

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

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.

Plan your approach to authentication,

authorisation auditing and administration.

Develop a multidimensional plan that includes macro-segmentation and micro-segmentation. Simulate. Test and validate the approach developed in Step 3. Use the resulting insights to fine-tune

security policies.

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

As you embark on your ZTNA journey it's

Risks, rules and rewards

and rewards. Risks to consider:

important to consider the risks, rules

Inconsistent security policies introduce weakness

Rewards to reap:

within a macro-segment

and implicit trust allows previously trusted users, devices and applications to go unchecked

Unauthorised devices not managed by IT can

· U.S. regulations include Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA)

no matter where the institution is located

- Expansive protection: Authenticate every connection and assign permissions to each user and device with network access control lists and role-based access
- **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
- network resources and make informed decisions about new technology strategies

• Increased IT effectivity: Ensure the appropriate use of

expensive mitigation measures will be required in response to cyberattacks

Financial benefits: Reduces the risk that



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)

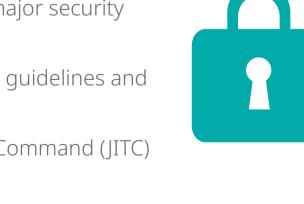
compliance tests

proven cybersecurity

you to deliver secure

networking solutions

solutions. We work with

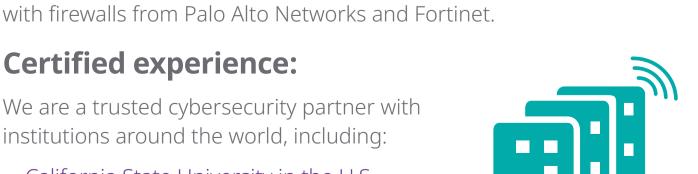


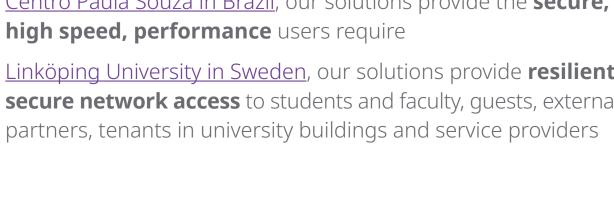
 U.S. Federal Information Processing Standard (FIPS) 140-2 ALE solutions expand our customers' investments by integrating with firewalls from Palo Alto Networks and Fortinet.

our solutions enable a reliable and flexible

- institutions around the world, including: California State University in the U.S.,
- network with enhanced security, Wi-Fi everywhere and open, shared cloud services · Centro Paula Souza in Brazil, our solutions provide the secure,
- · 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

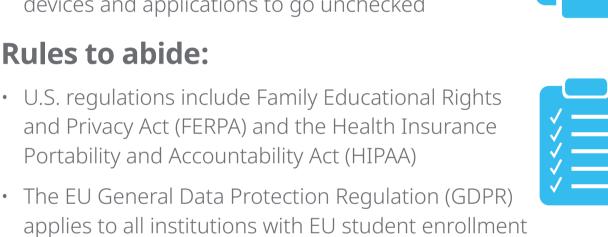
Learn how we can help your academic institution focus on teaching and learning while we focus on protecting your network.



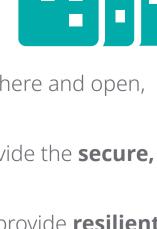




wreak havoc Networks with static security segmentation Rules to abide:









All rights reserved in all countries. DID23020902EN (May 2023)