K-12 Security Essentials for Beginners

jamf

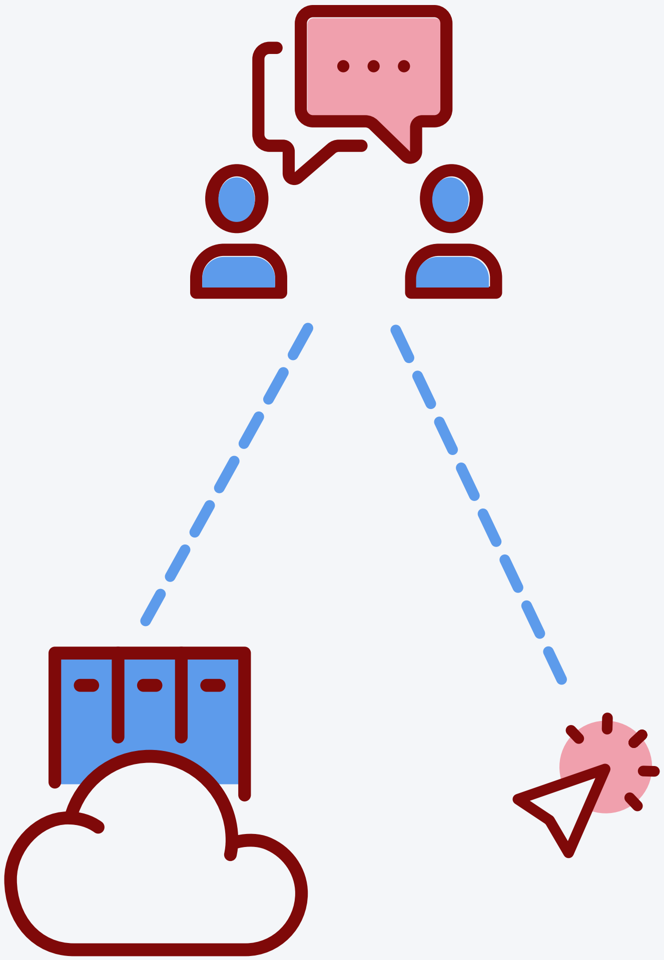
There are few industries that have felt the transformational touch of technology quite like education.

The advancements in personal computing and the development of cloud-based services have revolutionized some core tenets to how learning occurs, such as:

- Access to books and resources have grown exponentially, extending beyond physical limitations.
- Global lines of communications between students, teachers and parents are immediately available.
- Standardized testing has been streamlined by moving to computer-based models.
- The varying needs of students can be addressed through one common device with specialized apps.
- Convergence between multiple modalities of education and teaching styles can be achieved by integrating multiple technological tools.
- Distance learning has proven to be a viable method of education, despite an ongoing pandemic or other global crisis.

Creating a vision

It's clear that technology as a whole has been embraced by K-12 education since day one when one of Apple's earliest computers, the Apple IIe, taught young minds in 1983 how to add, read and type. Those children are now adults – and in some instances educators themselves – continuing this practice by using the latest MacBook Air and iPad, alongside a growing catalog of nearly 2 million apps, to educate the students of today.



Unlike forty years ago when cybersecurity wasn't even a term to consider, today's modern computing landscape is vastly different. Even going fifteen years back, it wasn't anything like the present, filled with myriad threats to the security of your devices. From restricting access to critical data and services by infecting them with ransomware to compromising student records and sensitive data through data breaches – current threats may even pose a significant safety-to-life risk through the unauthorized capture of privacy data.

This e-book isn't intended to instill fear, but rather raise awareness of the very real and sometimes scary security concerns that affect education.

Creating a vision

Taking a step back from the scarier elements, more often, threats manifest as loss of device usage and/or limited access to resources. In turn, these delays prevent learning from taking place. Furthermore, regulations in place to curb these situations from occurring are sometimes tied to funding structures that directly impact a school's ability to provide the level of service their stakeholders and communities require if a violation to compliance has been deemed.

