DEVICE MANAGEMENT AND SECURITY

DISTANCE LEARNING PLAYBOOK

Smarter technology for all

Lenovo

WHAT YOU'LL LEARN IN THIS PLAYBOOK:

- Challenges and solutions for device visibility
- The dangers of inertia and the high cost of uncertainty without persistent access to your devices
- How to use the comprehensive, layered security solution you already have in every PC
- Security checklist for IT when evaluating district goals vs. current readiness

ABSOLUTE®

FROM COMPLEX TO CHAOTIC: MANAGING IT IN THE NEW NORMAL

For years, K-12 educators have had their hands full. Busy students, crowded classrooms, and flat budgets. Rising expectations and shrinking timelines. More devices, more applications, more connections and more technology risks.

And that's before everything went sideways. Before the world as we know it changed.

Now, learning environments look radically different — and include even more devices in even more places. For schools offering remote and hybrid classes, K-12 IT administrators are now the lifeline to their lessons. Along with all the new devices, new applications, and new services come new expectations. Being able to see and manage the entire IT environment is critical to meeting them.

IN A REMOTE LEARNING WORLD, THE DEVICE STILL RULES

While it is sometimes true in the classroom, it is nearly always true in distance learning: the device matters. A computer is essential for creativity, productivity, and collaboration. That means IT must work even harder to keep devices managed and secured. Because a failed device doesn't just mean an interruption — it means learning stops.

What's more, with many students learning remotely, any issues with their devices are taking place outside the safe perimeter of the school network. Visibility — where are devices and what are they doing — is the first line of defense. Plus, solving any specific issues at scale — such as a failed update or network-wide breach — gets significantly more complex. IT staff is in one place, students are distributed, and the clock is ticking.

Beyond accidental drops and spills, the devices that are used for distance learning are at risk from:

- New/unfamiliar tools and services that introduce IT complexity.
- Applications that suddenly stop working.
- Important security controls that fail.
- Lack of integration with IT management solutions.
- Limited visibility beyond traditional campus perimeters.

MANAGING THE DEVICE LIFECYCLE: SAME RISKS, NEW REALITIES

With the growing need to manage and secure devices remotely, IT teams at school districts nationwide are being forced to rethink the device management lifecycle. While the big milestones — from deployment to decommissioning — haven't changed, IT must now manage the timeline from remote locations, replacing physical access with total clarity, persistent insights, and agility at scale.

CLARITY

- Is our inventory accurate?
- Is a device ready for deployment or can it be redeployed?
- Has it been properly provisioned?
- Is it secure?

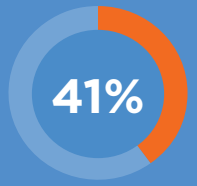
INSIGHTS

- Where is the device and what is it doing?
- Are installed applications and agents working properly?
- Which applications, devices, teachers, or students are having issues?

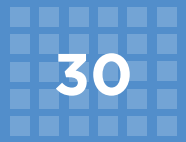
AGILITY

- Can the device be updated?
- Can security threats be mitigated?
- Can the device be secured/reset if lost or stolen?

36% of all devices have gone dark between August to October this year



41% of school IT teams said tracking lost or missing devices is a big challenge



30 devices missing on average at each school in past 9 months

Source:
Distance Learning Study. Hanover Research, 2020.

Lenovo

THE DANGER OF INERTIA

From software patches to preventive maintenance, devices require constant care and attention to ensure reliability. Once installed, any application or service will begin to degrade and critical tools and services begin to fail.

These errors can quickly cascade. If an encryption service fails, data is no longer protected. Then if a manageability agent also fails, IT will be unaware of the issue and unable to mitigate it. Schools need to do whatever it takes to make their devices more resilient.

THE HIGH COSTS OF UNCERTAINTY

In the best-case scenario, district IT leaders can solve these manageability and security dilemmas, under intense pressure and expectations. But the worst case is not knowing what they don't know, leaving them in the dark about what needs fixing. For the average school district, lack of visibility and control has serious consequences.

Take for example older devices, which make up nearly half the devices being deployed into remote/hybrid learning programs. IT is forced to manage and secure these out-of-date devices, already a more difficult task, via Remote Desktop protocol (RDP) applications.

Before the move to distance learning, IT could quickly gain access to a device, either physically or over a local network, on either a regular maintenance basis or as required. But new realities mean IT must address most device issues remotely — often in real-time.

> "Before we started using Absolute, we realized we took a lot of things for granted. That we knew where devices were, and that everything was working. Probably because addressing issues was pretty simple, we probably weren't as rigorous as we could have been."
>
> *— Medium-sized School District in Kansas*

CHALLENGING NUMBERS

The challenge for schools and districts is two-fold. After installing controls on devices, they need to get visibility into their ongoing performance.

EDUCATIONAL DEVICE MANAGEMENT CHALLENGES

DEVICE READINESS	DEVICE MANAGEMENT
Devices need serious remediation to be ready to keep students learning and collaborating. It starts with IT building a baseline of visibility and manageability across all deployed devices. The numbers are jarring: • On average, schools have had 30 devices go missing in the past nine months.[1] • 36% of devices were dark between August to October of this year.[1] • Nearly three out of four school devices have an out-of-date OS.[1]	Even when software is installed, it's quickly degrading. Even when devices are updated, critical agents can degrade, leaving devices insecure and unmanageable. Research on endpoint controls shows that: • 38% of vs require at least one repair monthly.[2] • 56% of client/patch management agents fail.[2] • 42% of schools have students or staff that circumvent security.[2]

IT staff can't secure what they can't manage, and they can't manage what they can't see. So, as device dependency ramps up, what's the solution?

