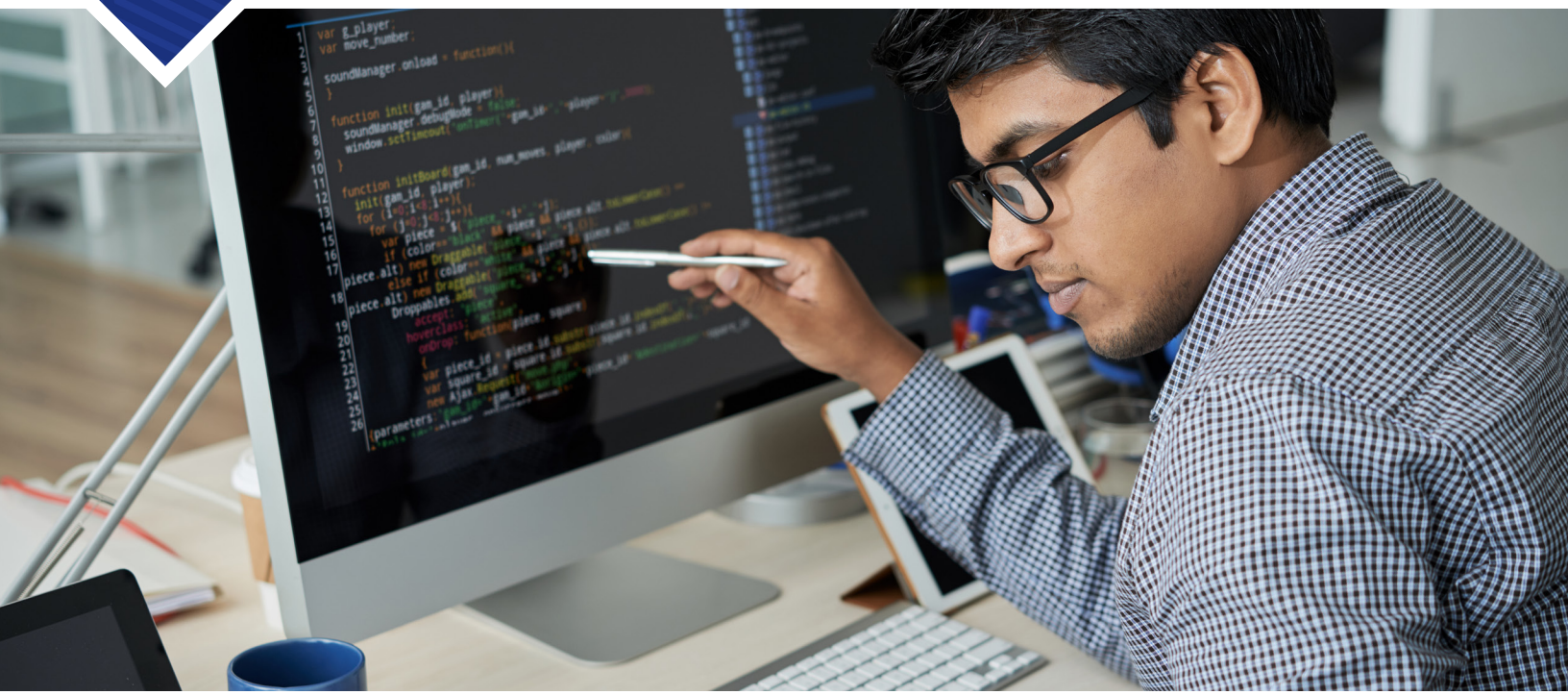
Advancing Campus Network Security with Zero Trust

Rising cyberattacks, new federal requirements, and an evolving higher education landscape have pushed cybersecurity to the forefront for just about every college and university IT leader. Here's how zero trust can help institutions prepare for current and future threats.

PRESENTED BY: CAMPUS TECHNOLOGY

SPONSORED BY: Charter COMMUNICATIONS | Spectrum ENTERPRISE



Finding Ways to Solve the Cybersecurity Challenge

New federal mandate adds urgency to campus network security.

CYBERSECURITY HAS BEEN A KEY PRIORITY among campus IT leaders for years, but new federal requirements ramp up the importance of these efforts even further.

In a **February 2023 announcement**, the U.S. Department of Education's Federal Student Aid (FSA) office published new information security requirements for all institutions that administer federal student aid.