In this e-book, we address the unique cybersecurity threats that impact K-12 education, highlight why it is so critical to proactively address them and:

- **Look at the crucial role cybersecurity plays today – and in the future of education to come.**
- **Illustrate the external and internal threats that make up the majority of malicious attacks against K-12.**
- **Identify which practices can be strengthened to safeguard devices, confidential data and students.**
- **Address common misconceptions relating to Apple and security.**
- **Discuss how stakeholders training programs contribute to successful cybersecurity programs.**
- **Explain how Jamf solutions mitigate risk while comprehensively securing your endpoint fleet.**

Welcome to Hogwarts

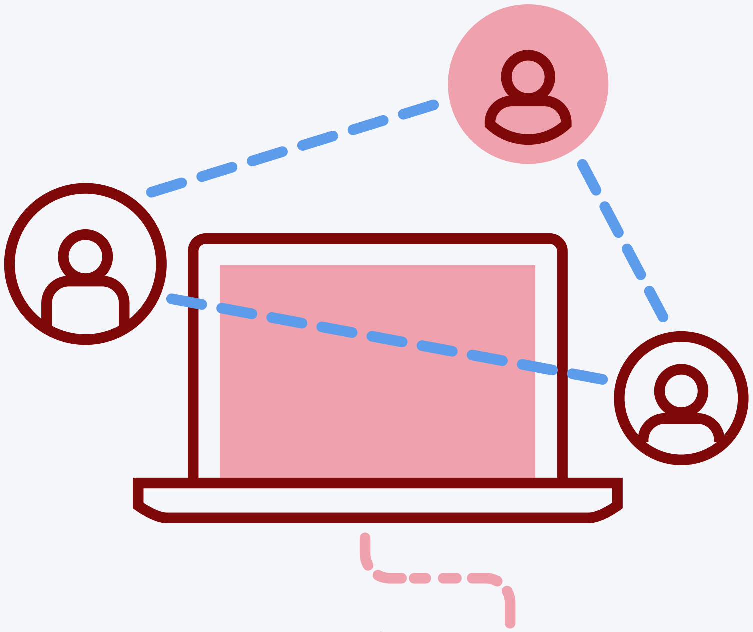
In the Wizarding World of Harry Potter, the titular character – a student with incredible potential – attends Hogwarts where he and fellow students receive an education in several different modalities relating to magic. But that isn't the extent of the knowledge the educators impart, is it?

No, it isn't. In fact, the students of Hogwarts, much like the real-world counterparts in K-12 schools, embark on a journey of knowledge in many different subjects throughout their time in school. Some are academic, others extra-curricular – but all form a tightly-knit and cohesive bond that makes up a comprehensive, well-balanced education.

Well, cybersecurity and how it addresses the unique needs and requirements of the K-12 education sector – when implemented successfully – works in much the same fashion. After all, there is no single charm, like Lumos, to illuminate the secrets of endpoint protection. Instead, a collection of tools, combined with best practices and end-user training work in conjunction to maintain the security posture of your school's infrastructure.

Why is cybersecurity so important?

Aside from the reasons listed before, to ensure the safety, confidentiality and integrity of your endpoints — students, data, and devices — cybersecurity's importance is heightened due to a few education-specific challenges that, at times, prevent organizations from implementing the proper solutions to mitigate malicious threats and combat attacks.



Budget constraints

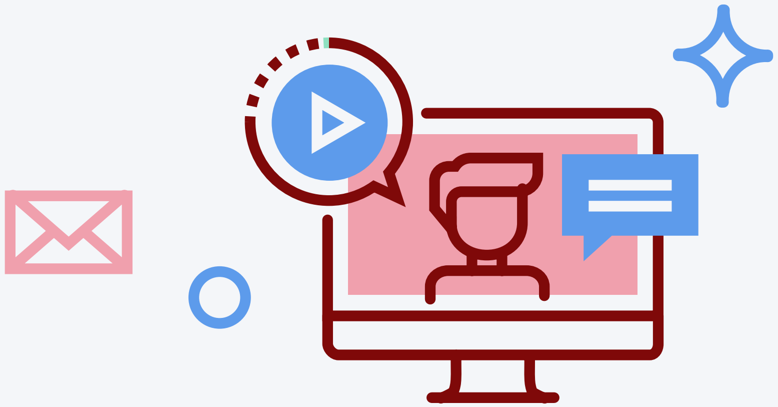
A Forbes article about how US schools are struggling to fund in our future notes that "states that have achieved both equity and adequacy see stronger achievement and graduation rates…". Ask almost any educator looking to get a replacement bulb for their LCD projector or stronger access point to handle the number of users connecting to Wi-Fi and they've often heard a reply about lack of funding being the culprit as to why they didn't get what they requested.

