5 Modern Security Tenets

Higher Education Admins Need To Implement

jamf

Security in Higher Education can be tricky for institutions to harness effectively. Sure, it shares many similarities with enterprise protections, but what truly makes securing HiEd challenging are the strategies needed to protect students and faculty – using both institutionally issued and personally owned devices – while keeping institutional resources safeguarded.

Achieving this is a significant challenge for HiEd, especially with the ever-growing bullseye on every user, device, and protected resource. For example, as part of its Verizon 2024 Data Breach Investigations Report on the state of security, Verizon found that Education placed 6th out of 21 industries based on the total number of incidents that occurred (1,780). Education also achieved 1st place, with 1,537 of those incidents leading to a confirmed data breach.

In other words, as threat actors increasingly target higher education, the main methods they use to exploit vulnerabilities and gain unauthorized access to personal, private, and institutional data are system intrusions, social engineering, and misconfiguration errors.

What to expect (and what's expected of you)

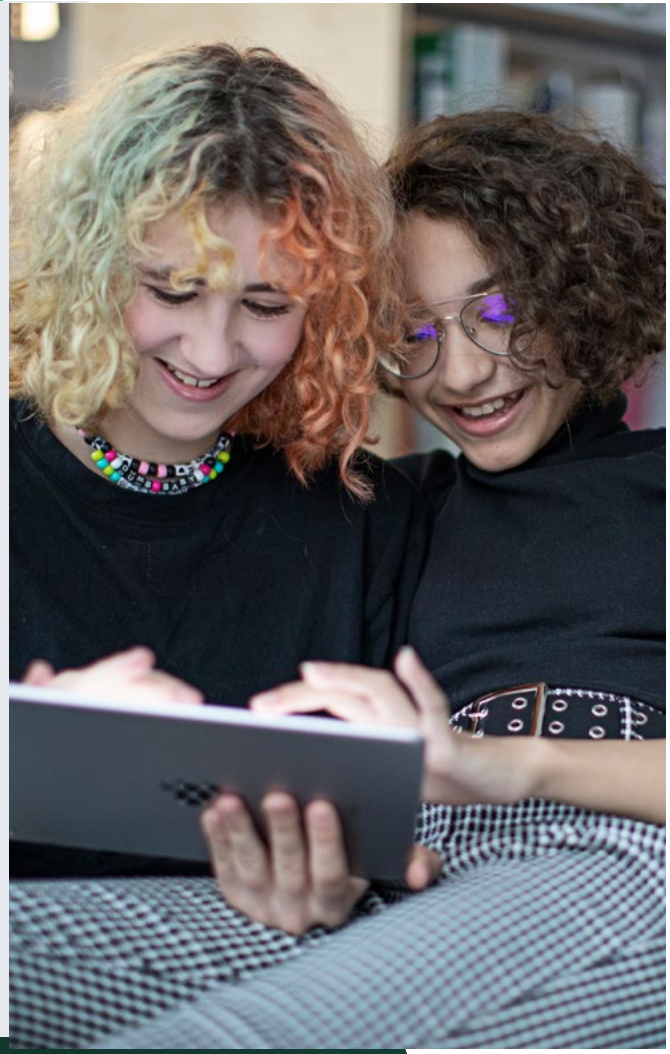
Higher education faces unique security challenges that are further complicated by regulatory requirements for data collection, use, sharing, storage, and destruction. These challenges are intensified by a constantly evolving threat landscape, which develops sophisticated new threats to exploit vulnerabilities, making it much harder for IT and security teams to address them effectively.

But you're not alone.

In this e-book, we dig into five critical things administrators can (and should) be doing right now to level the playing field and protect their users, devices, data, networks and infrastructure from security threats.

The 5 security tenets we discuss in this book are:

1. Integrating solutions
2. Hardening device configurations
3. Securing all endpoints
4. Managing compliance
5. Iterative lifecycles



Prerequisites for Security Success

Like any learning environment, there are a few rules that should be followed to set yourself up for success. In this case, these “rules” are predicated on meeting certain expectations before getting started.

After all, the solutions presented in this e-book will not be the panacea institutions are looking for if foundational-level security tools and processes are not already in place.

These pre-requisites are:

- **Risk assessments** performed and thoroughly vetted
- **Mobile Device Management(MDM) software** setup to manage and **deploy Apple devices**
- **Cloud-based identity** configured to provision accounts and permissions
- Basic security deployed, such as Firewalls and **actively monitored endpoints**
- Administrative controls, such as **Acceptable Use Policies** aligned to institutional needs and requirements

1. Integrating Solutions

Integrating solutions opens the door to enhanced protections and advanced workflows; both of which shorten the length of time between when issues are discovered and remediated.

Why is integration critical to addressing modern threats?

