vmware®

HIGHER EDUCATION

Five Lessons Learned from the Pivot to a Distributed Workforce

Delivering Continuity and Scale with a Remote Work Strategy

Economic and social drivers are pushing remote work and learning into the forefront of every institution's agenda. It's a capability that can't be dismissed. The future of education demands that instructors, administrators, and those in support roles are fluidly able to move between in-person and online educational models.

The importance of facilitating remote work and learning is further amplified during pandemics, disasters, and other unforeseen events that force many educational institutions to give their employees the resources they need to stay productive while they are at home. But giving a large number of end users access to institutional resources *quickly* is no easy task. The ability to scale is also a hurdle to overcome. How can institutions ensure core systems are scaled to handle the load, how can they quickly scale up to meet changing needs, and—equally important—scale down later when the load on those systems subsides? There may also be additional challenges, such as supporting a wide variety of device types that may be managed or unmanaged. Network traffic and connectivity, as well as security, are other critical factors that need to be considered.

Given the circumstances of the recent global pandemic, institutions did the best they could to initially respond with the resources and technologies they had available. As we start to turn the corner on the initial "Respond" phase, it's time to reflect on what worked, what didn't, and how to plan for the future. As they say, hindsight is 20/20. So let's take a look at five lessons we learned when a majority of the campus-bound workforce suddenly shifted to a distributed one.

THE 3 PHASES OF DIGITAL PREPAREDNESS

RESPOND

Focus: Business Continuity for critical services, operations, and personnel

ADAPT

Focus: Resiliency to evolve systems, people, and processes to a new reality

ACCELERATE

Focus: Digital-First model for universities and IT, to build a sustained competitive advantage and harden against a future crisis

Lesson 1: Doubling Down on VPN? You Can Do Better

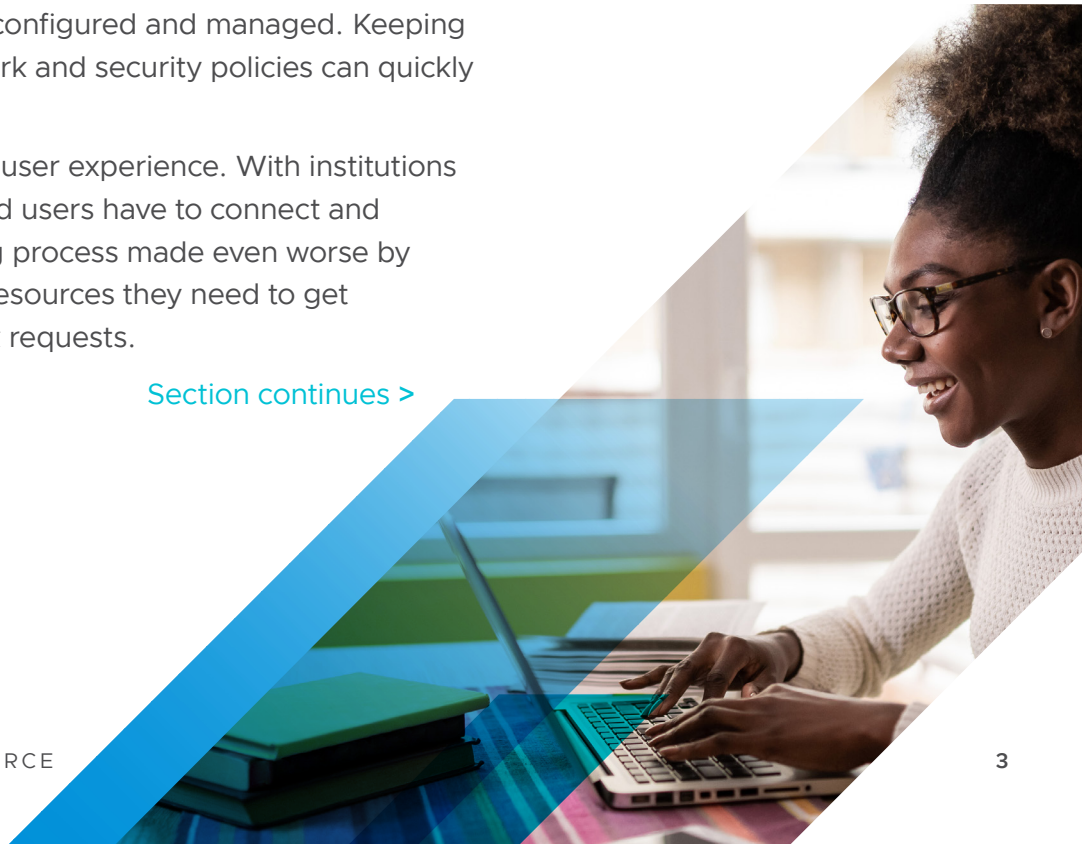
A common way for institutions to provide their users secure access to the campus network is through a virtual private network (VPN). Many organizations opted to expand their VPN to accommodate larger numbers of employees working from home. But VPN was never designed to handle the complexity of the way we work and architect our data centers today.

