Assessing Higher Ed's security needs

Why it’s critical to your overall security posture

Summary

Understanding the security needs of higher education is a nuanced task that requires keeping many spinning plates in the air at the same time. **It’s part theoretical, part practical.** Despite this duality, it has its roots firmly planted in logic that leverages key telemetry data gathered through risk assessments and monitoring to not only gain visibility into vulnerabilities but mitigate them before they lead to a security incident.

All this doesn’t occur in a vacuum, but rather in conjunction with understanding how identified threats to your security posture impact compliance with applicable regulatory requirements and policies. These may encompass data security, confidentiality of staff and student records and user privacy protections, to name a few crucial ones. When combined, all of these components serve as the blueprint that drives security tooling, helping institutions achieve (and maintain lock-step with) their path to compliance.

In this technical paper, we discuss:

- What types of risk impact the education sector
- How collecting telemetry data provides visibility into device health and your overall security posture
- Why assessing risk must be performed at a regular cadence, iteratively, as part of the security stack
- How this data aids your organization in not only determining its security needs but also how it can be used to protect against current and future risk vectors
- Why integrating risk data with endpoint security solutions helps schools maintain a strong security posture while meeting compliance goals

Having your finger on the pulse of your institution's security posture is crucial to the continuing success of any academic institution. Ask any administrator — **"How do you *ensure* success for your stakeholders?"** — and they'll surely tell you that being able to understand the unique needs of stakeholders and balancing them against the needs of the institution sets everyone up for success.

Succeeding with your cybersecurity program is analogous to institutional success mentioned above. The foundation of your security program lies in gathering useful bits of information relating to device health, and making that information actionable. **Specifically, by analyzing rich telemetry data, educated decisions can be made that effectively minimize risks while maximizing the user experience for all stakeholders.** This is especially true of higher education which has kept its doors open, despite global health crises, economic downturns or changes in how students prefer to learn (face-to-face vs remote learning).

Regardless of the issue, adaptability has been a key to success for institutions of higher learning. The same applies to cybersecurity — both being able to assess your infrastructure but also making the adjustments necessary to maintain a strong, healthy security posture. *Put more succinctly: being able to assess what your security needs are* ***while*** *dynamically adapting to address concerns.*

Much like continuing education, cybersecurity is an ongoing and evolutionary process.

Instead of solely looking outward to assess the needs of their stakeholders, administrators must look inward to determine what's needed to continue safe IT and Security processes that protect students, educators, staff, sensitive data and endpoints used for learning holistically, end-to-end across the entire infrastructure. This reflective process is integral to the risk assessment, and the insights derived from this task cover a broad spectrum – from devices and software tools to the infrastructure handling sensitive data, as well as the processes and policies governing them, all while ensuring compliance. Combined, they paint a picture of what an institution's security posture currently looks like.

One thing risk assessment is not is a “one and done” process.

With this information, IT and Security teams are empowered to assess the risks and liabilities inherent in their current cybersecurity strategy. This “status screenshot” provides them the answer to the question, **“Where are we currently?”**, referring to where you stand in the context of your compliance path. Marrying risk assessment data to industry security standards answers the question, ***“Where do we need/want to be?”.*** The path in between both points provides you with the steps necessary to correct the course.

That is, to make the changes necessary to:

- Standardize management
- Patch vulnerabilities
- Mitigate threats
- Minimize risk
- Enforce compliance

One thing risk assessment is not is a “one and done” process. Per best practices, risk assessments should be performed on a regular cadence. Because of the evolving nature of technology, everything’s always in a transient state. This goes double for security because bugs are a naturally recurring issue leading to vulnerabilities that lower the security posture as it increases attack surfaces — ultimately placing devices, users and data at risk of compromise.

All this is apart from the real-world concern that threat actors are actively targeting educational networks with increased frequency, a fact supported in Verizon’s Data Breach Investigation Report for 2023, where it found that education once again made it to the **top 5 list of most targeted industries globally.**

Put simply: instead of waiting for threat actors to probe and test your network defenses for signs of weakness and reveal attack vectors to exploit, education administrators must perform cybersecurity risk assessments regularly.

