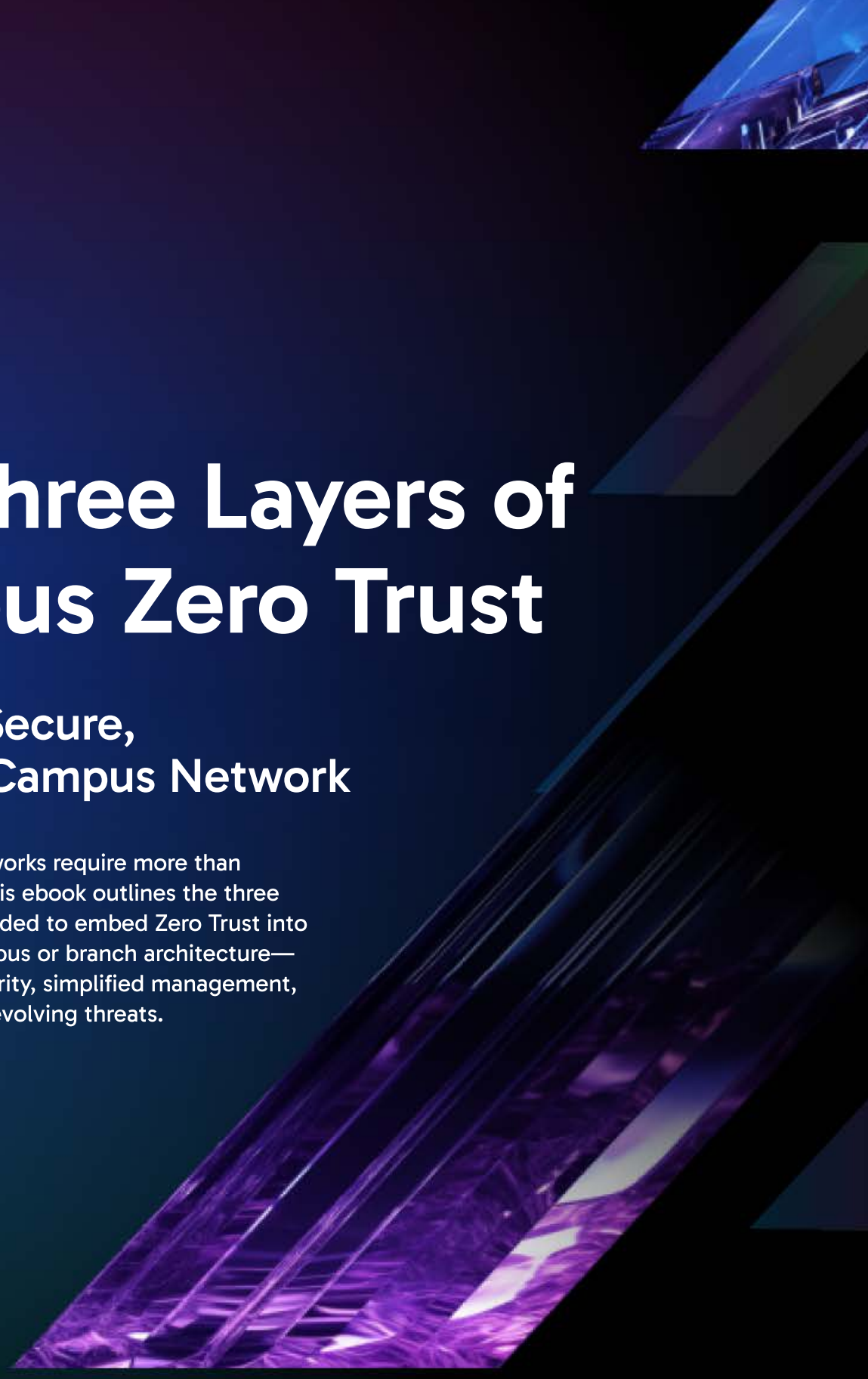
nile

The Three Layers of Campus Zero Trust

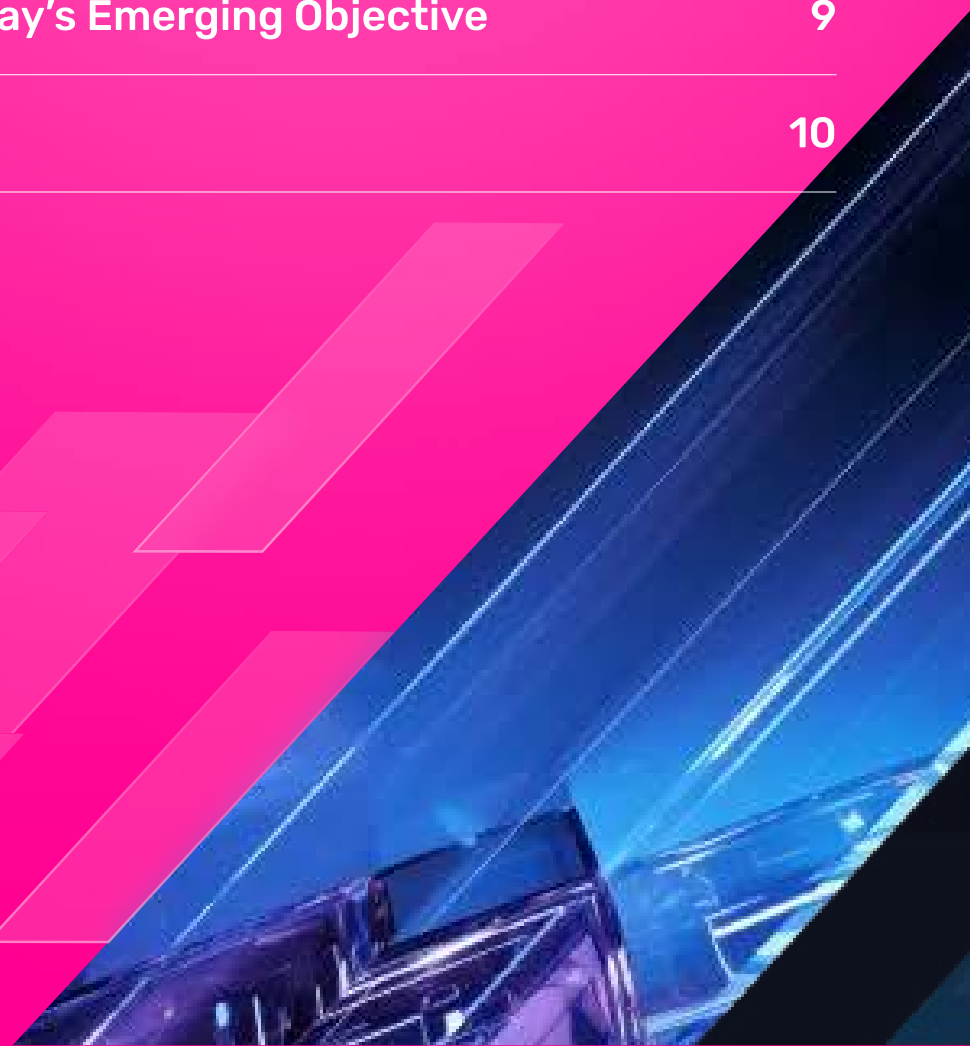
Building a Secure, Zero Trust Campus Network

Today's enterprise networks require more than perimeter defenses. This ebook outlines the three foundational layers needed to embed Zero Trust into every part of your campus or branch architecture—ensuring stronger security, simplified management, and resilience against evolving threats.



nilesecure.com

Table of content



Overview

Zero Trust remains the most talked-about cybersecurity strategy today for addressing the modern threat landscape —and for good reason.

A Gartner 2024 survey reports that 63% of enterprises worldwide have fully or partially implemented a zero trust strategy. However, these strategies address less than 50% of their environment, mitigating less than 25% of overall enterprise risk.

Gartner

While different framework definitions exist in the industry, such as NIST's 800-207 Zero Trust Architecture and Forrester's Zero Trust Extended model, Zero Trust is built on three foundational principles:

