



# 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.

#### 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](https://enterprise.spectrum.com).