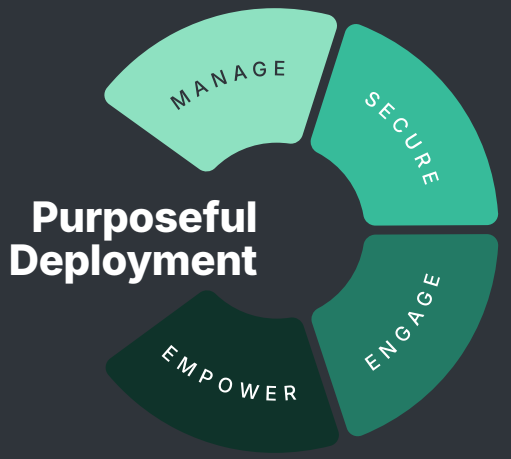
jamf



How to Secure K-12 Devices and Protect Student Privacy

Schools use technology in a variety of ways: to enhance learning, to make lesson planning easier for teachers, to catalog student data, and so on. This means that schools hold a host of data, including sensitive Personally Identifiable Information (PII) that attackers crave.

With a **75% increase** from 2023 to 2024, **education topped the chart** as the most targeted industry for cyberattacks globally — **at a whopping 3574/week**. Attackers are hungry for student data — and cybersecurity is critical to protecting it. A security compromise can affect students in multiple ways:

- Their data can be exposed and exploited.
- Data around their background, well-being, discipline, attitudes and more can alienate them from their peers.
- Learning can be interrupted as systems are restored — often taking a lot of time and money.

Schools combat threats by logging relevant endpoint data for compliance or incident response. And many choose Apple devices for their built-in security features.

While Apple devices provide a secure foundation, attackers are continually finding ways to bypass these features. **Layering security solutions on top is a necessity.**

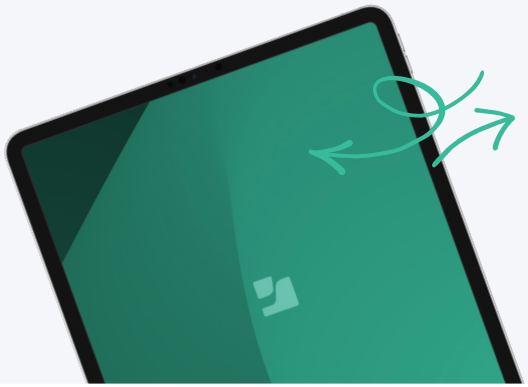
There are a lot of options out there, but it's not sufficient to choose one without significant forethought. Some solutions can look a lot like the very threats we're trying to prevent as they:

- Are too intrusive and disruptive
- Undermine privacy
- Reduce trust in the institution

That's where **purpose** comes in. In the second e-book in our purposeful deployment series, we'll talk about what it means to obtain privacy and security with **purpose**. We'll learn why it matters, how to find your purpose and how Jamf can help.

Threats to security

External threats



Cryptojacking

Cryptojacking malware takes over devices to generate cryptocurrency. Affected devices often become overwhelmed by the background processes required, rendering them unusable for anything else — including learning.

Ransomware

Ransomware affects the data on a system or device, encrypting the data and preventing access. Users must pay to regain access. Some ransomware also exfiltrates data to be sold or demands an additional ransom for its return—with no guarantees. This can shut down a school's operations, throwing a wrench into teachers' planned lessons and students' learning experience.

Phishing

Phishing attacks use social engineering tactics to collect information from users, like their login credentials. This could be a carefully constructed email or a lookalike website that tricks users into inputting their data. If not protected, younger students, in particular, can fall for these attacks.

Malware

Malware is any software code designed for malicious purposes. It can steal information, give attackers access to your systems and deliver other harmful programs to your device.

Man-in-the-Middle (MitM)

MitM attacks occur when a bad actor intercepts communication between two parties. The attacker may impersonate your school's Wi-Fi, for example, collecting data from unsuspecting users that connect to it.

Spyware

Spyware is privacy-violating malware that watches users' every move, collecting passwords, browsing history and more.

Deep dive: Defend against common external threats

Tap below for continued education

Free downloads that aren't worth the cost.

Malware in K-12 for Beginners >

Feeling salty about a clogged inbox?

Spam in K-12 for Beginners>

Keep your CPUs out of the crypto mines.

