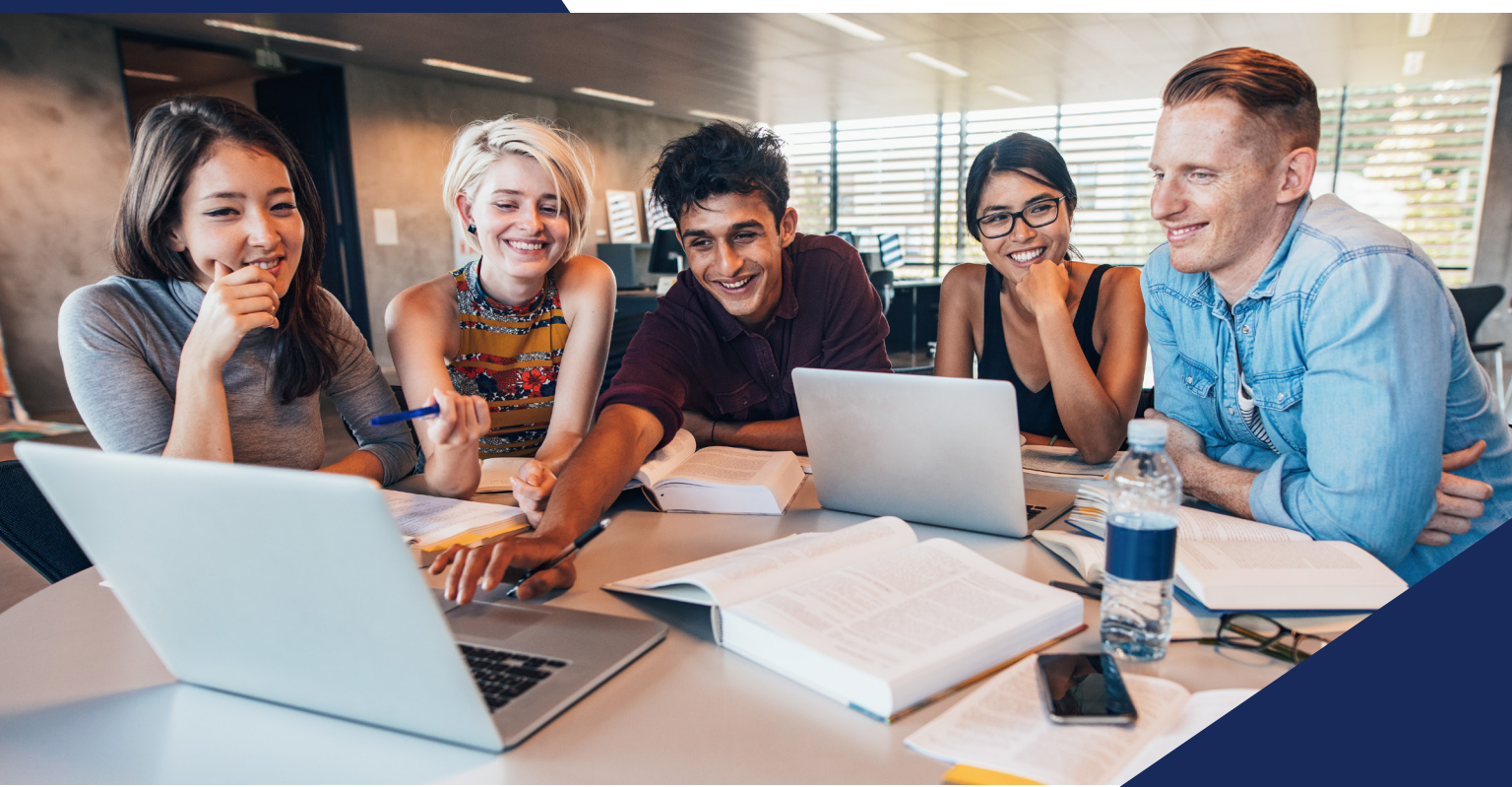
What to Know About **'Zero Trust'** in Higher Education

With cyberthreats on the rise, zero trust should be an integral part of your institution's cybersecurity strategy. In this white paper sponsored by Spectrum Enterprise, learn the top considerations and keys to success for a zero trust approach to network security.



