Microsoft

3 Keys to Security and Compliance for Your School

Table of contents

Introduction

A perfect storm

At K-12 schools around the world, a perfect storm regarding security is building, fueled by a combination of high-pressure challenges that are unique to the education field.

Schools are a treasure trove of valuable personal student data.

→ But schools don't have a strong security position to protect that data and defend against attacks. 60 percent of US K-12 data breaches in 2018 included student data.[1]

Adoption of technology in classrooms supports personalized learning and greater learning outcomes.

→ But it also expands the school's digital estate, giving bad actors more surface area to attack.

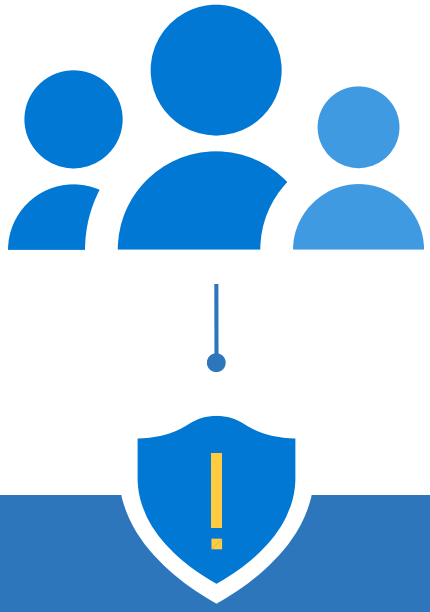
Schools are filled with inquisitive minds; curious students who are encouraged to explore and share through new technology.

→ But this also opens the door to breaches through unsecured apps and collaboration tools.

Security is a big concern for K-12 CIOs.

→ But they express less confidence in their cybersecurity teams than other respondents. These same CIOs anticipate more severe and complex cybersecurity issues in K-12.

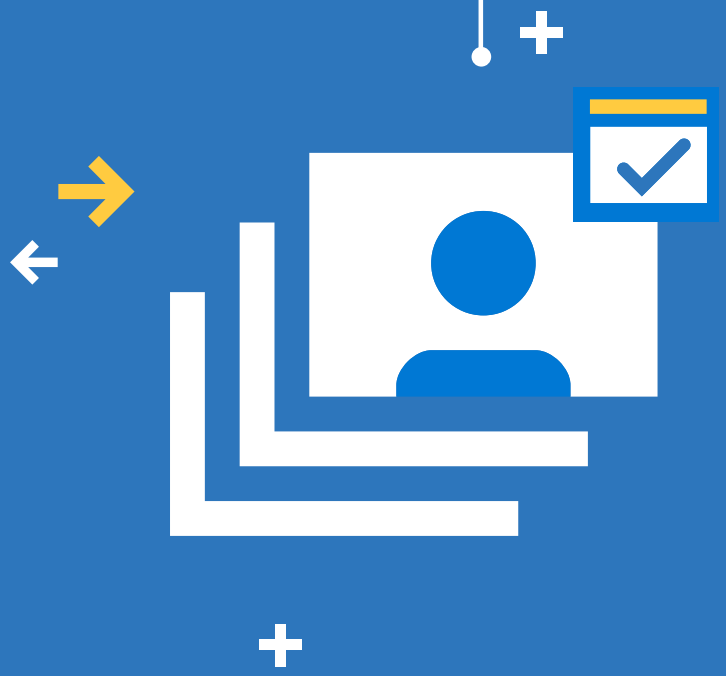
Schools are deeply invested in the safety of their students and are under tremendous pressure to keep student data safe, reduce exposure to risks, detect attacks, and respond to threats. Doing this as the perfect storm builds is imperative, but it can also be overwhelming.



In this e-book we'll show you how it's completely possible to address this challenge, in spite of the obstacles in front of you.

Let's get started.

Key 01



- Protect from the inside
- Understand the technology needs of students and educators
- Manage access

Protect from the inside

Where to start? The most natural place to significantly reduce your school's exposure to security risk takes just one initiative: making sure your teachers, staff, and students don't accidentally create data breaches.