Cryptojacking in K-12 for Beginners>

Caught suspicious links in your inbox? Don't fall hook, line and sinker.

Phishing in K-12 for Beginners>

Internal threats

Social engineering

Social engineering attacks take advantage of users' naivete or lack of education to gather information. Students, teachers, and admins risk data theft and security breaches when attackers use fake messages or impersonation to gain unauthorized access.

Out-of-date devices and apps

Out-of-date devices and apps often lack the latest security enhancements and features. With the right tools, automatic updates can be an easy win for your security posture.

Shadow IT

Shadow IT occurs when end users install unapproved software or otherwise circumvent security controls. Providing a variety of approved apps and making it easy to request new ones can reduce the odds of rogue installs.

Human error

Human error can lead to breaches or dissemination of data — like if a user leaves a sticky note with their login credentials or accidentally emails the wrong recipient.

Misconfigurations

Misconfigurations can create vulnerabilities in your system. For example, weak password enforcement, inadequate content filtering and a lack of access controls can make it easier for attackers to gain access.

Schools are subject to regulations

Like many other institutions, schools are subject to data protection laws. For instance, the U.S. **Family Educational Rights and Privacy Act** (FERPA) prevents the distribution of PII in educational records without written consent. U.S. schools funded by E-Rate discounts or by the Department of Education are subject to the **Children's Internet Protection Act** (CIPA) and the **Protection of Pupil Rights Amendment** (PRPA), respectively. Schools in the EU must comply with **GDPR** practices, while the U.K. offers **statutory guidance for schools** on safeguarding children.

All this is to say that schools likely already have security tools in place to meet these requirements. Is it enough? Are you truly using these tools to achieve your goals or just checking a box? Ideally these tools enhance learning and simplify teaching — while delivering security and privacy. But reality can look different.

jamf

Finding purpose

External threats, internal threats, compliance requirements and privacy concerns all make security a top priority. But to protect devices effectively, you must also understand the purpose behind your deployment.

School decision-makers want students to learn and teachers to feel empowered. Technology can support this — if chosen with a clear purpose in mind. Educational technology shouldn't be allowed to just run amok, violating privacy standards for the sake of "security." Alternatively, it shouldn't lock down devices so tightly that they're secure simply because no one can access anything useful when they need to.

Translating your purpose into your security stack isn't always straightforward. Answering these questions is a good place to start.

Consider:

1. **Where are end-user devices used: At school? Home? Elsewhere?**

2. **Are devices used by more than one individual? Are they shared at school or at home?**

3. **Are devices used for independent learning away from the classroom?**

4. **Do students have access to email on the device?**

5. **What is the desired stance on student privacy for your deployment?**

6. **Do all students receive digital literacy training, including cybersecurity training on malware, phishing and other threats?**

Exploring these questions can help admins balance security, privacy and learning.

