Top Network Practices to Support Hybrid Work

Published 8 April 2022 - ID G00765086 - 10 min read

By Analyst(s): Karen Brown, Andrew Lerner, Mike Toussaint

Initiatives: Cloud and Edge Infrastructure

The COVID-19 pandemic accelerated hybrid work operations. Cloud and edge I&O leaders can use this research to quickly identify best practices to support a workforce that primarily requires consistent and secure access to data and workloads at home and in the office.

Overview

Key Findings

- IT leaders are making the hybrid work environment a permanent part of their network operations.
- Organizations desire consistent connectivity, performance and security in a home office or in-office workstation.
- Traditional network security needs to adapt to hybrid work, with consistent policies applied no matter the users' locations.

Recommendations

I&O leaders supporting cloud and edge infrastructure users should:

- Reinforce operations by adopting minimum connectivity standards for home and corporate office scenarios.
- Optimize availability, security and performance for home office workers by enabling dual tunneling with secure web gateway (SWG) protection, and layer on backup and network optimization options.
- Improve visibility and user experience for home office workers via products such as lightweight SD-WAN appliances that provide additional traffic prioritization and enterprise-grade security.

- Bolster network security by evolving toward zero trust network access (ZTNA) principles.

Strategic Planning Assumption

By 2026, 75% of workers will continue to split time between home and traditional office locations, down slightly from 77% at the height of the pandemic in 2021.

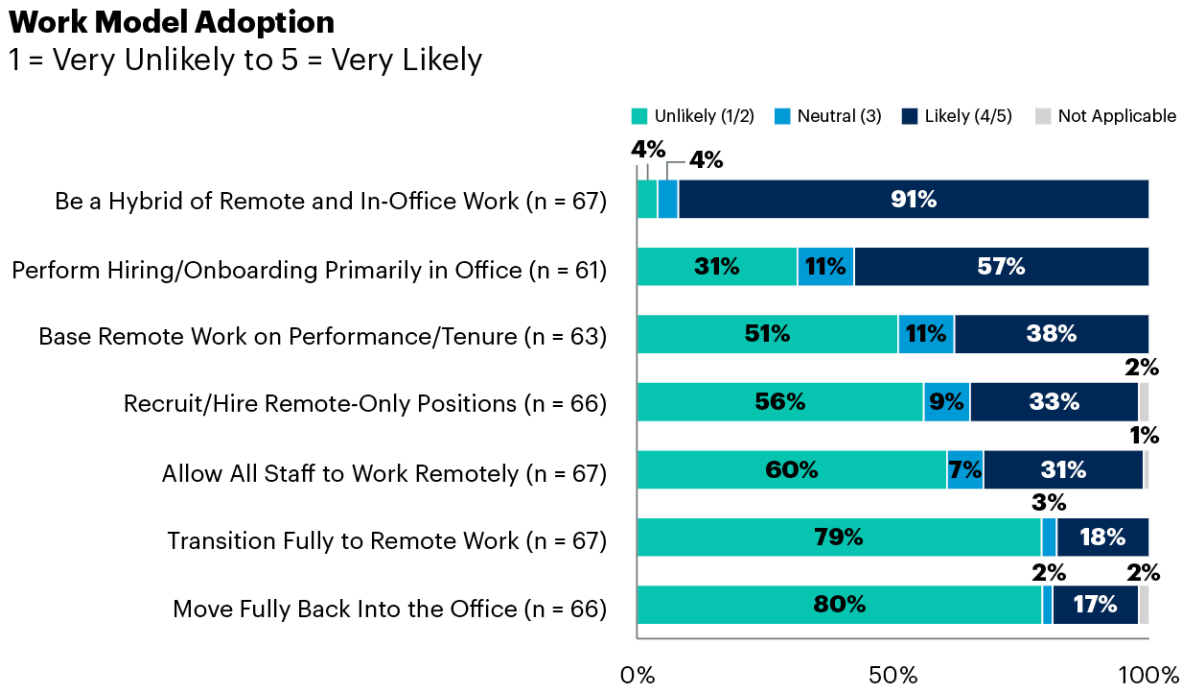
Introduction

With many of today's workers permanently splitting time between home and traditional office spaces, I&O leaders must evolve their connectivity strategies to fit this hybrid work model.

For this reason, IT leaders must treat remote user connections as an integrated WAN extension. In this architecture, all users no matter their location, are supported by minimum connection and performance standards based on type of work, endpoint and application requirements, and integrated and uniform security policies.

Based on the 2021 Gartner Work From Home Survey, hybrid home-office work arrangements will continue long after the current pandemic recedes (see Figure 1). Indeed, hybrid work — with the flexibility to move from home to traditional office environments — gives organizations operational immunity against disruptions from future pandemics.

