Cyber Essentials in Education

jamf

Cybersecurity + EDU can be a difficult class to pass, but it doesn't have to be like a Calculus problem to solve. With Cyber Essentials, the United Kingdom and the National Cyber Security Centre have developed a certification path for schools to help them protect their students, educators, devices and data from criminals and cyber attacks.

In this e-book, you will learn:

- How changes to education have impacted cybersecurity threats
- What are ten basic security controls that EDU should be implementing
- What Cyber Essentials is and how it works
- How earning this certification can help your institution mitigate many of the challenges to cybersecurity

Cybersecurity is less a singular practice or the implementation of a product to keep your students, educators and their devices safe — more a way of life. Put another way, “it’s not the destination, it’s the journey”, to quote Ralph Waldo Emerson. Better still, it’s the on-going, never-ending path that IT and Security teams must walk to fortify educational network resources in order to keep data secure and privacy safe from threat actors or any unauthorized access.

All this may seem daunting. And honestly, to those that aren’t well versed in the latest cyber threats, it may be a difficult journey...but not an impossible one, especially when schools partner with industry leading organizations that serve as experts in the realm of securing computing assets like macOS and iOS-based devices. With the right team by your side, educators have the freedom to help themselves and their students succeed with Apple, confident in the knowledge that the “heavy lifting”, as far as cybersecurity is concerned, is handled through the combined support of their partners.

> **It’s not the destination, it’s the journey.**
>
> — Ralph Waldo Emerson

So, who represents this group of partners?

Great question! It starts with you, the educator, and your team of IT and/or Security professionals, if that support is available to you. Next, we move on to the obvious choice: Apple. Their security and privacy-first approach to the MacBook Pro and iPad is second to none. Additionally, the software they develop embraces this approach by incorporating it directly into macOS, iOS and iPadOS at a foundational level – not as an afterthought.

Moving along to the following partner is Jamf – the industry leader in device management and security solutions with an Apple-only focus. Jamf solutions such as Jamf School are designed to be powerful enough to manage devices, configure security settings and integrate with a whole host of software services from various vendors that educators rely on — such as Google — to manage digital classrooms and interface with their students. And yet, Jamf School is easy to learn because it was developed with simplicity in mind to help admins take care of day-to-day issues that arise.

Lastly, there are certification partners. In this case, the Cyber Essentials certification that not only helps you to guard your organization against cyberattack, including the most common threats, but also demonstrates your institutions commitment to cybersecurity

Before we dive into Cyber Essentials certification however, let's first discuss how cybersecurity changes have impacted education, the change to learning environments and the shift to mobile devices, shall we?

Winds of change

If you haven't picked-up by now, cybersecurity is dynamic, meaning it is ever-changing and constantly in motion. There may have been a time when Mac barely had any malware authored for the platform, not as much because it was impenetrable but more because it wasn't as popular a target as other operating systems.

The explosive growth of Apple products and its meteoric rise in popularity among consumers and all types of organizations has made certain that malware authors stand up and take notice of the fertile, untapped grounds awaiting them in the form of hundreds of millions of Apple users worldwide.

Jamf Threat Labs, the security and research arm of Jamf actively monitors and studies all manner of threats affecting macOS and iOS-based users to not only incorporate the latest protections into Jamf solutions, but also to determine attack trends and use that data to provide guidance for our products and customers alike, to best secure their environments.

Access to learning from anywhere, at anytime

Among the changes that have occurred in education within the last few years, few have had the greatest impact that remote learning has. Not just due to safety precautions spurred by the global pandemic, but the sudden need to shift operations from the face-to-face model to one that required a substantial change in infrastructure. Not to forget changes to security, permitting remote access to educational resources for all stakeholders and a modern computing device for each student and educator to learn and teach from respectively.