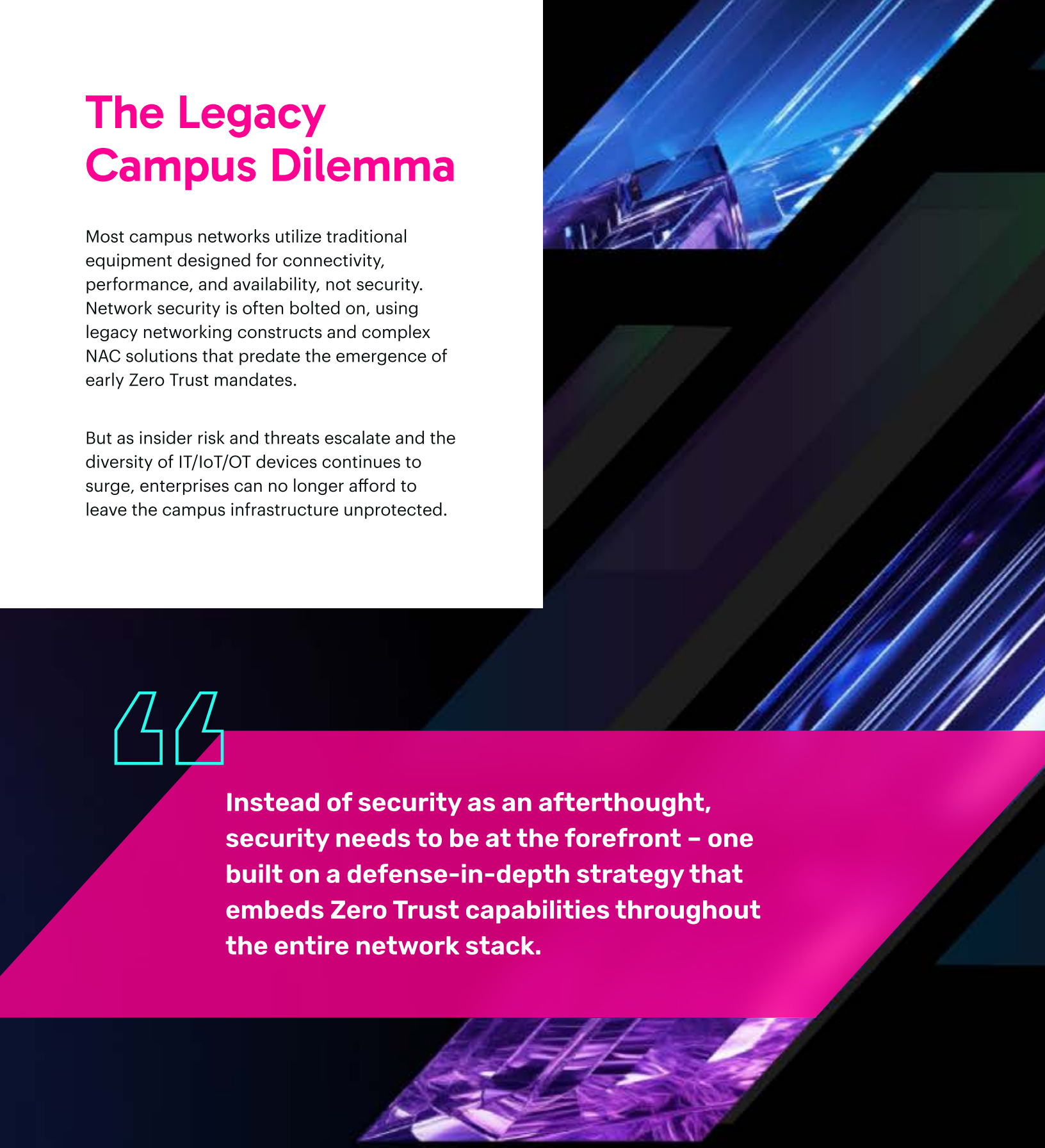
- **Never Trust – Always Verify**
- **Identity-based Least Privilege Access with context awareness**
- **Minimize Impact of a Breach – Contain Lateral Movement**

These principles have redefined secure remote access to applications, evidenced by the success of cloud-delivered SSE solutions like ZTNA and CASB. But in the campus environment, where a combination of users and enterprise resources co-exist and connect over a common wired and wireless infrastructure, the Zero Trust architecture must address the entire threat landscape within the campus and branch.

The Legacy Campus Dilemma

Most campus networks utilize traditional equipment designed for connectivity, performance, and availability, not security. Network security is often bolted on, using legacy networking constructs and complex NAC solutions that predate the emergence of early Zero Trust mandates.

But as insider risk and threats escalate and the diversity of IT/IoT/OT devices continues to surge, enterprises can no longer afford to leave the campus infrastructure unprotected.



Instead of security as an afterthought, security needs to be at the forefront – one built on a defense-in-depth strategy that embeds Zero Trust capabilities throughout the entire network stack.

In today's evolving threat landscape, Campus Zero Trust isn't optional – it's mission-critical.

nile

The Three Layers of Campus Zero Trust

To fully realize a Zero Trust campus or branch network, security must be natively embedded and vertically integrated across three essential layers:

Layer 1. Zero Trust Infrastructure – Harden the Network

In Campus Zero Trust, the "Never trust, always verify" tenet applies to the infrastructure itself. Each method for accessing the hardware within the network must be hardened or eliminated to reduce the attack surface visible to internal or external threat actors.

