zscaler™

White Paper

How Security and User Experience Can Power Your Hybrid Workforce's Productivity

Introduction

The future of work is hybrid. Many organizations undertook rapid technology transformation to allow for remote work during the past three years, but it's now clear that both remote and on-site working models have their benefits. The sudden shift to work-from-home taught business leaders that there's real value in what they were missing: face-to-face collaboration to improve team-building and strengthen organizational cultures. At the same time, though, decision-makers have learned that remote work can support high levels of productivity while making it easier for employees to maintain work-life balance.

In order to get the best of both worlds, many businesses are now calling employees back into physical offices some of the time. But they're doing so in ways that are more flexible, adaptable, and varied than ever before.

As many as 77% of businesses have adopted permanent hybrid work policies, with the most popular scheduling model being hybrid–at–will, in which employees get to choose which days they work in the office. The biggest benefit of this model is that it maximizes flexibility for employees, leading to higher job satisfaction rates and, often, greater productivity.

Improving productivity and promoting job satisfaction is especially important today, when demand for highly–qualified knowledge workers continues to outpace their supply. Despite ongoing economic uncertainties, the current labor market remains historically tight. Data gathered by the U.S. Chamber of Commerce shows that there are more than 10 million job openings in the U.S., with only 6 million unemployed workers available to take these jobs. As a result, companies of all sizes, across all industries, are struggling to fill positions ranging from front–line workers to the C–suite.

The current labor shortage makes it absolutely imperative for organizations to provide their users with technology–enabled experiences that will contribute to job satisfaction and productivity, both when they're in the office and when they're working from home or other locations.

However, not every organization has created a long–term strategy for ensuring that all employees, no matter where they're located, are able to access all the applications they need to get their jobs done—a strategy that will allow for seamless, secure access, and a consistent experience, regardless of whether apps are hosted in the cloud or a private data center.

What's needed are new solutions that ensure great user experiences while also protecting organizations against cybersecurity risks. As organizations settle into building longer–term working strategies, it will be particularly important to ensure that both remote and in–office employees have equally good experiences and equally strong protections (and that these remain consistent as people move back and forth between working from home and working on site).

Securing the Hybrid Workforce: What's Needed

In the past, technology stakeholders often thought of robust security and ease of access to resources as desirable aims that were inherently at odds with one another. Nowadays, modern cloud–based solutions make it possible to provide users with fast, seamless application access without compromising on security. And IT leaders can enable always–on threat protection and low–latency connectivity no matter where employees are located.

In the race to enable hybrid work adoption, such solutions make it possible to meet the two main requirements for success by allowing for both **security** and **high–quality user experiences**. Let's take a closer look at what's involved.

User experience

Traditional hub-and-spoke networks weren't built to meet the needs—or enhance the productivity—of the hybrid workforce. In networks designed according to this model, security policies are enforced by a stack of security appliances and firewalls located within a central corporate data center, and all traffic has to be routed through this hub. Backhauling traffic in this way slows application performance, which is especially problematic for today's video conferencing software and other modern collaboration tools. These don't work well when there's latency, but they're increasingly central in daily workflows.

Traditional security architectures simply cannot support effortless remote access to resources. Instead, there's a need to implement cumbersome solutions like virtual private networks (VPNs) with complex login workflows. This means that, by necessity, remote workers will have to access business-critical applications and other resources in ways that are very different from what they'd do in the office.

With increasingly distributed workforces, it's also becoming more and more difficult for IT teams to track and resolve issues impacting end users. Existing tools for device, network, and application monitoring can only see fragments of the application delivery chain. This means that there are blind spots between the user's device and the app, and, in order to gain visibility, IT operations and service desk teams have to manually export and correlate data from multiple tools. The end result of this lack of end-to-end visibility into digital experience is that IT teams are forced into "firefighter mode." They're constantly struggling to resolve problems after they've been reported, rather than being able to proactively identify and resolve them before users are impacted.

What's needed is a solution that provides fast, seamless access to the internet and private and software-as-a-service (SaaS) applications from anywhere, making it possible to provide the best possible user experiences to all employees at all times. From a technical perspective, this can be achieved through direct peering, which ensures the shortest-possible path between users and their destination applications. By eliminating the need for VPNs and firewalls, direct peering dramatically reduces latency.

Also needed are solutions that will empower IT teams to monitor digital experiences in real time, so that they can immediately see what end users are experiencing. This makes it possible to optimize performance before users even notice issues.