FSA noted that colleges and universities administering federal student aid fall under the Gramm-Leach-Bliley Act, and therefore changes to the act's Standards for Safeguarding Customer Information published by the Federal Trade Commission — which oversees compliance with the act — apply to such institutions.

Colleges and universities have until June 9, 2023, to comply with the new rules, which require institutions to:

- **Designate a qualified person who's responsible for overseeing and implementing their information security programs.**
- **Base their information security programs on a comprehensive risk assessment.**
- **Design and implement safeguards to control the risks identified in this risk assessment.**
- **Regularly test and monitor the effectiveness of these safeguards.**

- **Evaluate and adjust their information security programs in light of the results from this testing and monitoring.**
- **Implement policies and procedures to ensure that personnel can enact their information security programs effectively.**
- **Address how they'll oversee their information security providers.**

Colleges and universities that maintain information on at least 5,000 students also must create an incident response plan, and the person in charge of information security at these institutions must regularly report to the board of trustees and the executive cabinet about their information security programs.

Education Is a Growing Target

The new mandates come as education continues to account for a growing percentage of cyberattacks across all industry sectors. In fact, one industry-based assessment **noted** that the percentage of incidents targeting education jumped from 2.8 percent in 2021 to 7.3 percent in 2022.

In **separate guidance** issued to colleges and universities, FSA said it has developed a fact sheet with **advice** on how to establish an incident response plan. In addition, the agency noted that a recent report from the Cybersecurity and Infrastructure Security Agency (CISA), titled "**Partnering to Safeguard K-12 Organizations from Cybersecurity Threats**," describes how a small number of steps can reduce cybersecurity risks significantly.

Although the report is aimed at K-12 institutions, colleges and universities may find its recommendations useful as well, FSA observed. These recommendations include:

- **Develop a cyber incident response plan that leverages the NIST Cybersecurity Framework.**
- **Minimize the burden of security by migrating IT services to more secure cloud versions.**
- **Build a relationship with CISA and FBI regional cybersecurity personnel.**
- **Implement multi-factor authentication (MFA).**
- **Prioritize patch management.**
- **Perform and test data backups.**
- **Create a training and awareness campaign.**

The CISA report adds an important caveat to the above recommendations: "Change must come from the top down." It's critical for education leadership to establish and reinforce a cybersecure culture, CISA emphasized, to support cybersecurity efforts on campus. "Information technology and cybersecurity personnel cannot bear the burden alone."

