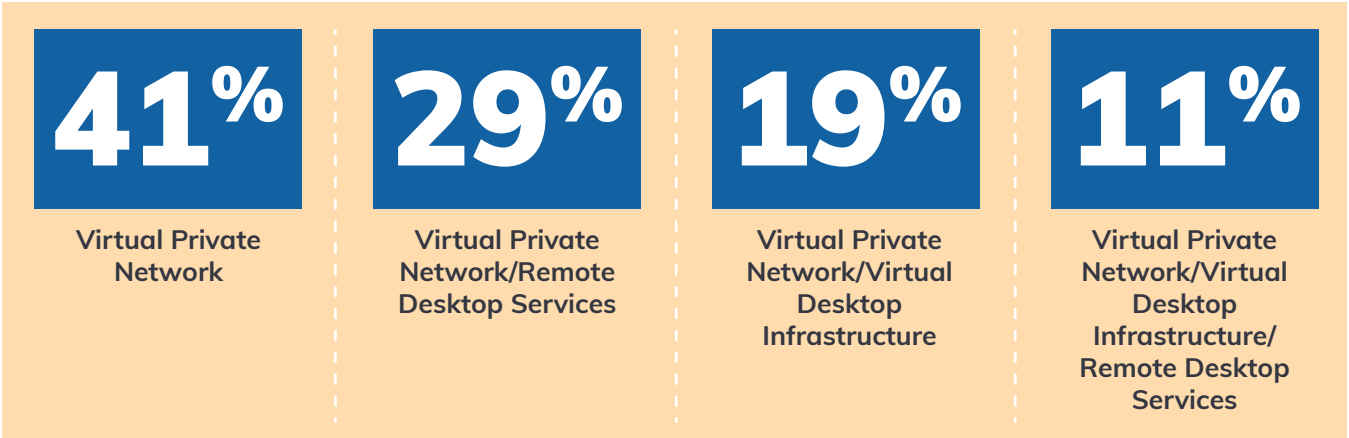
As pandemic "change agents," tech leaders are well-positioned to help their organizations for the next phase of the evolving workplace—ensuring that they deploy the right technologies to meet the needs of hybrid workers while creating a flexible, productive, and secure environment for in-office and remote workers alike. But as the research indicates, more work is needed to bring this concept to fruition.

HMG Strategy has partnered with Zscaler to gain a deeper understanding of the challenges and opportunities companies are facing in their transition to a hybrid work environment, including the technological and cultural barriers to achieving a secure and flexible hybrid workplace. In this research report, you'll discover:

- The technical difficulties in achieving a secure and flexible hybrid workplace, including the shortcomings of legacy infrastructure such as VPN technologies
- The risks organizations face in securing access to applications for a hybrid workforce
- The security challenges associated with providing access to private applications for remote and in-office workers
- A robust architecture as a solution to the security pitfalls to the hybrid work environment with zero trust

The Means to Application Access

What forms of application access technologies are you currently using?



Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

"Most organizations are surviving with their transitions from remote to hybrid work, but they aren't thriving."

BRYAN GREEN
CISO Americas
Zscaler

Overcoming the Barriers to a Secure, Flexible Hybrid Workplace

While companies have continued to adopt software as a service (SaaS) and public cloud services over the past several years, many organizations are still very much on their cloud migration journeys. Over the next year, 63% of companies plan to shift most or all of their IT infrastructure to the cloud, up from the current figure of 41%, according to a study by Foundry.

And while cloud adoption is moving quickly, companies still have a massive amount of investment in data centers and on-premises infrastructure.

“Despite the fact that it’s been 16 years since AWS began launching public and private cloud infrastructure, COVID only began accelerating the massive push to remote work two years ago,” said Green, “so there’s a very long tail where companies need to address the challenges associated with the complexities of people, processes, and technologies in their organizations.”

Leadership dynamics are another complex issue associated with the shift to hybrid work. Given the enormous real estate investments companies have tied up in owned or leased office space, many senior executives want to ensure that office space is utilized effectively. In some instances, senior management is mandating that employees work two or three days per week in a dedicated office, though many employees have continued to push back on these directives.

In the first week following Labor Day 2022, office usage in 10 major metro areas in the US neared 50% of 2020’s pre-pandemic attendance, according to research compiled by Kastle Systems, a managed security company that tracks entries into office buildings. In-office attendance is still lower than what it was prior to the pandemic, although various studies have shown an uptick over the past several months.