Budget concerns are often at the core of infrastructure upgrades seeking to update networking equipment for faster connectivity or to support more devices as districts adopt a 1:1 device model, as well as, the procurement of security services that detect and prevent malware on school-owned equipment.

Legacy infrastructure

Going hand-in-glove with budget constraints, schools are often forced to “do more with less”. This means keeping obsolete, outdated equipment in use long after a vendor stops supporting it. While these antiquated devices still work, technically speaking, they often lack the resources necessary to meet the minimum requirements of modern apps and services, such as computer-based testing (CBT).

Other times, the devices themselves straddle the line of usability causing a variety of issues for students and teachers. Making it worse still is the fact that these older devices and apps are no longer supported meaning security patches that normally correct bugs in software and close vulnerabilities used by malicious threat actors to gain unauthorized access to data are left uncorrected. This leaves a gaping hole in security without a means of defense until new equipment and/or applications are purchased.



Shadow IT

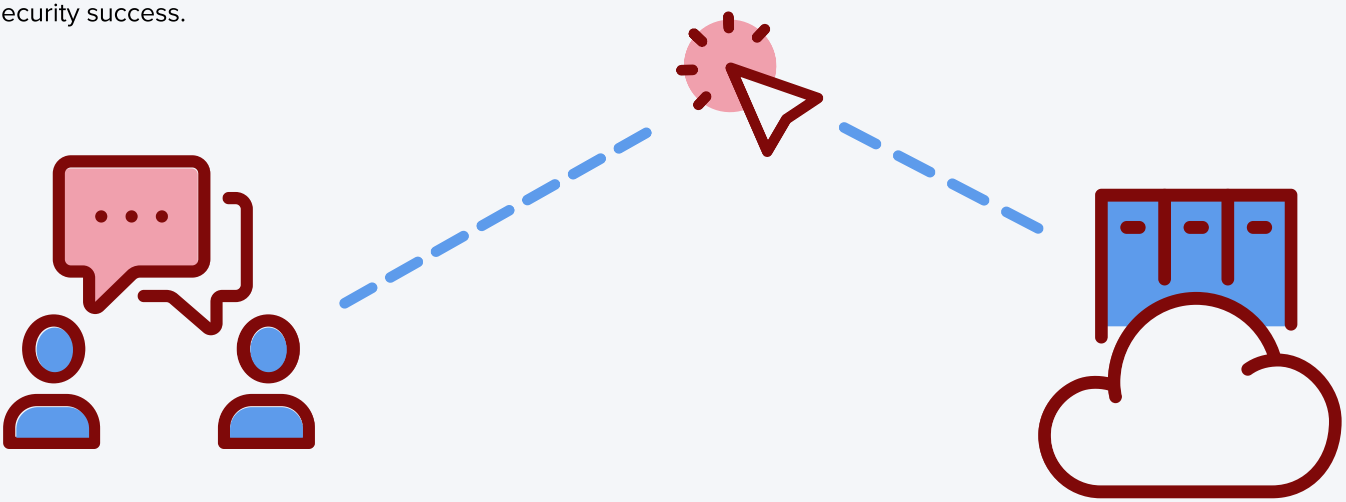
The definition of shadow IT is the use of any type of information technology device, app or service that is not managed or approved by the district’s IT department. This can and does refer to bringing in a personal computer that gets around the strict configurations of school-issued devices, your own Wi-Fi router from home to “add or expand” the wireless bandwidth in your classroom or office and any application or service used in conjunction with work as a student or educator not approved for use such as a personal Dropbox.

This seems harmless enough, especially when budgeting concerns limit access to technology that makes life easier, but it can lead to a huge problem. These apps/services are not properly vetted to reveals if there are any concerns or liabilities involved in using them within the district’s network.