jamf

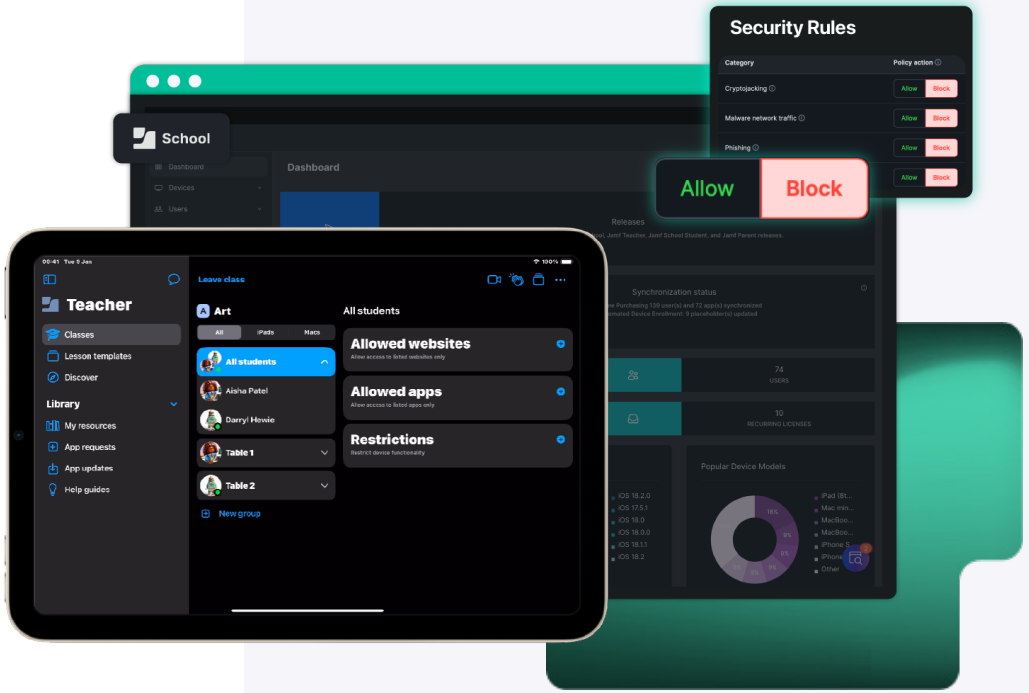
Keep even the scariest attacks at bay

Web threat protection

Any device connected to the internet is vulnerable to potential attacks such as malware, phishing attempts, command-and control servers and beyond. Students may come across these attacks on websites, infected apps or messages they receive.

Defend against these with web threat protection capabilities. Even if students come into contact with these threats, Jamf can prevent them from executing. This protects your data and preserves student safety — even if students don't recognize the danger. With web threat protection:

- Devices are protected, regardless of a student's experience with technology.
- School data doesn't travel on insecure connections.
- Devices are protected against even the newest threats.



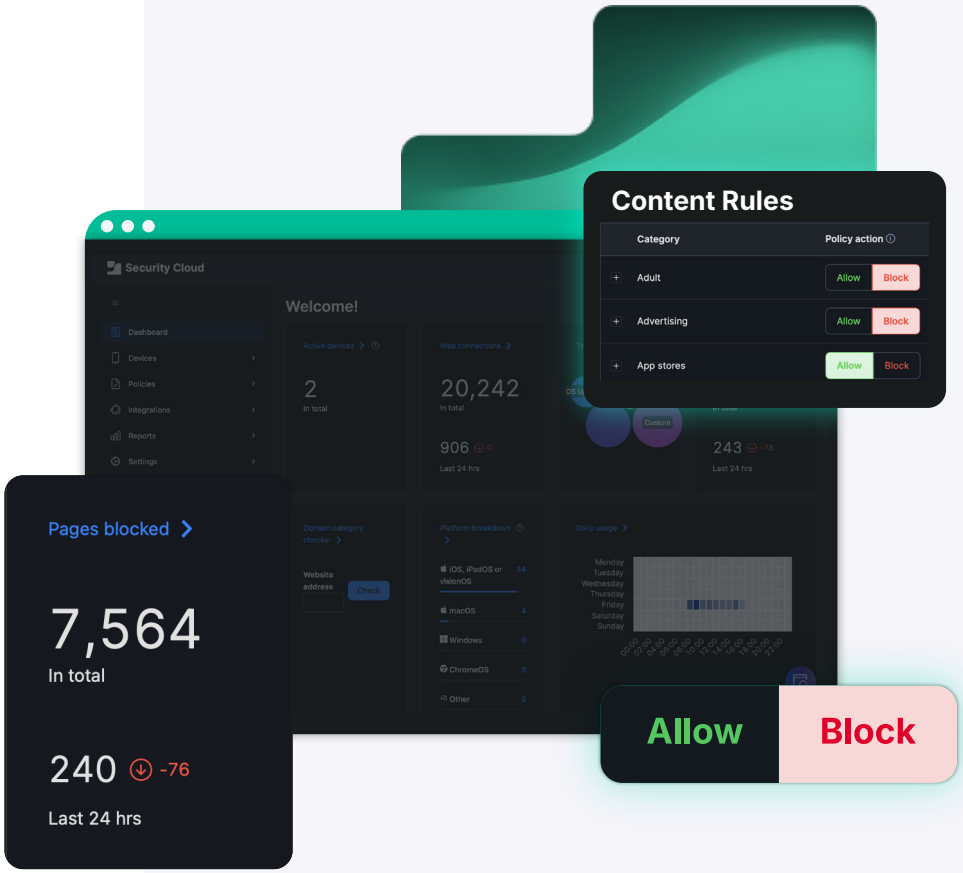
Focused and safe browsing

Content filtering

With the internet at their fingertips, students are tempted by entertainment and distraction. This can lead them down paths that disrupt their learning — or worse, put them or their personal information at risk.

