HYPORI™
VIRTUAL MOBILITY

COVID-19-Related Remote Learning and The Use of Personal Mobile Devices

WHITEPAPER

Summary

As of fall 2020, the global COVID-19 pandemic continues to have significant economic, medical, social, and educational impacts. Shifts to remote operations and learning have meant changes for businesses, families, and children. When COVID-19 hit, nearly all US schools closed their doors and moved to a remote learning model. At the time, in the spring of 2020, this move was expected to last weeks. Weeks turned into months with schools remaining closed to in-person learning through the end of the 2019-2020 academic year.

Today, as US schools plan for the 2020-2021 academic year, **remote learning** is the new nationwide norm for nearly every school. At the heart of this issue is technology. When students are at home, they need access to the school curriculum, teachers, and classroom activities. Teachers and other staff need remote access to school networks as well. Remote education cannot be effective if all students, teachers, and other staff do not have access to information through secure, functioning mobile devices.

The Situation

As a result of COVID-19, few US school districts have announced on-time in-person reopening plans for the 2020-2021 academic year.

Instead, a large percentage of schools plan soft reopenings with weeks of remote learning before in-person instruction begins. According to a recent poll, **over 60% of school districts plan to offer a hybrid learning model** that is likely to last months if not the entire academic year, possibly depending on the timing of a COVID-19 vaccine. Concern for practical remote learning technology tools increases as remote education becomes a long-term reality for millions of students, teachers, and other staff.

Whether students provide their own devices or schools hand them out, mobile device use is on the rise. Many households currently own devices, others use school-issued devices, and others await their school districts' assignment. In 2020, US education shipments of laptops, tablets, and Chromebooks could jump by 27%, bringing the total number of school device shipments to 18 million, increasing 4 million units from 2019.

In addition to mobile devices, an active remote learning program means students and teachers can securely and seamlessly access virtual classrooms, lessons, homework, and other online learning tools. Students and teachers will participate in teleconferencing, share work, and connect to school servers daily. At the same time, remote administrative and IT staff need access to school network systems and data.

The Problem

As a reality in tens of thousands of schools nationwide, remote learning programs need tools, curriculum, and staff. While K-12 leaders address immediate priorities, including how to deliver high-quality remote instruction, how to reach and engage students online, and how to answer all users' technical questions, maintaining cybersecurity must be considered. Millions of devices, once connected to school district firewalls, will now remotely connect to district networks.

In May-June 2020, 61% of nearly **7.7 million enterprise malware events occurred in the education sector,** making it the most affected industry nationwide. As schools have shifted to remote learning due to COVID-19, criminals have an even greater opportunity for wrongdoing.

Because many K-12 IT departments rely on firewalls instead of cloud application security, and remote learning means millions of distinct access points to school networks and systems, cybersecurity issues are on the rise. This new education paradigm exposes schools to network-wide security concerns and a variety of cyberattacks. For example, according to the FBI, the COVID-19-related spike in phishing scams continues with malware introduction a common practice. When students, teachers, and administrators visit sites, click on links, or download material through unsecured home routers, the risks compound. Just one unprotected device could compromise the entire school network with unsafe file downloads and inappropriate site access wreaking havoc on a system.

Even for those school systems that use cloud-based applications rather than locally hosted software, thus safeguarding network servers, they have rushed to provide remote learning options and are often using untested cloud-based apps and services. These apps and services increase vulnerability and susceptibility to breaches. Outside of the school network, traditional next-gen firewalls and web content filters add no value. Without the right cloud security tools in place, cloud account takeovers are easier to accomplish.

Without an effective virtual device security solution, school networks, systems, and their data, including the curriculum, but also personnel records, student files, and other sensitive information, are at risk.

