Malwarebytes

eBOOK

Education cybersecurity: A flexible approach to protecting school devices

Table of contents

Introduction

Educational institutions are working through an unprecedented situation as they adjust their IT environments to support both remote staff and remote learning models during the COVID-19 pandemic. Across the globe, students are now receiving distance learning, usually from home, leveraging a range of technologies. Students are using their own devices or school-issued devices and attending classes through online video conference platforms, such as Zoom, Google Meet, and others. To make sure all students have access to remote instruction, some schools are also issuing hot spot devices to provide student households with WiFi access.

5 minute read

Grab a coffee, sit down, and spend a few minutes with us. With our help, you'll soon be on your way to protecting your educational institution from cyberthreats in this new world of distance learning.

Learn how selecting a vendor that provides a flexible approach to your endpoint security will deliver protection that spans your workstations, servers, and devices while requiring less time and specialized training from your IT team.

The closure of schools and shift to full-time online learning in the wake of the coronavirus pandemic has created a stressful situation that impacts the emotional wellbeing of educational staff and students, as well as their family members.

And even though IT staff at school districts and universities are experiencing overload like never before, cybercriminals are not giving them a hall pass. Never ones to slow down or pass up an opportunity, cyber criminals are increasing their efforts and already compromised 284 educational entities with successful ransomware attacks in the first quarter of 2020. [1]

The day-to-day job of protecting educational institutions from malware is hard. Undeniably, the current crisis further complicates matters.

[1] Dark Reading. Pandemic Could Make Schools Bigger Targets of Ransomware Attacks. April 2020.

The challenges of protecting school endpoints are now magnified

For the IT staff managing cybersecurity, this difficult time has functioned as a magnifying glass, intensifying the difficulties educational institutions have traditionally faced in safeguarding the servers and devices in today’s 21st century-connected classrooms. Now that the definition of “classroom” has moved beyond the confines of the school’s walls, providing endpoint protection must address these issues. →

Challenge 1

Legacy systems with diverse operating systems

The majority of educational institutions are permanent buildings and most of this infrastructure requires repairs, renovations, and modernizations. This dated infrastructure also extends to technology with the presence of legacy software and outdated operating systems. This makes school networks more vulnerable—driving the need for a 21st century makeover to better protect the school's digital assets.

Yet, this need has quickly become a declining priority in the wake of the global pandemic. Instead, IT teams must now make the most of their existing systems. Investments in upgrades to the legacy IT infrastructure must now be put aside, as educational institutions must now divert their limited funding to supplying technology to help all students access distance learning models.

The pandemic appears to have made schools bigger targets for cyberattacks. Safeguarding educational IT systems will be more complicated if the district's current endpoint protection software isn't flexible enough to remotely protect multiple school-issued and personal devices and operating systems.

Challenge 2

Limited IT resources

The need for skilled IT security professionals is not keeping pace with demand, and there will be an estimated 3.5 million unfilled cybersecurity positions by 2021.[2] This resource shortage especially impacts the education sector.

While the malware risk has fallen squarely on IT's shoulders to burden, schools face limited funding and resources to hire and retain staff with the security specialization required to manage it.

Now in the time of a pandemic, educational IT departments are stretched even further to move huge mountains with the same limited resources.

[2] WhiteHat Security. Unfilled Jobs in Cybersecurity.

Challenge 3

Siloed environments

Educational IT environments are some of the most complex for security teams to manage. Schools have multiple classrooms and campuses with a range of technology needs that must be supported and protected across multiple locations.

Orchestrating endpoint security across these siloed environments has always been a complex challenge, and it just got a lot more complicated.

With students and staff working and learning from home at unprecedented rates, the institution's IT environment has moved past the traditional perimeter, which means IT teams must figure out how to protect these machines, and, if they're school-issued devices, how to manage them remotely. And then there's the server-based IT infrastructure to consider. If the IT team is sheltering in place, they need an easy way to remotely manage the endpoint protection for these servers.

