nile

Nile Trust Service

A Revolutionary New Campus Zero Trust Network Security Model

nilesecure.com

Network security has rapidly evolved, driven by shifting user behavior, the rise of IoT devices, increased remote work, escalating cybersecurity threats, and the high costs of cyber incidents. This evolution from traditional perimeter security to Zero Trust has driven organizations to address campus LAN vulnerabilities. Many have implemented enhanced visibility measures along with NAC and segmentation solutions, though these additions often prove challenging to manage.

More recently, a movement toward cloud-based security has led IT organizations to adopt Secure Service Edge (SSE) and various endpoint security solutions, such as Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR), for secure remote access. However, foundational network security gaps remain largely unaddressed.

Traditional network security architectures have struggled to keep up with recent strategic changes. It's time for a fresh approach—one that removes known vulnerabilities and enables efficient, effective use of enterprise-grade security solutions without adding complexity. A shift that would benefit both IT organizations and enhance the user experience.

Midsize enterprise (MSE) IT leaders face significant security challenges when trying to deliver IT services with small IT teams and limited IT budgets. Across industries, MSE IT budgets average 4.9% of annual revenue, but only 5% of this IT budget allotment is dedicated to security.

Source: Gartner, Cybersecurity Outlook for Midize Enterprise, 2024

Introducing the Nile Trust Service

With these fundamental changes in mind, Nile has redesigned campus and branch enterprise networks to incorporate Zero Trust principles and advanced segmentation techniques at its core. Moving forward, cloud-based security solutions can be seamlessly added while taking advantage of an industry-first network security model that eliminates VLANs and prevents the spread of threats through lateral movement.

Rather than relying on traditional, outdated approaches, Nile offers organizations a new, secure network foundation that eliminates obsolete protocols and known vulnerabilities. This approach effectively prevents the spread of malware, ransomware, and insider threats while safeguarding internal and user-owned resources more efficiently. It also strengthens compliance efforts and may reduce cybersecurity premiums.

To that end, the Nile Trust Service delivers the following:

Elimination of Security Gaps

A Campus Zero Trust architecture with comprehensive security improvements that extend from the infrastructure to policy enforcement and the protection of all stored data.

IT Resource Productivity

Built-in segmentation, visibility, and threat containment that eliminates complex and costly integration projects.

Future Proofing

The ability to easily leverage built-in Nile services that provide universal policy enforcement and support for emerging technologies, such as AI, without increasing security risk or hampering the performance of the network.

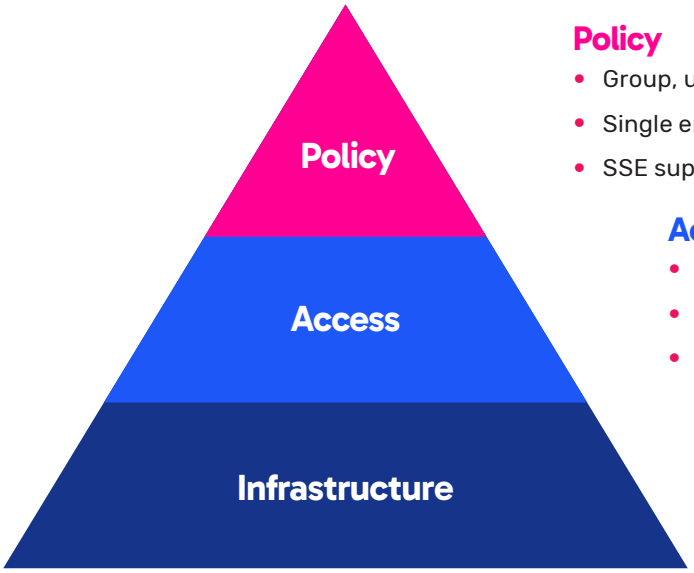
The Campus Zero Trust Architecture

Organizations can now breathe easier as long-standing vulnerabilities in traditional infrastructure have been effectively addressed. For example, eliminating console ports closes a key entry point for attackers, while automated configuration changes help prevent errors and malicious actions. The Nile Access Service also seamlessly includes the detection of rogue access points and containment of unknown endpoints.