SPONSORED BY:

Spectrum ENTERPRISE™

PRODUCED BY:

CAMPUS TECHNOLOGY

Colleges and universities are being targeted by increasingly sophisticated cyberattacks. These attacks can be devastating to institutions; in spring 2022, an Illinois college announced that it was **closing its doors for good** after a cyberattack crippled its operations for several weeks.

As campus leaders look to protect their data and networks from a barrage of threats, the nature of cybersecurity is changing. With a growing number of applications now running in the cloud and users accessing resources from remote locations, campus networks can no longer be protected by establishing strong perimeter defenses, like a castle being guarded by a moat. Instead, institutions need modern cybersecurity defenses that extend the network edge to each user and application.

Keeping campus networks secure requires strategic thinking in combination with smart policies and technologies. An approach that is becoming more popular across public and private organizations alike is the concept of "zero trust."

What Zero Trust Is and How It Works

According to the National Institute of Standards and Technology (NIST), "Zero trust is the term for 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 significant shift in philosophy. Traditionally, once users have logged onto a campus network and been authenticated, they've generally had wide latitude to explore and access basic institutional resources. To expand on the castle analogy, the underlying assumption has been that anyone who was allowed inside the castle walls belonged there and was trusted to move around freely.

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

Cybersecurity by the Numbers

As campus leaders consider adopting a zero trust approach to network security, here are some cybersecurity facts to be aware of:

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

74% **of ransomware attacks** in higher education were successful in 2021, resulting in a move to encrypted data.

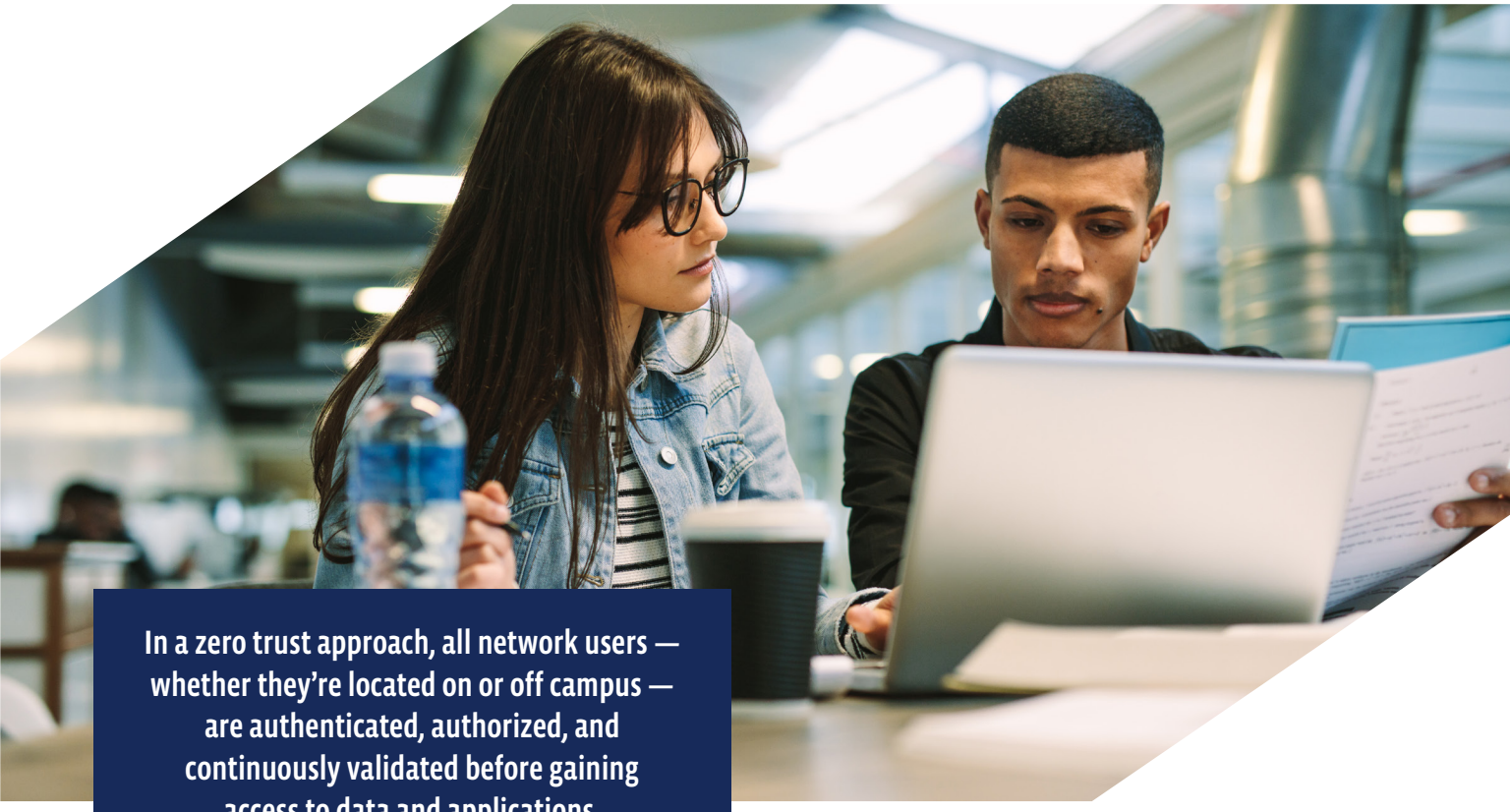
$1.42 **million is the average cost** to resolve a ransomware attack in higher education. This includes not only the cost of paying the ransom, but the cost of restoring applications and data systems to their original state.

