vmware

Optimize Your Network for the Distributed Workforce: Eight Ways to Win

The events of early 2020 created the largest remote work pilot the world has seen. Shelter-in-place mandates meant most everyone worked from home, with employees striving to stay connected and productive. Meanwhile, IT teams scrambled to spin up infrastructures that could support their unplanned work-from-home staff.

Now, many organizations are realizing that there are benefits to having a distributed workforce—if they can solve the biggest technology challenge that remote work presents: network access and management. Remote workers have been wrestling with a plethora of network-related problems, from overly complex login and authentication processes to slow-running apps. IT teams have been struggling to secure and optimize a suddenly perimeterless network that is being accessed from unknown devices and unknown locations.

This eight-point checklist covers VMware Future Ready™ Workforce Solutions for optimizing the remote employees' extended network for improved user experience, performance and security.

1. Verify what isn't visible.

With a distributed workforce, the network security perimeter has vanished. Most users are outside of the firewall, which means you are relying on usernames and passwords for data protection.

Solve for this by implementing a Zero-Trust security approach to access. This "never trust, always verify" strategy ensures continuous verification and limits access from end to end, thereby reducing the attack surface wherever possible. Opt for a digital workspace platform, such as VMware Workspace ONE®, then use conditional access policies through VMware Workspace ONE® Access that take device health into account. You can do this through unified endpoint management (UEM), mobile application management (MAM), lightweight forms of device registration, or integration with a modern security platform.

2. Update how you authenticate.

When employees are remote and using personal devices, connecting to on-premises apps can be complex and convoluted. Think multiple multifactor authorization prompts and similar sources of frustration. Figuring out which password is for what app and then navigating cumbersome login processes can make accessing apps feel like a full-time job. And end users aren't the only employees impacted by complex authentication requirements. IT help desk teams around the world are receiving unmanageable numbers of trouble tickets requesting password resets.

What's the solution? App federation and conditional access. Federation is a process in which one single system is responsible for the authentication of a user. Federation at scale allows distributed systems to work together. When you federate your apps and enable them with single sign-on, you can provide a seamless authentication process for remote workers.

3. Make last-mile connections a first priority.

Remote workers might be experiencing slow connections as a result of other people in their household or neighborhood hogging bandwidth with nonstop video conferences or Netflix bingeing. We all know that when the network slows, frustration spikes and productivity can plummet.

One problem is that traditional network configurations require software-as-service (SaaS) apps and apps with cloud connectivity to be routed back to the data center. This can lead to VPN congestion, performance problems, and a poor user experience. SD-WAN, however, can positively transform user experience for critical business apps and solve for slow last-mile connections. VMware SD-WAN by VeloCloud®, for example, classifies and prioritizes real-time apps over others during network congestion or brownouts. This solution uses SD-WAN Gateways to route SaaS and infrastructure-as-a-service (IaaS) application traffic to the provider's front door without unwanted backhaul.

4. Change the way you WAN.

Organizations are using virtual desktop infrastructure (VDI) to deliver apps more effectively to their work-from-home staff, primarily because it provides flexibility and ease while maintaining security.

But these benefits can be compromised by poor remote display performance, which can happen when virtual applications and desktops are delivered across a WAN that suffers from limited bandwidth or poor connectivity.

Here again, VMware SD-WAN shines strong. It simplifies WAN deployment with a cloud-delivered model that is easy to deploy and manage. VMware SD-WAN also prioritizes VDI streams over noncritical traffic during times of congestion. The use of replicating packets ensures that users don't suffer session loss during brownout conditions caused by packet loss.

5. To make legacy apps fly, use VDI.

Employees are likely to find that their at-home experience with legacy client-server apps doesn't mirror their in-office experience due to latency and bandwidth challenges.

If remote apps are running too slowly, consider running them from your data center using VDI. You want a solution that simplifies the management and delivery of virtual desktops. That way you control, manage, protect and deliver apps at the speed that remote users require.

6. Modernize how you manage.

Legacy processes for OS updates and app distribution were designed when devices were primarily located in-network. While VPNs are sufficient for occasional connections, they simply can't scale to support a remote-first workforce. As a result, it can be problematic to push security patches and app updates from traditional on-premises PCLM solutions.

Fortunately, modern management can right these wrongs. VMware Workspace ONE enables modern management to simplify IT operations, harden security, and deliver ready-to-work experiences across every app and endpoint—physical and virtual.

7. Reach remote Windows devices with ease.

If you've always depended on your network and firewall to protect your Windows devices, your new-found remote workforce presents problems when it comes to ensuring security and performance. Once again, lack of visibility is the enemy, creating increased risk and decreased productivity for users.

SD-WAN, which has its roots in the software-defined networking practice of decoupling network software services from the underlying hardware, simplifies branch office—or home office—networking. The VMware SD-WAN solution offers secure segmentation to ensure that home-office users' apps and data aren't shared with other users on the network. Best of all, it includes a built-in firewall, but you can use a third-party security vendor firewall as well.

8. Keep cloud app traffic in the cloud.

If remote workers need to access cloud-hosted apps, why not connect them directly to those apps versus routing them to your data center, introducing unwanted latency and poor user experience?

The VMware SD-WAN solution includes SD-WAN Gateways that are hosted strategically at the nearest entry point to the cloud, such as Zoom, Salesforce, and VMware Horizon® on VMware Cloud on AWS or VMware Horizon Cloud on Microsoft Azure. Home users have low-latency, expedited access to all SaaS apps without the need to backhaul traffic to your data center before routing to the cloud destinations.

Support Your Anywhere Organization's Extended Network

Many organizations have traditionally viewed digital transformation as an opportunity for innovation rather than a requirement for resiliency. However, the largely unplanned shift to a distributed workforce model makes extended network performance and security a top-of-mind topic for everyone.

Learn more about VMware Future Ready™ Workforce Solutions that optimize your remote employees' extended network for improved performance, better user experience, and increased security, in our buyer's guide.