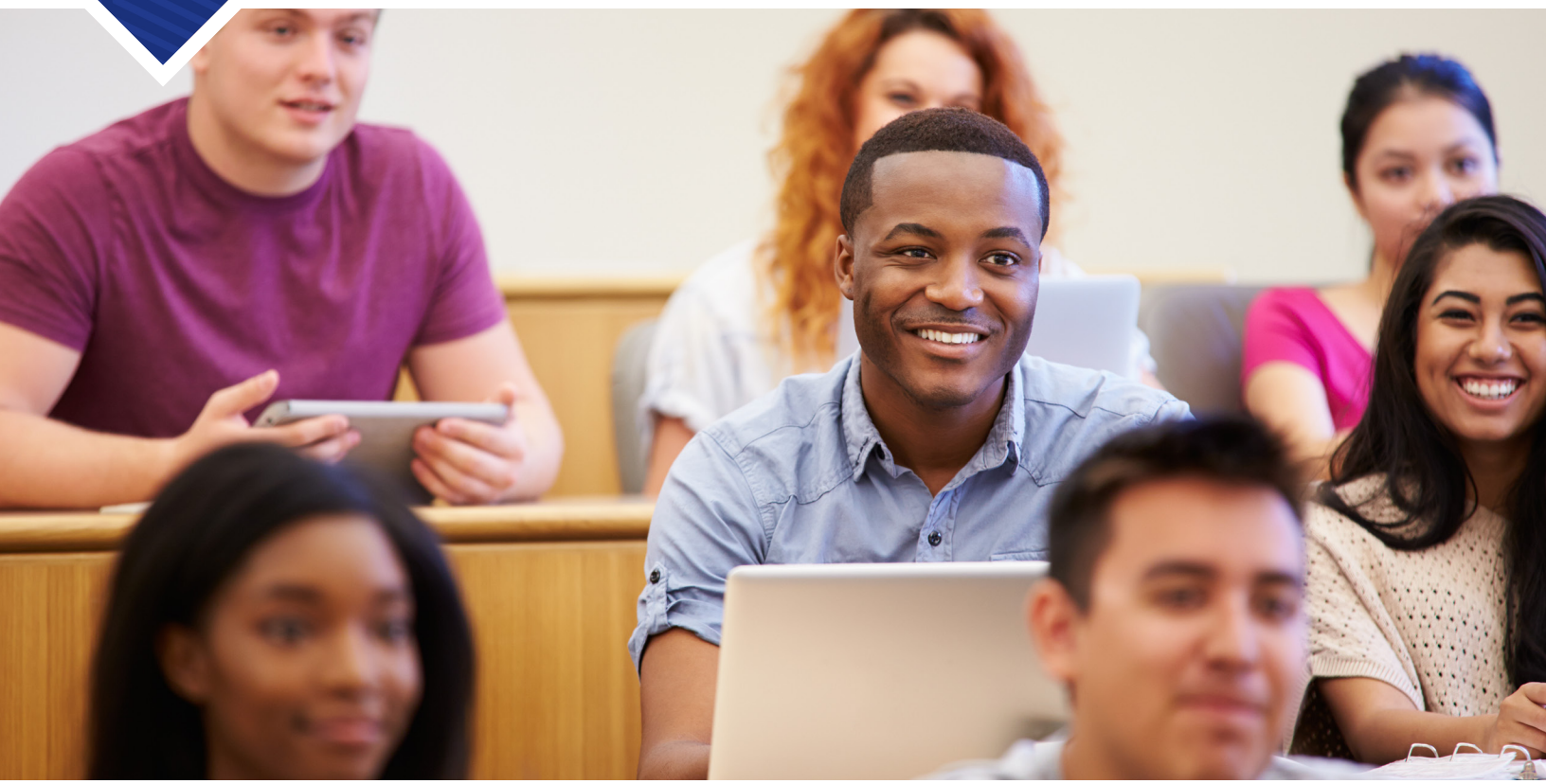
CYBERSECURITY BY THE NUMBERS

64% of IT professionals in higher education say their institution was targeted by a ransomware attack in 2021.

$1.42 million is the average cost of resolving a ransomware attack in higher education. This includes not only the cost of paying the ransom, but the cost of restoring applications and data systems to their original state.

40% of colleges and universities need at least a month to recover from a ransomware attack.

Source: Sophos, "**The State of Ransomware in Education 2022**."



Zero Trust: A New Paradigm

Here's how the zero-trust approach to cybersecurity can protect campus networks.

AS CAMPUS LEADERS LOOK TO SHIELD THEIR network from attacks, the nature of cybersecurity is changing. With more applications running in the cloud and users accessing resources from any location, college and university networks can no longer be protected by merely establishing strong perimeter defenses. Instead, institutions need modern defenses that extend the network edge to each user and application.

An approach that's catching on among all types of organizations is the concept of "zero trust."

Zero Trust Defined

According to the National Institute of Standards and Technology (NIST), zero trust is "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location."

Zero trust involves a shift in philosophy. In the past, once users have logged onto a campus network and been authenticated, they've generally had wide latitude to explore and access basic resources.

Zero trust eliminates the assumption that anyone on the network can be trusted. In a zero-trust

approach, all network users are authenticated, authorized, and continuously validated before gaining access to data and applications, whether they're located on or off campus.

Zero trust arose from the recognition that modern IT systems are highly distributed. For many institutions, the pandemic has provided a clear proof of concept that not every user of the network is going to be on campus.

To implement this approach, colleges and universities need strong identity and access management tools to verify users' credentials. Campus IT staff must know who's on the network at all times, as well as which applications they're using and how they're connecting.

Zero trust also calls for networks to be finely segmented, with permission to access various resources depending on contextual factors such as the user's role, device, location, and the application or data being requested.

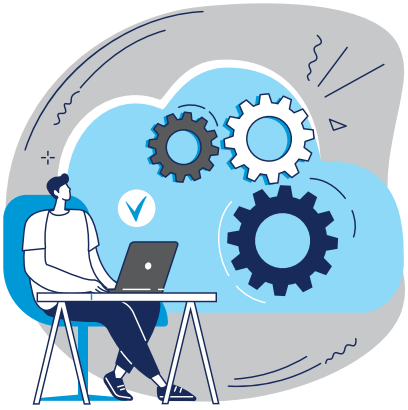
Benefits of Adoption

By 2025, 60 percent of organizations worldwide will embrace zero trust as a starting point for their cybersecurity strategy, **Gartner predicts**. One reason so many organizations are moving in this direction is because it ensures that network users are only accessing the data and resources they're authorized to use.