Content filtering keeps students on task and out of harm's way by blocking traffic based on preset categories such as messaging, entertainment, games, and adult content. With content filtering:

- Students stay more focused on learning.
- Teachers don't have to compete for attention.
- IT can worry less about devices at risk.



Security with no borders

On-device functionality

With school-managed devices on protected networks, schools can get a sense about how secure their device are. But what about outside the school building, at students' homes? Or on public Wi-Fi?

The need for protection doesn't disappear. On-device security remains essential. On iPad and Mac, content filtering works directly on the device, across any network, in any location. On-device protection means:

- Students can learn safely and securely, even away from school.
- Browsing history is processed on-device, protecting privacy.
- Security controls can't be bypassed by third-party services.

Here are just a few key benefits Jamf specifically brings:

- Machine Learning that detects phishing attempts at the device level.
- Custom rules get evaluated on the device to ensure security polices are enforced.
- Compatible with third-party VPN, proxy, and DNS services, with no option for users to bypass.

Uninterrupted learning

Endpoint protection

Even with the best threat defense, malware can end up on your device. Detecting these threats is a necessary capability in your security stack.

Jamf identifies threats of many types — spyware, cryptojacking malware, phishing attacks and more — and can quickly fix the problem. With Jamf:

- Learning isn't disrupted by out-of-commission devices.
- Fast remediation reduces the impact of successful attacks.
- Devices are protected against a wide variety of malware families and threat types.

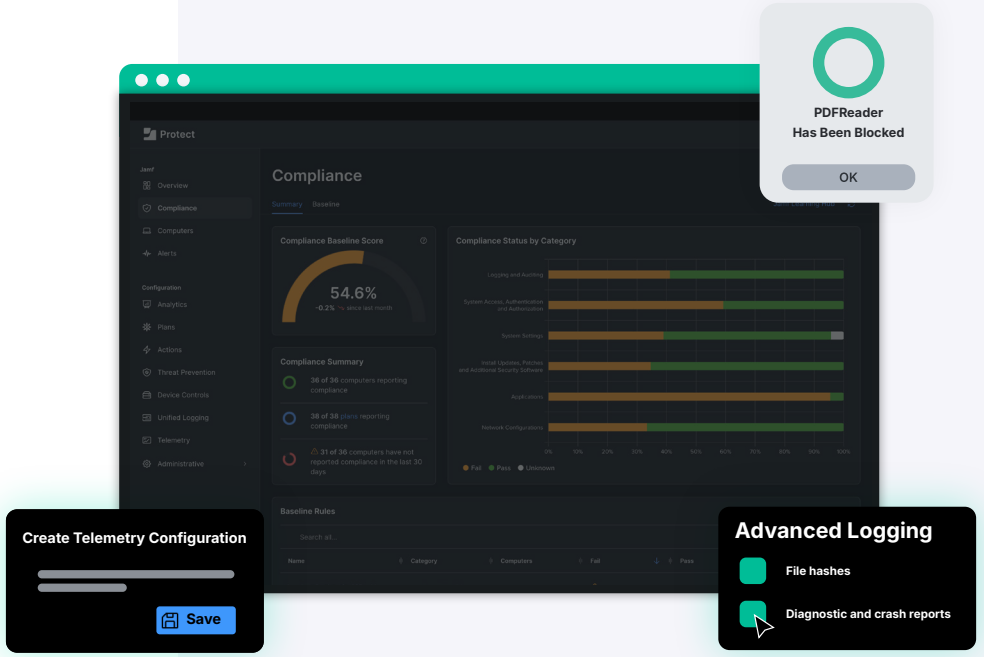
Full system transparency

SIEM/SOAR integrations

It's impossible to know how secure your device fleet is without insight into their status. Integrating your management and security software with your security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions grants vision into fleet health and is necessary in today's device security world.

