SOLUTION BRIEF

Nile Trust Service:

A Modern Approach For IT Leaders To Campus And Branch Security

IT leaders today are tasked with everything from addressing the mounting use of IoT devices connecting to their wired and wireless networks and increasingly sophisticated malware and AI generated attacks. Identifying vulnerabilities and proactively addressing key risks is critical to safeguarding the business.

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

1

Outdated infrastructure

Many organizations still rely on LAN designs and segmentation principles developed over 30 years ago.

2

Diverse users / devices

Employees, guests, and IoT devices that each introduce distinct and unpredictable security challenges.

3

Zero Trust complexity

Attempts to layer on security frequently amounts to 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.

Achieving Zero Trust Compliance

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

The confusion tied to implementing Zero Trust principles has caused organizations to enforce 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 achieve desired results:

- Implement Zero Trust in the LAN that satisfies strong end-user and IoT security requirements.
- Eliminate outdated security principles such as VLANs, that add legacy complexity and cost.
- Address the integration of secure access service edge (SASE) and security service edge (SSE) platforms with LAN security to ensure a seamless end-user experience.

> **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

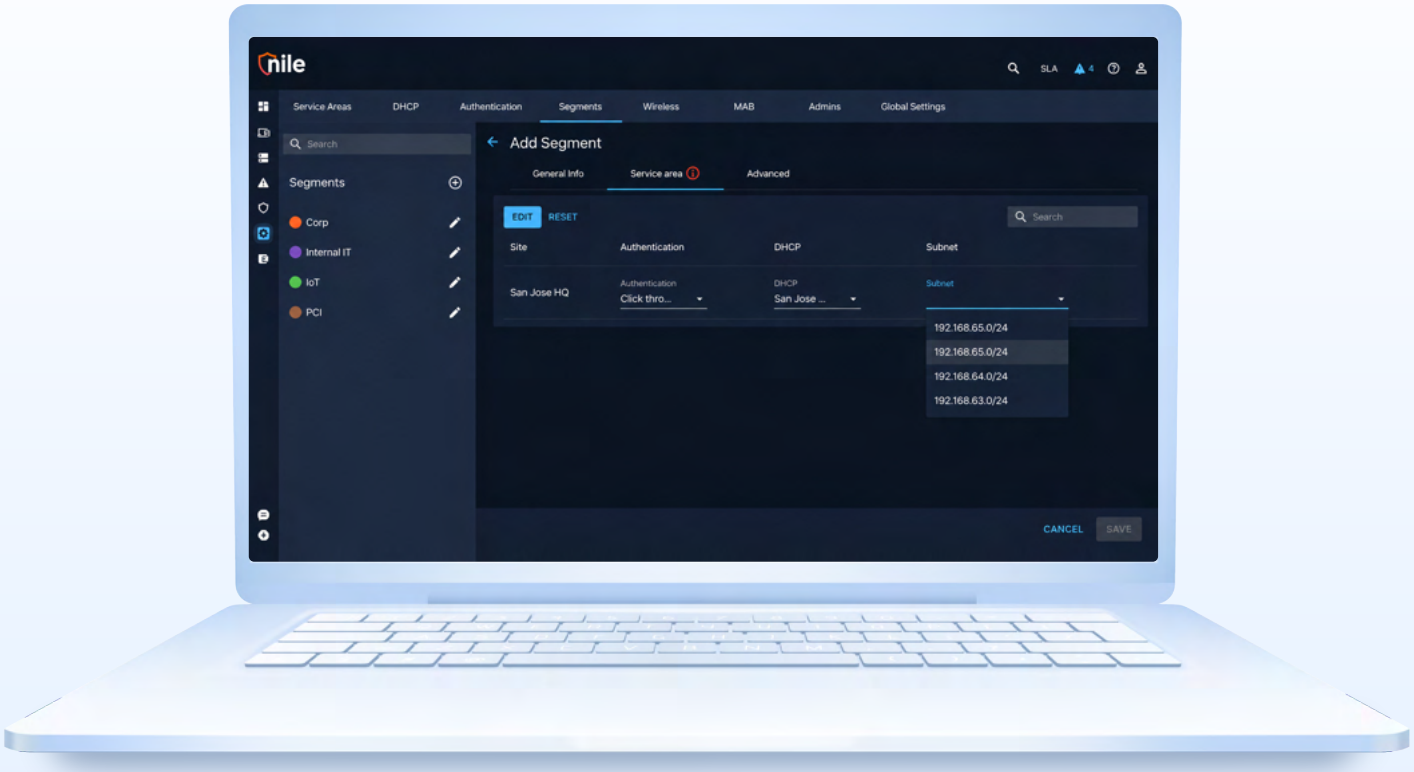
Initial steps must be taken to determine where previous Zero Trust efforts were successful and pinpoint where legacy tech, cost, or complexity blocked compliance initiatives. If roadblocks were encountered, what hampered meeting any internal or external requirements. The steps to take:

1. Determine if existing legacy network infrastructure and software will support evolving Zero Trust initiatives without impacting IT resources, budget, users, and business objectives.

2. Ensure that a vendor natively supports the integration of LAN Zero Trust principles and the security offered by leading SASE/ SSE solutions.

3. Explore a network vendor’s ability to automatically place endpoint devices into a “segment of one” without additional complexity to minimize any attacks or threats.

4. Identify the long-term value of security add-ons, such as NAC appliances, that a modern network architecture natively supports, allowing you to eliminate unwanted complexity.



The Nile Zero Trust Advantage

Nile's Zero Trust Fabric includes modern security principles that offer customers a new level of security and visibility that eliminates legacy vulnerabilities, prevents attacks from moving laterally, and ensures a unified experience regardless of whether connecting remotely or in the office, factory, distribution center, conference center or classroom.

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

About Nile

Nile is a pioneer and leader in secure networking-as-a-service (NaaS). With AI-powered service delivery and autonomous operations, Nile solutions cut through complexity and cost versus legacy networking solutions, while delivering radical operational simplicity and user experiences.

Ready to Get Started?

Request a Demo