ePlus Whitepaper

Where Technology Means More®

Rethinking Remote Work

Contents

Problem Statement

Blended work environments are here to stay. Not every company or industry will go all in with remote, every industry will need to adapt to support it at some level. Even those organizations dead-set against remote work must consider how to account for it within business continuity strategies.

Long gone are the days of extending Virtual Private Network (VPN) access to the corporate network and issuing a laptop. Users and customers demand more. Delivering a downgraded work experience equates to downgraded productivity and profitability. Work must be extended without productivity degradations, ensuring remote work doesn't drag down the business.

Background

Remote work has roots as old as the internet boom, but has been gaining serious traction over the last decade. 2020 accelerated this with global challenges that catapulted remote work into the headlines, literally. This headfirst dive into remote work left many companies ready to embrace it permanently. Those that chose not to embrace it have still been forced to address it for special cases, and emergency situations.

Delivering remote work effectively requires the integration of identity, security, connectivity, and quality across a spiderweb of distributed users and resources. This distributed system lacks central points of control for IT staff to provide security, visibility, and quality controls. Simply spending more on VPN access to centralize this traffic is a less than ideal solution.

Remote users don't typically need wide open access to everything. Instead, they need specific resources at specific times. Opening the corporate network wide open with VPN access goes against modern security principles like Zero Trust and Defense in Depth. It also adds network chokepoints and latency that decrease user experience.

Modern solutions must work inside out to drive productivity and job satisfaction from remote teams. Solutions must start with how the user interacts with their team and their customers.

How do they collaborate? From there, the scope expands into ensuring that user's identity, and using it for security authorization across corporate assets. This continues to radiate out through network connectivity to the applications. Today, those applications live in a mix of private and public cloud resources.

Traditional security and networking architectures don't stand up to this two-sided distribution. More diverse and adaptable solutions are required, leading a push towards software defined. Systems supporting this type of distributed work must have deep visibility and robust adaptability.

This complex mix of integration points require a ground up rethink of how we deliver remote work, and what user experience should look like for different users. Solutions need to address integrating remote and office work. This includes both creating balance between those in the office and remote, and users who switch between the two.

Solution

The solution is designing groups for your user types. As not all users are created equal, we usually recommend selecting three groups. This provides options without unnecessary complication. Typical groups are Software-as-a-Service (SaaS) users, average users, and power users. Each group requires a different set of tools, and a standardized technology package can be defined from there.

For productivity, users will rely on collaboration architectures like Cisco Webex and Unified Call Manager (UCM) cloud. These tools provide seamless collaboration from the cloud, greatly reducing management overhead. Integrating Webex into workflows provides consistency between office and remote work. This allows teams to collaborate effectively as the workforce continues to blend.

SaaS users are relying on secure web connections to access cloud applications. Because these applications are naturally distributed, there is no specialized connectivity need. There is a need to secure the system, verify the user's identity, and share that identity with a Single Sign On

(SSO) system. Utilizing Cisco's security architecture and solutions, like Advanced Malware Protection (AMP), protects the user and device while Cisco Duo verifies identity and Cisco CloudLock manages access. A layer above this is Cisco Umbrella, which provides security at the DNS level.

Average users receive all of the security of SaaS users, but may require VPN access to the corporate network as well. Utilizing Cisco AnyConnect, users can authenticate to Duo, then securely authenticate and connect to enterprise resources. Once connected, these users will have access to authorized services as if they were connected in the office.

Power users can rely on 'always-on' connections by extending Cisco's enterprise architectures through SD-WAN or campus wireless directly to the users' home. This provides a 'branch-like' experience allowing users to authenticate and connect devices natively to corporate wireless, and have that traffic securely tunneled via their broadband connection. This extends the features of power users even further and can be combined with video conferencing like Cisco's Webex DeskPro.

Bridging the connectivity from users across public and private cloud resources requires a new approach. A software defined approach. Utilizing Cisco's SD-WAN public and private resources are integrated seamlessly, allowing faster cloud access as well as simplified distribution. This also provides the central visibility required to architect modern security. This is exactly why the Cisco security suite discussed above can be integrated directly into Cisco SD-WAN.

SD-WAN provides the centralized connectivity and manageability combined with zero-touch provisioning allowing for extremely agile IT operations. This allows rapid response to a change in business or mission requirements and simplified scale out of remote users, edge computing resources or new connections around the globe. Cisco's SD-WAN architecture also provides the foundation required to drive Secure Access Secure Edge (SASE) environments by integrating security control into a converged platform.

With SD-WAN in place, operations teams gain visibility into the distributed spiderweb of users and resources. This visibility translates into benefits in user-experience and security. With integrated delivery of applications to remote and office user's IT teams, it can be responsive to user needs and network performance issues.

Conclusion

Building the right remote work environment has moved from fantasy to reality. Luckily, the tools to do so effectively have matured quite a bit. The key to building remote teams effectively is empowering them with the right tools to collaborate, while providing transparent security to keep your data safe. Finally, it requires layering in modern networking practices in the form of SD-WAN in order to provide the visibility and security required.

The ePlus team has plenty of experience helping customers design and deploy remote work strategies. Our team of seasoned architects and engineers can help guide you through the current recommended practices and assist in defining the right remote work environment for your business.

Leveraging Cisco's industry leading technology portfolio, ePlus can help you design the right solutions for your team.

References

1. Cisco – https://www.cisco.com/c/en/us/products/security/secure-remote-worker-solution.html
2. Cisco - https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html