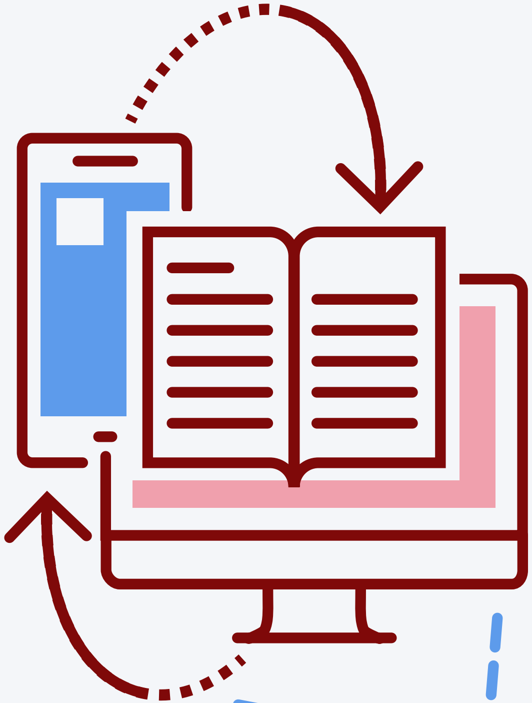
Lack of security awareness training

Who has the time to learn about security on top of prepping the classroom, resolving minor (and not so minor) issues, caring for the students, drawing up lesson plans, grading tests and, you know, teaching? We know, it's tough!

Sadly, threat actors know this too and they not only leverage this to their gain, but continually count on time crunch and the lack of security awareness training to attack the education sector. Training your staff, students and parents to actively spot email-based malicious content or text message scams, and develop greater security hygiene practices at school and home is critical to your cybersecurity success.



“He who must not be named”



The first step the magicians in the Harry Potter series took toward facing their fears was acknowledging them and personifying it by name: Voldemort. It wasn’t until this was done that the protagonists could mount a defense against the evils which threatened them.

Similarly, one of the first things to do in cybersecurity is perform a risk assessment to determine what equipment, apps, services, etc., are used by the school district, how often, to what degree and how it ranks based on its criticality. Once this has been done, you can then “face your fears” by knowing what types of threats affect the items within your risk assessment.

> While these lists can, and will, change depending on your district’s infrastructure needs, there are several threats that are accepted as being universal in their targeting of K-12 education.

External Threats

Among the varied types of threats that emerge from external sources, some of the most disruptive ones come from certain types of malware and Denial of Service (DoS) attacks. The latter seeks to prevent access to applications, services and websites by sending a flood of requests to the targeted service essentially preventing it from responding to any requests — legitimate or otherwise — affecting even some larger school districts in recent years. Making matters worse, these types of attacks can be amplified through multiple computers to form a Distributed Denial of Service (DDoS), which make it much more difficult to protect against.

The former threat relies on a type of malware called ransomware that gets its name by encrypting commonly used file types, like DOCX and PDF, with a randomly generated key. Once done, the malware signals back to a remote server where a request is made to decrypt or unlock your documents in exchange for a monetary payment. These can range from thousands of dollars to millions of dollars.

> **“57% of reported ransomware incidents involved K-12 schools – more than twice the number of school ransomware attacks reported in the earlier months of 2020.”**
>
> – Joint Cybersecurity Advisory coauthored by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)

Other external threats and attacks frequently targeting K-12 systems are:

Malware: A general classification for all pieces of malicious code, like a virus that runs on a device with the aim of obtaining unauthorized access to the device and/or data, and those connected to it within the same network.

Spyware: This type of malware operates discretely as it gathers information about the user. It obtains data, such as documents, pictures and often looks for Personally identifiable Information (PII) that can later be sold by attackers, such as social security numbers, student records, recordings made from built-in cameras and microphones, location data, credit card and financial credentials.

Man-in-the-Middle (MitM): When connecting to your school's Wi-Fi network, do you know it's connecting to the correct service? The aim of MitM attacks is to trick users into connecting to an attacker's website or service that is posing as a legitimate one to harvest credentials that are later used to gain further access to district resources.

Phishing: Similar to MitM above, phishing also relies on social engineering to fool a user but not through technology necessarily. Often, these attacks occur within email, text message and old-fashioned phone calls, persuading (or threatening) users with penalties, in order to get users to divulge sensitive information later used to compromise systems further and perform data breaches.

Vulnerability Scanning: Based on a legitimate IT process, scanning for issues helps teams to determine what problems exist in order to resolve them before they lead to a security incident. Threat actors have access to the same tools as the good guys and use them to actively determine which devices are vulnerable, then pivot to attack that weakness.

Communications Hijacking: Attacks against popular video and communications software, such as Teams and Zoom, occur when rooms have improperly configured settings, permitting outside attackers to disrupt communications, compromise conversations, endanger the wellbeing of students and/or expose sensitive information.