Source:
[1] "Distance Learning's Impact on Education IT," Absolute, September 2020.
[2] "Cybersecurity and Education: The State of the Digital District in 2020," Absolute, 2020. Web.

GAINING CONFIDENCE, END-TO-END

Any IT challenge is made worse by complexity. Unfortunately, even with district-wide standardization, IT rarely gets to manage a single device model and OS. Instead, they must find a way to create solutions that integrate universal controls into existing vendor, OEM, and OS capabilities. There must be a management and security framework that goes deep and wide.

COMPREHENSIVE, LAYERED SECURITY

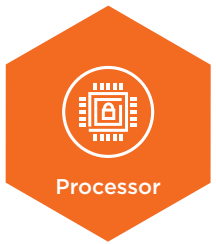
Despite being among the top three priorities for IT leaders in education[3], cybersecurity remains a challenge in schools, exposing staff and students to threats. The threats are amplified with the greater complexity of device and application management as schools react to the COVID-19 pandemic.

It is reported that, today, ransomware accounts for approximately 80% of malware infections in education, up from 48% in 2019, and unwitting insiders are responsible for 33% of incidents. Interestingly, education is the only sector where malware distribution to victims was more common via web sites than email.[4]

DEEPLY LAYERED VISIBILITY AND DEFENSE

Firmware

Visibility at the firmware layer lets you see the full stack. It's also tamper-proof and can be enabled with no help from the manufacturer.



Processor

The processor and motherboard help build a root of trust that ensures secure BOOT and hardware operations.

Operating System

The operating system manages user identity and access, login authentication, and drive and data encryption. The OS can also provide baseline malware and AV protection.

3rd Party Software/Agents

Installed software helps manage user behavior and protects against advanced threats and monitoring via agents and a console.

Source:
[3] CoSN K-12 2020 Hurdles and Accelerators. Consortium for School Networking, 2020. Web.
[4] Verizon's 2020 Data Breach Investigations Report. Verizon, 2020. Web.

With Absolute® Persistence® embedded into the firmware of endpoint devices by most of the world's largest PC OEMs, K-12 IT leaders achieve a digital tether that provides an unbreakable connection between any device and the school that manages it.

ENSURING PEACE OF MIND

So, what does end-to-end security look like? How do successful districts and schools empower both teachers and IT to be efficient and effective? Teachers are on the digital front line, with IT standing behind them. Ready to take on the challenges of today and ensuring they're ready to respond to future disruptions — whatever that new normal might be.

"Initially, stop loss was the primary reason we chose Absolute, but what keeps us at the table today is their ability to innovate and provide us with more information about what's being stored on the devices and what's being utilized. I continue to choose Absolute because of their innovation. They help us stay ahead and offer the latest advantages to our students and faculty."

— Chris Cummings, Information Technology, Teaching & Learning, Klein ISD

MISSION CHECKLIST FOR IT

GOALS	WHAT IT SHOULD REPORT ON	CAPABILITIES REQUIRED
 Mitigating device drift	1. Are devices still in the district? 2. Are devices lost or stolen? 3. Can I take action on missing devices? 4. Can I improve my device recovery rate?	• Geolocation • Geofencing • Missing Devices Report • Freeze • Call-In History Reports • Investigations and Recovery • Persistence® technology embedded in firmware
 Security	1. When devices connect back to the school network after being on home networks, will they be safe — or introduce risk? 2. Will devices contain sensitive family data?	• AV Compliance/Install Rate Reporting • EDD Scan for Sensitive Data
 Facilitating distance learning	1. Are online learning tools being used as expected? 2. Which ones have the greatest adoption?	• Web Usage Reporting
 Ensuring endpoint resilience	1. Can IT manage, repair, and remediate IT issues when devices are off network and IT staff is working from home?	• Reach Scripting (push applications, change device settings, etc.) • Application Persistence [25] • Detailed Device Data Reporting (troubleshooting and investigation)

BUILDING THE PLANE WHILE FLYING IT

The pandemic's arrival in early 2020 threw many districts into the deep end. While remote learning was already being implemented in bits and pieces, suddenly schools and districts were forced to scale numbers and accelerate timelines. All while keeping the experiences secure.

The difference between Spring and Fall 2020 was a little bit of time and a whole lot of partnership. By leveraging the expertise of educators, administrators, and their technology partners, districts are able to take the lessons learned early on and build them into best practices going forward. No matter what drives the next new normal, districts will be better prepared to adapt and respond.

> "With the right technology resources in place, including Absolute, we can ensure an exceptional, seamless remote learning experience."
>
> *— Small Charter School in Pennsylvania*

Education is designed to give students the skills they need to embrace coming opportunities with confidence. Schools and districts need that same certainty. And it starts with a digital learning ecosystem that is as resilient as the teachers and students it serves, regardless of the learning model they choose to adopt. To do this, they need to ensure their approaches are built on Endpoint Resilience™ technology — an emerging and critical KPI for school security strategy. All Lenovo devices work seamlessly with Absolute and can help districts protect their hardware investments and the communities they serve.

For more information, visit absolute.com/Lenovo

ABSOLUTE®