

Comprehensive cybersecurity on campus

A comprehensive cybersecurity strategy is required to stop unauthorised users, devices and applications from accessing the network in this zero trust era.

Five-steps to protect your campus

Traditional security strategies are no longer sufficient to ward off bad actors. Following are five steps to a **Zero Trust Network Access (ZTNA)** strategy to deliver the 'trust no one' coverage you need.

1

Monitor. Create an inventory of all devices and applications — authorised and unauthorised — that request or deliver information on the network, as well as the protocols they use.

2

Assess and validate your inventory. Assess devices and applications by type and role. This can identify shadow IT devices that can be eliminated to immediately reduce the attack surface.

3

Plan your approach to authentication, authorisation auditing and administration. Develop a multidimensional plan that includes macro-segmentation and micro-segmentation.

4

Simulate. Test and validate the approach developed in Step 3. Use the resulting insights to fine-tune security policies.

5

Enforce. Security policies can be enforced at the edge of the network, where users, devices and applications attempt to access it.

Risks, rules and rewards

As you embark on your ZTNA journey it's important to consider the **risks, rules** and **rewards**.

Risks to consider:

- Unauthorised devices not managed by IT can wreak havoc
- Inconsistent security policies introduce weakness
- Networks with static security segmentation and implicit trust allows previously trusted users, devices and applications to go unchecked



Rules to abide:

- U.S. regulations include Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA)
- The EU General Data Protection Regulation (GDPR) applies to all institutions with EU student enrollment no matter where the institution is located



Rewards to reap:

- **Expansive protection:** Authenticate every connection and assign permissions to each user and device with network access control lists and role-based access
- **Reduce the risk of attack propagation:** Provide granular control by micro-segmenting user traffic within a macro-segment
- **Enhanced reputation:** Best practices with diligent processes can boost an institutions' brand and public image
- **Improved academic results:** Innovative digital technologies improve learning opportunities and student success
- **Increased IT effectivity:** Ensure the appropriate use of network resources and make informed decisions about new technology strategies
- **Financial benefits:** Reduces the risk that expensive mitigation measures will be required in response to cyberattacks



Your cybersecurity partner

An experienced partner can provide insight and proven cybersecurity solutions. We work with you to deliver secure networking solutions that fit your strategy.



Certified secure:

ALE networking solutions meet major security standards, including the:

- International Common Criteria guidelines and specifications for IT security
- U.S. Joint Interoperability Test Command (JITC) compliance tests
- U.S. Federal Information Processing Standard (FIPS) 140-2



ALE solutions expand our customers' investments by integrating with firewalls from Palo Alto Networks and Fortinet.

Certified experience:

We are a trusted cybersecurity partner with institutions around the world, including:

- [California State University in the U.S.](#), our solutions enable a **reliable and flexible network** with enhanced security, Wi-Fi everywhere and open, shared cloud services
- [Centro Paula Souza in Brazil](#), our solutions provide the **secure, high speed, performance** users require
- [Linköping University in Sweden](#), our solutions provide **resilient, secure network access** to students and faculty, guests, external partners, tenants in university buildings and service providers



[Learn how we can help your academic institution](#)

focus on teaching and learning while we focus on protecting your network.