Not only does zero trust provide enhanced security against both external and internal threats, it also helps institutions respond to attacks faster and more effectively if someone does breach the network.

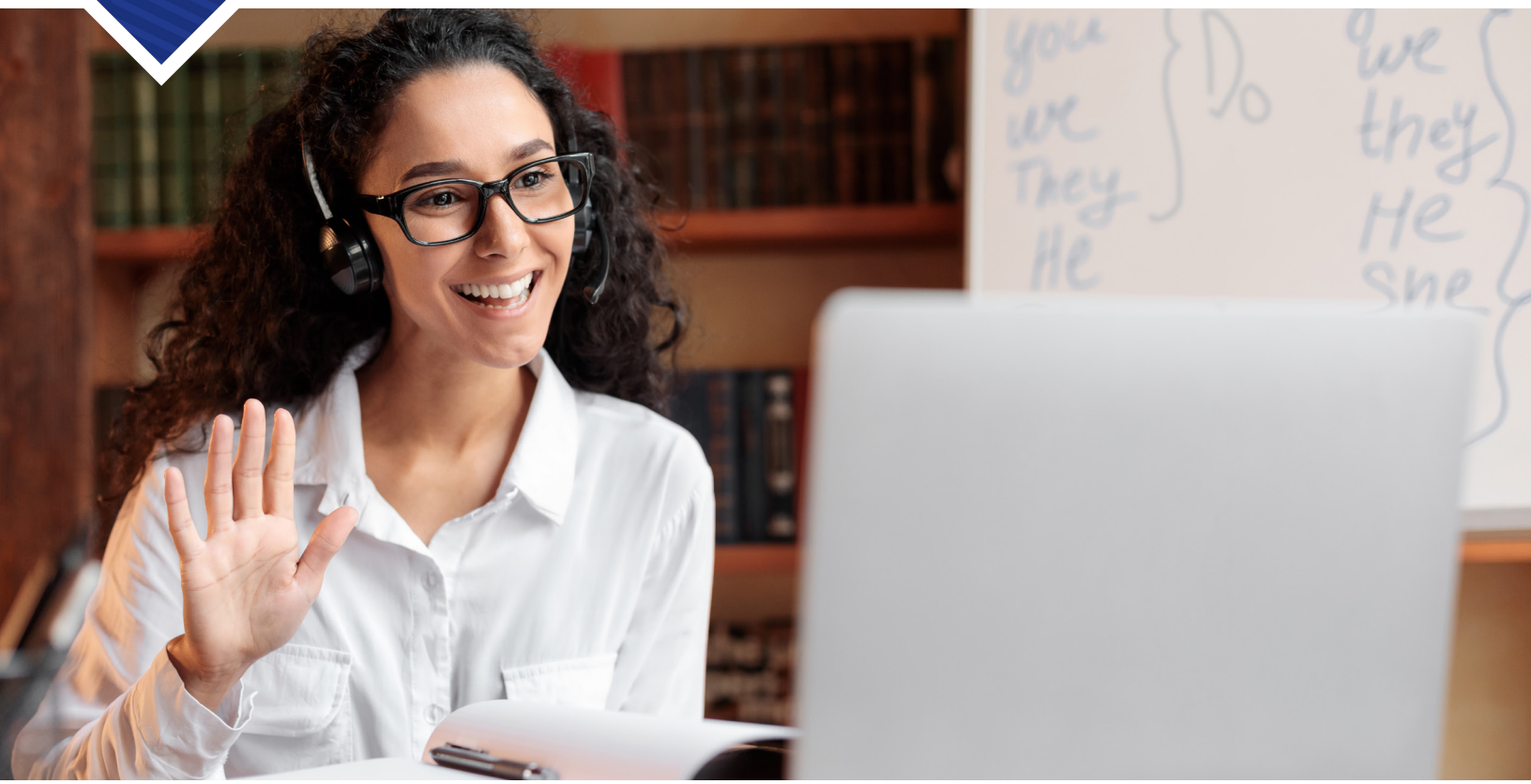
Under a zero-trust approach, IT staff have full visibility into the devices on their network — and they're constantly tracking these devices. This means IT staff should be able to identify attacks or anomalies nearly instantly as they occur, thus accelerating their response time.