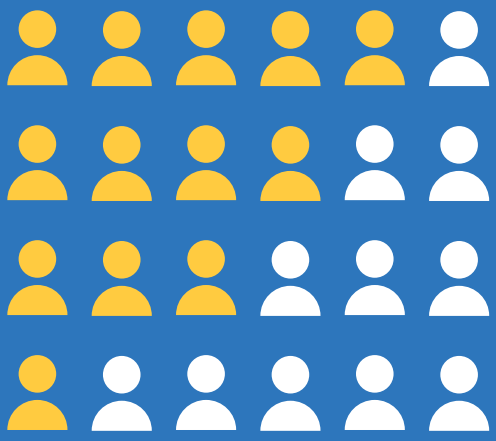
Internal data breaches are primarily caused by two issues:

01 Teachers, staff, and students independently using apps and technology that fit their needs, but which haven't been reviewed for security compliance.

02 Password and access violations. This one is also a threat from the outside, as we'll talk about later.

51%

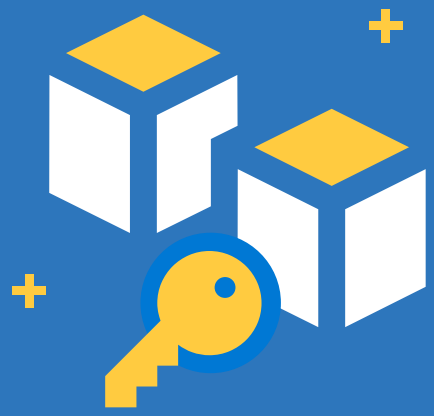
More than half of all K-12 digital breaches in 2017 were inadvertently caused by members of school communities, not by outside hackers.[1]



Understand the technology needs of students and educators

To combat the challenge of multiple point solutions, school technology decision makers first need to audit teachers, staff, and students to understand what kind of technology they need. This is part of creating an environment where the tech needs of your teachers and students are easily met, so there's less risk of them needing to find alternative solutions. Students and teachers are resourceful and will find a way to get their needs met if no help is available.

Microsoft Store Apps for Education meet strict security requirements. Giving your school access to this marketplace ensures they can find the tools they need while maintaining a strong security profile.



Manage access

Password and access violations can happen accidentally or intentionally. When teachers, staff, and students have difficulty accessing information, they'll try to find ways around IT and security policies to get what they need most efficiently. Give them easy access to approved data and tools across devices, both on school grounds and remotely, with Azure Active Directory. You can also restrict access to those who need it, creating a wall around sensitive data.

Using multifactor authentication (such as requiring a code sent to the user's smartphone) is another layer of security that should become standard for all but the most public information.

Monitoring security alerts when IDs are blocked means you can act quickly when threats arise, and wipe devices remotely, if necessary.

As you look for solutions, work toward maintaining security while providing technology that improves the user experience, such as Windows Hello, which uses biometrics for password-less strong authentication.

Key 02

- Defend against outside threats
- Understand common cyberattacks
- Reduce vulnerable entry points with secure technology
- Prevent attacks
- Make identities secure
- Keep monitoring

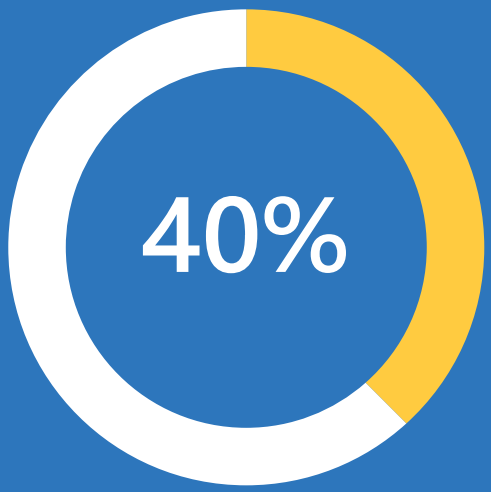
Defend against outside threats

Cyberattackers have refined their methods over time. This puts more pressure on detection and defense. At the most basic level, education and awareness go a long way toward thwarting attacks—don't open spam, don't click on links from people you don't know. But maintaining strong awareness across an entire school or district with a high level of success is a challenge. People make mistakes. What can you do about that? Automate your defenses against outside threats by bringing intelligent technology to your school.