Integrate your SIEM/SOAR with Jamf and:

- Stay on top of device compliance and logs
- Gain deep understanding of your network and devices
- Be better prepared to address device issues — reducing recovery times in case of an incident



Stay informed and ready for action

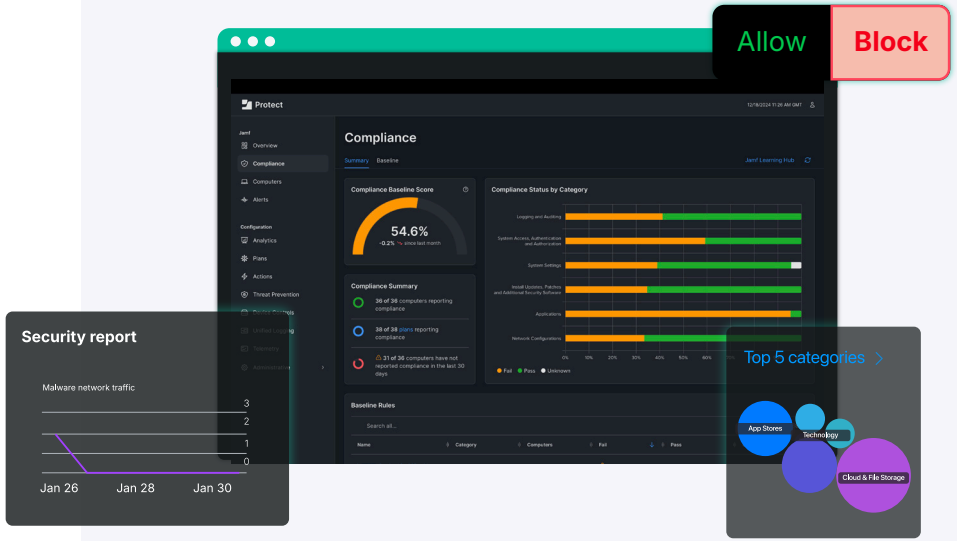
Security reporting

Simple reporting is necessary for admins to make sure their devices are enrolled, compliant and behaving correctly. Jamf gives admins reports that:

- Show what devices are enrolled in MDM and their compliance status
- List spam, malware, cryptojacking and phishing sites that were accessed and blocked
- Show data usage based on the day and time
- Display what site categories are visited by users

With these reports, admins can:

- Take immediate action in case of an incident
- Adjust their defense strategy based on user behavior
- Deliver informed records about their device fleet in case of audits or other inquiries



Models of Purposeful Deployment

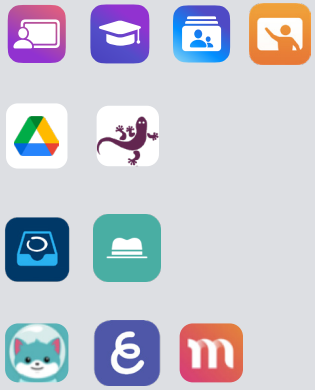
Once you've **found your purpose**, the details of your deployment strategy fall into place and you're left with one that:

- Influences and accelerates learning
- Creates equitable student opportunities
- Ensures secure and scalable deployment

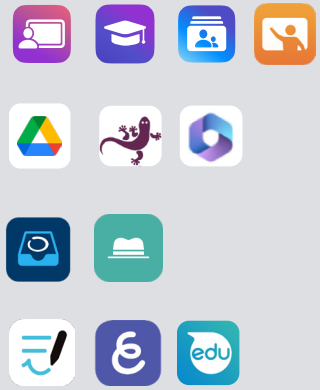
Management and security make up your foundation: IT can provide apps, devices and procedures that empower and engage learners and educators — without compromising security and privacy.

Your purposeful deployment journey begins to look like this:

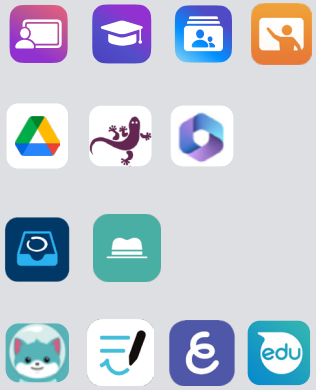
Primary
K-5



Secondary
Middle, High



Trust
District



Manage and Secure

Engage and Empower

jamf

IT-enabled security and privacy for next-level, fearless learning

A purposeful deployment starts with a clear strategy that integrates security and management seamlessly, ensuring K-12 devices are not only protected but aligned with the needs of your school community.

Reinforcing your devices with Jamf security allows for worry-free and uninterrupted learning — helping students and teachers thrive while reducing the risk of data loss and device compromise.

With powerful threat prevention and content filtering features:

- IT can keep devices in compliance and protected from a wide array of threats.
- Teachers can stay focused on teaching without devices going out of commission or distracting students.
- Precious student and school data stays private and out of attackers' hands.

See how the right tech enhances the learning experience.

Try Jamf today

jamf