CYBER RESILIENCE FOR HIGHER ED:

Keep Higher Education Running with Identity-Based Microsegmentation

Zero Networks stops lateral movement and contains every attack automatically

Campus networks evolve constantly – students become staff, staff hold multiple roles, guest devices connect, and third-party platforms handle coursework, grades, and research data. Security can't slow any of that down. It has to work in the background, containing risk without adding friction.

That's where Zero Networks' automated, identity-driven microsegmentation comes in.

What Zero Networks Delivers: Capabilities Tailored to Higher Education

Identity-based microsegmentation

Access follows the person, not a static network rule, so entitlements stay accurate as roles change.

Automated policy lifecycle

Policies are generated based on learned network behavior via Zero's deterministic, human-on-the-loop automation engine and enforced without manual rule-writing or ongoing tuning.

Just-in-time MFA for privileged access

With patented network-layer MFA, sensitive systems (grading, research data, admin tools) require identity verification before they can be accessed.

Governed third-party and BYOD access

Extends identity-based controls to student devices and third parties, giving security teams full visibility into and control over every connection.

Agentless deployment

Zero Networks' agentless architecture seamlessly integrates with existing infrastructure and orchestrates native controls.

90%+ segmentation coverage within 90 days

Close the pathways attackers depend on to spread – no manual burden or risk of disruption.

Where Risk Lives in Higher Ed Networks — and How Zero Networks Contains It

The Problem	What It Looks Like	How Zero Helps
Role transitions without access cleanup	A student becomes a TA, then a tutor, then re-enrolls as a grad student. They keep accumulating access at every stage. Old entitlements become open pathways.	**Identity-based access controls dynamically adapt to network changes, so entitlements reflect a person's current role – automatically, without a manual deprovisioning cycle that never catches up.**
Multi-role identity governance	Students and staff hold several roles at once – TA and research assistant, adjunct and administrator – creating overlapping access that's hard to audit and easy for an attacker to exploit.	**Every identity is restricted to only pre-approved assets and logon types – no matter how many roles or systems someone has touched over time, access stays scoped to what's actually needed, without requiring manual upkeep.**
Third-party platform compromise	When a widely used third-party platform is breached, the damage can cascade to higher ed networks.	**Third-party connections are constrained to least privilege; microsegmentation contains compromises automatically, so a breach in one system doesn't become a campus-wide outage.**
BYOD without full device control	Students and faculty connect to the network with their own devices, leaving security teams with limited visibility and control.	**Zero's Secure Remote Access solution enforces the same least privilege controls for users connecting from BYOD devices and delivers end-to-end network visibility, enabling security teams to uncover previously hidden devices and activity.**
AI tools and agents on campus	AI tools and agents are adopted across daily work – often without explicit approval or oversight, creating a fast-growing blind spot.	**AI Segmentation delivers visibility and control over AI – governing which AI tools users can reach, segmenting AI infrastructure, and constraining agent access to least privilege.**

Contain threats by design to make cyber resilience your default. See how Zero Networks secures the systems that keep higher education running.

Request a Demo →

ZERO. Networks