vmware

Three Critical Strategies for a Digital Learning Environment

Three Critical Strategies for a Digital Learning Environment

Enabling remote learning with digital tools is the most critical conversation in education today, bringing IT and educators together to empower students.

Educational institutions, from K–12 school to colleges and universities, have long been places that embrace digital innovation. Now, in response to COVID-19, millions of students around the world have transitioned to remote learning. Digital learning technologies have been elevated from their already important role to being absolutely essential for nearly all forms of educating students, and teachers have been asked to be experts in a range of collaboration apps and technologies. Through the tireless and creative work of educators, IT administrators, and staff, students are adjusting to changes at unprecedented speed and having positive education experiences thanks to digital technology.

Transitioning to an education environment that is so heavily dependent on technology is not easy, though. Educators and IT administrators must support a wide variety of institutional and personal devices and operating systems—Android and iOS tablets, Chromebooks, macOS and Windows laptops—and various new software-as-service (SaaS) apps with web, native, and mobile clients. They must remotely support students and teachers with different levels of technology experience and comfort. By using a digital learning environment platform that comprises management capabilities for all devices, security controls, and access and identity controls, educational institutions can ensure that technology is readily at hand to support the learning process, anywhere, any time.

This brief explores how a digital learning environment strategy can provide the foundation for a positive technology experience and successful student outcomes. It addresses education-specific issues, including:

Elevating the student and educator experience

Implementing a zero trust model to protect all constituents

Adopting new ways of learning and teaching

Elevate the Student and Educator Experience

The experience provided by technology now plays an indispensable role in successful outcomes for students, as well as in supporting a positive work environment for teachers. Students often have varying levels of access to technology, and the parents and teachers that support them can have varying levels of experience and comfort when working with technology, as well. In many environments, a patchwork of different tools is used, resulting in gaps and a frustrating technological situation. Providing all students, faculty, and staff with seamless access to technology—with a consumer-simple, user-friendly experience—is key to enabling successful outcomes.

Successful onboarding

Giving students and educators access to their devices, applications, and data is a critical first step, but there are challenges that must be addressed for onboarding to be successful.

District- and institutional-owned device deployments are expanding rapidly, but when time is of the essence, legacy approaches like manual image provisioning are just not fast enough. Instead, automatic enrollment and provisioning workflows enabled by modern management techniques are needed.

Personally owned devices are often used as an alternative, but then application access and support can become more complicated. For example, teachers and students might only be trained on how to access an application on the institution's officially supported operating system. When remote learning orders go into effect, students might need to rely on a personal device at home. If the personal device has a different operating system than what teachers and students were trained on, the process of accessing an application can be different. Troubleshooting these access issues erodes valuable instruction time. If teachers and students also have to juggle multiple sets of credentials, additional time is lost.

To avoid access issues, students and teachers need to be able to find all their applications—including web, SaaS, mobile, and virtual apps and desktops—in one place, access them with single sign-on (SSO), and be able to switch contexts fluidly.

Delivering an exceptional student and educator experience

Imagine a world where a newly enrolled student is sent a preconfigured device and upon starting it for the first time finds SSO access to all the required applications in one location. Or, where a teacher is able to help students smoothly move from one task to another without technological distractions, even when students are using a variety of devices and operating systems. Or, a world where remote students can access high-powered virtual lab environments that support the most demanding design, engineering, and mathematics applications.

These scenarios are not far-fetched. Rather, it is possible today for countless organizations that support modern device management, access management, and desktop virtualization technologies. A modern digital education environment is critical in providing successful outcomes for students and positive experiences for educators.

Implement a Zero Trust Security Model

Keeping students safe is a top priority for everyone in the educational realm. In addition, schools and colleges must comply with national, state, and district-level guidelines and regulations, especially pertaining to what students can access and the privacy of student information.

Unfortunately, many traditional security and management tools were built on a perimeter-centric model that assumes that learning happens within a classroom, in a school building, or on campus, and these tools often focus on institutionally owned devices. In today's environment, this perimeter-centric model presents a host of issues. When students, faculty, and staff are remote, network-based filtering, firewalls, and other controls might not offer the appropriate protection. When learning and teaching takes place using personal devices not managed by IT, security policies and risk mitigations might not be in place. It can be impossible to fully manage and secure the full range of common devices and operating systems—including iPads, Chromebooks, macOS devices, Android tablets, and Windows 10 devices—with legacy client management platforms. Compounding all these difficulties is the tendency that security, identity, and client management tools are often in separate silos.

Moving to a modern digital learning environment requires modern management and security concepts, such as unified endpoint management and a zero trust framework.

