Securing the Distance Learner and Teacher

Threats and Mitigation Strategies

Many school districts do not recognize all the perils associated with distance learning because it is new to them. With all the technology previously contained at school sites, there was a lot of protection at that perimeter. Now, school districts have to think about scenarios such as bring your own device (BYOD) in zero-trust networks. To mitigate threats, for example, network attacks, video collaboration tool attacks, or privacy and data loss, school districts have to start implementing measures such as patching and data encryption.

Solutions for securing teacher and student devices

BYOD

Some basic security measures for students accessing resources in the data center or private cloud with BYOD are implementing basic controls around what they are allowed to access, considering what their rights are, and understanding what policies affect that.

Multi-factor authentication should be a minimum requirement so there is no data loss just through poor authentication methods. School districts may be able to require patching on those devices to make sure this minimum is met. Full-disk encryption to protect data is an additional option that makes sense. Part of meeting these basics is student education. Students must know they should not skip or cancel patch updates.

District Assets in Unsecured Environments (VPN)

District-owned devices are going to be significantly different from BYOD from a policy enforcement perspective. These devices will be used at home, perhaps for the first time in a zero-trust network environment, so we need to leverage security protocols such as secure boot. Students should not be able to plug in another device and boot from that device for any reason. If the device is lost or stolen, we don’t want any of that student data being exposed or vulnerable because somebody can boot from, for example, a Windows PE disk.

Some security will be consistent between BYOD and district devices such as enterprise rights management and multi-factor authentication for the public cloud, but when the school district has control over the device, they can enforce patching, disk encryption, local firewall policies, and secure boot.

As-a-Service-Clients

When either BYOD or district assets are in use as a service client, the same security is in place, but in addition, it’s important to remember that services are in the public cloud, opening more malicious opportunities. Trying to close that network circle in any way possible, for example, through transport layer security in multifactor-authentication is a consideration.

Intel Technologies for Securing the Teacher Device

Intel offers foundational security from the hardware all the way through the operating system. With the technology that Intel brings, school districts can build a system with a comprehensive security footprint with tools like secure boot, hardware shield, which protects BIOS boot, and encryption acceleration.

Intel Threat Detection Technology

Now that district-owned devices are outside the walls of the data center, the threat landscape has greatly increased. Before, security was a concern, but it was all behind a perimeter, a closed loop. These same devices are now out in the wild, exposed to predators, and there’s a front door to the data center.

In addition to secure boot and threat detection technologies, Intel can also provide some incredible encryption technology. Previously, encryption slowed everything down, but that’s not the case anymore. Because we’re doing encryption in silicon, as the bits are being stored or moved through the network or through the CPU, all the encryption can happen without impact to speed.

Security/Privacy Tips and Tricks

First, always scrutinize default settings. It may be convenient to use the default setting of a video conferencing platform, for example, but what are we allowing it to do? A simple example is that if a student can change their display name, that means the default setting did not require an authenticated user, so there was no identity management for that meeting. School districts should be looking at the default settings for A/V conferencing tools, content repositories, and mobile apps.
Whenever possible, we want to integrate these new systems and applications with existing identity management systems.

Distributing recommendations based on district policy surrounding privacy and security can further help, especially in BYOD scenarios. Getting teachers and students on board with district policies will improve everyone's experience in this virtual world.

Security: What Can we do Short Term and Long Term?

Short Term Recommendations

- Educate all users about the risks and district policies for ensuring compliance.
- Enforce, where possible, solutions such as patching, enterprise rights management, and turning on transport layer security.
- Make sure endpoint security agents are up to date and enforce those strict security policies.
- Enable full disk encryption.

Long-term Recommendations

- Craft strategic initiatives and implement a plan for zero-trust network access.
- Use multi-factor authentication everywhere possible.
- Strengthen enterprise rights management.
- Look at each stack solution as well as auditing, including the possibility of penetration testing events.
- Extend enterprise security as much as possible to the virtual classroom, with the management of devices at a minimum.

Recommendations for students and parents

- Update your system, for example, making sure Audio/Visual and endpoint security are updated.
- Turn on the local firewall to restrict traffic.
- Close all apps that are not in use.
- Change default usernames and passwords for systems and equipment.

The new virtual classroom in distance learning has unfortunately brought out some bad actors that know they can take advantage of this situation. The actions required for privacy and security may seem overwhelming to all parties, but with education and compliance, some simple steps can make a big difference. Working in advance to prevent security breaches is far better than trying to deal with them once they happen.