SOLUTION BRIEF

Zscaler & Nile

Unified network access and policy enforcement for users and IoT whether on-premises or remote.

Quick Glance – Integration Highlights

- Provides universal cloud-based SSE controls to campus connected devices
- All campus traffic automatically routed to Zscaler Internet Access instance for policy enforcement
- Strengthen your security posture on all fronts
- Simple 2-minute activation, with automated orchestration

The Market Challenge

With today's hybrid work model, organizations want the same Zero Trust protection for in-office users and devices that remote users already receive through cloud-delivered SSE solutions. But legacy campus networks were not built to deliver that level of consistent security and policy enforcement.

As a result, organizations are often forced to deploy and manage separate solutions for the campus, including firewalls, NAC, and other point products. What they need instead is a simpler approach that extends consistent protection and policy enforcement across campus, branch, and remote environments.

The Solution

Together, Nile and Zscaler deliver a modern joint solution for campus and branch environments that allows organizations to enforce consistent policies for users as well as IoT and OT devices, aligned with the protection delivered by cloud-based SSE and ZTNA solutions. Customers gain the benefits of cloud-based security, where the network plays a key role in protecting data and assets without requiring add-on solutions, extra agents, or complex integration projects.

The AI-powered Nile Secure NaaS, with built-in Zero Trust security, solves today's growing campus security challenges by providing a highly secure network that includes per-device isolation of all wired and wireless devices and Layer 3 segmentation by design. The addition of Nile's integration with Zscaler ensures all traffic is forwarded to Zscaler's Internet Access solution. Local East/West traffic can be handled by Zscaler or Nile depending on device type.

Solution Components / Key Features

Enhanced policy enforcement via Zscaler Internet Access (ZIA) for all endpoint devices regardless of connection, whether on-premises or remote.

Per-device isolation without the use of VLANs via Nile Secure NaaS's built-in Zero Trust security and Layer 3 segmentation.

Simplified IoT and BYOD security as all traffic can be forwarded to ZIA for inspection or selectively allowed via Nile's identity-based segmentation.

Encryption of all on-premises traffic for each connected wired or wireless device that traverses Nile Secure NaaS.

Simple connectivity that uses existing LAN-to-WAN services, including Nile Edge Service, to connect users and devices to the local Zscaler Internet Access instance.

Why It Matters

This combination of cloud and on-premises Zero Trust security offers a more consistent and efficient security model that provides secure, reliable access regardless of device or location, with a common approach to policy enforcement. On-premises environments no longer have to be the weakest link.

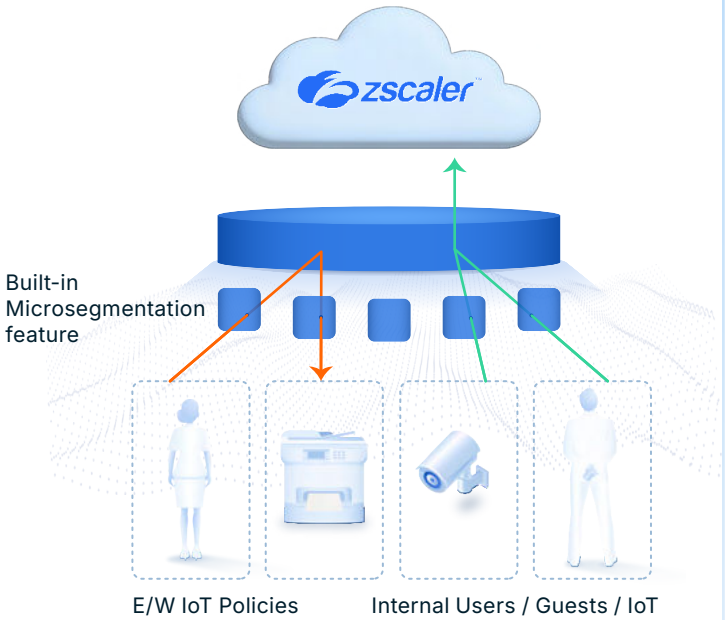
USE CASE 1

Unified policy enforcement

Zero Trust isolation and policy enforcement is achievable via cloud-delivered and on-premises integration. By channeling all traffic through a north-south pipeline, organizations can ensure consistent policy enforcement regardless of device type or location.

The solution isolates individual users and devices, allowing no communication unless explicitly permitted by policies enforced by Zscaler Internet Access (ZIA). Data flows between devices or users are encrypted and tunneled individually for inspection, guaranteeing only authorized flows between source and destination are permitted.

With Zscaler and Nile, your network is better protected, ensuring stronger protection for your valuable data and assets.



Nile Access Service

USE CASE 2

A secure hybrid work model

With today's hybrid work, managing disparate policy enforcement solutions for users connecting remotely versus when they're in a corporate office or branch is cumbersome. This joint solution for on-premises and remote user access delivers built-in Zero Trust security features that complement today's modern SSE solutions.

With the isolation of individual devices, Layer 3 segmentation, and Zscaler Internet Access policy enforcement, users gain a more consistent security experience.

The result is a combination of built-in Zero Trust security and SSE features that deliver consistent policy enforcement and scale without the complexity.

USE CASE 3

Zero Trust IoT security

IoT devices are no longer weak links within networks as this joint solution eliminates legacy VLANs and associated security risks, IoT vulnerabilities, and threats caused by lateral movement. Per-device isolation and forwarding of traffic to your Zscaler Internet Access instance provides a stronger approach to IoT security, all without software agents or complex configuration steps.

Organizations gain the advantage of built-in Zero Trust segmentation across wired and wireless environments, and the ability to leverage consistent policy enforcement via Zscaler's SSE capabilities. IoT devices are no longer easy targets for malware to spread throughout the organization.

Key Benefits

BENEFITS	OUTCOMES
Improved security posture	Unified security with consistent protection for all users, devices, and apps, regardless of location
Enhanced visibility and control	Deep network and security event insights for improved decision-making and responses to threats
Scale and flexibility	As organizations evolve, a unified solution easily scales to accommodate new use cases, and applications
Unified policy management	Centrally manage both remote and on-premises security functions with more consistent enforcement
Cost and IT efficiency	Single framework that reduces the need for separate solutions, ongoing maintenance, and support costs

Conclusion

Deliver enhanced user and IoT device network security with Zscaler and Nile

Experience a modern Zero Trust approach that replaces legacy security architectures built around VLANs and firewalls. All connections are authorized based on shared user identity, business policies, and context, including location, device status, and authentication and authorization privileges. The result is reduced risk, an improved user experience, and simplified management and deployment.

About Nile

Nile is a pioneer and leader in Secure Networking-as-a-Service (NaaS). It's leading a fundamental shift in the industry with a clean-slate approach that brings the power of zero-trust, autonomous operations and cloud to deliver compelling business outcomes and act as a force multiplier for IT. Nile solutions cut through complexity and cost versus legacy solutions, while delivering radical operational simplicity, security and speed with stellar user experiences.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

Ready to Get Started?

Request a Demo