Where assessed data is not just used to provide insight as to the current state of security for all resources but to iteratively inform the comprehensive cybersecurity plan, including defense-in-depth strategies such as:

- Stages in the device and application lifecycles
- Procuring, configuring and deploying security controls
- Meeting regulatory goals and enforcing compliance
- Identifying existing and novel threats while assigning criticality and severity levels
- Maintaining alignment between risk appetite and mitigation strategies
- Revising and implementing incident response procedures
- Updating and instituting threat prevention strategies, like end-user training

Instead of waiting for threat actors to probe and test your network defenses for signs of weakness and reveal attack vectors to exploit, education administrators must perform cybersecurity risk assessments regularly.

Risk assessment

We've talked about why risk assessments are important, but what does one look like?
And what's actually at risk?

While the exact details can vary from one school to another, it boils down to understanding:

- The modern threat landscape
- Your site's vulnerabilities
- The likelihood of an attack
- The impact an attack will have on your institution
- How quickly it can recover from a serious attack

Let's look at some questions that a risk assessment has to answer.

> "Learning is not attained by chance. It must be sought for with ardour and attended with diligence."
>
> **- Abigail Adams**

Where is my site vulnerable?

There are many points of entry an attacker can use to exploit your system. This includes any hardware, software, interfaces, staffing shortages and vendor interactions with your network infrastructure, as well as any stakeholder who has access to these components. Vulnerabilities also crop up in your Security processes and IT policies.

To get a good understanding of your infrastructure, it's necessary to classify and inventory these components. You should know:

- What devices are accessing your network
- Who has access to your data
- If you're following security best practices (e.g. least privilege access, strong password policies, etc.)
- If your vendors introduce vulnerabilities to your systems
- If stakeholders are well-trained on potential threats and practice good security hygiene

What threats are out there?

Assessing risk also means knowing what threats are out there and how they can affect your devices. This helps your IT and Security teams evaluate what is most vulnerable, how likely an attack is and what impact cyberattacks could have on your institution.

Referencing the MITRE ATT&CK framework, for example, gives Security teams the information they need to understand how bad actors could attack your system. And for unknown threats, teams can consider threat hunting and using AI and machine learning (ML) software to identify suspicious or malicious behavior. AI and ML work tirelessly behind the scenes to identify anomalies outside your network's baseline behavior. Their ability to process enormous datasets of threat intelligence and pattern-matching data makes these critical tools in your cybersecurity arsenal. Additionally, the data gleaned from this software can be shared with the larger security community, further enhancing the threat knowledge base of cybersecurity professionals everywhere.

Knowing common threat vectors can help you prioritize what parts of your infrastructure need the most defense. Threats come in many forms — according to Verizon's 2023 Data Breach Investigation Report, the main ways attackers infiltrated organizations **were with stolen credentials, phishing and exploiting vulnerabilities.** Generally, the overwhelming source of data breaches **(72%) comes from totally external sources, with a non-trivial amount (40%) targeting compromising credentials.** Defending against these threats requires thoughtful analysis of your current setups and policies — more on defending against these later.

72%
of data breaches come from external sources

40%
of data breaches target compromised credentials

What impact would a cyber attack have on my organization?

Understanding the likelihood of a threat helps with prioritization in your defense strategy. But another part of this is understanding the impact a threat has on your school's mission. This can be financial, with the average cost of a critical infrastructure data breach — a category the education sector fits into — at **5.04 million USD** in 2023, according to IBM's Cost of a Data Breach Report. **This is up 1.26 million USD from the average cost of other industries at 3.78 million USD**, or a difference of 28.6% higher data breach costs for education. It can be time lost, with an average of 277 days taken to identify and contain a breach.

5.04M USD
The average cost of a critical infrastructure data breach

Or, it can hurt your relationship with stakeholders, whether via reputation or by steep fines levied as violations of regulations, like the General Data Protection Regulation (GDPR), which can range from 10 million EUR, or 2% of the institution's worldwide annual revenue for less severe infringements to 20 million EUR, or 4% of the institution's worldwide annual revenue for higher severity infringements — whichever amounts are higher. Not to mention, additional fines from governing agencies if your institution is found to be out of compliance with any other applicable state, federal and/or regional standards.