Figure 1: Vast Majority of Respondents Adopting Hybrid Model of Work



n = base varies; excluding "don't know"

Q. How likely is it that your organization plans for the following work models?

Source: 2021 Gartner Work from Home Survey; Gartner's Research Circle members

Note: Percentages may not add to sum due to rounding.

765086_C

Gartner

This research focuses on the knowledge workers who primarily split time between home and office locations, and only occasionally travel for business. However, most of the advice in this document is also applicable to full-time, home-based workers such as remote contact center agents.

Analysis

Establish Minimum Home and Corporate Office Connectivity Standards

To optimize network performance, I&O leaders must set minimum network connectivity standards for remote work. This includes recommended standards for network performance, such as bandwidth upload and download speeds. For example:

- **Persona:** Standard knowledge workers using office productivity suites, CRM, web-based apps and unified communications as a service (UCaaS), including video calls.
- **Minimum download speed:** 50 Mbps [1]

- **Minimum upload speed:** 5 Mbps
- **Average latency:** Not more than 100 ms round trip (50 ms one-way) to key real-time communications POPs such as Microsoft Teams, Zoom and WebEX. Not more than 200 ms round trip to other application locations

These guidelines will suffice for most common work-from-home user-to-application scenarios, but it does not guarantee that *all* apps will work uniformly for *all* users. We recommend creating more specific guidelines for specific personas (such as financial traders, contact center agents, etc.) that include their associated network needs based on their application usage (high bandwidth, low latency, etc.). There will be variances based on geographic location, application bandwidth and packet performance requirements. Furthermore, we recognize that because of quality variations among local network providers, minimum service levels will not be available to all remote employees, particularly those in rural or less-populated areas. However, these guidelines can dramatically decrease the likelihood of performance issues.

To reinforce these minimum standards, I&O leaders should negotiate blanket service contracts with providers that cover substantial percentages of their user base. Discounts from bulk enterprise agreements usually result in per-user savings of 25% to 50% versus what individual employees would be able to negotiate on their own. [2]

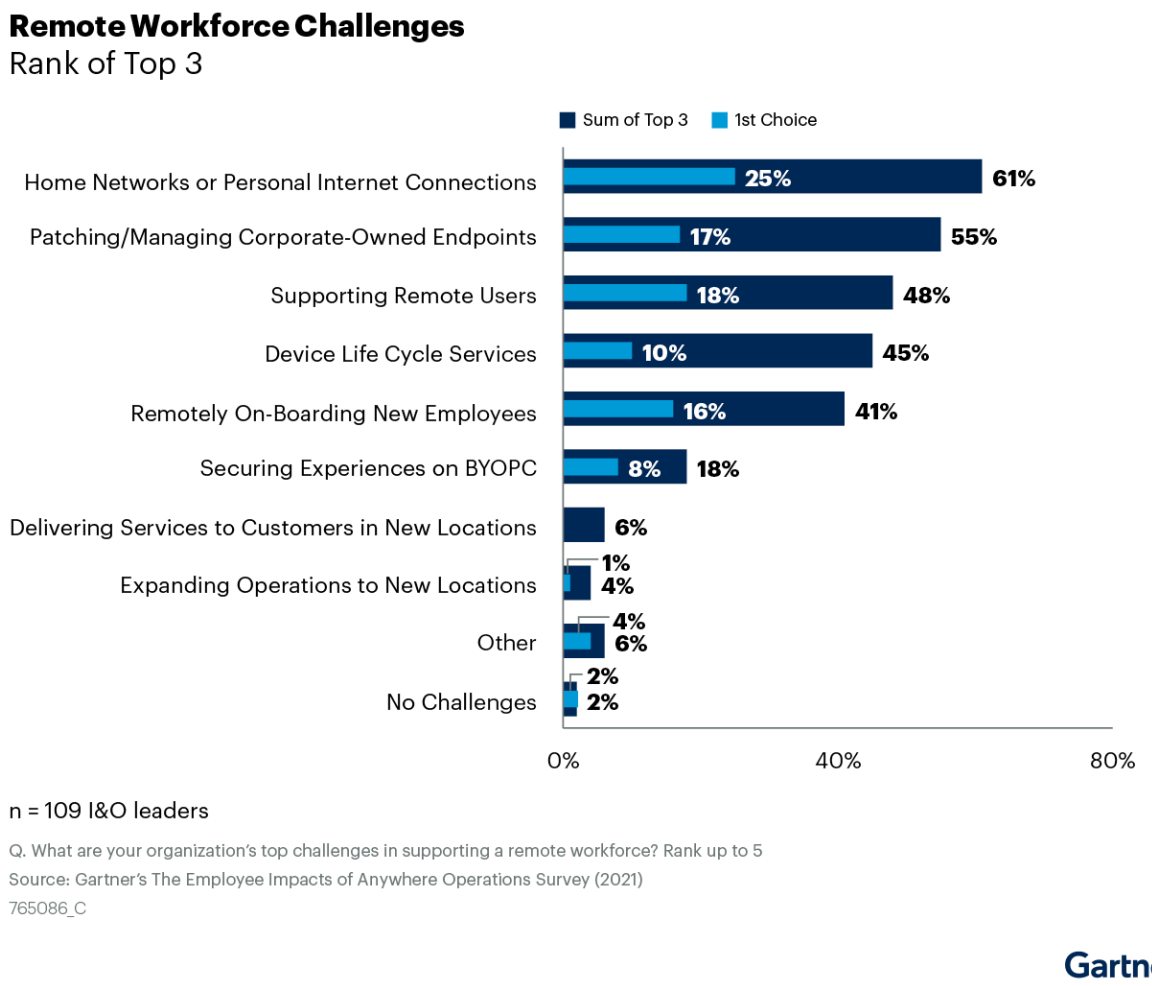
If blanket contracts are not possible, then I&O should fund and/or reimburse home internet broadband costs (at least 50% of employee costs). This may require co-funding via internal partnerships with finance or facilities. This is very similar in principle to issuing a mobile phone or laptop, and should be considered part of a work-from-home package.