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

61% **of data was returned** to colleges and universities that were victimized by a ransomware attack in 2021, after paying the ransom.

49% **of higher education IT leaders** say the level of cybersecurity they need to qualify for cyber insurance is even greater now than last year.

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



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

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

In other words, instead of roaming the castle freely, users are being stopped and asked to show their ID in every hallway and before entering every room. Zero trust is characterized by the principle: "Never trust, always verify."

To implement this approach, higher education institutions need strong identity and access management tools in place to verify users' credentials. IT staff must be able to know who is on the network at all times, as well as which applications they're using and how they're connecting. Campus networks must be finely segmented, and permission to access various resources should depend on contextual factors such as the user's role, device, location, and the application or data being requested.

Benefits of Adopting Zero Trust

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.

"The zero trust model protects institutions against the misuse of their resources," said John Sands, a professor of IT and chair of the Computer Integrated Technology Department at Moraine Valley Community College in Illinois, where he directs the college's Center for Systems Security and Information Assurance (CSSIA).

"For example," Sands explained, "we have students who come into open computer labs and install peer-to-peer file servers on our network with an unauthorized VPN. Those types of threats are totally eliminated with a zero trust approach."

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, campus IT staff have full visibility into the devices on their network — and they're constantly tracking these devices. This means

that IT staff should be able to identify attacks or anomalies nearly instantly as they occur, thus accelerating the 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.

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

Main Challenges

The biggest benefit to adopting zero trust is also the biggest challenge for campus IT staff when implementing it: This approach to cybersecurity makes access to network resources more difficult. As a result, legitimate users may require more technical support when navigating the network.

"New users in particular might run into more problems logging in, and they might need help in accessing the resources they need," Sands said. Accordingly, colleges and universities should plan for an uptick in user questions and support tickets as they move to a zero trust approach.

Because permission to access data and resources is granted based on factors such as a user's role at the institution, campus IT leaders are tasked with keeping user profiles up-to-date. This can be challenging to manage, especially within a campus setting — where student turnover happens every semester and visiting lecturers frequently come and go.

Think of how many student employees colleges and universities hire every year, such as for work-study programs or research opportunities. When students get a job working in the library, for instance, they might need access to library-specific network resources. If they start working in a lab, they might require access to sensitive research.

Not only are network users coming and going all the time, but their roles on campus frequently change as well — and many of these changes require updates to their network permissions.

Keys to Success

While zero trust can be challenging to implement, its potential for mitigating risks and improving network security can be enormous. Here are five keys to success when moving ahead with a zero trust approach.

Get the support of senior leadership.

Zero trust can help colleges and universities secure their networks and data more effectively, but it will involve some cultural changes and a significant investment in time and resources. It's not a quick fix. Effective implementation requires engagement throughout the organization.

"You'll need the buy-in and support of executive-level leadership and each campus department," Sands said. To gain this support, IT leaders will need to explain the concept of zero trust and the benefits it can bring to cabinet members and other senior leaders.

Understand the impact to your entire organization.

To ensure a smooth transition, IT staff should anticipate the impact that zero trust might have on various campus departments.