By default, traditional infrastructure equipment is exposed to multiple attack vectors, including local access interfaces, configuration ports, and visibility into network topology. Ideally, a fully hardened Zero Trust network should:

- Eliminate, restrict or secure all device access methods and protocols, including administrative ports
- Eliminate configuration data and configuration as an attack vector
- Mandate mutual authentication among all peers in the campus fabric.
- Obfuscate the presence, identity, and topology of the network
- Encrypt all traffic across the fabric at line rate
- Block and secure all fabric ports by default and prevent any unauthenticated/ unauthorized user or device from connecting to the network
- Fully isolate every individual endpoint by default, and prevent all lateral movement

A deterministic, purpose-built, security-first infrastructure implementing these immutable practices minimizes the attack surface and establishes a Zero Trust foundation.

Layer 2. Zero Trust Access – Continuous Authentication & Authorization

Campus Zero Trust also includes a strict access policy for all endpoints.

The onboarding of users and devices must not only be fully secured, but continuous validation across all users and devices is required, including both managed and unmanaged IT, IoT, and OT assets.

A comprehensive Campus Zero Trust Access layer includes:

- A set of strong authentication techniques that work collectively across users & devices
- Integrated user identification & device fingerprinting during onboarding
- Fully secured ports by default, allowing access only from authenticated endpoints
- Continuous authentication, verification, and real-time evaluation of security posture, trust level, and compliance
- Continuous monitoring of user group identity and employment status
- Automated spoofing detection to prevent masquerading and unsanctioned devices from being on the network
- Endpoint behavioral analysis and anomaly detection

By enforcing a strict policy that blocks all unauthenticated or unauthorized access, and continuously monitoring every endpoint, the network ensures that access decisions remain accurate, even as context or threat levels evolve.

Regardless of whether access is through wired or wireless infrastructure, no unauthenticated or unauthorized devices should be permitted onto the network.

Layer 3. Zero Trust Policy – Identity & Context-Aware Control

Campus Zero Trust enforces least-privilege, identity-based policies when users, devices or applications attempt to access other users, devices, or applications, By minimizing the access privileges, the attack surface can be minimized across all resource types.

In Campus Zero Trust, VLANs are not used as a security perimeter – access policies are instead decoupled from networking constructs altogether and all endpoints are isolated by default, eliminating lateral movement. In alignment with zero trust principles, an access policy identifying source and destination endpoints or groups must be defined before traffic through the fabric is permitted. Additionally, these policies support conditional access through context awareness. Attributes are evaluated in real-time as part of the enforcement process, including contextual information such as:

- Device/user identity and category (e.g., corporate, BYOD)
- Real-time security posture
- Identity risk level
- Location and time-of-day

Access to any resource, whether user, device, or application, is governed by the Zero Trust Policy layer with a "default deny" policy, ensuring that access is only ever granted if a policy permits it. Recontextualization of endpoints is continuous to ensure an accurate representation of the endpoint's state before policy is applied. Identity-based policy enables portable, fine-grained access control that adjusts dynamically to changes in user roles, context, or behavior.

Implementing Campus Zero Trust Policy allows enterprises to reap substantial advantages, including:

- Enhanced security posture through minimizing resource access to only what's required
- Reduced risk of manual configuration errors through access policies tied to identity and not to networking constructs
- Improved compliance and auditability by ensuring that users and devices can access resources suited to their roles or functions, while also simplifying the tracking of resource access

Traditional segmentation methods based on static networking constructs like VLANs do not scale, lack portability, and most importantly, assume devices within the same VLAN are trusted. This opens the door to lateral movement and exposes sensitive data to unnecessary risk.

Orchestrating Zero Trust – Centralized Visibility, Control, Integration & Assurance

An effective Campus Zero Trust framework requires a centralized orchestration layer that delivers visibility, policy control, integration, and assurance across the entire enterprise. This orchestration system must manage and automate security policies consistently across the three core layers of Zero Trust: Infrastructure, Access, and Policy.