“Management in a lot of organizations are faced with the reality that they have these massive investments in real estate,” said Green. “They want people to be there to collaborate, so it’s a very difficult challenge.”

Tackling the Cybersecurity Challenges

When companies made the pivot to remote work in March 2020, this exposed a number of shortcomings in their approach to monitoring and safeguarding a remote workforce. For starters, many organizations have relied on virtual private networks (VPNs) for employees to send and receive data across shared or public networks. This exposed a number of vulnerabilities with VPNs:

- Each VPN gateway has an inbound listener that makes it an exposed attack surface itself.
- The VPN gateway becomes a jumping-off point for more sophisticated attacks by hackers.
- The nature of a VPN is inherently open, which forces security teams to explicitly lock employees out of applications and systems they don’t or shouldn’t have access rights to.

Modernizing the Hybrid Workplace

Many of the challenges associated with achieving a secure and agile hybrid workplace are tied to outdated infrastructure, combined with a lack of tools that are needed to prevent data loss and unauthorized access to applications.

The Primary Barriers to a Secure, Flexible Hybrid Workplace

30%

Even though we actively enable BYOD, we do not have the tools needed to minimize the risk of data loss and unauthorized access to internal resources

20%

Our VPN infrastructure noticeably slows down internet connectivity and negatively impacts employee productivity

7%

Even though we actively enable BYOD, we do not have the tools needed to minimize the risk of data loss and unauthorized access to internal resources; Our business relies on third-party contractors and partners, but providing them with secure access to internal applications is a challenge

22%

Our business relies on third-party contractors and partners, but providing them with secure access to internal applications is a challenge

16%

Our VDI network latency frustrates employees and makes even the simplest tasks impossible on virtual desktops

5%

Our VDI network latency frustrates employees and makes even the simplest tasks impossible on virtual desktops; Our business relies on third-party contractors and partners, but providing them with secure access to internal applications is a challenge

Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

"If you have some combination of remote access VPNs and site-to-site VPNs, you end up with this massive attack surface where users or malicious actors can potentially enumerate your infrastructure."

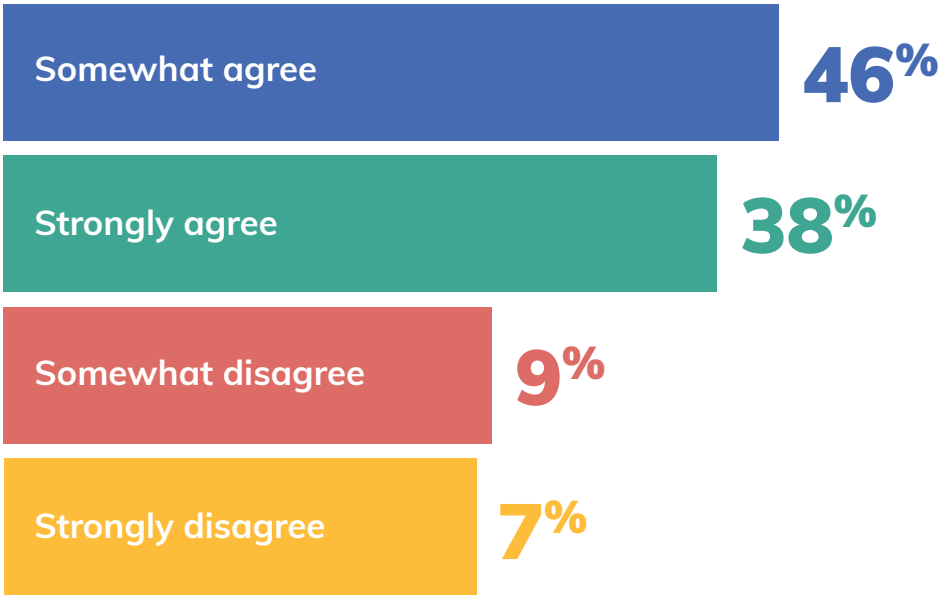
BRYAN GREEN
CISO Americas
Zscaler

"When you create a VPN connection, you are effectively extending the corporate network out to various locations," said Green, who worked on Cisco VPN concentrators starting in 2003. "If you have some combination of remote access VPNs and site-to-site VPNs, you end up with this massive attack surface where users or malicious actors can potentially enumerate your infrastructure. Unless there are certain types of firewalls or certain types of segmentation, they really have carte blanche access to infrastructure."

A Productivity Thief

The use of remote access and site-to-site VPNs not only exponentially expands an organization's attack surface, but also stagnates the productivity of hybrid employees.