What's next?

Naturally, the larger the impact of an attack, the higher the priority to defend applicable systems. This is also true for attacks with higher likelihood. The combination of these two metrics — impact and likelihood — helps quantify how risky certain threats are to your center of higher learning. Having a good understanding of the risk gives you the knowledge needed to prioritize and determine:

- What critical systems need the most protection (i.e. will cause the greatest loss toward mission-critical function)
- What controls should be implemented for the best defense strategy
- What software tools can enhance your security posture
- How much risk you can tolerate (i.e. your risk appetite)

Once you have the information needed from your risk assessment, it's time to implement what you've learned.

In the next sections, we'll get into the nitty-gritty about how to evaluate your network and device telemetry and what guidelines you can use when developing or revising your security policies.

Visibility and monitoring

So, you've assessed risks, identified them and adjusted your risk appetite to align with your tolerance level. Furthermore, you've made the necessary changes to procure and configure security controls to mitigate risks. Your security posture is strong and stakeholders have received the requisite training needed to identify current threats while understanding that they need to be reported and not acted upon. Endpoints are secured from threats and compliance goals have been achieved, with all devices falling within scope…now what?

Are IT and Security teams simply done with their work and can take an early (and likely, much-needed) holiday? ***Not quite.***

Once again, the dynamic nature of technology is ever present and in this case, it means that just because something is secured right now, today, doesn't mean that it will forever remain secure. The key to keeping your devices, infrastructure and overall, institution safe from pervasive security threats lies in the understanding of the health statuses of its endpoints at any given time. Obtaining this critical insight is accomplished through monitoring.

The telemetry data recorded from actively monitoring devices' health status contains a wealth of information that is table stakes for maintaining device and infrastructure security postures.

Not just that, but when speaking of compliance (which we'll dive into in a later section), telemetry data is the key ingredient to ensuring that endpoints are configured properly to meet regulatory requirements, but also provide the metrics by which you can prove that endpoints were, in fact, compliant at any given time. Showing proof of compliance is a critical requirement when seeking regulatory certification, such as PCI-DSS, for schools to be able to accept and process card payments for books and classes securely.

Of additional importance, visibility gleaned through monitoring serves to inform decision-making at all levels of the device and application lifecycles. The nature of the monitoring process serves to provide IT/Security teams with up-to-date information regarding the health of their devices, the software running on them and the actions taken by end-users. But it also provides administrators and management with rich telemetry data to iteratively make informed determinations relating to any adjustments needed to ensure devices remain compliant, users remain safe and data stays secure.

> "The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn."
>
> **— Alvin Toffler**

What kind of data is collected through monitoring?

Before diving into the types of telemetry data gathered through monitoring, let's first touch upon the two types of monitoring:

1. **Passive:** Health data is gathered slowly, usually over a period of time so as to minimize any impact on the end user or the performance levels of the device being monitored. As such, the infrequent nature of the data capture means it can take more time to collect telemetry data and therefore, delay the creation of a fully-formed device baseline. Also, any delays in data gathering could have a direct impact on the accuracy or timeliness of the data, especially if days or months pass between data captures.

2. **Active:** Health data is communicated from endpoints frequently. In fact, endpoint polling occurs regularly and is communicated to a centralized repository, often in real-time.

Though nearly identical in terms of what data is captured, the major differences between Passive and Active are:

- **How** telemetry data is captured
- The **length of time** in which it takes to build a baseline profile
- The **accuracy** of the information
- The **frequency of updates** to the telemetry data

While both types of monitoring provide their pluses and minuses, the fact remains that the modern threat landscape is too vast and changes too rapidly for anything other than active monitoring to be an effective means of gathering the most up-to-date device health data, and converting that into actionable data to fill the gaps in your security plan. A security axiom in SecurityWeek sums up the criticality of this process precisely, “you can't protect what you can't see.”

Types of telemetry data collected and what it means for your security posture:

OS updates:

Determine OS update levels to know if devices are receiving the latest protection against known threats while minimizing vulnerabilities and if devices support the newest features.

App patch levels:

Like the OS, apps require patches to ensure that they are keeping data protected during processing while fixing bugs and mitigating vulnerabilities that could otherwise introduce risk.