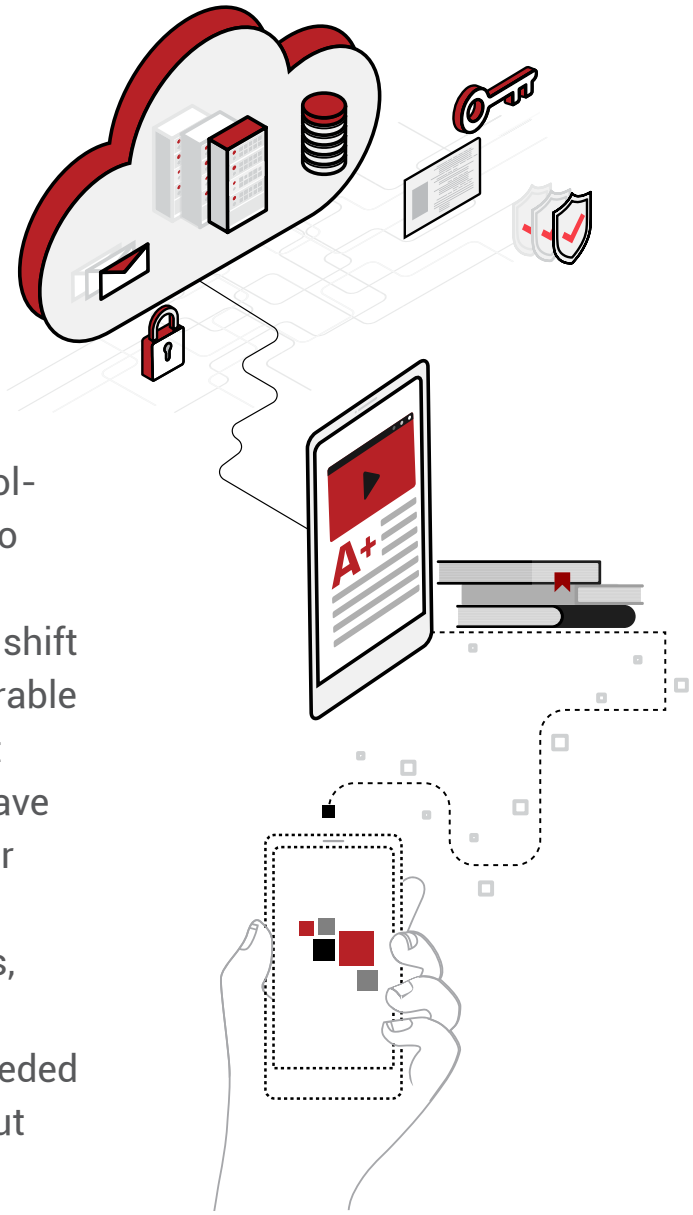
Visibility into malfeasance is also a remote learning cybersecurity concern. For IT, the difference between authorized and unauthorized access is indistinguishable. Typically, IT uses firewalls to monitor student and staff district network access to resources. However, when users access and create information in cloud apps like G Suite and Microsoft 365, without the right tools, system admins lose this visibility. Such usage is an inherent risk in any cloud computing environment, but it's worse in remote learning.

When IT cannot see who accesses what, data leaks happen. For example, an internal authorized user might accidentally share personal information. Or, a hacker might gain access to sensitive information via an account takeover. Regardless of why a system is compromised, no district wants to share student or staff personal information publicly. Additionally, whether remote or not, school districts need to comply with FERPA and HIPAA regulations. Such compliance is of particular concern during tax season, for example, when criminals seek employee W-2s.

Whether by illegal means or user error, cybersecurity in remote learning is a problem that needs a solution or students, teachers, staff, and schools won't be safe.

The Solution

The **Hypori Virtual Mobility** device eliminates the cybersecurity risks associated with remote learning. Hypori's solution securely contains all school data, from curriculum to personnel records, in a virtual school-owned data center with 100% separation from end-user personal information and activities. Since all school data resides safely on the school-owned virtual device, there is no need to secure students', teachers', and staff's personal devices. With Hypori, schools shift cybersecurity management from vulnerable personal devices to virtual devices that sit securely in a data center. Schools have no access to personal data on end-user devices, and no exposure should they be compromised. With Hypori, students, teachers, and staff have secure virtual access to all the school information needed for successful remote education without threatening cybersecurity.



To learn more about Hypori Virtual Mobility, contact us for a demonstration today.

Contact us

info@hypori.com

*The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide the secure communications path. Intelligent Waves, LLC's Hypori Client v4.1 for iOS and Android is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

11 March 2019

hypori.com