The cost to the enterprise varies widely per geography and availability of services, but generally ranges $50 to $100 per month per household. For example, 1,000 users would equate to $500,000 per year if reimbursed at 50%. While this may seem high, it can be fully or partially offset by the reduction of costs for facilities, including real estate and security.

Optimize Availability, Security and Performance for Home Office Workers

I&O leaders see home networks as the top challenge in supporting their remote workforce, according to Gartner's 2021 survey, The Employee Impacts of Anywhere Operations (see Figure 2). [3] Fortunately, there are technology options that can improve home connections' availability, security and performance.

Figure 2: Remote Workforce Challenges



n = 109 I&O leaders

Q. What are your organization's top challenges in supporting a remote workforce? Rank up to 5

Source: Gartner's The Employee Impacts of Anywhere Operations Survey (2021)

765086_C

Gartner

Use Dual Tunneling to Decrease Network Traffic

Home-based workers use their connections for enterprise and private activities, generating additional network traffic. To improve performance, I&O users should enable dual tunneling. This diverts some SaaS application and activity traffic, such as visiting a news website or checking personal email from a corporate network. Dual tunneling also:

- Provides better performance for remote workers who access globally distributed cloud services
- Reduces bandwidth requirements for traffic funneled through the corporate network's security stack

With dual tunneling, personal data traffic does not pass through the corporate security stack. To eliminate this inherent security risk, organizations should employ dual tunneling with a cloud SWG. This adds controls that restrict access to malicious or unapproved sites (see Security Best Practices for Work-From-Home Scenarios).

Consider CDNs to Boost Security and Videoconferencing Performance

Content delivery networks (CDNs) have evolved beyond simple edge file storage and delivery to support web applications, APIs and enterprise security. Given increased work-from-home use of web conferencing, CDNs can be worth the additional cost for many organizations, as they accelerate video protocols, streamline access requests (request collapse) and reduce latency to improve performance.

Beyond conferencing, CDNs can improve API response and protection, ZTNA and control, secure access service edge (SASE) functions, and threat mitigation services (see Market Guide for Global CDN).

Improve Home Connectivity Uptime

With lagging repair times and “best effort” data speeds, home broadband connections can be a challenge when used for business connectivity. Not only does uptime for these broadband services hover in the 99% or less range, but also repair times can stretch into multiple business days — in contrast with office enterprise connectivity that is generally backed by far superior SLAs.

To better ensure uptime, organizations should invest in wireless backup services for high-priority home office workers via cellular-enabled routers or stand-alone hot spot devices. 4G and emerging 5G backup service options are increasingly available, often as part of discounted corporate service plans.

Resolve Connectivity Problems with Troubleshooting, Optimization Tools

Even where data speeds meet minimum thresholds, home broadband connections may still produce poor application performance. The result can be a flood of trouble tickets from home workers, placing a burden on organizations’ IT departments.

The root cause may lie in the worker's router, company-issued laptop, wired or Wi-Fi connection, the ISP provider's data throttling, data traffic volume capping policies, or performance issues at the server or application level. To efficiently identify and fix issues, I&O leaders should evaluate digital experience monitoring (DEM) tools that offer granular performance data across all device, connection and service domains. These tools are available stand-alone for $3 to $5 monthly per endpoint, but increasingly they are also being incorporated into select vendors' SASE solutions (see How to Monitor and Troubleshoot Remote Workers' Applications Performance).