Some institutions continue to struggle with this tangential shift on how learning is accomplished. True to form, bad actors took a beat to upgrade their methods and attack infrastructures too, shifting their operations to take advantage of the unbalance brought about by the new changes. Attackers began targeting remote users with aggressive phishing campaigns, disrupted virtual classrooms with ease, compromising devices with malware and gained unauthorized access to sensitive data by pivoting access through cloud-based storage services.

A bit of good news though has been the shift toward mobile devices, like the Apple iPad. The thin, lightweight and extremely powerful yet versatile tablet, with incredible battery life and strong protections baked right in, makes it the ideal educational tool for educators and students alike. The blend of modern technology in an affordable package, combined with support for many of the apps and services educators rely on, plus being a ubiquitous communications tool truly allows for learning to occur anywhere, anytime with no equal.

Where are these trends pointing?

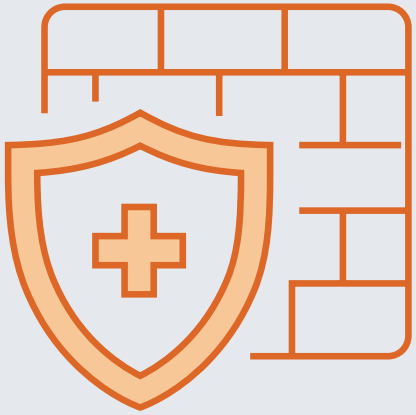
According to the Security 360: Annual Trends Report by Jamf, some key takeaways in the last year are:

- Malware installations on remote devices **doubled**.
- Risky device configurations negatively impacted **1/5 of organizations**.
- Compromised devices accessing collaboration apps (like Zoom and Microsoft Teams) increased from **34% to 64%**.
- Almost **half** of users surveyed admitted to not using VPN technology, despite understanding the importance it plays in securing network traffic.
- Mac-based malware **continues to grow** in prevalence but also sophistication with attackers upgrading their methods and targets to improve efficacy.
- Apple is the number one brand used in **phishing** campaigns in 2021
- Privacy is just as **critical** to device security as it is to the end-user. Moreover, compliance with regulations has increased its focus on maintaining end-user privacy as a key factor.

While threats, much like fashion, are subject to trends, some of these run their course and fizzle out (I'm looking at you shoulder pads from the 80's). Others evolve over time, growing into something far different —and potentially worse— than its initial outing.

That said, remember that cybersecurity is an ongoing path that must be forged. And, just as you'd have tools to build something like a new deck to your front porch, in this case you leverage security controls to aid you in strengthening your security posture against risk, threats and attacks – new and yet to be seen.

10 basic security controls

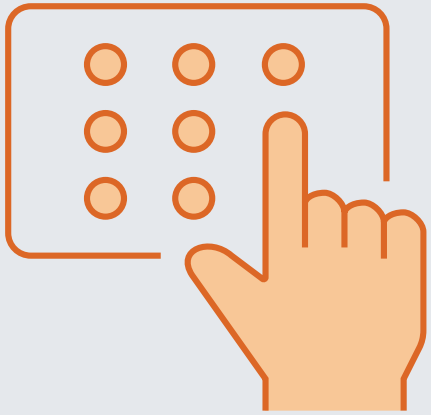


1 Firewalls

Firewalls function as the barrier between the internal networks, which need to remain secure, and the Internet, which should be treated with caution. They should be installed on any device that can access the Internet. They're particularly important when staff use public or otherwise insecure Wi-Fi, whether they're using school or college devices or their own to access work resources.

2 Secure configuration

The default configurations on devices and software are often as open as possible to make things convenient and easy to use, but they also provide more access points for unauthorized users. Disabling or removing any unnecessary functions and changing default passwords reduce the risk of a security breach.