Configuration settings:

Hardening devices is critical to the security posture. Not just because you want to ensure that they are properly configured for maximum security, but to also minimize the possibility of misconfigurations, which contribute to 21% of error-related data breaches (Verizon Data Breach Investigation Report 2023).

Network activity:

What web-based content are devices communicating with? Are untrusted connections being secured? Which ports are being used to transfer data? Answers to these and other important questions surrounding network utilization are critical to determining the security posture of your devices.

Behavioral analysis:

Users, regardless of whether they're students, educators or faculty are generally considered the weakest link in the security chain for good reason. Varying levels of understanding contribute to the continued success of social engineering attacks. By understanding how users perform on their devices, administrators get a clearer picture of how user-introduced risks occur and therefore, how to better protect against them.

System processes:

It is imperative to endpoint security that administrators know what apps are running on devices. This not only speaks to the average baseline of the device itself but also alerts admins to the usage of unsanctioned (Shadow IT) or disallowed (Restricted) tools that may otherwise lower security by allowing for data leaks to occur or increase risks to user privacy.

Types of telemetry data collected and what it means for your security posture:

Malicious code:

The presence of malicious codes can occur in various forms. From downloading a trojan disguised as a legitimate app to unknowingly visiting a compromised website to seemingly dormant threats running in the background – any of these are capable of potentially impacting compliance, especially considering growing adoption and attack trends related to computers across the modern threat landscape, which includes mobile devices.

Error logging:

Devices log everything and the more devices IT and Security teams are responsible for the harder it is to address each and every issue logged. This is great for threat actors and bad for administrators but it doesn't have to be when managed properly by leveraging Security Information and Event Management (SIEM) solutions to make sense of the potentially overwhelming telemetry stream by sorting and classifying detected issues, prioritizing them based on severity level.

Authentication auditing:

Authentication protocols and password management act as the keys that unlock a device and the sensitive data they contain. Having a bigger, stronger lock or complex password scheme doesn't reveal if stakeholders are sharing credentials or have had their accounts compromised – this goes double for remote learning environments where teachers and students rely on a mix of institutionally- and personally-owned devices for teaching/learning. Policy-based management enforces security on remote endpoints while keeping protected resources safeguarded regardless of device type or OS platform.

Audit compliance:

Visibility into endpoint health is just as much about what is there as it is about what's not there. This is especially crucial in regulated sectors, like education. The ability of campuses to know where they stand at each step of their compliance path, including what's necessary to address compliance issues while providing evidence that issues have been remediated is tantamount to fully adhering to applicable data security and privacy protection laws.

But, can telemetry data be used to mitigate risk automatically?

Yes, it can. As a matter of fact, in light of several factors that make managing risk significantly more difficult, like:

- Managing large numbers of devices and different device types
- Maintaining security across a fleet of personally- and institutionally-owned devices
- Supporting stakeholders in remote and hybrid environments
- Convergence of two or more threat types to execute complex, multi-pronged attacks against targets
- Enforcing security settings to maintain endpoint compliance

...automating the collection, analysis and sorting of telemetry data is preferred to going through each stage manually. Given the sheer volume of data to comb through, the quantity of time in completing each as quickly as possible, and of course, the sheer limitations that we as humans can only do so much before requiring breaks for food and rest.

None of these significant limitations apply to technology.

Leveraging systems to perform the “heavy lifting” through automation saves precious time and money — resources that are better served to prevent attacks from occurring successfully than scrambling to clean up in their wake.

Active monitoring is the second layer (after risk assessment) in your security plan to understand the security needs of Higher Ed. By continuously monitoring device fleets, telemetry data is gathered and delivered in real time. This provides up-to-date endpoint health data, which is then analyzed and processed by endpoint security solutions to determine how each device stacks up security-wise. Any identified deficiencies or flagged anomalous behaviors should be automated to trigger alerts, ensuring timely notification to IT/Security teams, at the very least. While manual processes must rely on human intervention to proceed, automation determines next steps and executes workflows in incident response automatically. Examples include preventing known malware — which according to the report earlier by Verizon, showed up in 40% of breaches. Or quarantining endpoints that have been infected with ransomware (which was present in 30% of breaches.)