"Some parts might not be impacted very much," Sands said. "For others, it could have a significant impact. For example, a processing center that is processing payments could be much more sensitive to any changes that could create issues for users."

Develop a multiyear strategy.

It's likely that zero trust will take some time to implement. Some steps will be easier to take than others; for instance, adopting strong identity and access management is a logical place to start. Network segmentation is typically a heavier lift, as it can be tricky to reengineer networks while people are still using those assets — like building an airplane and flying it at the same time.

As you're moving ahead with zero trust, don't forget about commonsense security controls

that you can put into place in the meantime, such as multifactor authentication, DDoS protection, and training users how to spot phishing campaigns.

Create an awareness campaign.

It's not only senior leaders who need to understand how zero trust works: Students, employees, and other network users also should become familiar with the concept.

"Campus IT departments should lead some type of training or awareness campaign before implementing zero trust, so people understand why you're moving to this approach, how the model works, and where to get help if they run into any issues," Sands advised.

Work with a trusted security partner.

Because adopting zero trust can be complicated, colleges and universities can benefit from partnering with a company that has extensive network security experience to help with this transition.

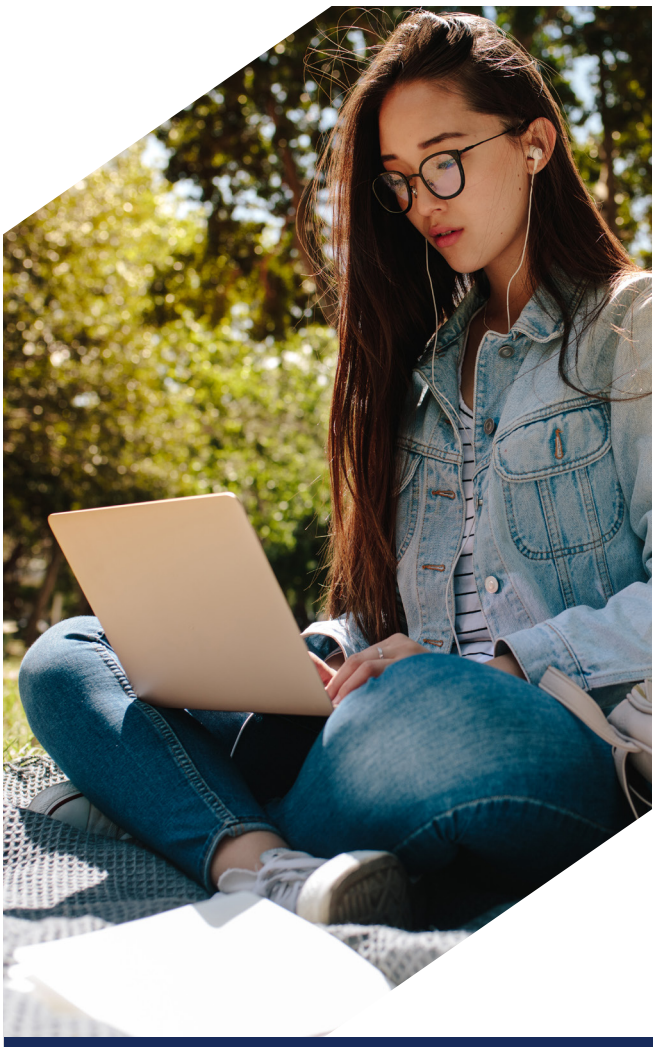
That's true any time, but especially as many institutions are struggling with significant labor shortages in the wake of the pandemic. IT departments are **among the hardest-hit areas**, and a big reason for that is the high-pressure role that technology staff played in moving campus operations online during the pandemic — which has led to burnout among many IT employees.

With campus IT staff stretched thin, a reliable service provider with experience in serving the higher education market can help make the move to zero trust as seamless as possible.

Improving Confidence and Minimizing Risk

As colleges and universities face an increase in cyberthreats, zero trust can help prevent and mitigate attacks on their networks — resulting in fewer service disruptions, less risk and greater peace of mind for campus leaders.

"There's no denying we're a target," Sands concluded, referring to the rise in cyberattacks on colleges and universities. "Zero trust gives stakeholders more confidence that network resources and data are going to be protected."



About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes **networking and managed services solutions**: **Internet access**, **Ethernet access and networks**, **Voice** and **TV solutions**. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit **enterprise.spectrum.com.**