

Secure-by-Default Campus Networks

VLAN-Free Connectivity for the AI Era

Higher-ed cannot address Zero Trust by layering more controls onto a network built for connectivity — the security boundary must be native to the architecture.

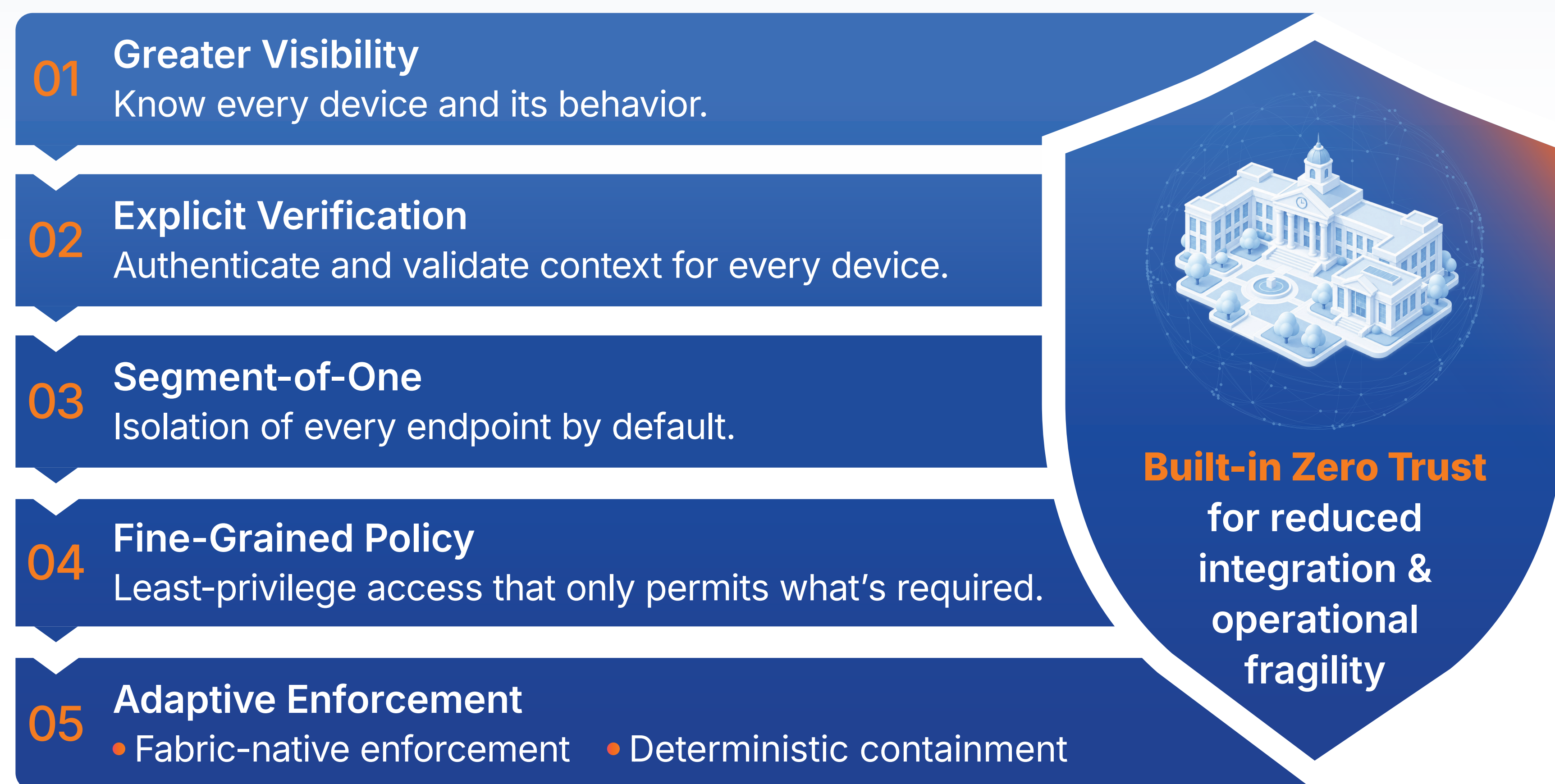
An ever-expanding attack surface



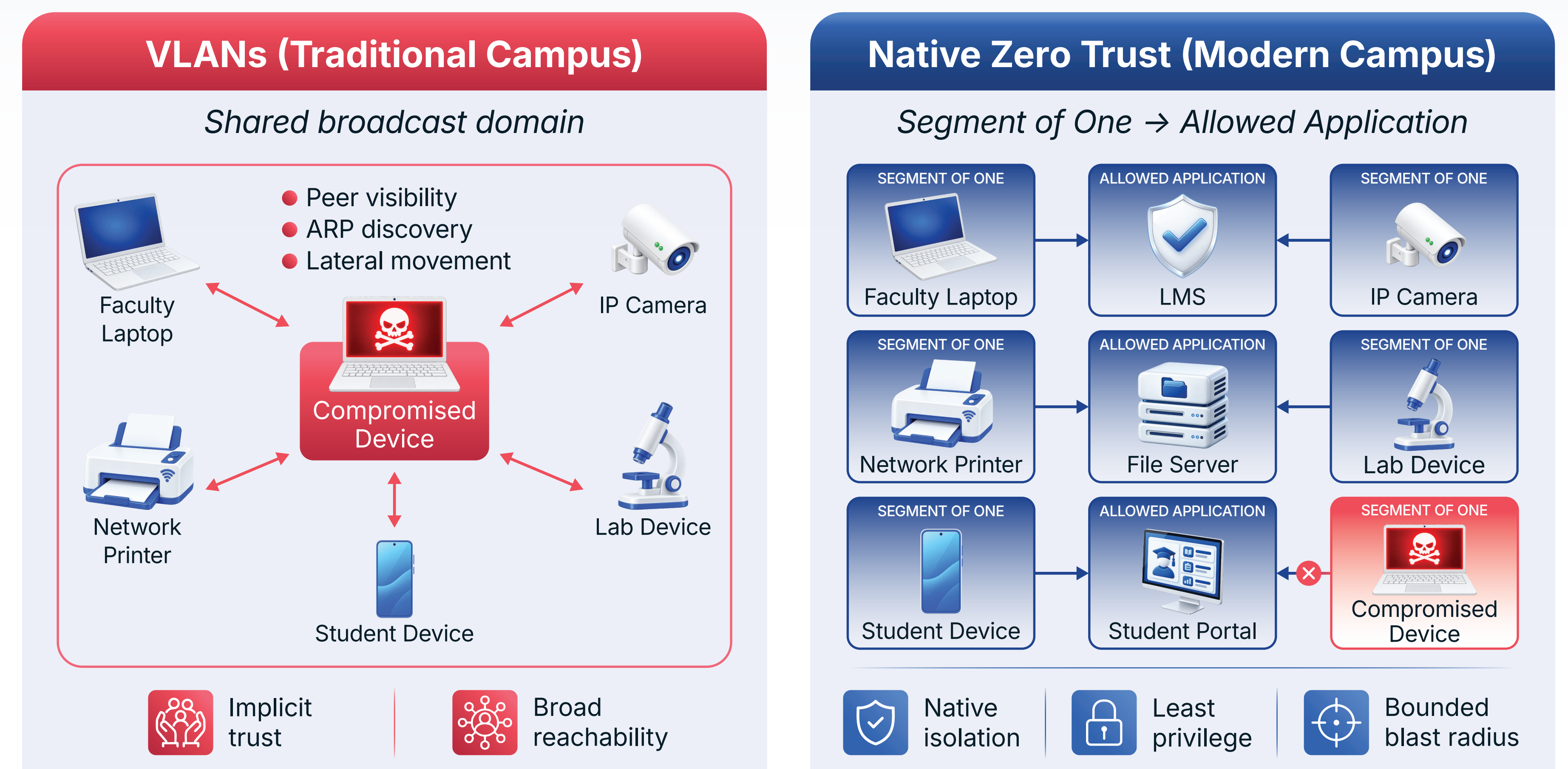
- 🚫 VLANs organize connectivity — but leave you open to topology-based trust.
- 🚫 Layered tools create policy and response dependencies.
- 🚫 BYOD, unmanaged, and IoT/OT devices cannot host agents.

The network must be your primary protection layer, especially for devices that do not support agents.

The 5 steps to a more secure campus



VLANs vs Native Zero Trust



VLANs connect devices. Zero Trust constrains what each device can see and reach.

Industry-Leading Outcomes

- Granular segmentation for greater AI threat containment
- Most secure **Guest Access** with isolation of traffic from campus resources
- Built-in Access Controls & Enforcement** eliminate the need for complex NAC
- Industry's easiest to manage student **Personal Area Networking (Trust Circles)**

All Delivered as-a-Service

- ✓ 99%+ reduction in trouble tickets
- ✓ Autonomous day-2 operations
- ✓ Out-of-the-box Zero Trust security

Secure-by-default NaaS For Lean IT

Nile Secure NaaS

An Innovative Alternative to Legacy Wired and Wireless Networking

Scan to learn more