By converging tooling within your security stack, like MDM and Endpoint Security for example, gaps between security and management are eliminated. Two individual tools become recalibrated to function as a single, powerful solution that offers protection and mitigation workflows that work in tandem.

"Shared knowledge is exponential power."

— Dr. Myra Gray

Telemetry data gathered through active monitoring enables administrators to identify vulnerabilities present within devices used on educational networks in real time. And when rich telemetry is securely shared with MDM, the resulting policy-based management serves as a trigger that deploys remediation workflows that **automatically patch apps** and vulnerabilities to prevent exploits on personal and institutionally owned devices.

A few key benefits of integrating management, identity and security solutions:

- Telemetry data is shared securely and in real-time, allowing actions to be based on the **latest device health information**
- Seamless, policy-based remediation of threats and vulnerabilities without prompting for user interaction
- Holistic prevention of malicious threats while **ensuring access to protected resources remains encrypted** over any network connection
- Ensure devices remain complaint, regardless of ownership model, by aligning compliance requirements with security plans

2. Device hardening and configuration

Secure institutionally issued and personally owned devices by sharing rich telemetry data between solutions to enforce endpoint compliance.

How can devices be secure if they're not being effectively managed? Conversely, how can devices be considered managed if they're not secure?

Management and security are two halves of a whole

In the case of HiEd, the word “devices” connotes any computing technology used to facilitate learning by students, educators or faculty regardless of:

- Who owns the device
- What type of device it is
- What operating system it runs

A vulnerable, personally owned device can just as easily be compromised to perform a data breach as an institutionally owned one. This doesn’t advocate restricting personal devices from being used because, let’s face it, the reality of manual block lists reads well in theory but is a different matter altogether in practice. They are quite time-consuming, cumbersome and frankly not as effective, as decades of iron-fisted IT management styles have proven. More specifically, **common security misconceptions** do nothing to prevent users from bringing in their personal devices or trying to access protected resources with them, so risk remains ever-present.

Put another way, which of the following are easier to effectively secure: the devices you can see or those you can't?

The latter describes an escalation of commitment, a behavior pattern that sees groups continue a course of action even in the face of increasingly negative outcomes. The former, however, focuses on achieving security by relying on flexibility to adapt.

In the case of cybersecurity, by **applying device-hardening best practices to all endpoints** accessing HiEd resources, privacy is upheld while security is maintained through the following means:

- Protections are standardized, aligning closely with institutional needs, risk tolerance and your overall security posture
- Detection of vulnerabilities and threats is tied to security frameworks, **establishing secure configuration baselines** strengthening device security posture
- Compliance is enforced through policy-based management workflows that are automatically triggered based on real-time device health data changes
- Patch management lifecycles occur at a regular cadence, ensuring that all devices regardless of ownership model are up-to-date

3. Endpoint security

Apply comprehensive protections in a layered approach for defense-in-depth against multiple threat vectors, performing threat hunting and deploying automated remediation workflows.

Sum of its parts

The overarching theme of this guide is to protect devices, users and data from modern threats by leveraging technologies through integration. Doing so transforms individual security controls into the comprehensive workflows necessary to face the evolving challenges targeting the education sector.

Security tools are, no doubt, critical to addressing these challenges. But what individual controls lack due to isolation, integration unlocks, resulting in robust solutions that extend protections holistically across your entire infrastructure.

Malware prevention is a core component of **endpoint security**. This allows for on-device protection of malicious code, but what about network-based threats? This is where identity and access management combined with endpoint security plays a crucial role. These measures prevent in-network attacks by requiring user authentication before granting access to educational resources and encrypting connections to ensure data integrity over any network. Additionally, they protect against common network-based attacks, such as Man-in-the-Middle (MitM) attacks.

"Stop trying to drive the car straight when the road curves." — Jay Shetty

In the previous section, we touched upon the benefits of integrating management and security. In addition to automated remediation workflows, there are additional feature sets that free up administrators to focus on enriching the student and faculty's user experience.

For example, introducing machine learning (ML), a subset of artificial intelligence (AI), aids cybersecurity professionals by performing threat-hunting to **identify and mitigate sophisticated threats**, as well as unknown ones, such as those that often lurk undetected while gathering reconnaissance data on your network...until an incident occurs.

Speaking of the unknown, it's no surprise that **phishing is the top choice for threat actors** targeting their victims. The anonymity of these attacks lends itself perfectly to catching the greatest number of victims with the largest net, with the least amount of effort possible.

Content filters can restrict access to known phishing websites, surely, but if a user clicks on a malicious link, it's game over. Seamless integration between security tools adds layers of protection for mobile devices – including keeping users safe even when they click on malicious links – effectively **preventing zero-day phishing threats**. And because it's in-network, this solution is OS-agnostic, meaning any device type running macOS, iOS/iPadOS, Android and Windows remains safeguarded.