Other, more advanced workflows are possible by further integrating endpoint security solutions with other tooling, such as identity and mobile device management to create robust workflows that offer greater automation capabilities. These will be discussed in greater detail in the next section.

Compliance

There are curated quotes about education carefully placed throughout this technical paper that tie together thought-provoking analysis with central themes that IT and Security professionals may find poignant as they perform due diligence to assess risk, in preparation for better understanding the criticality of their institution's security needs. The intention is to bridge any gaps while establishing the understanding that each stage in the process is critical on its own. Furthermore, each phase is linked to the next by taking the information present and using it as a starting point to inform the next step in the path.

> "The whole purpose of education is to turn mirrors into windows."
>
> **- Sydney J. Harris**

Understanding your security needs doesn't just mean knowing what security issues are present at a given time, but also speaks to knowing what must be done to resolve them. It's also about understanding which strategies to choose that best ensure your endpoints remain in scope with your compliance needs. The end goal is to remain compliant with applicable regulatory requirements while maintaining alignment with internal policies and standards – with both serving as tentpoles that uphold security and user privacy. **In short: mitigating risk using a structured framework that keeps your device and organizational security postures strong.**

> "If you think education is expensive, try estimating the cost of ignorance."
>
> **- Howard Gardner**

Ignorance of best practices that shore up security vulnerabilities and minimize risk is one of the key themes threat actors are counting on. This can be expanded to anything/anyone that may knowingly or unknowingly introduce risk. After all, risk equals a liability that could otherwise lead to exploiting a vulnerability or lead to a data breach.

When it comes to understanding your security needs, it is futile to worry about the multitude of potential threat actors themselves instead of the immediate, more concrete state of your network. Your attention is better served on the variety of risks themselves and not so much where they may come from. This framing helps administrators understand the threats themselves and subsequently, focus on how to best move forward to maintain compliance by keeping devices, users and data protected against both current, growing and evolving threats.

Which industry guidance helps to identify and minimize different types of risks?

It's important to distinguish between guidelines, frameworks and baselines before going further. **Guidelines** share an affinity with best practices. They're not hard rules that must be followed, but rather a grouping of industry practices that are considered sound to help organizations make sense of what the preferred desire is when managing various forms of risk in a general capacity.

Frameworks on the other hand, though sharing a similar DNA as best practices, aim to synthesize all of the information, practices, settings, controls and workflows necessary to meet or exceed a specific policy or compliance requirement.

For their role in achieving and maintaining compliance, baselines share similarities with the two former guidance types, but from a slightly different angle. Whereas guidelines provide ideas for best security practices and frameworks organize them in a structured way, formatting them to achieve a particular compliance-specific endgame, baselines aren't implemented in the same way as the former two guidance types. They act, in essence, as barometers that administrators can use to measure their current level of success in their compliance path and/or achieving institutional goals.

In lay terms, guidelines are like ingredients. Frameworks are the result of combining ingredients to create a certain type of meal. Lastly, baselines act as judges to determine if the meal was prepared properly, according to the ingredients used and recipe followed. Does that make sense?

Now that we understand these differences, we move forward with frameworks and baselines, since we're aiming to best understand our security needs and of course, address them as accurately as possible.

Frameworks commonly used in security planning

National Institute for Standards and Technology (NIST) SP 800-53, Rev. 5

Security and Privacy Controls for Information Systems and Organizations, provides “a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets…from a diverse set of threats and risks.”

NISTIR 8011, Vol. 4

Automation Support for Security Control Assessments, focuses on the “automation of security control assessment within each individual information security capability” while it simultaneously “addresses the management of risk created by defects present in software on the network.”

ISO/IEC 27001

Information Security Management Systems (ISMS), is among the best-known standards for defining requirements that must be met by an ISMS. The framework provides holistic “guidance for establishing, implementing, maintaining and continually improving an information security management system.”

Cyber Essentials

A U.K.-based initiative that provides guidance to “protect your organisation, whatever its size, against a whole range of the most common cyber attacks.” It offers multiple tiers, including carrying out a hands-on technical verification to ascertain compliance.