Internal Threats

Now let's be clear, any of the external threats listed above can be leveraged as an internal threat. The two are not mutually exclusive, however, the deciding factor is where the threat emanates from: internal user or an external, unknown entity. With that said, here is a list of common internal threats affecting K-12:

Social Engineering: While touched upon in the phishing section earlier, it deserves an additional mention since it is often the gateway that allows threats to succeed. For example, holding the door open for someone entering a secured entrance. The gesture is kind but may allow unauthorized persons to enter areas they are restricted from accessing.

Weak Passwords: The easier a password is to remember, the easier it will be to guess. This, combined with stolen credentials below, are two completely avoidable threat scenarios.

Stolen Credentials: Increased password complexity and the sheer number of passwords in use in both personal and professional lives can lead to writing credentials down, say, on a sticky note behind your keyboard or monitor. It may sound laughable but this poses a grave security threat for the user and their data.

Devices Not Up-to-Date: All devices and apps require frequent updates to "patch" bugs and vulnerabilities. Without the latest patches installed, devices are open to internal and external threats, making it trivial for threats to bypass built-in protections, gather sensitive data and further discovery of connected resources.

Data Theft/Exfiltration: Something as ubiquitous as a USB Flash Drive allows data to be stored and moved between devices, and is useful when taking work home with you. However, it can serve a more nefarious purpose as a means to move data from a secure location to a potentially unsecured one or aid in the removal of confidential records.

Misconfigured Settings: Computer settings are a lot like preferences, we all have them and they can differ from person to person. However, sometimes settings need to be set a certain way in order to secure devices and avoid potential issues, such as removing the ability for a web browser to store credentials to prevent anyone from simply walking up to a device and gaining access to your sensitive data.

Removing Endpoint Protection: While this has become more difficult to do over the years, it is still a possibility, with users often citing a decline in performance as the main reason, to remove the same software that protects your device against malware threats.

Shadow IT: Discussed previously, shadow IT's aim is to resolve a problem, despite often leaving one or more security-based problems in its wake.

You may be thinking, how is this critical to student success, how does it affect student performance? Cyber security has both a direct and indirect impact on a stakeholders ability to learn and work.

Digital divide

Depending on your demographics, the number of students without access to reliable broadband Internet access at home could vary from the average of 40%, as noted in a survey by the Public Policy Institute of California (PPIC). While there have been a number of local, state and federal initiatives to boast the number of devices in the hands of educators and students in recent years, the digital divide is still a very real concern for many school districts, especially when factoring in that these devices and mobile hotspot Internet access are the only means they have to take part in distance learning or perform their home learning assignments.

No access to devices or resources

Simply put, if a device is inaccessible due to a technical issue, is currently sitting with IT in triage or waiting on a 3rd-party vendor for service, then staff or student are essentially without their tools. Same thing applies to software or services that are unavailable. If they cannot be accessed, that represents lost opportunities for teaching and learning.

Funding tied to student progress/test results

Like the digital divide mentioned above, the topic of testing results and student progress affecting the amount of funding received may well vary from district to district and be based greatly on demographics for your area.

- Performance pay or promotions for educators and administrators
- One-time bonuses for educators
- Increased funding for schools or school programs
- Access to certain grants or alternative forms of funding
- Low performing schools may be required to offer tutoring
- Poorly performing schools may find educators and administrators replaced

Student online safety

We all agree that the safety of students and staff are of paramount importance in K-12 education. Due to the increase in security threats as technology embeds itself deeper into our daily lives, plus the growth of cybersecurity attacks targeting the education sector, the days of simply installing antivirus software on your devices are long gone.

In addition to malware threats and attacks on apps and services, there are malicious threat actors looking to capitalize by breaching networks to obtain student records to sell on the dark web. Worse still, lacking the proper security controls can endanger the well-being of stakeholders by spying on them unknowingly through cameras or microphones, tracking their locations, or by posing as someone they know to commit more severe crimes. Educating students on the importance of online safety while guiding them in learning the skills to self-identify threats is key to a robust online security curriculum.

Ask M.O.M.

Back in the Wizarding World of Harry Potter, the Ministry of Magic act as the gatekeepers of information and all things relating to magic. In the K-12 education sector, you've got Jamf to help cut through the misinformation to determine what security practices best apply to your unique needs and, of course, work with you every step of the way to implement them successfully.