Security is a primary issue with VPN. Threats often piggyback on connections from insecure or unmanaged endpoints and, once able to penetrate the campus network, they get unfettered access.

In addition, VPN is difficult to manage. Increasingly complex architectures and distributed networks require more and more VPN appliances, each of which must be configured and managed. Keeping track of everything on the network and the corresponding network and security policies can quickly become complicated and even unmanageable.

The complexity of the VPN network also will likely lead to a poor user experience. With institutions hosting applications and data across various sites and clouds, end users have to connect and disconnect to these different servers—a tedious, time-consuming process made even worse by network latency. When VPN is the path between users and the resources they need to get their work done, any issues are going to lead to urgent help desk requests.

Section continues >



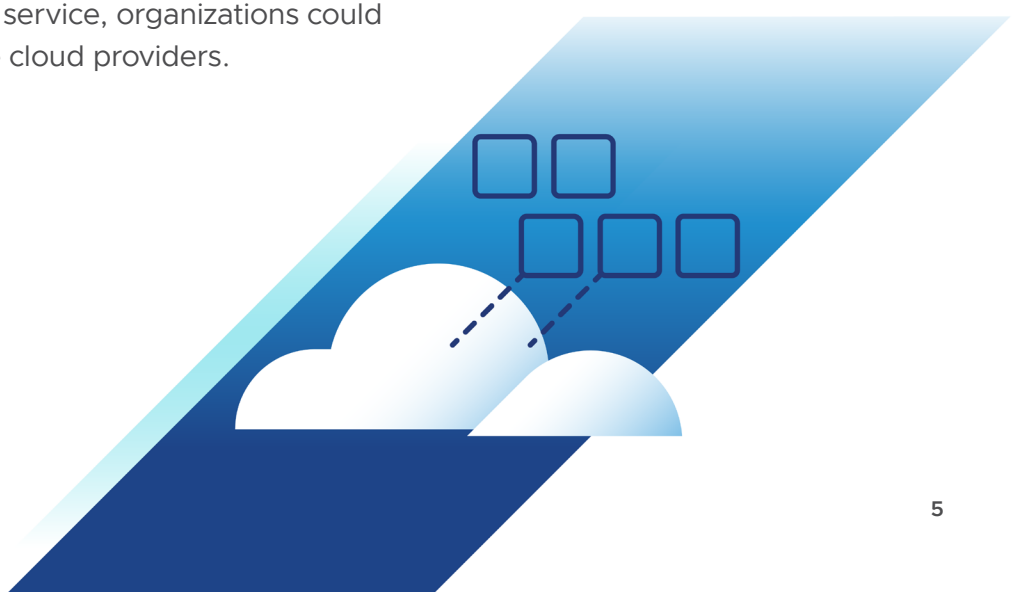
There are alternatives to VPN that more easily adapt to modern data center architectures. VMware Future Ready™ Workforce Solutions include *VMware Workspace ONE®*, a powerful digital workspace platform that provides secure and conditional access to the digital workspace, easily accessible by end users through single sign-on (SSO). Workspace ONE has an intrinsic approach to security with access to identity, device, location, and behavioral data that is synthesized in real time and used to make decisions about access to campus resources. Known as *Zero Trust Network Access*, this intelligent conditional access technology greatly reduces risk and simplifies management.