MITRE ATT&CK

A global knowledge base of tactics used by cyber adversaries, based on observations of real-world techniques. It is also used as “a foundation for the development of specific threat models and methodologies” across various industries, communities and endpoint security solutions.

Payment Card Industry Data Security Standard (PCI-DSS)

The de facto information security standard used by organizations, governing the “technical and operational requirements” of handling credit card payment data and is enforced by major card issuers globally.

Control Objectives for Information and related Technology (COBIT) 2019

A framework created by ISACA that focuses on and defines generic processes for IT management and links them to business and IT-related goals. A measurement component is included to ensure team accountability while flexibly allowing tie-ins with other frameworks, like ISO 27001, ITIL and popular project management frameworks.

Cybersecurity Maturity Model Certification (CMMC) 2.0

Set upon the foundation of the security requirements from several NIST special publications, the multi-level model provides Federally-mandated certification levels for Higher Ed institutions that work with government, helping them to cumulatively meet robust cybersecurity paradigms utilizing “CMMC levels and associated sets of practices across domains.”

OWASP Risk Assessment

Consisting of security testing, risk assessment and scanning tools, this framework by OWASP seeks to eliminate the uncertainty stemming from compatibility and complexity related to environmental setup processes to allow a simple way to “analyse and review their code quality and vulnerabilities without any additional setup” as well as “help developers to write and produce secure code.”

macOS Security Compliance Project (mSCP)

The joint project of federal operational IT Security staff from NIST, National Aeronautics and Space Administration (NASA), Defense Information Systems Agency (DISA), and Los Alamos National Laboratory (LANL) “is an open source effort to provide a programmatic approach to generating security guidance”, including configuration settings that may be deployed to attain compliance with specific regulatory goals, like FERPA and PCI-DSS.

The role of baselines in cybersecurity

Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)

A configuration standard managed by the U.S. Department of Defense (DoD), STIGs contain specific requirements for securing computing systems — from logical designs to protocols that run on hardware appliances to the software that's run on them, these guides aim to "enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities."

Federal Information Processing Standards (FIPS) 200

Also developed by NIST for the U.S., these standards are for use in non-military computing devices, systems used by the American government and contractors. While the FIPS standards cover a range of security baselines, FIPS 200 provides standards to ensure that data used by or on behalf of federal agencies meet the minimum information security requirements for each category in the objectives, ensuring the "appropriate levels of information security according to a range of risk levels" while classifying the impact levels for security objectives based on the C.I.A. triad.

NIST SP 800-39

Broad-based guidance useful when integrating with a comprehensive, Enterprise Risk Management (ERM) solution. The document provides "specific details of assessing, responding to, and monitoring risk on an ongoing basis" in conjunction with other standards, guidelines and frameworks.

Center for Internet Security (CIS)

"The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families." Developed as part of a consensus-based effort of global cybersecurity experts, each benchmark provides secure configuration guides that are accepted and used by governments and industries worldwide and even integrated as a foundational base in some endpoint security solutions.

Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Performance Goals (CPGs)

Developed in coordination with CISA, NIST and the interagency community, these CPGs act as broad "baseline cybersecurity performance goals that are consistent across all critical infrastructure sectors", like educational institutions of all sizes to kickstart their cybersecurity efforts, all while serving as a benchmark for the measurement and improvement of cybersecurity maturity to stop critical Higher Ed threats, such as increasing ransomware campaigns.

Risk assessment + continuous monitoring + security guidance = compliance managed

Singularly, each of these components serves institutions to a certain extent, but join them together, and not only will you be able to:

- Determine your liabilities
- Know endpoint health status levels
- Minimize the attack surface by hardening settings
- Achieve your compliance goals

You will also be able to maintain compliance by establishing baselines and then measuring against them by proactively monitoring and reassessing rich telemetry data, completing the loop to iteratively improve the security posture of your devices – and that of your infrastructure overall.

As mentioned previously, it's an evolving process – not a static one. More path than a destination, the loop mentioned in the prior paragraph does not close out once it is achieved, but rather it continues to go in a cycle, touching upon and informing each phase, security control, process, workflow, requirement, policy and setting configured for each device, end user and sensitive piece of data, extending across your infrastructure.