Before we get ahead of ourselves, let's take a moment to address some of the common views and misconceptions pertaining to Apple security, including perceptions about the role cybersecurity plays in K-12 education.

Apple doesn't get viruses: This was never completely true, Mac just weren't as popular. Therefore, malicious actors focused on Windows which had a larger market share. In recent years, this has changed dramatically and Apple's skyrocketing growth has proven to be a sizable target.

Education is highly targeted: True. In fact, a report by Bitdefender found that K-12 is ranked as number two, just behind retail, as the highest target for ransomware. While malware represents only one type of threat, it is among the more significant threats.

Education is weak on security: This is certainly how it is perceived according to threat analysis and report findings, such as one conducted by Security Scorecard which found that, "out of 17 industries in the U.S., Education comes last in terms of total cybersecurity." Specifically, the report noted that patching cadence and app and network security were among the highest concerning pain points.

Security is difficult & costly: There is a dearth of cybersecurity professionals, this much is known. Part of this is due to it not being an easy job to do. With that said, knowing your environment, assessing your needs and working with trusted partners to address those concerns is paramount for a successful cybersecurity program. Trusting the "hype" without verifying the solutions is a recipe for disaster, making it a difficult path to maneuver, and a potentially costly one at that. In that same vein, throwing your hands up in defeat has the potential to leave your district open to threats, with the process to clean up a data breach and address compliance penalties being a steep cost.

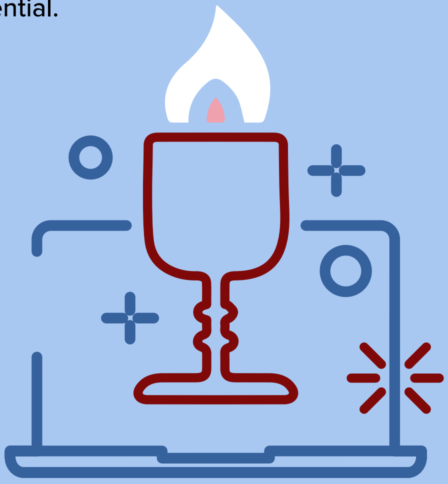
Ask M.O.M.

> “Hackers only need to get it right once; we need to get it right every time.”
>
> – Chris Triolo, a security professional at HP

One size fits all solutions: Going hand in glove with the difficulty vs cost above, is the myth of the “one size fits all” solution. A vendor can develop multiple solutions that work together to address many threats, sure, but this specifically refers to a single product that claims to address all threat aspects. Historically, products such as these have lacked in several of its aims, and in the cybersecurity realm that won’t cut it.

It’s an IT problem: This is more of a generic view held by many but is important to the discussion of K-12 education. When framed within concerns over budgets and time, it’s easy for a stakeholder to feel as though there’s a line in the sand the demarcates where their job functions end and another role begins. The truth is security – like littering – is everyone’s problem and it’s one that takes the effort of all stakeholders to uphold. Consider the analogy about a chain being as strong as its weakest link.

Don’t worry about security unless you’re hacked: Dubbed the “bury your head in the sand” approach, nothing could be further from the truth. The fact is that, at one point, all institutions were not affected by a security breach...until they were. Being proactive versus reactive offers district’s the opportunity to monitor for threats, detect points of concern and remedy them to prevent threats from evolving into something far more consequential.



Jamf + Apple

Working closely with Apple, each solution is purpose-built to not only protect your devices, users and data, but to do so using the smallest number of resources, so as to work seamlessly within the user experience Apple products are known for.

Together, merging the services and equipment Apple provides alongside Jamf solutions that address and exceed the unique needs of the K-12 education sector. Students and teachers can feel empowered, prioritizing the use of technology in new and imaginative ways, while IT and Security teams can rest assured that risks are mitigated and threats minimized by solutions that target device management, identity provisioning and authentication and endpoint protection in background.