To what extent do you agree that frustratingly slow VPN performance negatively impacts the productivity of hybrid employees?



Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

The inherent vulnerabilities associated with the use of VPNs are just a few of the reasons why organizations should transition to a zero trust architecture to safeguard the hybrid workplace. A zero trust architecture can not only insulate organizations against costly breaches, but also provide companies with reduced complexity, stronger data protection, and a better employee experience while eliminating the attack surface.

In the next sections of the report, we'll explore the security challenges associated with overprivileged access along with the operational and business benefits of adopting a zero trust strategy.

Eliminating Overprivileged Access for a Secure Hybrid Environment

Although many organizations have had subsets of remote employees for years, the widespread digital pivot that companies were forced to make in March 2020 exponentially expanded each organization's digital footprint—and attack surface.

As companies continue to expand their adoption of public clouds, this also increases the risk of overprivileged access and the exposure of critical data.

The Risk Exposure to Hybrid Workforce

Legacy infrastructures applied to a hybrid workplace create multiple exposures that security teams must contend with, including overprivileged application access for employees and contractors as well as compromised users who access network resources.

What risks do you face when securing access to applications for a hybrid workforce?

31%	26%	18%	15%	10%
Overprivileged access for employees or third-party vendors	Compromised users accessing network resources	Accidental and/or malicious data loss	High-risk devices accessing network resources (e.g., unknown, noncompliant	Application attacks (e.g., denial of service, cross-site scripting, injection)

Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

"Overprivileged access is a tremendous security problem that we face, and it's one that we've struggled to address as an industry," said Green. Green draws an analogy to customer interactions at a bank branch. At a bank branch, a customer doesn't provide each teller or bank employee with a key to their safe deposit box. But when it comes to providing employees and users with logical access to different types of applications based on their roles, "it's much more challenging to implement compared to physical access," said Green.

Fortunately, modern tools such as cloud infrastructure entitlement management (CIEM) address the risks associated with overprivileged access by providing deep visibility into cloud entitlements and access risks while enabling organizations to adopt a least privilege strategy.

In the final section of the research report, we'll share the factors that are prompting security and technology leaders to adopt zero trust security strategies, along with the operational and business benefits for applying a zero trust model.

Lacking Confidence in Existing Security Tools

Just one-third of security and technology leaders expressed strong confidence that their organization's existing security tools would be able to identify a compromised user or insider threat accessing network resources.

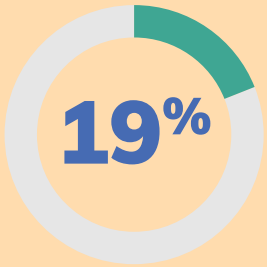
How confident are you that your existing security tools would be able to identify a compromised user or insider threat accessing network resources?

Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

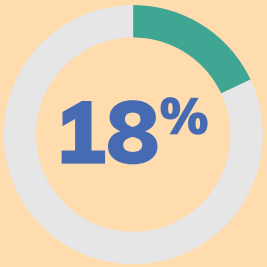
The Security Shortcomings of Private Applications Access

It's not just public applications that are exposed to security vulnerabilities. Private applications that are made available through internet gateways can also be vulnerable to attacks.

Which of the following scenarios have you encountered when providing access to private applications for remote and in-office workers?

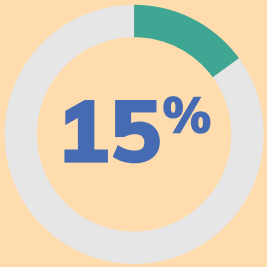


Users experience frustration due to inconsistent access policies and connectivity issues

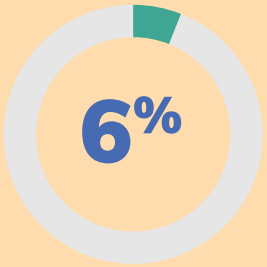


Private applications are exposed to the internet in order to provide access, which makes them vulnerable to attacks

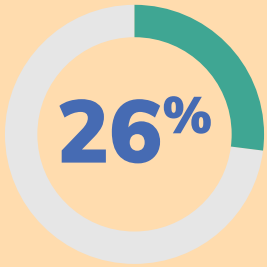
Employees and third-party users have full access to the corporate network, which increases risks for lateral movement



We backhaul remote users to our data centers to access private applications, which slows down their Internet connection



We hairpin in-office/branch users to our data center to access private applications, which negatively impacts performance



We have not experienced any of these scenarios

Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

The Journey to a Zero Trust Strategy

With the increased security concerns associated with unmanaged personal devices in a work-from-home setting, the continued reliance upon virtual private networks (VPNs) has left too many organizations exposed. Add to this the vulnerabilities associated with overprivileged application access, and it's clear that the legacy infrastructure many organizations have in place to support a hybrid workforce is simply an untenable situation.

