Prepared for

CLOUD3RINK

Hybrid Workers Need Remote Connectivity That Balances Security and User Experience

November 2023 EMA White Paper
By **Shamus McGillicuddy**, Vice President of Research
Network Infrastructure and Operations

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

IT Organizations are Struggling to Support Today's Permanent Hybrid Workforce

While many high-profile employers have issued return-to-office mandates, remote work still dominates the economy. According to Enterprise Management Associates (EMA) research, 94% of companies have seen a permanent increase in remote workers since the COVID-19 pandemic.[1]

Hybrid and Remote Work is Expanding

Return-to-office policies aren't making a dent in the hybrid and remote work trend. The average enterprise IT organization reports that 43% of the employees it supports work from home, and that number will reach 49% by 2025. At the same time, 39% of remote workers in the typical enterprise are hybrid workers, meaning they split their time between a corporate office and a home office.

With hybrid and remote work permanent realities, IT organizations need to protect data while also supporting productivity. Thus, they need secure remote access solutions that provide protected connections with a good quality of experience. Unfortunately, only 32% of IT organizations claim to have been completely successful with supporting the connectivity requirements of remote workers.

The Hybrid Work Challenge

EMA identified several sources of pain when IT organizations try to support the connectivity requirements of hybrid and remote workers. First, 31% are struggling significantly with compliance and security risk. Applications and data that were once accessed only within a network perimeter are now accessed from hundreds or thousands of employees' homes. Legacy remote connectivity solutions are not robust enough to protect the network. Next, IT organizations tell EMA that IT leadership is undermining remote connectivity strategy (27%). CIOs and CISOs are failing to direct engineering and operations teams on what solutions to adopt.

[1] All research data cited in this paper was originally published in the August 2023 research report, "Modernizing Network Engineering and Operations in the Era of Hybrid and Remote Work."

Another fundamental issue is the lack of control over employees' networks (24%). Many hybrid workers have poor Wi-Fi setups and unreliable internet providers. Also, employees often have family or roommates who are also working from home and competing for bandwidth. Shortages of technical personnel plague 24% of IT organizations because there aren't enough engineers to implement and support remote connectivity solutions effectively. Finally, 22% are struggling with collaboration issues between silos. In particular, network and security teams are in conflict over what kinds of technology to implement for hybrid workers.

Meanwhile, hybrid work is pushing network teams to the breaking point. EMA found that 73% of network operations teams have observed increased workloads on staff since hybrid and remote work spiked during the pandemic. More than half of network teams reported that these remote workers have also slowed down their ability to resolve network problems.

"The increased workload came when we started doing hybrid work," said an IT manager at a mid-sized software company. "Now we're supporting both, keeping the office running and everyone's home setup."

With the network perimeter now expanding into employees' homes, network teams often lack control over remote connectivity strategy. Only 27% of network teams have significant influence over how hybrid and remote workers connect to networks. Instead, IT security usually sets the agenda. Network teams will need to partner with security and other groups to ensure that the right networking solution is adopted.

They will have to act fast because end users are demanding more of their networks. Eighty-nine percent of IT organizations observed increased usage of real-time communication applications over the last few years. Hybrid and remote workers rely on video and collaboration applications to remain productive and connected to coworkers. These applications are highly sensitive to poor network conditions.

The Path to Balancing Security and User Experience is Unclear

IT organizations have always strived to deliver services in a way that balances security and user experience. When it comes to remote and hybrid work, this goal is difficult to achieve. For instance, 20% of organizations tell EMA that they sacrifice security to protect the user experience of their remote users. Meanwhile, 46% sacrifice user experience in favor of security. Only 34% try to balance the two. Few pursue a balanced approach because organizations struggle to find a technology solution that can deliver it.

Vendors are approaching the issue of secure remote connectivity from several directions. The typical enterprise uses at least two solutions to cover all requirements. For instance, 61% still use a legacy VPN, a technology that lacks granular control over resources accessed through a network connection. VPNs are also vulnerable to stolen credentials – and they do nothing to support a good user experience. In fact, only 47% believe VPNs are effective for today's remote access requirements.

"We pushed [our VPN] out to everybody [during the pandemic]. We realized it was not something that we could sustain long-term," said the director of IT infrastructure for a multi-billion dollar media company.

As enterprises look beyond legacy VPN, they will discover myriad options. It can be difficult to know what direction to go. Forty-two percent of IT organizations are using a secure access service edge (SASE) solution for remote access. SASE combines multiple connectivity and cloud-based security technologies. The technology can be complex to implement, and the cloud-based security components can add latency to a remote connection.

Forty-two percent of organizations use secure direct access to a public cloud. This connectivity option is not applicable to assets hosted in a private data center, and it's also siloed to an individual cloud provider. Multi-cloud enterprises will find this option adds too much complexity. It also does nothing for user experience.

Zero trust network access (ZTNA), which 34% of organizations use, offers effective, granular access policies and controls, but the technology also relies on cloud-based gateways that can introduce latency. ZTNA also lacks the ability to optimize user experience.

More than 20% use SD-WAN solutions for remote connectivity. These solutions offer security and performance, but they're designed for connecting branch offices. They usually rely on hardware at the user's location, which can be expensive and difficult to manage at scale.

Hybrid Access as a Service Offers a Path Forward

IT organizations tell EMA that four factors principally drive their secure remote connectivity strategies:

- Employee productivity (45%)
- Security policies (42%)
- Employee satisfaction (39%)
- Operational overhead (33%)

Thus, the ideal remote connectivity solution must be secure, deliver a good user experience, and be easy to implement. Many solutions can address the security requirements, but very few can deliver on the latter requirements, especially in a software-only package.

Network teams should set the following requirements when seeking a remote access solution for hybrid workers. First, it should be cloud-native, adhering to the principles of simplicity, ease of deployment, and ease of user. By adopting an as-a-service offering for hybrid access, IT organizations can ensure that they can operate their networks efficiently.

Next, of course, the solution should be highly secure. IT managers should be able to design and enforce access policies easily, with granular controls over how and when users can access certain assets. This solution should adhere to zero trust security principles of least privileged access.

Finally, the solution should enable high performance connections. This is difficult to deliver over the home internet connections of remote workers, but solutions exist that can enhance experience in software via optimal path selection, preemptive packet recovery, traffic and protocol optimization, and other techniques.

Given the wide variety of solutions that enterprises use today to address secure remote connectivity, some IT organizations may struggle to navigate the market and find something that can address these requirements. EMA suggests a focus on hybrid access as a service (HAaaS) that meets the requirements described.

To see an example of HAaaS in action, check out this **case study** from Cloudbrink.

About Cloudbrink

Cloudbrink brings the industry's first high-performance secure connectivity to the modern hybrid workforce anywhere in the world. The company uses AI and ML to provide edge-native hybrid access as a service (HAaaS). HAaaS delivers accelerated performance for cloud, SaaS, and data center applications.

Cloudbrink's software-only solution includes the world's first personal **SD-WAN** with high-performance zero-trust access (**ZTA**) and **Automated Moving Target Defense** (AMTD) security. With the ability to use thousands of dynamic PoPs called FAST edges, Cloudbrink provides an in-office experience with a 30x increase in application performance and reduced operational complexity for network, security, and IT administrators.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com**. You can also follow EMA on **X** or **LinkedIn**.

This report, in whole or in part, may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2023 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common law trademarks of Enterprise Management Associates, Inc.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4362.110223