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."