Between 2015 and 2016, ransomware attacks increased

6,000%.

In 2016 ransomware was in almost 40% of all spam messages.[2]



Common cyberattacks

Phishing

This is an email that looks legitimate, but it tries to trick you into opening an infected file or going to a malicious website in order to steal credentials or other personal information.

Baiting

Infected USB drives or disks are left in public places, in hopes that someone will insert them into a computer. On the web, a similar thing can happen. For example, someone thinks they're downloading free music, but the file turns out to be infected with malicious software.

Watering hole

Attackers inject malicious code into the public pages of a site. When a victim visits the compromised site, that code is installed on their computer.

Pretexting

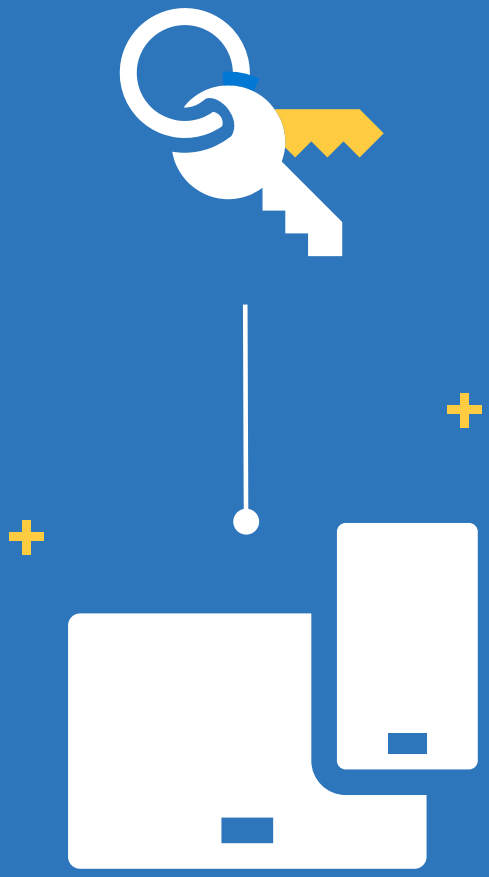
Creates a fake scenario to gain user trust in order to steal personal information.

Ransomware

Ransomware is malicious software that allows attackers to gain control of a computer or network, which they then hold ransom for a fee.

Reduce vulnerable entry points with secure technology

Combating outside threats includes building controls into devices, apps, and the network. Take a hard look at every part of your technology chain, from the network to the laptops, tablets, and apps being used. For example, the built-in security on the devices you use in your school should include antivirus software, automatic security updates, and password protection. Some devices are made more secure than others, and this is also true for apps. Starting with secure devices and a robust network security profile can deter and deflect attacks at the perimeter.



Learn about security in Microsoft devices for education ›

Prevent attacks

Detect attacks and block them faster with advanced analytics and machine learning. You can be proactive, not reactive. Azure Advanced Threat Protection (Azure ATP) gives you rich forensics on advanced attacks, user behavior, and compromised identities through powerful machine learning and analytics. For example, if a student signs into her computer on a typical Tuesday morning at school in New York, and then shortly thereafter she signs in from Prague, Azure ATP recognizes that this second sign-in is invalid and prevents access.

Keep monitoring

Once you've reduced the surface area, implemented technology that prevents attacks, and secured identities, don't stop there. Now you must continuously assess your security. With the right tool, like Azure ATP, this is easily and automatically done. Be prepared to address vulnerabilities that come up, and stay clear about your risks as attackers become more sophisticated.