Furthermore, I&O leaders can improve network performance for home-based workers via client-based network optimization tools such as software agents installed on devices. These tools can, among other things, adjust data compression and device configuration to boost performance. Tooling from vendors such as Cisco, Hewlett Packard Enterprise (HPE) and Replify are available and help to provide this capability.

Improve Visibility and User Experience

Consumer-grade and legacy small branch routers provide extremely limited visibility into application or network performance. Remote user support is challenging due to the degree of variability in the experience of remote users. These issues are addressable by deploying enterprise-focused products, including SD-WAN devices designed for individual and microbranch sites (see Magic Quadrant for WAN Edge Infrastructure).

Work-from-home users will not have full SD-WAN functionality, which requires at least two WAN connections to support dynamic path determination. However, they can still take advantage of other technologies intrinsic to SD-WAN, which will increase the capability to deliver improved application experience and performance over broadband internet connections.

SD-WAN solutions can improve application performance via several mechanisms that deliver cloud-based application and network protocol enhancements. For example, most SD-WAN appliances offer forward error correction for real-time applications, which can mitigate the impact of high packet loss. Finally, deep application- and policy-based routing capabilities prioritize and protect real-time and mission-critical corporate traffic over background traffic.

Because SD-WAN is a centrally managed routing platform, organizations can monitor the quality and overall status of work-from-home users through these microbranch appliances, which can typically support between five and 50 users each and are managed as any other WAN branch. As a result, application, performance, and security policies can be streamlined through a single interface, enabling ease of administration for thousands of users.

In addition to SD-WAN technologies, I&O leaders must invest in tools that can predict and detect issues that impact users — specifically DEM tools, as previously noted. These end-user monitoring tools enable consistent application experience and proactive troubleshooting capabilities (see Market Guide for Digital Experience Monitoring).

Bolster Security With ZTNA

The long-standing foundational technology for remote workers is traditional workstation-based VPN products. However, in the past few years, attackers have expanded tactics to exploit the increased number of work-from-home users. Traditional VPN implementations have shortcomings around security, flexibility and scalability that have created challenges for enterprises. Most of these challenges can be addressed by modernizing remote access to include ZTNA products.

ZTNA products provide secure connectivity for remote users and grant access to users based on the identity of user, device and contextual information, such as time of day or day of the week. When replacing legacy network-level VPN access, ZTNA enables a simpler way to configure contextual, risk-based and least privilege access to applications. Based on our analysis and client feedback, cloud-based ZTNA services improve the flexibility, agility and scalability of remote access. ZTNA is often delivered via consumption-based pricing charged on a per user per month basis, generally in the $5 to $10 (out-the door) range.

The ZTNA market has continued to mature and grow at a rapid pace, and there are many viable ZTNA offerings on the market (see Market Guide for Zero Trust Network Access and How to Select the Right ZTNA Offering). Refer to Security Best Practices for Work-From-Home Scenarios for an in-depth comprehensive analysis on this topic.

As a result, organizations should pilot ZTNA products for remote access modernization. We recommend phasing out legacy “full-tunnel” VPN implementations for users who don’t need full network access. We also recommend switching to cloud-based ZTNA services when refreshing traditional VPN solutions if there are limitations in capacity due to an expanded remote workforce.

Evidence

Organizations' adoption of hybrid work is based on Gartner research, including the **2022 View From the Board Directors Survey** and **2021 Work From Home Survey**. The Work From Home Survey was conducted online from 21 September through 1 October 2021 to reassess the impact of the pandemic — specifically, how well organizations are managing through increased remote work. In total, participants included 67 Research Circle members, 36 IT and Business Leaders Research Circle members, 16 Customer Service and Support Research Circle members, three Technology Provider Leader Research Circle members (tech CEOs) and nine from an open link. Respondents were from North America (63%), EMEA (22%), Asia/Pacific (9%) and Latin America (6%).

[1] Gartner analysts reviewed bandwidth recommendations from multiple sources including the U.S. Federal Communications Commission (FCC), and for specific applications including Microsoft Teams and Cisco Webex.

[2] This research draws on other research and client interactions.

[3] The **2021 Gartner the Employee Impacts of Anywhere Operations Survey** was conducted online from 4 May through 16 May 2021 to understand the current use and future plans of leaders in workplace I&O. In total, 109 IT and business leaders participated, coming from a range of regions, including: North America (47%), EMEA (35%) Asia/Pacific (9%) and Latin America (8%). Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Gartner Peer Connect Perspectives: Troubleshooting Network Issues While Working From Home

Future of Work Trends: Everything Goes Hybrid

Predicts 2022: Connecting the Digital Enterprise

Security Best Practices for Work-From-Home Scenarios