> "Change is the end result of all true learning."
>
> **- Leo Buscaglia**

Whether you're an IT admin at a large university whose goal is to help measure compliance status or a Security professional for a small- to medium-sized college that wishes to align internal policies and administrative controls like Acceptable Use Policies (AUPs) to industry best cybersecurity strategies – think of each core component as smaller pieces to the bigger puzzle. Pieces that form together to provide a clear view of a larger picture: a greater understanding of the gaps in your security and the information necessary to fill them.

You may be thinking, "I'm a MacAdmin. I know exactly which risks impact the campus network yet I'm drowning in device health data. Furthermore, security guidance obtained highlight discrepancies between ***where we currently are*** and ***where we need to be*** on our compliance path. But, what now?!

How do we go from *here* to *there*?"

Enter Jamf

Helping higher education succeed with Apple. That is more than just a saying, it's engrained into Jamf's mission statement. And more to the point – it's just what we do. Jamf isn't the only solution in Apple management and security simply because we say so. No, what gives Jamf this reputation is the best-of-breed solutions we develop that help countless customers successfully manage tens of millions of devices across different industries worldwide.

Partnering with Jamf is not a contract — it's a relationship. One that begins from the very first meeting with sales all the way through engineering and success team members to ensure that you're maximizing potential with Apple products in your learning environment. In the sections below, we'll touch upon how Jamf cares about your institution's needs through its commitment to providing you with the tools to comprehensively and holistically manage your Apple fleet while identifying, understanding and meeting your unique institutional needs and compliance goals with our powerful, yet flexible device, identity and security management solutions that are always at the ready.

Take the guesswork out of endpoint validation

A considerable part of understanding your security needs involves knowing the status of the endpoints in use on and off campus. Without rich telemetry data to verify each device's health status, administrators are left with little more than conjecture. One that could be little more than a guess at best or an ill-judged miscalculation at worst – either with the potential for disastrous consequences, beginning by placing your network resources at risk.

Put simply, as administrators, you don't just **want** to know, but rather, you **need** to know where your security posture stands at all times. When it comes to compliance – whether enforcing regulations or aligning with institutional policies – you have the ability to verify endpoint health status at any given time and provide time-stamped proof that the needs of the institution (and your stakeholders) are being met every step of the way.

A key attack vector targeted by threat actors that impacts risk is social engineering. A real-world example of risks targeting higher education, such as the use of phishing campaigns, which introduces greater risk by compromising user's credentials is blocked by Jamf Safe Internet by effectively preventing access to malicious domains. Another example is the execution of ransomware code on victim devices, providing attackers with a means of extending the risk to other devices on the network. While Mac-based ransomware has not reached the critical mass of other platforms, Jamf Protect prevents executing malware, especially when the threat of ransomware still cracks the top 5 malware threat categories impacting macOS, with **malware authors continuing to target Apple devices** as recently as December 2023.

Endpoint security, such as Jamf Protect, adds a safety net to your macOS. On iOS and iPadOS mobile devices, Jamf Safe Internet ensures that all stakeholders are safeguarded against suspected threats, such as preventing malware through analysis of on-device and in-network threats for faster detection, quicker incident response and effective, automated threat mitigation and remediation **workflows that don't compromise security, privacy or performance.**

Extending protections across your infrastructure

Throughout this guide, we've discussed assessing Higher Ed security needs and how that understanding is crucial to the success of your overall security posture. In this section, we touch upon the tooling available from Jamf that helps to turn static telemetry data into actionable workflows to help admins manage their endpoints and proactively maintain compliance with the devices using their network — on campus and remotely.

Your needs don't begin when a device connects to educational resources for the first time – it starts before the device is even unboxed. Allow us to explain.

Zero-touch deployment refers to a process by which **devices are ready to use the moment the end-user powers on their device** for the first time. This process however requires not only understanding institutional needs but also what risks exist so that the deployment workflow integrates between Apple (where devices are procured from) and automatically, yet securely enrolled in Jamf seamlessly.

