eBook

Higher Ed Campus LAN Security, With Built-in Zero Trust

Practical ways to resolve risk at the network layer

Table of Content

The Current State Of Higher Ed Campus Lan Security

An open and broadly accessible campus network, built to enable collaboration among students, faculty, researchers, and visitors, makes universities and colleges especially vulnerable to malware, ransomware, and IoT attacks. That level of accessibility, combined with often-outdated systems, makes universities a prime target for adversaries and nation-state actors.

> **"Ransomware attacks against schools, colleges, and universities rose 23% year over year in the first half of 2025, according to a report from Comparitech, a cybersecurity and online privacy product review website."**

Protecting against these threats requires more than just adding on firewalls, network access control (NAC), and antivirus software. Universities need a layered, proactive Zero Trust approach that combines technology, policy, and awareness. While malware prevention and containment are a priority, it's important not to create an environment where overly cumbersome enforcement results in frustration and help desk tickets.

Complexity and disruption are reasons many institutions remain wary of implementing a Zero Trust framework—not because they doubt its value—but because of assumed costs, operational burden, and resource requirements. However, with a proper approach and implementation steps, Zero Trust more than pays for itself in the long run—especially if it results in avoiding costly attacks.

The remainder of this eBook highlights why higher education networks are a target for internal and external threats, what went wrong in the past, and the steps CIOs and other network and security leaders can take to better address emerging threats and challenges.

Why Are Campuses Prime Targets?

In addition to a mix of IT-managed and BYOD, the explosion of IoT/OT devices (cameras, sensors, lab equipment, smart boards) has introduced blind spots. The need to balance accessibility with security has also proven a challenge for many. These other factors make colleges and universities attractive to adversaries:

Large and open networks

Collaboration, academic freedom, and a highly distributed attack surface create opportunities for adversaries to exploit many commonly known external and internal vulnerabilities.

Abundance of sensitive data

Vast amounts of information, including personal data specific to students, faculty, and staff, enrollment data, and sensitive intellectual property from research.

Lean IT

Departments with insufficient funding and persistent staffing shortages, making it difficult to combat increasing cyber threats, user behavior, and troubleshooting.

Human Vulerability

Students, faculty, and staff are often not trained in enterprise-level cybersecurity hygiene. This leaves them vulnerable to phishing and other social engineering attacks that give adversaries a foothold into the network.

Lastly, **higher education is a prime target for attackers—seen as both vulnerable and more likely to pay a ransom**. While payment does not guarantee a full recovery, the number of universities paying a ransom increased from 47% in 2023 to 62% in 20241.

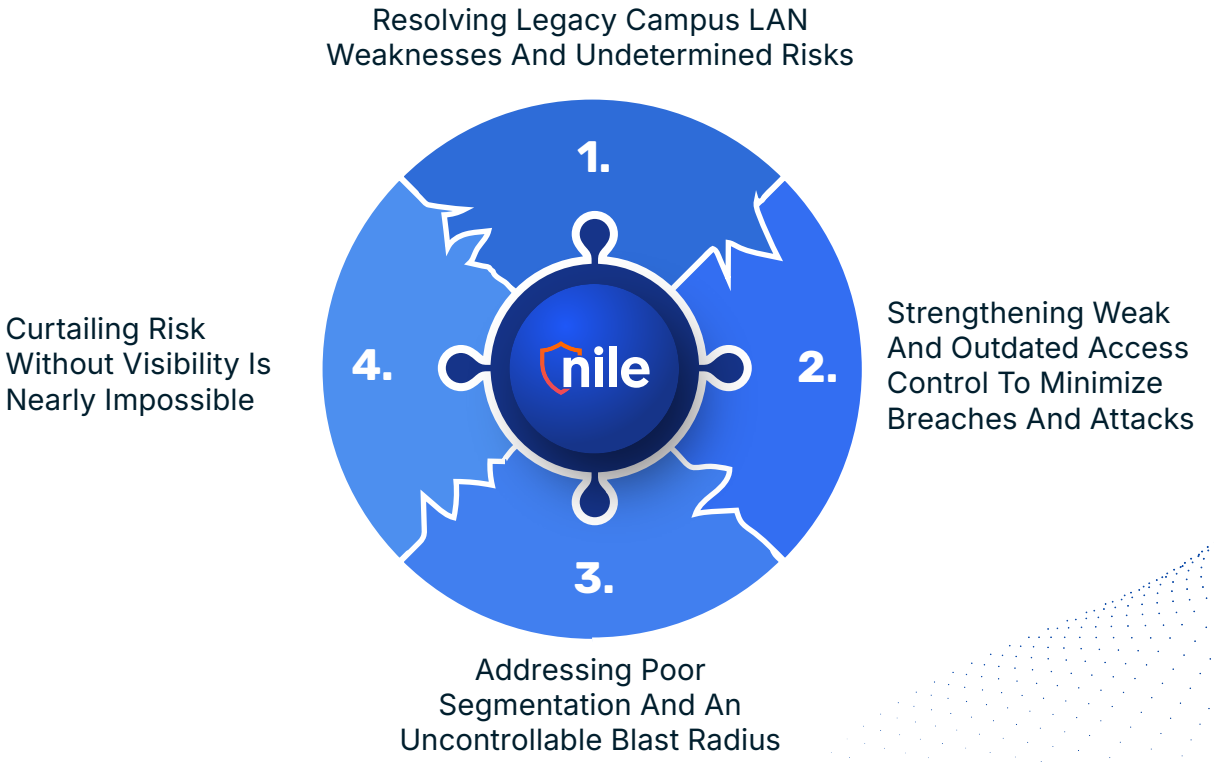
Why Legacy Cybersecurity Frameworks Have Failed