With security and compliance in mind, the Nile Trust Service offers IT organizations a comprehensive Zero Trust model for their entire wired and wireless network. It delivers this solution without added complexity or cost, regardless of business type, size, or the number of users and IoT devices.

- **Zero Trust Infrastructure** - A new class of enterprise wired and wireless hardware and software designed to eliminate intentional attacks, as well as unintentional errors that expose critical assets and resources today. Automated configuration and software upgrades create a secure environment, helping organizations stay confident in the face of undisclosed vulnerabilities and zero-day threats.
- **Zero Trust Access** - The mandating of secure authentication and authorization of each connected device via single sign-on (SSO), multi-factor authentication (MFA), System for Cross-domain Identity Management (SCIM), and automated re-authorization of computers, phones, and IoT to ensure behavior and compliance requirements.
- **Zero Trust Policy** - Comprehensive Firewall and SSE support for the monitoring and enforcement of all traffic with granular controls, enabling rapid detection of malware and the containment of any unusual activity.

Encryption of all traffic passing through the Nile Access Service, along with data stored in the Nile Cloud, is seamlessly integrated into our offering. For added protection, IT organizations can leverage Bring Your Own Key (BYOK) to secure their data in the cloud to comply with internal security requirements and regulations in healthcare and other highly monitored industries.



Policy

- Group, user, IoT based behavior
- Single enforcement point, full control
- SSE support for cloud security unification

Access

- Dynamic device fingerprinting
- Built-in access control
- Full SSO, SCIM, RADIUS support

Infrastructure

- Per-device isolation& threat prevention
- Built-in L3 segmentation without VLANs
- Automated configuration

IT Resource Productivity

Building from a foundation based on modern Campus Zero Trust principles that require fewer add-on security solutions and integration allows IT teams of all sizes to offer their organizations a more secure environment while greatly enhancing the user experience. This is surprisingly challenging for IT organizations as the core of legacy network architecture design has remained stagnant.

Complex VLAN management tasks and costly Layer 3 segmentation projects are a thing of the past. There's no longer a need to implement outdated NAC solutions or roll out new SD-WAN and EVPN/VXLAN projects to ensure consistent access and policy enforcement, no matter the location. Instead of spending months to uplevel the segmentation of a network IT teams can focus on more business-critical opportunities as colorless ports, per-device isolation and Layer 3 is a standard Nile Trust Service feature.

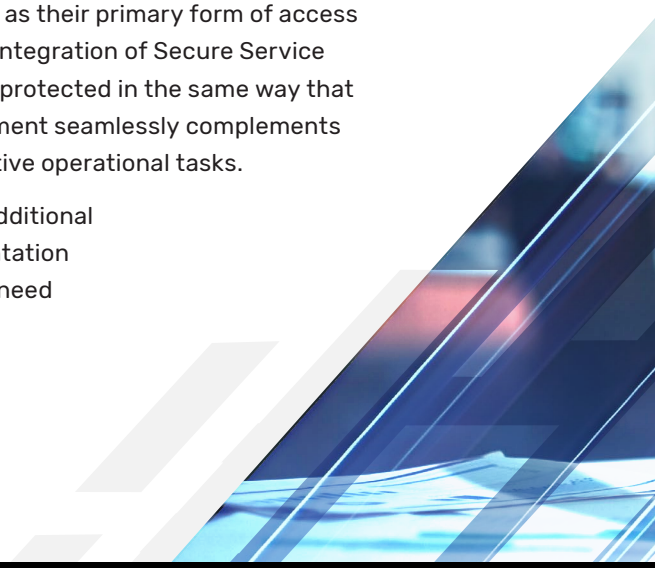
This foundational design principle within the Nile Access Service architecture enables easier containment or elimination of threats that exploit lateral movement through VLANs. Traditional network architectures often lead to alarming delays in detecting breaches, requiring specialized security skills. This provides IT organizations of all sizes an industry-first alternative.

The average response time to a cyber breach in 2024 is a critical factor for businesses, with an average of 277 days needed to identify and contain a breach.