4. Compliance management

Ensure security plans align with compliance goals and regulatory requirements. Streamline compliance initiatives by implementing standards and security frameworks across your infrastructure, extending guidance holistically to any device connecting to educational resources.

Syllabus for Achieving Compliance

The first step on any compliance path is typically a risk assessment. Once you know what's at stake, you can implement how to protect it.

Something of an unsaid precursor should be your mindset, however. The understanding that, achieving and maintaining compliance, is an ongoing process. One that requires holistic measures (achieve) to be applied broadly to and enforced on (maintain) all devices communicating with higher education infrastructures. This is not dissimilar to a Ulysses Pact, also known as a **Ulysses Contract**.

What is a Ulysses Pact and how does that aid my university's compliance path?

Simply put, decisions or actions taken in the present are designed to keep you from changing them in the future. For example, we established that compliance applies to institutionally owned devices as much as personal devices.

With Ulysses Pacts in mind, requiring enrollment in an institutional MDM for both ensures that baseline configurations are applied to devices regardless of their ownership levels. Ergo, a standard of compliance is established that MDM also enforces, thereby maintaining compliance. Because device and user enrollment profile types may be used concurrently, management keeps educational and personal data isolated on personal devices; **ensuring data security without impacting user privacy**.

Another example is how device management and cybersecurity standards come together as a "technical Ulysses Pact" used to maintain compliance. **Jamf Compliance Editor** (JCE), a tool built upon the macOS Security Compliance Project (mSCP), is used to **create customized, hardened configuration profiles based on established security standards** from:

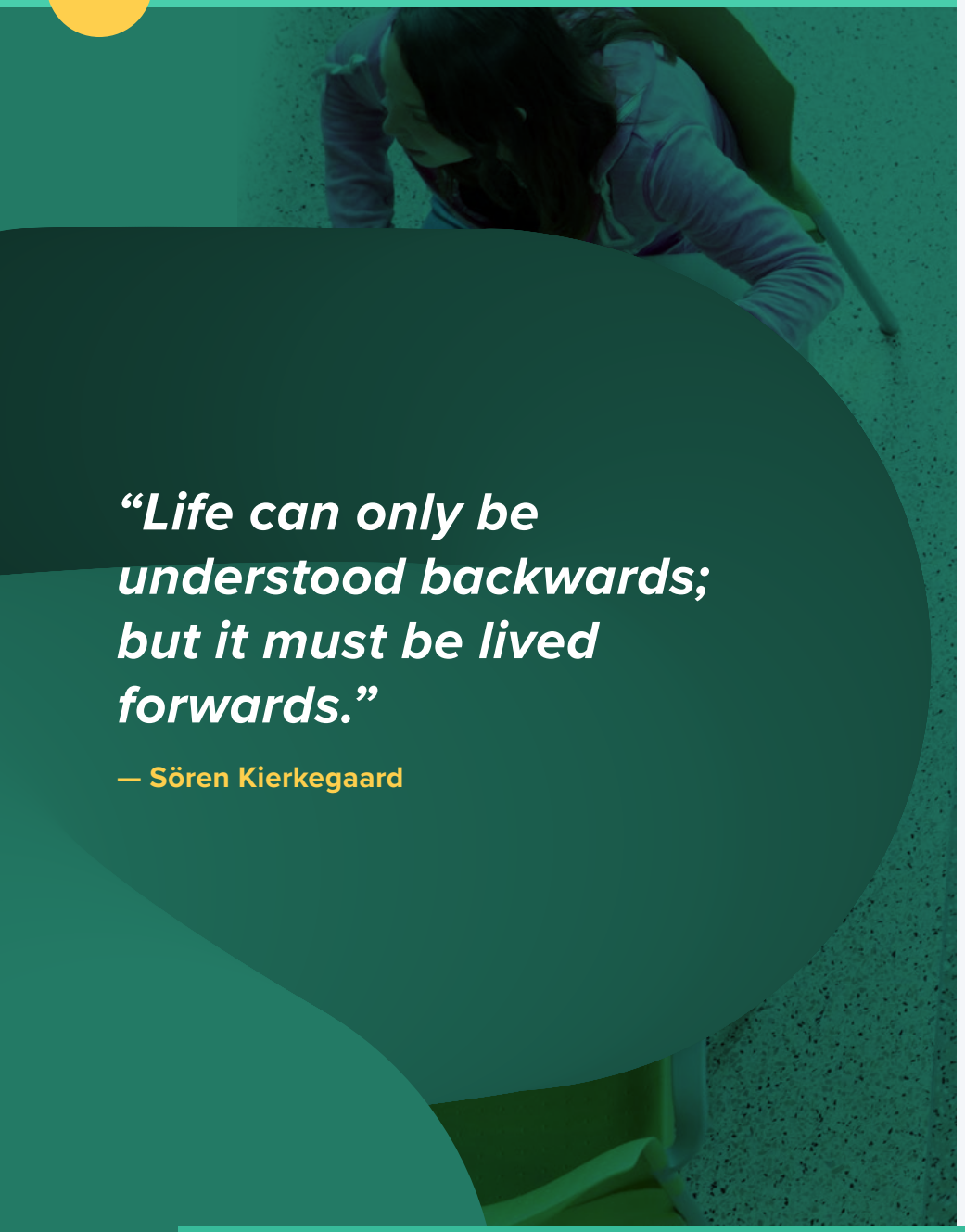
- National Institute of Standards and Technology (NIST)
- Defense Information Systems Agency (DISA)
- Center for Internet Security (CIS)
- Cybersecurity Maturity Model Certification (CMMC)
- Committee on National Security Systems Instruction (CNSSI)