Many other institutions have chosen to bypass VPN by virtualizing their desktops and applications with *VMware Horizon®*, part of the Workspace ONE platform. Virtualizing desktops and applications in the data center enables end users to access their desktops and all their assigned resources through a browser or client on their endpoint. Horizon provides end users with easy access to their desktop and resources through SSO that is reinforced by multifactor authentication methods, including SAML, RSA, smartcards, and many more.

Lesson 2: Take Advantage of Cloud Resources to Quickly Boost Capacity

When the pandemic hit, institutions wanted to build or expand their existing virtual desktop and application environments quickly because they knew those environments would be a secure and manageable way to deliver resources to additional end users and use cases. The challenge was getting enough capacity to virtualize hundreds, if not thousands, of virtual desktops quickly. The ability to quickly burst into the cloud—or even multiple clouds—adds a whole new dimension of available capacity.

VMware Horizon has several deployment options that enable organizations to deploy on-premises, through hybrid cloud, or in a wide variety of public cloud options. Institutions can leverage *VMware Cloud™ on AWS* or deploy Horizon on *Dell EMC*, *Microsoft Azure*, *Google Cloud VMware Engine*, *IBM Cloud*, and many more partner clouds. Key hybrid use cases such as burst and Business Continuity and Disaster Recovery (BC/DR) are enabled by Horizon capabilities. These include the ability to create brand-new desktops on demand, in seconds, and to create a global entitlement across pods, sites, and clouds. Many institutions were able to easily expand their existing Horizon environments in days and, with Horizon Cloud providing desktop as a service, organizations could take advantage of offloading management to vendors and hyperscale cloud providers.



Lesson 3: Provide Flexibility to Support All Device Types

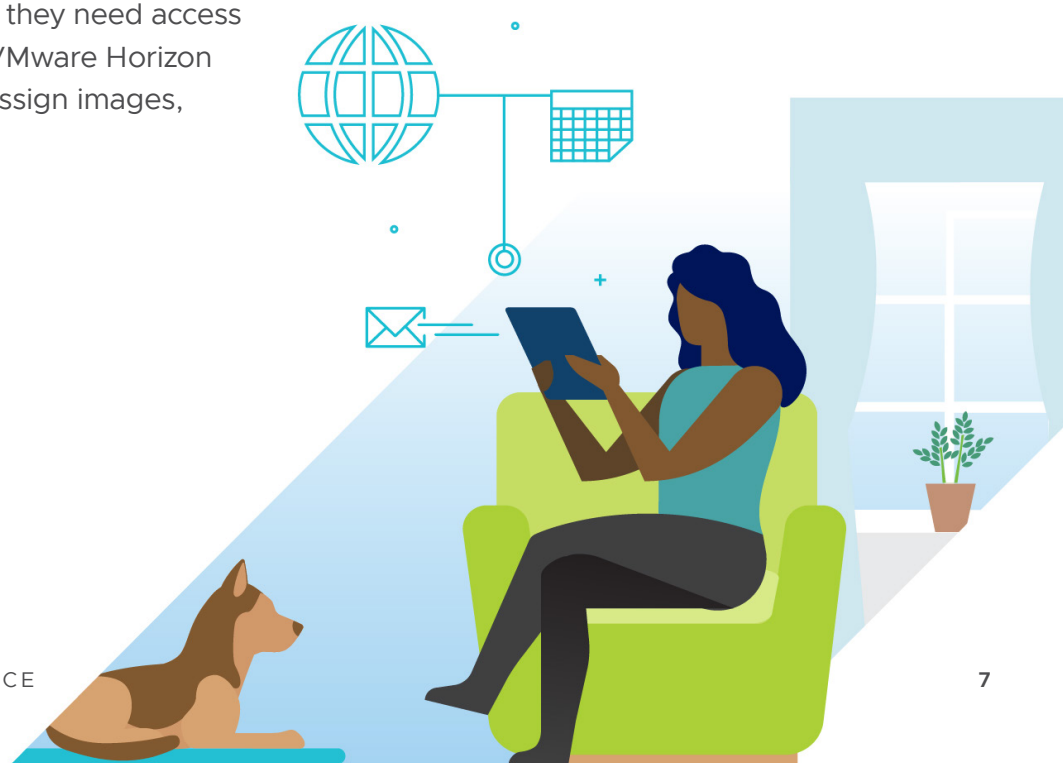
One day end users were on campus; the next day they were sheltering in place at home. If a student or an employee doesn't have a university-owned device, how are they going to securely access university resources? Institutions that wanted to purchase endpoints for their users were met with long lead times due to high demand and limited supply. Some allowed end users to use unmanaged personal devices, even though these devices pose a security threat if they are used to access the campus network.

