Start with the End(point) in Mind

The right security solution will protect schools against ransomware and other threats while still allowing teaching and learning to continue.

Bill Harrod
Public Sector CTO
Ivanti

IMAGINE THIS SCENARIO: A TEACHER'S MOUSE dies at home while she's preparing a lesson. She goes rummaging and quickly finds an old mouse with its USB dongle still intact. She lugs her laptop to school, plugs the dongle in, and the operating system begins downloading and installing a driver that just happens to open a vulnerability allowing users to gain system privileges through the device – privileges that would allow someone else to install whatever he or she chooses, including malware.

The endpoint – whether a mouse, a mobile device or something else – has come to represent the weakest link in the chain of K-12 cybersecurity. If district IT can't secure all of those myriad endpoints attaching to the network, a break-in leading to ransomware or a data breach is a very real possibility. The question becomes, how can IT address the threats and risks schools are facing while also making sure users – students, teachers, administrators and staff – have the access they need?

Achieving Zero Trust

While the concept of zero trust serves as a useful framework for understanding the goal of posting a guard at every entry and maintaining clear lines of authorization and authentication, getting it done is another matter. Somebody has to do the work of implementing endpoint management and security.

Consider the challenge of mobile endpoint patching. IT churns through cycles continuously applying long lists of patches, mitigating risks for which there may be no exploit and that may not be in line for attack. According to a recent Ivanti report, "**Patch Management Challenges**," 71% of IT and security professionals find patching to be overly complex and time-consuming. And the patching efforts may only address district-owned devices along with the small share of end users with their own devices who are willing to go through the patch process. What about everybody and everything else?

The key is knowing what patches are crucial and being able to prioritize patch decisions that are going to provide the greatest security. The patch management approach needs to apply threat intelligence and risk assessment. Then it needs to be enabled on ***all*** devices – district-owned or not – without the process relying on interaction from users.

Access Control Decisions

At the same time, IT needs to discover new devices coming onto the network, whether those are sensors running in the new ventilation system, a Bluetooth speaker operating in the school media lab or the principal's new Apple Watch.

What's required is a solution that can handle decision making on a lot of fronts efficiently:

- Vetting the network from which the user or component is transmitting – is it a home hotspot, a coffee shop Wi-Fi network or the public library?
- Validating that the device is in compliance – that it hasn't been rooted or jailbroken.
- Confirming that the applications being used are authorized and haven't been compromised.
- Validating users' credentials based on multifactor authentication.

All of those feed into making access control decisions that grant the right people the right access to the right applications and data from anywhere at any time.

Ingrained Intelligence

The job of K-12 cybersecurity begins and ends with the endpoint and making sure it's no longer the weakest link. Ivanti does that by producing integrated solutions with risk intelligence and hyper automation for delivering:

- Mobile endpoint security management
- Risk-based access control
- Patch management
- Asset discovery
- Service management

Ivanti leverages artificial intelligence and machine learning to be able to synthesize a vast amount of data from sensors, scanners and other software. Our solutions remediate ever-evolving threats, detect anomalies and react to policy violations in components or hardware about to fail or showing signs of failure. Then we're able to remediate those possible problems through an automated service management platform – long before a human would know to intervene.

One outcome is that schools with constrained IT resources can do more by becoming as efficient as possible. More importantly, the "now everywhere" district gains the ability to secure itself and be protected against ransomware and other threats while still allowing the teaching and learning to continue. And after all, that is the ultimate end point.

Bill Harrod *is the Public Sector CTO at Ivanti, joining as part of the MobileIron acquisition. He is an accomplished information security executive and cybersecurity professional with experience managing cybersecurity risk and designing and delivering security solutions to higher education, federal agencies and Fortune 500 companies.*

Endpoint Protection in Action

Like so many other districts in the country, a big school system in Texas had a large number of students who lacked access to the internet. To fill the gap when those kids were sent home for their learning, the district acquired a multitude of inexpensive Android phones to use for mobile hotspots. Using **Ivanti MobileIron Mobile Device Management**, IT locked down the phones to prevent them from being used for any other purpose. Thus, the district was able to get a lot of kids online quickly and cost-effectively. Every time one of those phones begins to connect, Ivanti's tool confirms that the devices connecting to it haven't been tampered with and that they're in compliance with the district usage policies.

Another district rolled out iPads early in the pandemic, but without any way of managing those devices. IT adopted **Ivanti MobileIron Unified Endpoint Management**, which helped ensure the devices are up-to-date, that the applications are approved, and that the data and resources being used remain secure. The tool provides native management of Apple technologies and enables IT to preconfigure iPads for elementary and middle school students and teachers, with the appropriate permissions, applications and folders. This eliminates downtime in the classroom stemming from configuration hassles.