Once customized to meet your compliance needs, JCE interfaces natively with your Jamf Pro instance and uploads the configurations, allowing admins to scope them for deployment to managed devices, and configure security settings that best meet the compliance needs of the institution.

Lastly, implementing policies within MDM provides enforcement of compliance standards by remediating devices should an unintentional misconfiguration or security event intentionally cause them to fall out of compliance.

5. Lifecycles

Create a feedback loop that feeds the subsequent phases of the device's lifecycle process. Continually changing, growing and adapting to meet the challenges of the modern threat landscape and evolving needs of the institution.



“Life can only be understood backwards; but it must be lived forwards.”

— Sören Kierkegaard

Continuing Education

Kierkgaard’s quote is used to illustrate a dichotomy between proactive and reactive strategies. Understanding the true impact of cybersecurity incidents can only be achieved after a data breach. Yet, regardless of the risk appetite, institutions must to do everything in their power to prevent breaches from occurring.

IT and Security rely on lifecycles to simplify managing a variety of facets: from devices to applications to cybersecurity controls to name a few. The core aim of each lifecycle is to minimize risk at each phase. Not unlike defense-in-depth strategies with layered security controls, a lifecycle approach to cybersecurity manages risk at each stage of a device’s usable life, using the strength of the previous stage as a foundation upon which the stages that follow can build.

For example:

- Procurement: Aquire hardware and software from trusted partners and developers, feeding directly into device management to secure the supply chain.
- Provision: Align institutional needs with standards and frameworks, applying them to integrated solutions to create baselines that enforce compliance.
- Deploy: Install standardized, hardened configuration settings and managed applications based on baselines for optimal performance and security.
- Manage: Ongoing, active monitoring of endpoint health combined with regular patch management cadences to minimize risk and maintain compliance.
- Decommission: Secure data erasure, license recovery, track inventory and perform device disposal (or redeployment); mitigating data loss.

The iterative nature of the lifecycle process forwards necessary information to the subsequent stage to aid administrators in not only addressing challenges in that phase but also serves to address any residual risks or shortcomings that may exist. This results in extending consistency across your infrastructure while **fortifying the actions and workflows in each phase**. Ultimately, shoring up deficiencies that would otherwise introduce unanticipated risk – leading to vulnerabilities, compromise and data breaches – that your cybersecurity plan may not address.

Takeaways

The syllabus for higher education lies squarely with integrating individual management, identity and security tools so that they work as a holistic solution. A solution that unlocks advanced workflows, allowing comprehensive controls to work together in a defense-in-depth strategy. Seamlessly identifying varied threats, preventing sophisticated attacks and mitigating risks vectors impacting learning and instruction occurring on any device, and using desktop and mobile operating systems over untrusted network connections from anywhere globally.

The keys to achieving this balance are:

- Developing a security plan based on a defense-in-depth strategy
- Integrating management, identity and security tools into a holistic solution
- Unlocking advanced workflows that are informed by active monitoring and securely share rich telemetry data about device health in real-time
- Provisioning cloud-based identity credentials and tying them to permissions limiting access to authorized users only
- Streamlining device hardening and secure configuration deployment through the establishment of baselines that align device security posture with risk tolerance
- Deploying on-device and in-network endpoint security controls that mitigate risk vectors, patch vulnerabilities and prevent data exfiltration
- Incorporating advanced technologies based on Zero Trust models to encrypt connection requests to protected resources that meet risk appetite
- Standardizing baselines to address institutional needs and compliance requirements by creating and deploying secure configurations based on industry best practices and security frameworks
- Enforcing compliance by instituting policy-based management that automatically mitigates risk factors, remediating non-compliant devices
- Leveraging AI/ML to aid automatically perform threat hunting for unknown threats in addition to defending against sophisticated, converged attacks

See how Jamf can help bring holistic, Apple device management and security to your campus.