Security With Future Proofing

For customers who have considered moving from on-premises firewalls as their primary form of access enforcement for the campus, the Nile Trust Service allows for the easy integration of Secure Service Edge (SSE) solutions. Enforcement for all wired and wireless devices is protected in the same way that SSE is used to secure remote access connections. Nile's cloud management seamlessly complements SSE solutions, removing the need for complex orchestration and repetitive operational tasks.

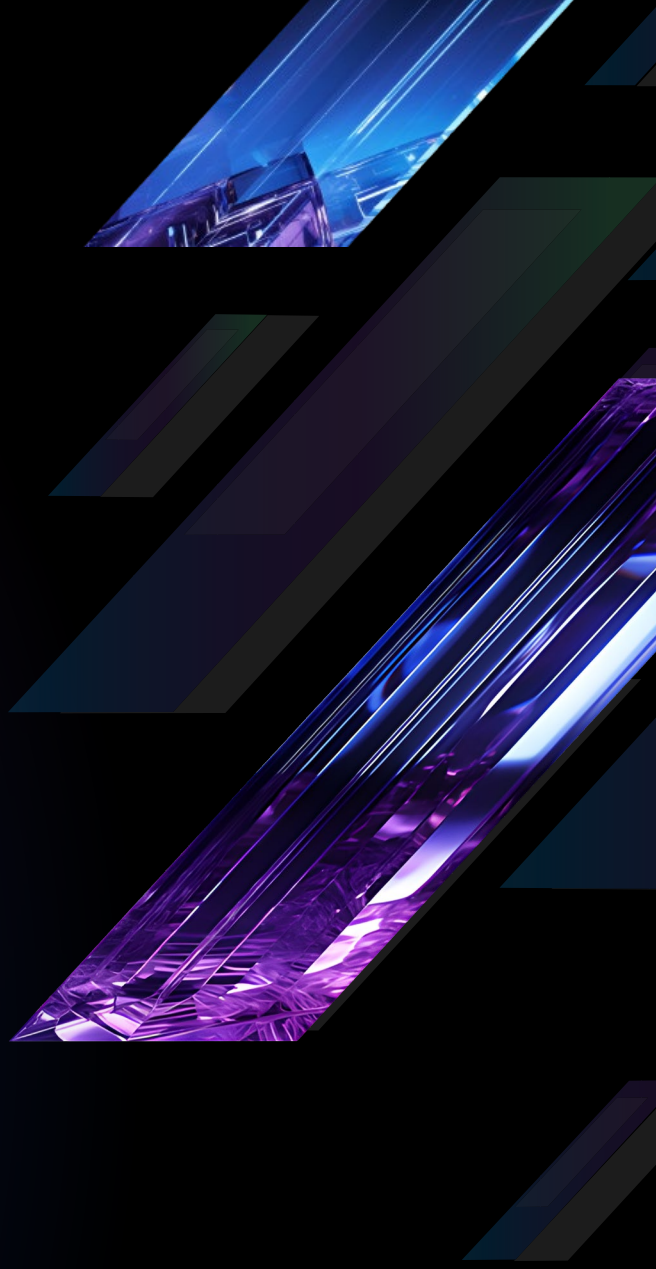
With Nile's per-device isolation, IoT devices and their traffic receive an additional layer of protection through today's SSE solutions. Built-in microsegmentation allows for easy creation of policies for IoT device traffic, eliminating the need to route traffic through the SSE solution beforehand.



A Solution for Network And Cloud Zero Trust Security

Given today's expanding threat landscape, every physical and organizational element must contribute to protecting critical resources—especially the campus network. Nile's AI-driven access service, with built-in Nile Zero Trust principles, ensures alignment between networking and security teams to address current and future network access and security challenges.

With a comprehensive Nile Trust Service foundation, networking and security teams can collaborate more effectively, enabling their organizations to leverage next-generation network and security services. This approach, delivered by design and as-a-Service, addresses the vulnerabilities found in over 98% of campus and branch environments in enterprise networks today.



nile

hello@nilesecure.com | **nilesecure.**com