Security

The large-scale adoption of remote work has led to an explosion in the size of the attack surface as many new devices attempt to connect to corporate networks to access resources. Threat actors are now setting their sights on oversubscribed VPNs and firewalls, looking for ways to circumvent the limited protections they provide. Once they do, they'll have full access to the network and all resources within it, leading to the potential exposure of the organization's most valuable data assets.

For effective breach prevention in today's complex computing ecosystems, it's time to eliminate the concept of access to the network as a whole. Instead, access should be granted only to individual applications, one at a time, as needed. This is consistent with the principle of microsegmentation, which is a core concept within the zero trust security approach. Adhering to this principle not only eliminates the possibility of lateral movement — when threat actors use

a single compromised account as a springboard from which to access other corporate resources — but also makes it so that applications aren't discoverable on the public internet. In essence, this eliminates the entire attack surface.

Legacy firewalls are incapable of detecting threats in encrypted traffic, though most attack traffic is encrypted nowadays; a new approach that can inspect all traffic, regardless of where it originates or where it's going, or whether devices involved are employee-owned or corporate-owned, is now critical for effective data protection.

New solutions are also needed that can enable security teams to enforce consistent data protection policies seamlessly, even across complex distributed environments.

The Zscaler Zero Trust Exchange: Enabling Universal Zero Trust Network Access for Applications and Users Everywhere

Growing numbers of organizations are adopting zero trust to secure their newly hybrid workforces. To help these organizations provide employees with secure access to the applications they need to stay productive — while minimizing costs and complexity — Zscaler built the Zero Trust Exchange. Designed to deliver zero trust security at enterprise scale, the Zero Trust Exchange makes it possible to enforce the principle of least-privileged access and to ensure that no user or application is ever inherently trusted, all from within a single platform capable of securing all user, workload, and device communications over any network, anywhere.

ZTNA for the Hybrid Workforce

Zero Trust Network Access (ZTNA) is a concept that's rapidly grown in popularity over the last few years as organizations look to reduce security risks while supporting hybrid and remote workforces. First introduced by analyst firm Gartner, the idea behind ZTNA involves creating an identity- and context-based logical access boundary around corporate applications and resources. To enforce this boundary, ZTNA services broker connections between authorized users and applications, granting access only in accordance with zero trust-based security policies.

The benefits of ZTNA far exceed its ability to replace VPNs, though, extending to users connecting from office locations as well as remotely. In Universal ZTNA, users enjoy the same degree of zero trust-based security whether they're working on-site or at home.

Achieving Universal ZTNA means that ZTNA capabilities have to be extended so that they work equally well for both on-site and remote users, ensuring that there will be no difference between their user experiences or security. To accomplish this, a solution must be able to provide the same direct, secure, user-to-application access both in the cloud and for local users accessing applications hosted in the corporate data center.

The Zero Trust Exchange is a cloud-native platform that brokers fast, secure connections to the internet, private, and SaaS applications from on-site and remote locations, while providing the best possible experiences for users and admins alike. The Zero Trust Exchange was built to balance user experience and security by offering:

- Fast, seamless access from everywhere: The Zero Trust Exchange ensures that traffic always takes the shortest path between users and destinations by taking advantage of direct peering with SaaS applications, and access via the broker that's closest to the user while eliminating the need for VPNs and firewalls.
- Reduced risks to the business: By providing direct access to applications, the Zero Trust Exchange enforces microsegmentation, creating one-to-one connections between users and applications to reduce the attack surface and prevent threats from moving across the network even if user accounts are compromised.
- Flawless digital experiences: With the Zero Trust exchange, IT teams can get ahead of poor end user experience by monitoring digital experiences to optimize performance. This makes it possible to rapidly fix any application, network, and device issues before they impact productivity.

The Zscaler Zero Trust Exchange is the perfect solution to achieve Universal ZTNA, especially now, with the introduction of the Zscaler Private Access (ZPA) Private Service Edge. The ZPA Private Service Edge extends all the benefits of the Zscaler Zero Trust Exchange to private apps hosted in the corporate data center. By extending the full set of Zero Trust Exchange capabilities to the private data center or public cloud edge, ZPA Private Service Edge makes it possible to reduce latency and improve application performance for in-office users as well as enforce zero trust security policies. With the ZPA Private Service Edge, these policies are enforced as close to the edge as possible, enabling both local and remote users to enjoy identical experiences, whether they're accessing apps in the data center or in the cloud.

The Zscaler Zero Trust Exchange enables organizations to realize a true zero trust security posture, and to do so in a way that's cost-effective and efficient, and that meets the full spectrum of security and performance needs of today's hybrid employees.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that 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. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com