Challenge 4

Tight budgets

In the public sector, educational institutions often have limited funding that must cover everything necessary to manage daily operations and delivery of instruction. With increased costs and funding that fails to match inflation, the education sector has some of the tightest budgets of all industries.

Now, in the midst of this global crisis, schools are challenged to find nonexistent funds to invest in new solutions that allow instructors to teach and staff to work remotely.

The future of these already-limited budgets is also in jeopardy. With global, national, and local regions experiencing spikes in unemployment and other economic disruptions, schools face uncertain cash flows due to the seismic impact on revenue sources.

Challenge 5

Open networks

Educational institutions today have wide-open campuses that often have just-as-wide-open gaps in cybersecurity protection. Sensitive information is difficult to secure because it's stored and shared across multiple departments. Likewise, students access data and submit assignments through secured and unsecured networks.

IT departments now have a far more difficult job as they face the challenges of distance learning and student-owned BYOD technology that an off-campus-instruction model introduces.

Open networks

Students and staff are now working from home networks that have a range of security standards—all of which are unmanaged by the school’s IT team. What if the home network doesn’t use a firewall, or unsafe passwords like “123456” are being used? Then, there’s the looming security risk of what will happen when these machines come back to the school network after a long period away. If the school’s endpoint security platform only provides limited offline protection and a patchwork of security tools, schools are bound to see a large spike in infections.

Adopting a flexible endpoint security approach

Considering the challenges, what's a school to do? Managing a mesh of legacy products and taking a reactive approach to endpoint security is no longer sufficient or sustainable. Cybercriminals have set their sights on the education sector, and a single, successful attack will wreak havoc during an already challenging time.

With the current and accelerating complexities, now more than ever, educational institutions need a vendor that provides an intuitive and flexible approach to endpoint security—one that provides the perfect balance between far-reaching, effective protection and simplicity to address the new and changing requirements for protecting schools.

At Malwarebytes, we call this the consumerization of cybersecurity. It's the right goal in today's market—to write robust cybersecurity products that provide organizations with comprehensive coverage and that are as simple to use as consumer technology.

So, what should you look for in a flexible approach to endpoint security?

Your endpoint security vendor should provide value that is specific to your educational IT team and make it easy to support your changing needs.

This covers several requirements:

Broad protection coverage

You should strive for protection that spans your workstations, servers, and BYOD devices to safeguard your remote staff and students, as well as your physical campus locations.

Your vendor should provide security options that support all of your environment needs and coverage for all of your operating systems.

Flexible licensing model

With the very definition of your school environment changing, your vendor should provide a range of licensing options to address your specific security needs.

A flexible, mix-and-match approach to licensing will allow you to purchase endpoint security to meet your entire environment needs or fill a specific security gap.

Managed or self-managed service options

Your endpoint security vendor should provide flexibility that allows you to decide how you want to manage the solution.

By choosing an endpoint security company that provides both managed service and self-service endpoint security options, you'll have the flexibility to adjust your IT management approach at any time.

Looking at the solution's capabilities, your ideal endpoint security product should smartly integrate a consumer user experience with the enterprise level functionality you need to combat the advanced threats educational institutions are experiencing.

Your requirements for this should include:

Active protection and automated remediation

Schools are under constant attack, and, as a top priority, your solution should provide effective protection using multiple detection techniques that provide full attack chain protection.

Your ideal solution should also provide automated threat remediation that allows you to quickly and efficiently restore endpoints to their pre-infected, trusted state.

Cloud-based single agent

With teachers and staff working remotely, your endpoint security solution should make management simple, from any location.

Selecting a cloud-based solution with a single agent will free up your IT resources, simplify management, and streamline your administration.

Comprehensive visibility

An endpoint security solution that provides strong threat visibility will allow you to effectively coordinate your security efforts.

Your solution should have an interface that's straightforward and easy to use across your servers, workstations, and devices. It should come with the ease of any of the consumer applications you might find installed on your cell phone.