It's best to have a strategy in place so you can easily support a wide array of device types and operating systems. There are a couple of ways to tackle this. One way is to provide the end user with a virtual desktop or virtual apps. Because end users are using their endpoint only to render the virtual desktop or virtual app, IT doesn't have to worry about securing or managing the endpoint. A virtual desktop or app solution also abstracts away the complexity of managing a wide variety of device types, operating systems, and versions. A complementary strategy is to leverage *VMware Workspace ONE UEM*, which allows admins to manage and secure a wide variety of endpoints, including mobile, desktop, rugged, and IoT devices. Workspace ONE in turn helps deliver a consistent experience that gives end users access to all their SaaS, web, and native apps from a single pane of glass.

Lesson 4: Don't Forget to Support All User Types

As students, faculty, and staff staff were forced off campus during the pandemic, some institutions found themselves scrambling to get certain groups of users the resources they needed. For example, power users like computer science professors and engineering students require high-powered workstations with graphics processing units (GPU).

A more agile approach is to provide power users with access to vGPU computing power through a virtual desktop, such as the virtual desktops offered through collaboration between VMware and partners such as NVIDIA, Intel, and AMD. In addition to enabling these users to work from any device, this approach enhances the security posture of the institution by keeping the IP in the data center and off the user's endpoint. It also allows end users to easily spin up multiple desktop VMs, which can be very useful if they need access to different operating systems as part of their environment. Last, VMware Horizon has powerful, centralized management tools that make it easy to assign images, apps, and resources to end users.