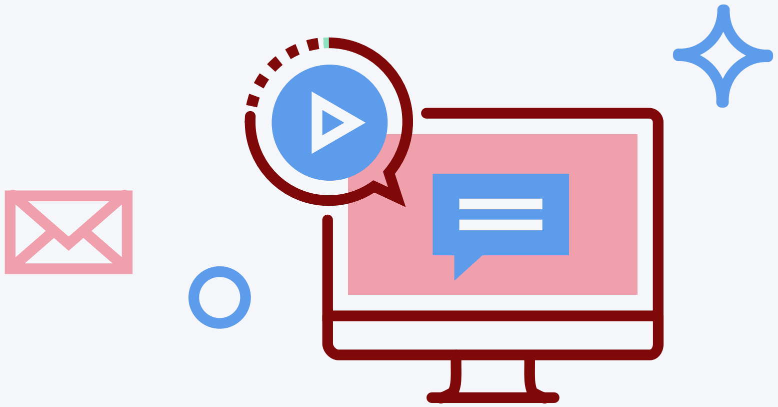
Apple School Manager (ASM)

Initialize the endpoint management process with the centralized, cloud-based console that is as powerful as it is easy to use. Provided free of charge by Apple, the service synchronizes purchases made with the online console and provide IT a means to establish a connection to the district's Mobile Device Management (MDM) software to facilitate automatically enrolling devices for management.

Jamf School

The flagship EDU solution designed to manage all devices in the Apple ecosystem yet tailored exclusively for teachers, instructional technologists and Mac admins in the education sector. The Jamf School MDM solution empowers over 36 million students globally by making it easy for educators to leverage classroom management functionality, curate apps, lesson content and restrictions and easily rollout managed Apple ID's without needing to be a wizard — technical or otherwise. Additionally, the built-in incident management system helps keep track of issues reported, like devices out on warranty repair, all of which ultimately build toward a successful cybersecurity strategy.

Learn More



Jamf Pro

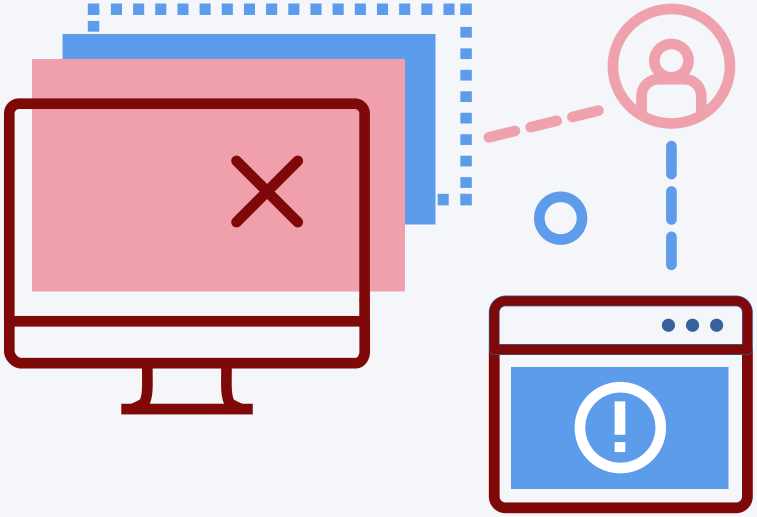
The industry-leading MDM solution for organizations that require an MDM platform with advanced functionality and support models. Jamf Pro includes all the same features as Jamf School while adding automation and robust integration with other products in your network and systems management stack, such as Application Programming Interface (API) access to secure communications between apps and services or highly technical features that provide dedicated IT teams the extra muscle needed to manage multiple schools or an entire school district.

Learn More

Jamf Connect

Leveraging centralized, cloud-based account management, Jamf Connect is the pivotal crux that allows accounts to be provisioned for users to authenticate to their Mac. More than that, it permits them to do so with just one account – no remembering multiple passwords – achieving true Single Sign-On (SSO) to access all assigned apps and services, including Multifactor Authentication (MFA) that adds a second layer of access protection.

Learn More



Jamf Protect

Jamf Protect puts the spotlight exclusively on Apple security by helping Security teams to prevent known malware, detect threats and use behavioral analytics to identify potential risks to your devices' health. Additionally, it boasts real-time alerts and logging, offering granular visibility into endpoints to not only achieve your regulatory compliance goals, but provides IT the opportunity to remediate issues and help users without getting in their way.

Learn More

Take your education technology to the next level

Want more details about what Jamf provides or have questions about implementing these tools in your own school? Start a free trial to jump right in.

Request Trial

Or contact your preferred reseller of Apple hardware.