What's more, because networks are highly segmented in a zero-trust approach, attackers are limited in how far they can move through the network laterally if they should gain access, which significantly reduces the surface area of an attack.



In a zero-trust approach, all network users are authenticated, authorized, and continuously validated before gaining access to data and applications, whether they're located on or off campus.

By limiting the attack surface and accelerating the response time, zero trust helps institutions minimize the damage caused by a successful cyberattack.



A Roadmap for Implementing Zero Trust

Adopting zero trust is a multistep process.

ZERO TRUST IS "NOT LIKE INSTALLING A firewall," according to IT consultant Joel Snyder, owner and senior partner at Opus One. "It involves moving from an old security architecture to a new one. That takes time and many steps."

Implementing zero trust is a journey — but the journey isn't necessarily linear.

"It's not so much about moving from point A to point Z," Snyder said. "It's often more cyclical in nature." Colleges and universities typically progress toward zero trust in phases. However, "phase two might involve redoing, refining, or improving some of the steps from phase one," he explained.

If zero trust is best accomplished in phases, then phase one involves having sound identity and access management (IAM) practices and technologies in place.

"Identity is your base for everything to do with zero trust," Snyder said. "Decisions about when and how to micro-segment your network, that's kind of up to you. But without a good identity and access management system as the foundation, nothing else is going to work."

Moving Toward Maturity

An Executive Order issued by the Biden Administration in 2021 called on federal agencies to develop migration plans for moving toward a zero trust architecture. To help agencies develop their plans, the Cybersecurity and Infrastructure Security Agency (CISA) created a draft version of a **Zero Trust Maturity Model** that colleges and universities can follow as well.

CISA's model is built on five distinct cybersecurity pillars: identity, devices, network environment, application workload, and data. For each pillar, the model describes what security might look like across three stages of zero trust maturity: traditional, advanced, and optimal. (For a breakdown this model across each maturity stage, see "A High-Level View of CISA's Zero Trust Maturity Model," below.)

Campus leaders must decide for themselves how far (and at what pace) they'd like to travel on the journey toward zero trust. "There's not one single product or approach," Snyder asserted.

A HIGH-LEVEL VIEW OF CISA'S ZERO TRUST MATURITY MODEL

PILLAR	TRADITIONAL	ADVANCED	OPTIMAL
IDENTITY	Password or multi-factor authentication (MFA) Limited risk assessment	MFA Some identity federation with cloud and on-premises systems	Continuous validation Real-time machine learning analysis
DEVICES	Limited visibility into compliance Simple inventory	Compliance enforcement employed Data access depends on device posture upon first access	Constant device security monitoring and validation Data access depends on real-time risk analytics
NETWORK ENVIRONMENT	Large macro-segmentation Minimal internal or external traffic encryption	Defined by ingress/egress micro-perimeters Basic analytics	Fully distributed ingress/egress micro-perimeters Machine learning-based threat protection All traffic is encrypted
APPLICATION WORKLOAD	Access based on local authorization Minimal integration with application workflow Some cloud accessibility	Access based on centralized authorization Basic integration into application workflow	Access is authorized continuously Strong integration into application workflow
DATA	Not well inventoried Static control Unencrypted	Least privilege controls Data stored in cloud or remote environments are encrypted at rest	Dynamic support All data are encrypted

Source: CISA

Securing the Network Edge

Here's what to look for in an authentication solution.

ZERO TRUST ACKNOWLEDGES THERE IS no longer a traditional network perimeter to be defended, because applications now exist in the cloud and users can log into the network from any location. Basically, the network edge extends to each user, and security is achieved by authenticating users' identities.

To secure the network edge under this new paradigm, colleges and universities need better visibility and control of who's using the network and what resources they have permission to access.

Zero trust involves authenticating users or devices whenever they try to gain access, verifying their identity and tracking their network use at every step. Once someone is granted access, their network activity is monitored to make sure they remain compliant with security policies.

Top Criteria

Colleges and universities need a robust identity and access management (IAM) solution to manage these tasks. Ideally, the platform that institutions choose should employ single sign-on (SSO) technology, streamlining users' access to multiple applications with a single network login. This eliminates the bad habits that users often fall into with their passwords, such as forgetting or reusing them. For IT departments, SSO serves

as a single, unified point of visibility for network authentication and access logs.