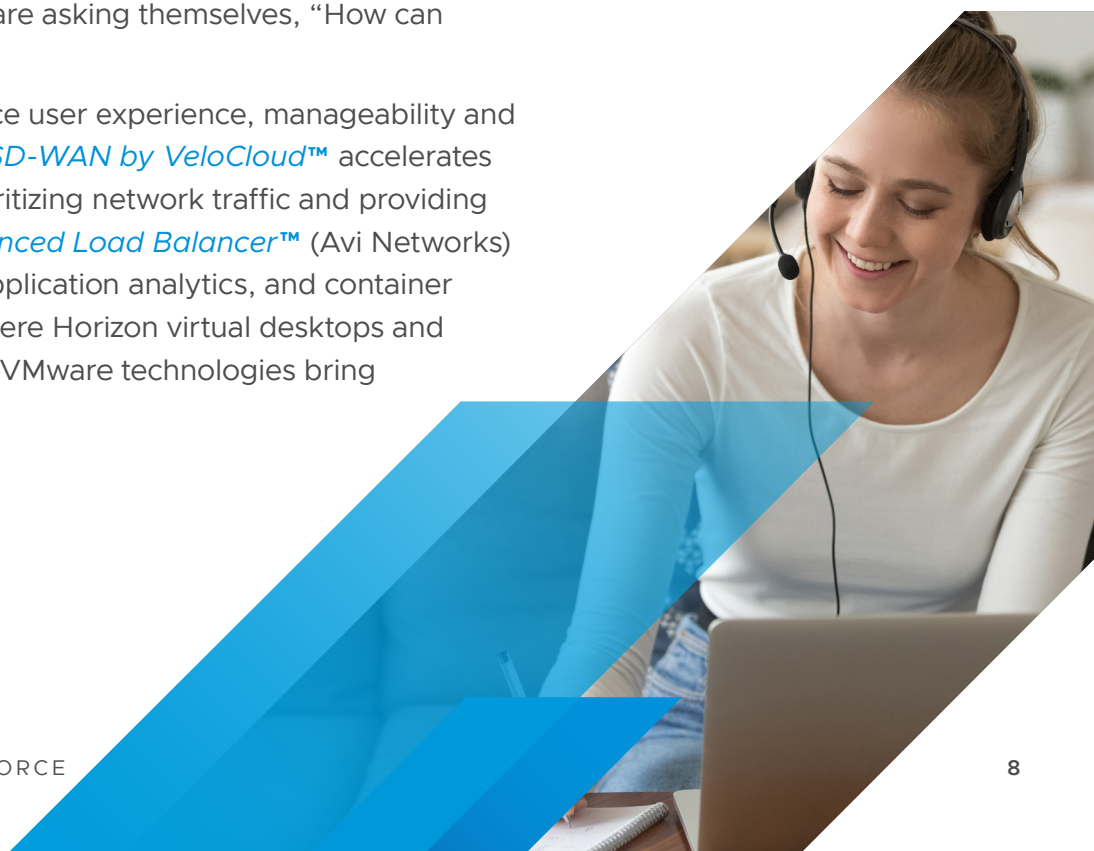


Lesson 5: Prioritize Exceptional User Experience, Manageability and Security to Quickly Scale

When the pandemic hit, many institutions asked, "What resources do we have available now, and how can we best put them to work?" Without a long-term plan in place, schools, colleges, and universities were often limited to doing more of the same: expanding their VPN to accommodate more users or extending their virtual desktop environment.

Assessing their situations after the Respond phase, many institutions are realizing that they have gaps in security, manageability, and user experience. And they are asking themselves, "How can we better position ourselves to respond in the future?"

An end-to-end approach with VMware technologies can enhance user experience, manageability and security across virtual desktop and app deployments. VMware *SD-WAN by VeloCloud*™ accelerates and ensures great virtual desktop and app performance by prioritizing network traffic and providing insights into app delivery across the WAN. VMware *NSX® Advanced Load Balancer*™ (Avi Networks) provides multi-cloud load balancing, web application firewall, application analytics, and container ingress services across on-premises data centers and clouds where Horizon virtual desktops and apps are hosted. These are just two of the many enhancements VMware technologies bring to Horizon deployments.



Get Started

Now is the time to take advantage of the lessons learned from recent unpredictable events to get ahead of the next crisis, and prepare for long-term success with a foundation of resilience and continuity that leads to productivity. Leveraging VMware Future Ready Workforce technologies like VMware Horizon gives institutions a long-term foundation and strategy to drive engagement and productivity through flexible hybrid and multi-cloud VDI and published app deployments. Organizations can quickly scale remote work efforts and deliver a modern and secure digital workspace for students, faculty, and staff to work from anywhere.

Take the next step toward enhancing your digital workspace journey. Learn how to plan for success in *Preparing Your Remote Work Environment for the Long Haul: How to design your environment with VMware Future Ready Workforce Solutions.* >

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com