Tools that support your "Tech Bench"

Schools have a lot of technical needs to keep equipment running smoothly and deliver curriculum on time.

Your vendor should provide tools that extend your tech bench capabilities and accelerate your system troubleshooting, such as system crash analyzers, OS troubleshooting tools, and more.

Malwarebytes:
Making educational institutions successful

During this unprecedented time, educational IT staff should not carry the burden of ineffective protection and resource-intensive endpoint management. Your IT needs and the way you deliver them have changed, and your endpoint security vendor should provide you with the flexibility to adapt to your changing needs with agility.

Malwarebytes understands the unique challenges that educational institutions face. That’s why our solution for educational institutions delivers effective protection and cuts through complexity to eliminate IT resource constraints. And we’ve prioritized flexibility at the center of education sector strategy so that you get effective endpoint security exactly the way you want it.

Education challenges resolved with Malwarebytes

Legacy systems with diverse OS

From servers to workstations and BYOD devices, we provide endpoint security solutions to protect your entire environment from zero-hour threats.

Our products provide support for Windows, Macintosh, and Chromebook in a lightweight package that won't weigh down machines.

Our protection for servers provides flexible management and speed for educational institutions of all sizes.

Limited IT resources

Our consumerization of security approach means we've automated and simplified capabilities at every turn to make your job as efficient as possible and to relieve your staff resources.

The solution provides you with ease of use through a single agent, cloud-based management, and a central console that increases visibility of your workstations and servers.

Siloed environments

With Malwarebytes, you gain a cloud-native solution that breaks down the siloes in your environment by extending your reach to protect your endpoints and manage security across your environments—all from a single console.

In the event of a successful attack, you can remediate endpoints through the cloud, regardless of their location.

Education challenges resolved with Malwarebytes

Tight budgets

Our flexible licensing model lets you select the product or products you need to secure your environment along with managed and unmanaged solution options.

We save your team time and money by providing schools with a specialized toolset. The Malwarebytes Toolset features more than 20 tools—developed for technicians by technicians—that streamline processes and procedures in malware remediation and computer repair. This level of breadth and depth increases your "tech bench" capabilities and ensures your team has the right tool at the right time to get the job done.

Open networks

In addition to managing school-owned endpoints, Malwarebytes provides flexible and affordable options for student BYOD protection, depending on the school management needs and laptop ownership (e.g., unmanaged, managed, or hybrid).

Beyond your endpoint security considerations, you should assess your posture for securing remote students and staff.

Secure your cloud data

Implement role-based access control to limit who can store, access, and share data on the cloud.

Create separate networks

Segment your network—both for cloud and on-premise infrastructure—

and monitor for traffic and anomalies.

Enable secure remote work over WiFi

Ask that your staff use their own router or modem, rather than renting. Also ask that they regularly update their WiFi password and remove unnecessary connected devices. If you can, provide VPN access as an option.

Provide security awareness training

Train staff with educational videos and online training resources on safe, remote use of school equipment.

Conclusion

Educational institutions will continue to be an attractive target for cybercriminals looking to take advantage of vulnerable systems. This is especially true now during the global need for distance-based instruction. The good news is that your school can navigate this with agility by choosing a vendor that provides a flexible approach to endpoint security.

Reconciling the security challenges your school faces by adopting a cloud-based endpoint protection solution that covers your remote and onsite IT needs will equip your IT team with the necessary capabilities for effective protection, without overtaxing your team's constrained resources.

This approach ensures your instructional hours are not interrupted, student and staff will remain protected in the event of an incident, and your educational ecosystem can continue to operate, whether it's all distance-based, on campus delivery, or a hybrid model that includes a combination of both approaches.

Schools have a mighty responsibility to protect students and prepare them for later years. **During this time and into the future, Malwarebytes is committed to partnering with you at every step of your schools' endpoint security needs to ensure your success.**

Learn more

For more information, visit:
malwarebytes.com/education/