Make identities secure

You can help protect student and teacher identities by using multifactor authentication for access to devices and apps, and by monitoring security alerts when IDs are blocked so you can take action.

Key 03

- Create a culture of vigilance and compliance
- Consider the governance and lifecycle of your data
- Build your own central command
- Form a holistic security strategy

Create a culture of vigilance and compliance

Developing a comprehensive security profile for your school means involving your teachers, staff, and students in the mission. Intelligent tools make this simple and quick. For example, data loss prevention technology flags any email that's being sent outside your organization with a "this person is outside your org" alert. Once your teachers, staff, and students recognize that this alert is a security protocol they must pay attention to, they'll respond to it appropriately. It becomes automatic for them, which strengthens your culture of vigilance and compliance.

Consider the governance and lifecycle of your data

Compliance with governance and data lifecycle requires end-to-end visibility and control. Start by understanding the security environment and risks, and then bring in controls that mitigate those risks.

With Microsoft 365, customers manage compliance from one central location across email, documents, chats, and channels with confidence that their organization's retention, deletion, records management, and eDiscovery requirements are met. With one location to manage compliance for the entire suite of capabilities, everything is simplified.

Build your own central command

Manage security from a single console, such as that included in Microsoft 365. This is simpler than managing a collection of point solutions. Similar to reducing the surface area for bad actors, this reduces the surface area of control so that you can have a single, powerful point of oversight.

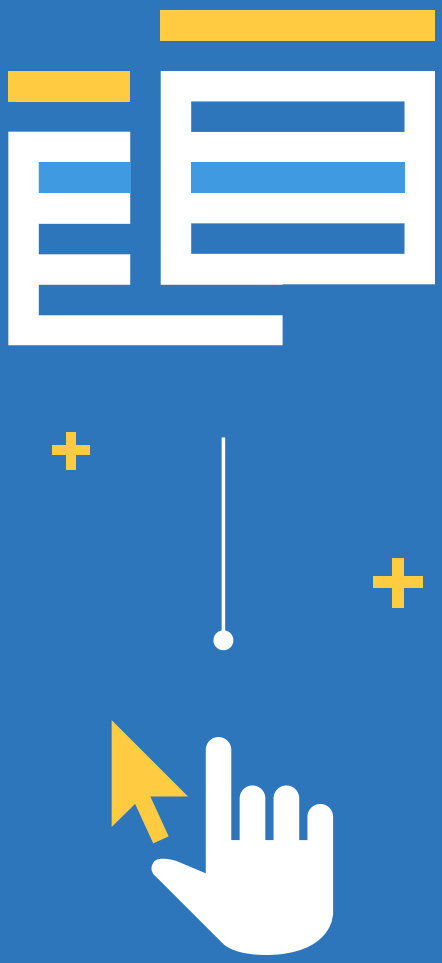
Form a holistic security strategy

Assess compliance risk, safeguard information anywhere it lives, and respond confidently with built-in search and discovery capabilities:

Track your compliance activities in one place so you always know the current status. With one dashboard in Microsoft 365, you can simplify monitoring and managing activities related to discovery, legal hold, and analytics. You can then look across all your devices to see if compliance risks exist and where they are.

Classify and categorize sensitive information, then apply policy to it. Put this capability in place so that the people who are using and generating sensitive information are in charge of categorizing it with one click.

Locate, identify, and retrieve relevant information, and put a legal hold on it. This capability can eliminate redundant effort and save review time, which means you can get back to school as fast as possible.



Microsoft

Conclusion

Secure your school, secure your students

Avoiding the perfect storm of security issues on K-12 campuses is imperative. You've been protecting your students for years, and new cybersecurity concerns add a complex digital element. Focusing on technology that enables student-centered learning while also ensuring maximum security is the key to success.

As your school works toward a security solution, let us know how we can help.

Our experts are standing by

Contact us

[1] Verizon Data Breach Investigations Report, 2017.

[2] Ransomware: How Consumers and Businesses Value Their Data, 2016, IBM.