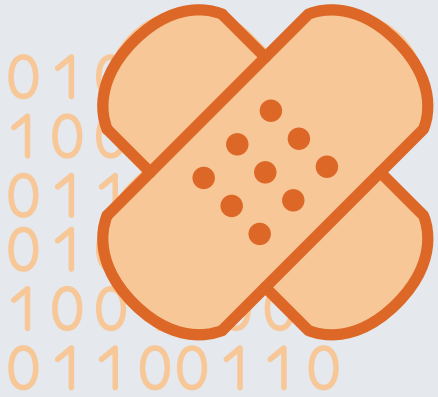


3 Access control

Giving a lot of people access to your data and services is convenient, but also means that there are more accounts that, if compromised, can lead to a serious breach of security. It also increases the chance of an unintentional breach, like someone accidentally deleting data that should be kept. Ensuring that access is given on a 'need-to-know' basis only, with 'access denied' as the default option, will help reduce the scope for a breach. On top of that, all accounts should be password-protected with strong passwords, and where the risk of a breach is particularly high, like the compromise of an admin account, you should consider implementing two-factor authentication (2FA). The cyber-attack described earlier could have been prevented with 2FA.

4 Malware protection

Malware such as viruses and ransomware can infect your systems when, for example, a member of staff is tricked by a phishing email. But it is also commonly introduced through removable storage drives like USB sticks. You can protect the organization from malware by using antivirus or anti-malware software, and techniques like "allow lists" and "sandboxing" (running an application in an isolated environment with no access to the rest of your networks or devices, to find out if it's malicious).



5 Patch management

Manufacturers and developers normally release regular updates that not only improve the software but also fix or ‘patch’ any discovered vulnerabilities. Installing those updates as soon as they’re available minimizes the time frame in which those vulnerabilities can be exploited. If the manufacturer stops offering support for the hardware/software you’re using, it’s time to replace it with a more up-to-date alternative or retire it.

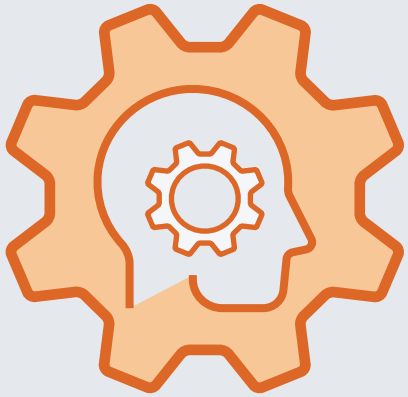
Note: The first five are all you’ll need to obtain the Cyber Essentials certification (discussed in further detail later), but at Jamf we believe there are a few other essentials that make a complete security solution.

6 Identity provision (IdP)

Cloud-based IDP allow for centralized management of user accounts and secure authentication utilizing the remote database to handle requests to educational resources – locally or externally – such as those served from web-based services, public and/or private clouds or Software-as-a-Service (SaaS) platforms. Authentication requests may also be provisioned through a portal, providing stakeholders one place to access all the resources they need by enabling Single Sign-On (SSO).

7 Zero Trust Network Access (ZTNA)

The modern solution for securing connections, not just network-based communications like VPN, but taking it a huge leap forward by enabling perimeter-less security. Implementing microtunnels that are application-specific to securely connect to resources from anywhere, over any communication standard. Furthermore, when integrated with IdP, stakeholders can access resources based on their credentials. Additionally, ZTNA can check for device health to determine if authorization should be granted or denied – until devices are brought into compliance – to mitigate risk.



8 Machine Learning

Automation is one small benefit to machine learning technologies. The ability for computers to quantify data streams and examine whether commonalities exist, such as correlating past attack data with that of a particular app, service or bad actor provides IT and Security teams incredible insight into not only the attacks that have occurred but details necessary to prevent future attacks before they happen. After all, the speed at which computers can analyze data is far greater than that of human being and what manual processes allow.

9 Mobile threat defense (MTD)

Similar to desktop-based security solutions, MTD offers prevention from malware and protection from security threats that target mobile devices, such as iPad and iPhone. Why a separate type of software to protect against these threats? Simply put, the design of mobile devices differs from how macOS-based devices operate. Threat actors must develop novel ways to attack mobile devices, necessitating a cloud-based solution that protects against a variety of unique mobile threats from malware to network-based attacks through policy-based management and regular device health checks to verify compliance.