- A modern unified endpoint management offering combines support for multiple device platforms, operating systems, and management modes into a single software platform. These modes provide full, tightly controlled management of institutional devices and options for device partitioning, application management, and device registration for personally owned student and faculty devices.
- While traditional security approaches focus on trusting all devices within a designated perimeter, the zero trust model considers all resources external and relies on continuous verification of devices, users, and applications to obtain access. For example, you can use conditional access rules to ensure that users can access resources only from devices that meet specified policies, regardless of whether the device is on or off the network.

IT administrators at educational institutions can also ensure secure remote access in a zero trust model by using virtual desktop infrastructure (VDI).

Adopt New Ways of Learning and Teaching

Educational institutions had very little notice when they transitioned to remote learning. The changes of 2020 have pushed the state of remote and digital teaching and learning to the forefront, fostering new ideas and creativity. In the future, the increased acceptance and usage of remote learning opens up opportunities for new educational models. In turn, these models can offer more equitable opportunities for all students.

To achieve the benefits of remote learning, schools and colleges must ensure equitable access to devices, applications, and Internet connectivity. Many students will need to be provided devices, headsets, and access to low-cost or free broadband support, LTE hotspots, or devices with integrated LTE connectivity.

To support these deployments, in addition to unified endpoint management and access management platforms, institutional IT departments might consider tools such as SD-WAN and telecom expense management. Other components of a digital learning environment strategy can include providing access to high-powered applications and workstations via VDI and remote support.

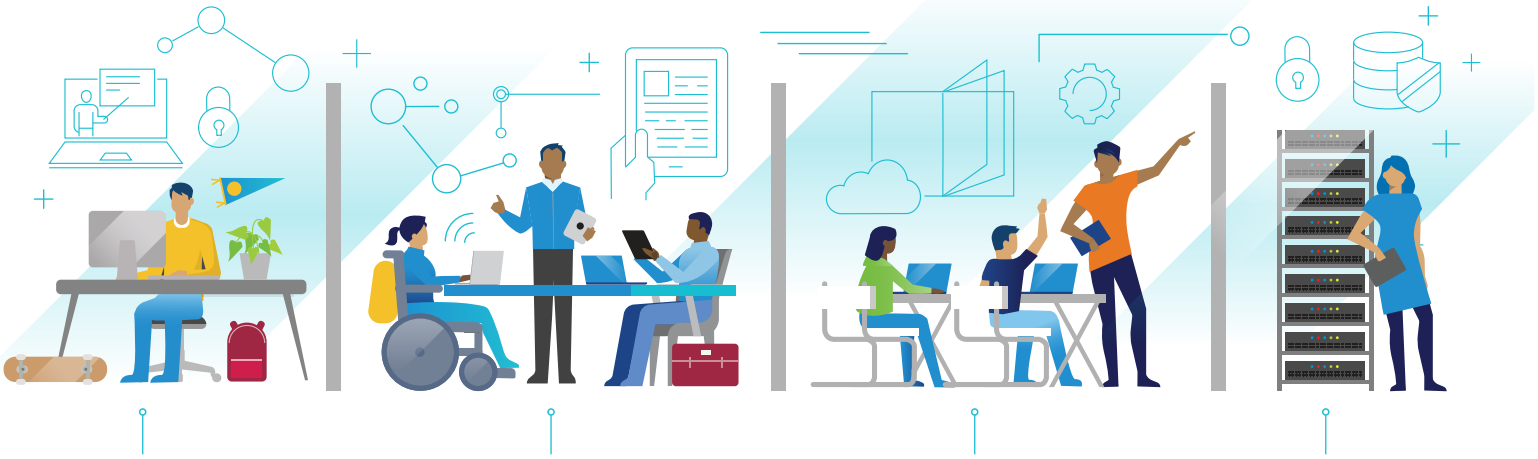
A secure digital learning environment is the answer. It can provide a centralized place to access diverse educational resources, with a rich and responsive experience that is consistent across all types of devices from any location.

VMware Workspace ONE: The Secure Digital Learning Environment

VMware Workspace ONE® delivers the flexibility and security required to meet the needs of a digital education environment.

Consistently ranked as a leader by industry analysts, Workspace ONE delivers best-in-class device management, access control, zero trust security, intelligence and analytics, and application and desktop virtualization to enable a rich learning environment anywhere.

With Workspace ONE, educational institutions can:



Deliver instruction from any device, any app, and any location

Increase student engagement by providing access to educational applications in a flexible digital learning environment, ranging from web and mobile applications to powerful virtual desktops

Create equal opportunities for all students by helping to deploy and manage devices and connectivity

Ensure student and educator safety through a zero trust security approach, providing privacy and protection from threats no matter where a device is used

The education environment is changing rapidly, and technology is one of the most critical aspects. VMware Workspace ONE is committed to providing the best possible experience for students and educators through a strong digital foundation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com VMW-WP-3CRITICALGOVL-USLET-20200617-WEB
6/20