Whether they're institutionally owned or personal devices belonging to end-users, **Jamf Pro** supports multiple ownership models, like BYOD, to manage enrolled devices. All while upholding user privacy. Speaking to security, our MDM solution offers administrators **same-day support for all Apple features, including security and privacy enhancements**, so that campus IT can support and manage the functionality that helps stakeholders work smarter, not harder, without having compromises, exceptions or tradeoffs made between security, privacy or the user experience.

Patch management is a critical part of the security equation. Deploying updates to operating systems and applications alike is fundamental to the success of any security plan. After all, what good is understanding your security needs if you can't do anything to remediate them? Once again, Jamf Pro shines in this arena by **helping MacAdmins make short work of the app lifecycle management** with bulk management commands to keep devices up-to-date with OS updates. And don't forget the apps – whether deployed via the App Store or third-party apps, Jamf's App Catalog ensures apps are securely sourced and always updated to the latest versions automatically. A feature that simplifies patch management workflows while freeing up administrators to refocus efforts on helping stakeholders get more out of their technology.

Streamlining identity and access provisioning is a tentpole to a comprehensive, defense-in-depth security strategy. Enforcing access security permissions by ensuring that only trusted users can access devices and resources from anywhere at any time makes all the difference when managing devices. This is especially true in distance learning models where educators and students may be physically disparate from one another or the nearest campus. Furthermore, set up stakeholders for success by offering them an easy way to authenticate to their devices – from a seamless onboarding experience (that's part of a zero-touch deployment) to easy, yet secure access to the resources they need – integrating **Jamf Connect** with your cloud-based identity provider (IdP) adds a layer of authentication alongside the added security of multi-factor authentication (MFA) to verify stakeholders are who they claim to be, reinforcing the paradigm that **effective, adaptive and flexible security isn't optional.**

When it comes to endpoint security on Mac and mobile devices alike, one of the most critical vehicles for delivery is over a network connection. In our always-connected world, network threat prevention is a key protection against web-based threats. **Jamf Safe Internet** prevents domains used in zero-day phishing attacks by blocking malicious URLs — even if users click on suspect links delivered via web, email or SMS. Moreover, stakeholder protections don't stop there thanks to DNS-over-HTTPS (DoH) technology preventing harmful content without invading user privacy.

If more granular management over web-based traffic is necessary, such as blocking websites based on harmful or illegal content, the built-in content filter allows administrators to customize the level of access controls that best fit your institution's specific needs. Integrating Jamf Safe Internet alongside Jamf Protect brings together IT and Security functionalities that are both a breeze to deploy while seamlessly keeping stakeholders safe — from on-device and in-network threats.

Three essential security elements – one trusted platform

> “Tell me and I forget, teach me and I may remember, involve me and I learn.”
>
> **- Benjamin Franklin**

Jamf’s **holistic approach to security**, touches upon each salient point discussed here and delivers a comprehensive solution that **supports the MDM and security needs of higher education**. One that extends across your infrastructure, by integrating management, identity and security solutions.

It melds:

- **Visibility and compliance** ↗
- **Endpoint protection** ↗
- **Device management** ↗

Each of these solutions plays a crucial role in an effective, defense-in-depth security strategy for universities. One that layers advanced access controls and secure configurations for devices, users and data. Leveraging rich telemetry data to adapt to any changes in your site’s security posture — at the device or institute levels, or both — maintaining security, preserving privacy and keeping compliant.

Flexibility + security for your entire device fleet – anytime, anywhere minus the complexity.

Get Started

jamf

www.jamf.com

Case studies

Don't just take our word for it — read for yourself as institutions of higher learning have implemented Jamf solutions, helping them succeed in securing their environments and achieving their compliance goals in record time.

University of Glasgow
Bringing Apple devices under the security of Jamf

Shenandoah University
A standardized platform for a better learning experience

Texas A&M
Efficiency and innovation in higher education with the Jamf platform

Oxford University
Keeping education on the cutting edge

University of Wisconsin-Eau Claire
Offering students and faculty a high-tech campus environment

University of Washington
Simplifying technology management and delivering on its commitment to education

Ohio State University
Pairing Mac experience with a robust management tool

Maryville University
Challenging the historical norm to deliver a hands-on experience that allows each student to thrive with their own unique learning style

Colgate University
Weaving technology into their overall philosophy while utilizing one solution to address many challenges