10 Regulation compliance

Speaking of compliance, education is a regulated industry. Globally, EDU is recognized among the top targets for cybersecurity attacks, while unfortunately ranking as the least secure among multiple industries. The combination of low security/high attack rate + government regulations means when a data breach does occur, it's a major problem for all stakeholders. Maintaining compliance, while easier said than done, is possible and offers schools the ability to maintain a strong security posture, minimize risk from threats, ensure devices are all configured according to required levels, while helping schools bounce back quicker if devices are compromised by keeping established baselines of device performance and configuration levels in check.

We now have a clearer idea of the cybersecurity landscape in education, including the myriad threats and challenges that impact modern learning. Additionally, we covered the basic security controls that best support EDU's goal of educating the future of tomorrow today. Let's revisit Cyber Essentials and how that can further aid education in service to its goal.

What is Cyber Essentials?

According to the UK's GDPR website, Cyber Essentials is "Cyber Essentials is a UK government scheme supported by the NCSC (National Cyber Security Centre), and is intended to help organsations of any size demonstrate their commitment to cyber security, while keeping the approach simple and the costs low."

The five basic security controls required are:

1. Firewalls
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

Focusing on **five** key cybersecurity controls, EDU can easily put these controls into production which provide protection "from around **80%** of common cyber attacks", according to the NCSC.

Why Cyber Essentials?

Schools and other educational institutions in the UK that receive ESFA funding were required to obtain Cyber Essentials certification, beginning in 2021. In doing so, education providers support the UK's push toward improving its cybersecurity in education, among other facets of society.

Achieving Cyber Essentials certification not only demonstrates EDU's commitment to students, educators and all stakeholders that cybersecurity and protecting user privacy are taken seriously. Through implementation of the security controls outlined below, EDU helps to raise security awareness within their schools, but also succeed in protecting the confidentiality and integrity of sensitive data with **"appropriate technical and organizational measures."**

How will Cyber Essentials help?

The Cyber Essentials scheme is designed to mitigate risk by minimizing threats from the most common cyber attacks. It is estimated by the NCSC that approximately **80% of all attacks rely on little to no cybersecurity threat protection, often being automated criminals operating remotely.**

By implementing the **five security controls** above, mitigation of these types of cyber threats may result in preventing cyber attacks *if/when* they occur. If an attack does result in compromising a device, the level of protection afforded by implementing adequate security controls in place could certainly minimize the attacks impact as the device's attack surface has been fortified.

Greater mitigation of an attack means less of a negative impact, while the time required to triage and remediate a device is cut shorter, allowing affected students and educators to get back to learning and teaching sooner rather than later.

How does Cyber Essentials certification work?

There are two tiers to Cyber Essentials certification. Each provides a level of assessment that must be undertaken by completing a self-assessment questionnaire (SAQ) to show that the five basic security controls have been implemented.

Cyber Essentials: SAQ must be completed.

Cyber Essentials Plus: In addition to the SAQ, this tier requires that a hands-on technical verification be completed, consisting of the following:

- External vulnerability scan
- On-site assessment
- Network-based vulnerability scan

For educational providers that wish to take a closer look at their cybersecurity readiness before applying for Cyber Essentials certification, they can take a free assessment with an assured service provider associated with the NCSC that consists of questions designed to provide schools with granular insight into their computer fleet and networks. Furthermore, the readiness check provides details regarding what must be included during the formal SAQ, so that nothing is left out or otherwise missed.

> The journey of a thousand miles begins with one step”
>
> – Lao Tzu

Jamf + Cyber Essentials certification
A winning combination for you, EDU and cybersecurity!

jamf

To learn more about applying for Cyber Essentials certification, visit the National Cyber Security Centre's website.

To see how Jamf can help you demonstrate your commitment to cybersecurity by safeguarding your school against cyber threats:

Learn More

Or contact your preferred reseller of Apple hardware.