For network and security leaders in higher education, diverse student needs, aging infrastructure, and limited budgets often take a backseat to audits and compliance, leaving fundamental risks unaddressed. To close these gaps and a fading perimeter, the adoption of Zero Trust principles is now a priority.

Guidance for implementing Zero Trust often defaults to its most basic recommendations: Multi-factor authentication (MFA), endpoint security, enhanced monitoring, and granular segmentation. While each is important, **one of the most critical aspects is often overlooked** — the campus LAN itself.

The campus LAN must evolve. Complex, bolt-on solutions to fix legacy hardware and software vulnerabilities are no longer enough — Zero Trust and micro-segmentation must be foundational elements of the architecture itself.

> **"Gartner's recent Predicts 2025: Scaling Zero-Trust Technology and Resilience report paints a sobering picture: by 2028, 30% of organizations are expected to abandon their zero-trust initiatives, citing complexity, lack of integration, cultural resistance, and limited vendor value. "**



Resolving Legacy Campus LAN Weaknesses And Undetermined Risks

Unlike typical enterprises, colleges and universities often have a fragmented IT landscape where departments operate independently with their own legacy network infrastructure and systems. Each of which typically leverages decades-old security protocols that are no longer sufficient-VLANs are just one example. This leads to network vulnerabilities and policy inconsistencies, making the implementation of a uniform Zero Trust strategy extremely challenging.

What's needed:

Consider a modern Network-as-a-Service (NaaS) model where **Zero Trust security is built into the network fabric by design**.

The campus LAN today must include the ability to secure all user, IT-managed, and IoT/OT devices to mitigate the spread of malware and ransomware, regardless of location, department, or building. A fully hardened environment must also include:

Secure LAN infrastructure

Network hardware should not be directly accessible. All local access methods, including unused Ethernet ports and administrative interfaces, should be eliminated, disabled, or restricted by default.

Modern security principles

Reduce reliance on manual configuration to limit errors that expand the attack surface. The network fabric should also conceal its topology and operations to make it harder for adversaries to discover and exploit resources.

End-to-End Encryption

All management, user, and IoT/OT traffic that traverses the campus LAN should be encrypted by default.

The end result is a wired and wireless campus network built on top of a Zero Trust Fabric, with security capabilities embedded—not bolted on—to eliminate legacy vulnerabilities and reduce complexity. A standardized NaaS architecture delivers a consistent model that enhances both security and compliance requirements at its core.

Strengthening Weak And Outdated Access Control To Minimize Breaches And Attacks

The next step in Campus Zero Trust defenses is controlling who and what connects to the network, be it laptops or IoT/OT devices. Institutions with legacy **Network Access Control (NAC) solutions face significant challenges** as these systems were developed for older static environments. Keeping pace with the modern campus's mobile and diverse user base, and density of devices is now a challenge.

What's needed:

Adopt strong **inline access control with authentication that moves beyond simple passwords and shared passkeys.**

Enforce multifactor authentication (MFA) for faculty, staff, and students where applicable. For added security, use MFA with single sign-on (SSO) for seamless access as your preferred model to leverage identity in order to reduce unauthorized access — a common entry point for adversaries. Also consider:

Identity-based access controls

Faculty, students, administrators, and IoT devices should all maintain tailored access rights, limiting their exposure if compromised.

Automated provisioning

To automate and streamline identity management, the System for Cross-domain Identity Management (SCIM), which is used to provision and deprovision user accounts, should be extended to include network access privileges.

