nile | SOLUTION BRIEF

Campus Zero Trust: Modern Alternative to Securing Evolving Threats

IT leaders today are tasked with everything from addressing remote access concerns and the mounting use of IoT to securing their campus networks from sophisticated malware and AI generated attacks. Identifying vulnerabilities and proactively addressing key risks is critical to safeguarding the business.

Unfortunately, campus and branch networks often represent the single greatest threat to an organization. This is due to several compounding factors, including:

- **Outdated infrastructure** – Many networks still rely on LAN designs and segmentation principles developed over 30 years ago, making them especially vulnerable.
- **Diverse users and devices** – Employees, guests, and IoT devices that each introduce distinct and often unpredictable security challenges.
- **Zero Trust complexity** – Attempts to layer on security frequently adds complexity and frustration without delivering the intended protection.

Together, these factors provide adversaries the opportunity to compromise a single device and move laterally across the network – launching malware, ransomware, and increasingly, remote access trojans (RATs) to seize control of resources, exfiltrate data, and disrupt operations.

Robust Design and Automated Deployment

As CIOs and IT leaders focus on addressing evolving network security initiatives, they're tasked with clearly defining if their current Zero Trust measures are proving adequate. According to Gartner Inc., the term "Zero Trust" has become excessively used and misapplied, leading to significant confusion and frustration among organizations.

Due to confusion regarding the effective implementation of Zero Trust principles, organizations have often enforced overly rigorous least-privilege policies, causing friction among departments, users, and network and security personnel. To avoid this, it is essential to properly map security requirements, identify all necessary components and processes, and align Zero Trust with overall organizational goals.

To begin, ensure that previous Zero Trust efforts related to complexity, cost, and user experience are addressed. Solutions that offer built-in Zero Trust that satisfy user role and IoT requirements are recommended. Additionally, consider the expanded attack surface introduced by remote work. Can the success organizations are experiencing with secure access service edge (SASE) and security service edge (SSE) platforms—along with the adoption of Zero Trust network access (ZTNA)—also play a role in campus and branch environments?

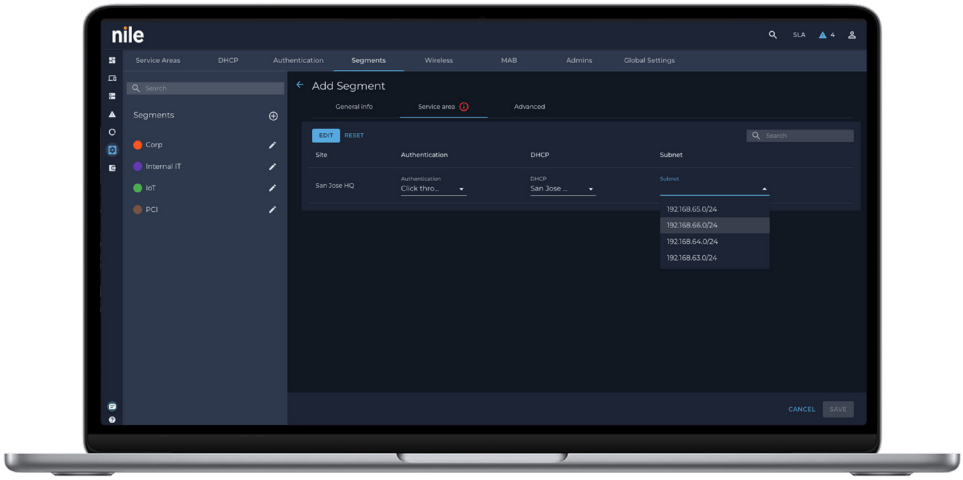
The term "Zero Trust" has become excessively used and misapplied, leading to significant confusion and a source of frustration among organizations.

Gartner Inc. Predicts 2025
Scaling Zero-Trust Technology & Resilience

Additional Recommendations

Initial steps must be taken to determine where Zero Trust was successful and why. The same can be said for where roadblocks were encountered, specifically if issues were tied to legacy infrastructure, complexity, cost, and the speed at which vulnerabilities were addressed by your current network vendor. This should include the following:

- Identify gaps and determine if existing legacy network infrastructure will support evolving Zero Trust initiatives without impacting IT resources, users, and business objectives
- Evaluate solutions that offer autonomous capabilities that extend from secure infrastructure and end-to-end encryption to built-in access control and granular policy enforcement
- Explore a network vendor's ability to automatically place endpoint devices into a "segment of one" without additional complexity to minimize exposure to any attacks or threats.
- Where equal campus and remote access security is required, ensure that a network vendor natively supports the integration of ZTNA principles into campus and branch use cases to provide the advantages of emerging Universal ZTNA, and its more adaptive and responsive security advantages.



Nile Access Service for Campus Networks

Nile delivers campus Zero Trust that is built-in and includes AI-powered network operations in a cloud-native as-a-Service delivery model. With a modernized autonomous networking architecture, customers gain a level of security and visibility that eliminates legacy vulnerabilities, prevents attacks from moving laterally, and ensures a unified experience regardless of connecting remotely or in the office, factory, distribution center, or university.

Organizations gain the advantage of modern network and Zero Trust principles without the cost, complexity, and deployment challenges.