An effective IAM solution also uses multi-factor authentication (MFA) to ensure that users really are who they say they are. Aside from a network password, authentication factors might include a specific device or location, a security key, or a fingerprint, for example.

To help campus leaders choose a high-quality IAM solution that meets their needs, here are some key questions to ask:

- **Does the solution ensure secure logins from any location, on or off premises, using FIDO-based security keys? (FIDO stands for Fast ID Online, an open industry standard for strong authentication.)**
- **Can the solution provide access control for both managed and unmanaged devices?**
- **Can the solution verify the security posture of all devices trying to access the network? For instance, can it ensure that these devices have critical software patches or endpoint security software installed?**
- **Does the solution alert you to unusual or suspicious login activity? Can it detect and automatically alert administrators to risky behaviors or events, such as enrollment of a new device or a device logging in from an unexpected location?**
- **Can you create and enforce stricter policies and controls for environments or applications with highly sensitive data, such as financial information?**
- **Does the solution provide adaptive policies and controls for different user groups or situations? (For instance, allowing users to authenticate less often when using the same device or letting users access certain applications only from campus-managed devices.)**

Zero trust acknowledges there is no longer a traditional network perimeter to be defended, because applications now exist in the cloud and users can log into the network from any location.

A high-quality IAM solution reduces the risk of a data breach by verifying users' identities using multiple factors. It gives you full visibility into all devices to make sure they meet your security standards before logging on. It lets you enforce access and security policies based on various user groups, devices, and application risks. And it streamlines the workflow for users with an SSO dashboard for accessing all applications.

4 Keys to Success with Zero Trust

These strategies will help institutions navigate the zero trust journey.

WHILE ZERO TRUST CAN BE CHALLENGING TO implement, its potential for reducing risks and improving network security is significant. Here are four keys to success when moving ahead with a zero-trust approach.

1: Focus on change management.

When embarking on any large-scale IT initiative, colleges and universities sometimes focus too much on the technology and not enough on the people and processes behind it. Taking a human-centered approach will greatly increase the likelihood of success.

To ensure a smooth transition, IT staff should anticipate the impact that zero trust might have on various campus operations and should plan accordingly. For instance, a business department that is processing payments might be sensitive to changes that could create problems for users.

"Zero trust is as much a cultural innovation as a technological one," consulting firm Deloitte observes. "Getting people to change their behavior requires communication and training." Campus IT departments should lead a training and awareness campaign before implementing zero trust, so students, employees, and other stakeholders understand the purpose of this approach, how zero trust works, and where to get help if they encounter any problems.

2: Have good inventory control.

For zero trust to work well, "you have to get rid of applications that provide implicit trust," said IT consultant Joel Snyder, "or you have to segment them off from the other parts of your network."

This requires having good visibility into the applications running on your network and a system for cataloging what these applications are and what ports they're using. "That can be difficult for higher education in particular," Snyder said, "because of the decentralized approach to IT and the siloed nature of various departments."

Campus IT staff must work with each department to identify where there might be rogue systems or applications, such as a research supercomputer running in someone's backyard, and separate these from the main network. "The problem with zero trust is that if someone isn't playing by the same rules, that can break everything," Snyder noted.

3: Keep user profiles up to date.

Under a zero-trust approach, permission to access data and resources is granted based on factors such as a user's role at the institution. This can be challenging to manage, especially within a campus environment — where student turnover happens every year and guest lecturers, research staff, and volunteers frequently come and go.

Not only are network users changing all the time, but their roles within the institution frequently evolve as well. These changes might require updates to a user's network permissions.

Identity management can be a very laborious process, and it involves close coordination with human resources departments. For zero trust to work effectively, colleges and universities will need to invest sufficient time and resources in keeping user profiles up to date.

4: Close the loop with client machines.

Zero trust requires strong endpoint security. The identity and access management solution you choose should be able to deny access to sensitive information if a user's device is vulnerable to an attack.

"Micro-segmentation is great, but it only solves the problem of an attacker's horizontal movement on your network," Snyder said. "Attacks that originate on a user's device are a much more urgent concern."

Denying network access unless users have anti-malware and other prerequisite software installed on their machine "is not an especially comfortable place for higher education," Snyder acknowledged. "But it's a part of zero trust that institutions tend to gloss over, and it's really important because that's where the biggest risk is."