Continuous verification

Implement a solution that eliminates the traditional "implicit trust" given to users and devices once on the network. A one-time check at the beginning of a session is no longer adequate, especially for IoT/OT devices.

By implementing a comprehensive Zero Trust framework directly into the network fabric, institutions can enhance the principle of least privilege access without adding complexity. This also allows for an improved experience for students, faculty, and staff, reducing "password fatigue" and potentially decreasingIT help desk calls.

Addressing Poor Segmentation And An Uncontrollable Blast Radius

Zero Trust emphasizes **microsegmentation as a core principle**, requiring organizations to isolate users and devices while enforcing dynamic, identity-based access policies. Yet most institutions still rely on legacy networks that deliver only rudimentary segmentation. Without granular, identity-aware controls, they operate from a weak foundation that creates a false sense of security.

What's needed:

Institutions must shift to a **network and Zero Trust Fabric that natively supports micro-segmentation**, granular traffic inspection, and policy control.

By verifying device and user identities, institutions can place every device into an isolated segment by default before granting access. This prevents lateral movement, enforces conditional access, and automatically contains devices that behave abnormally. Additional considerations include:

Context-aware policies

Access should restrict what individual devices can reach and also control who or what can communicate with them, helping contain unwanted visibility, access, and breaches.

Granular policy control

Leverage built-in enforcement to apply role- and identity-based policies that govern user and device behavior across the network. For example, students' devices can reach specific printers. Printers cannot communicate with research systems.

Secure Services Edge (SSE)

Where applicable and when budget allows, provide staff, researchers, administrative personnel, and select students unified, cloud-based SSE security for web, cloud services, and applications, supporting hybrid learning and campus operations by securing data and devices regardless of location.

By adopting a NaaS-delivered Zero Trust Fabric with built-in micro-segmentation, identity verification, and granular policy control, institutions can ensure that every user, device, and data flow is protected by default. Access is limited to what is necessary, abnormal behavior is contained automatically, and policies adapt based on identity, role, and context. Whether it's students, faculty, IoT devices, or guests, each is secured within its own boundaries.

Curtailing Risk Without Visibility Is Nearly Impossible

Devices of all types are connected to the network by students, staff, professors and visitors **without ITs knowledge**, affecting the performance of the network, and also introducing vulnerabilities. Malware then hides in unmanaged or unknown devices which can lead to severe consequences for both individuals and institutions, including data theft, financial losses, disruptions, and reputational

What's needed:

From a security perspective, **inline fingerprinting and traffic monitoring** have become the preferred model today.

Legacy out-of-band NAC solutions do not play a role in monitoring behavior or ensuring a device matches its fingerprint once a device has established connectivity, This leads to the need for additional solutions and dashboards, which escalates costs and complexity. Explore an alternative network architecture that includes the following:

Continuous device discovery

Inline fingerprinting versus out-of-band solutions help identify every device on the network, and monitor their traffic activity to ensure devices do not impersonate the behavior of another device type. This is done throughout the entire length of a connection.

Traffic monitoring

A built-in network enforcement capability that monitors all north-south and east-west traffic to spot anomalies, such as unusual data transfers and excessive data usage.

Centralized dashboard

Consolidate visibility tools so that IT teams aren't chasing blind spots across multiple tools. Shifting between dashboards leads to lost time and missed activity.

This final step ensures that "unknown devices and activity" do not go unnoticed and are addressed in real time. This is a major flaw in legacy environments where out-of-band access control, fingerprinting and traffic monitoring solutions are pieced together. By operating in the path of traffic, built-in solutions are better able to enforce policies and alert organizations to potential threats as soon as they are detected.

Conclusion

Colleges and universities of all sizes with overburdened IT teams face the tough challenge of managing networks based on outdated infrastructure and legacy security practices. Layering Zero Trust on top of this fragile foundation is even more challenging, as evolving threats require capabilities that existing infrastructure was never designed to support or protect against.

By following an AI-Powered NaaS strategy that includes built-in Zero Trust capabilities — adopting robust security principles, strengthening identity, ensuring visibility, leveraging cloud security, and establishing governance — universities can significantly reduce their operational burden and risk.

The goal is not to eliminate all risks — that's impossible. Instead, IT leaders and their staff must consider a campus network foundation that removes complexity and legacy vulnerabilities. This enables the network to withstand malware attempts, contain outbreaks, and protect the vital mission of education and research without disruption.

> **"The Nile NaaS solution gives us premium Wi-Fi, switches, and security that are better than anything we could build ourselves. We've gained an extremely high level of performance, Zero Trust security, and expertise backed by a financially-backed service guarantee."**