Built on a standardized architecture with embedded Zero Trust principles, the orchestration platform should coordinate connectivity and access privileges across distributed enforcement points—whether on-premises or in the cloud. Based on identity, context, and defined policies, it ensures the right traffic reaches the right security functions while enabling seamless integration with other enterprise and cloud-based services. This includes integration with services such as:

- Secure Service Edge (SSE) services like Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Zero Trust Network Access (ZTNA) or Cloud Access Service Broker (CASB)
- Secure Access Service Edge (SASE) architectures that unify SD-WAN and security
- Comprehensive guest access solution such as the secure Nile Guest Service
- Security and operations platforms, such as SIEMs and ITSM solutions

Enabling Universal Zero Trust

The orchestration platform is essential for realizing Universal Zero Trust—an emerging enterprise objective focused on unifying security controls and access policies across all environments: cloud, data centers, and physical campuses.

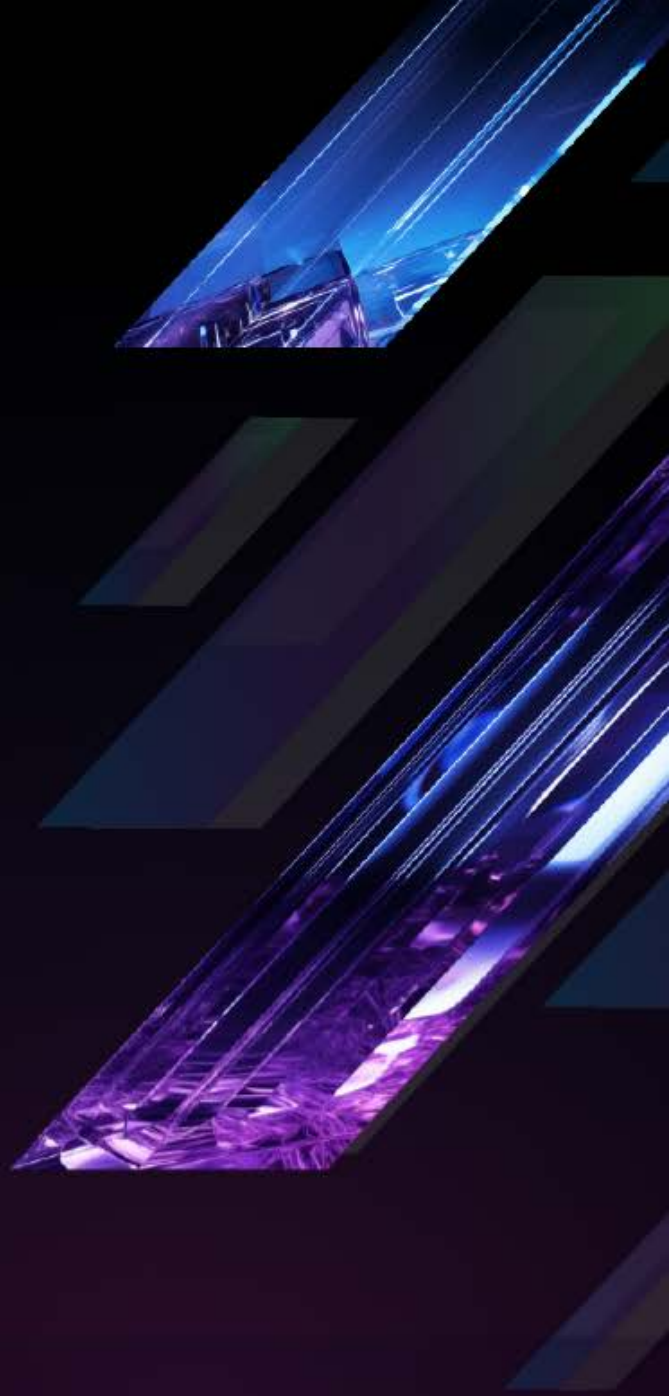
Universal Zero Trust delivers a consistent, least-privilege access experience for all users and devices, including unmanaged or IoT/OT endpoints, regardless of location. At the center of this model is centralized policy orchestration, which defines and enforces access rules across distributed enforcement points, guided by real-time identity and context.

Achieving this vision requires deep integration between Campus Zero Trust orchestration and SSE/SASE platforms at the policy tier. This integration enables an adaptive trust framework that supports unified access control, real-time posture assessment, and scalable policy enforcement across the entire enterprise.

Summary

Moving Towards a Secure Campus Future

Integrating Zero Trust principles into every layer of the network is the only way to deliver consistent, scalable protection in a campus environment increasingly targeted by advanced threats.



nile

info@nilesecure.com | nilesecure.com