These are just a few of the reasons why the majority of CISOs and enterprise security leaders are adopting modern zero trust architectures to shore up their defenses and safeguard the organization from end to end.

"First and foremost, a zero trust network access solution improves security outcomes in terms of a reduced attack surface," said Green. "Moreover, ZTNA dramatically improves user experience and performance."

C-level technology executives are seriously considering alternatives to legacy architecture as hybrid work becomes more widely established. Strengthening security while boosting productivity has been the driver for the majority of organizations to adopt ZTNA. All organizations that have embraced zero trust have seen significant reduction in cost and complexity, leading to a stronger focus on the business.

The Elements Behind Zero Trust Adoption

More than 35% of respondents are considering zero trust over legacy solutions to protect their tech stack and employees in the hybrid work environment.

What prompted your organization to adopt a zero trust security strategy?

29%

We are currently considering a transition to zero trust security but have not yet made a decision

- We recognized that traditional firewalls and VPNs are more easily circumvented by attackers and allowed for free lateral movement — **21%**
- We've transitioned to a zero trust strategy to enable secure, flexible hybrid workforce connectivity — **20%**
- We recognized that traditional firewalls and VPNs created a significant surface for attack — **15%**
- We are not currently planning to adopt a zero trust security strategy — **15%**

Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

"Let's say a malicious actor were to establish a foothold or compromise some infrastructure within your environment. From a kill chain perspective, you want to be able to make sure that they cannot continue to just move laterally throughout your organization," said Green. "Most importantly, that they're not able to exfiltrate any of that data from your environment so they can't steal confidential intellectual property, trade secrets, or customer data. I think the combination of those three things is really one of the most compelling reasons to move toward a zero trust access-based solution."

A zero trust strategy also offers additional benefits in a tight labor market. **Eighty-four percent** of the technology executives who participated in the HMG Strategy research study believe that enabling a flexible and secure hybrid work model has contributed to their organization's ability to attract and retain talent.

"I think the high percentage of executives who see this connection reflects the flexibility and freedom with how employees choose to work," said Green.

Fifty-five percent of respondents to the HMG Strategy research study indicate that the shift to hybrid work has led their organizations to reevaluate their legacy remote access infrastructure.

Meanwhile, as many executive teams have become cost-focused, the transition away from antiquated and expensive legacy controls to a modern zero trust infrastructure enables businesses to respond to shifting market conditions quickly and flexibly while reducing both costs and risks to the enterprise.

By replacing disparate legacy controls, a zero trust architecture also enables security teams to streamline and manage their overall security controls more effectively. "Moving toward a zero trust model really allows you to collapse a lot of the control in the enforcement plane, so that you can really just have a single pane of glass to implement a lot of these security controls," noted Green.

Since the digital workplace pivot in March 2020, employees have demonstrated not only how productive they can be while working remotely, but how much they crave more flexibility in their personal and professional lives. It's become increasingly apparent that the traditional nine-to-five, in-office environment is a thing of the past. Clearly, legacy technologies such as VPNs don't provide the flexibility or protection to safeguard sensitive data in a hybrid workplace. A new, more effective approach is needed.

Said Green, "Zero trust is a fantastic opportunity for organizations to improve how they can operate in a hybrid work environment."

The Zero Trust Technologies That Are Safeguarding Hybrid Work

Which of the following zero trust technologies is your organization currently using to enable secure hybrid work?

19%
Multifactor authentication

16%
Endpoint security

14%
Cloud firewall

10%
Data loss prevention

9%
Secure web gateway

32%
Other entries

Source: HMG Strategy's 2022 Secure Hybrid Workplace survey, 138 CIOs, CISOs, and technology executives, conducted in Q2 and Q3 2022.

About HMG Strategy

HMG Strategy is the world's leading digital platform for technology executives to reimagine the enterprise and reshape the business world. The HMG Strategy global network consists of more than 400,000 CIOs, CTOs, CISOs, CDOs, senior business technology executives, search industry executives, venture capitalists, industry experts and world-class thought leaders.

About Zscaler

Zscaler accelerates digital transformation so 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 SSE-based Zero Trust Exchange is the world's largest inline cloud security platform.