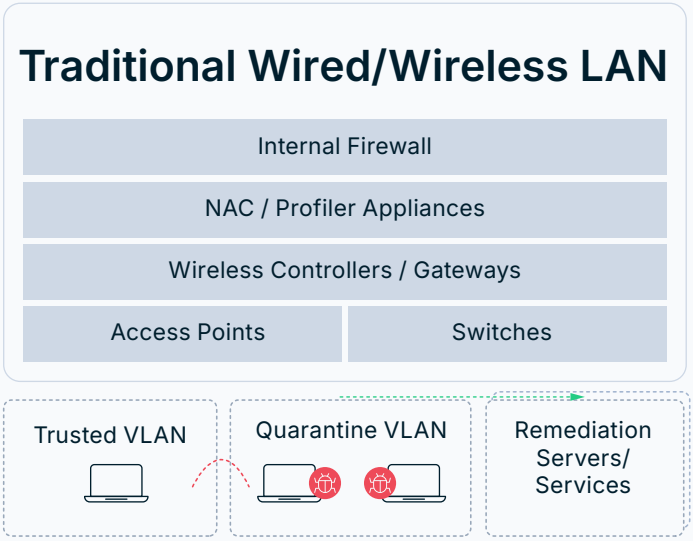
USE CASE

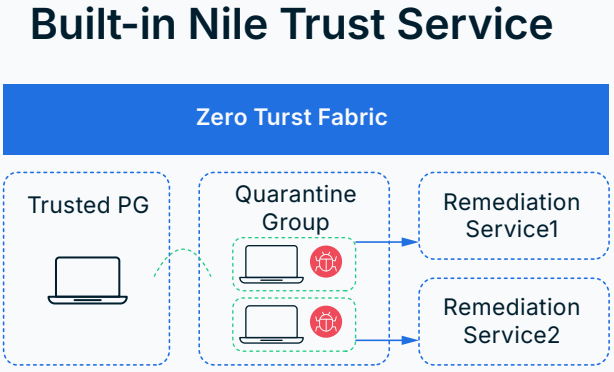
Breach And Malware Containment

Traditional Quarantining Methods Create Complexity And Security Gaps

Nile offers a modern approach – one that automatically isolates devices, restricts communications and controls a blast radius the radically improves compliance initiatives.



VLAN-based Quarantine



Device-specific Quarantine

- Unreliable, coarse containment
- Exposes devices to additional threats

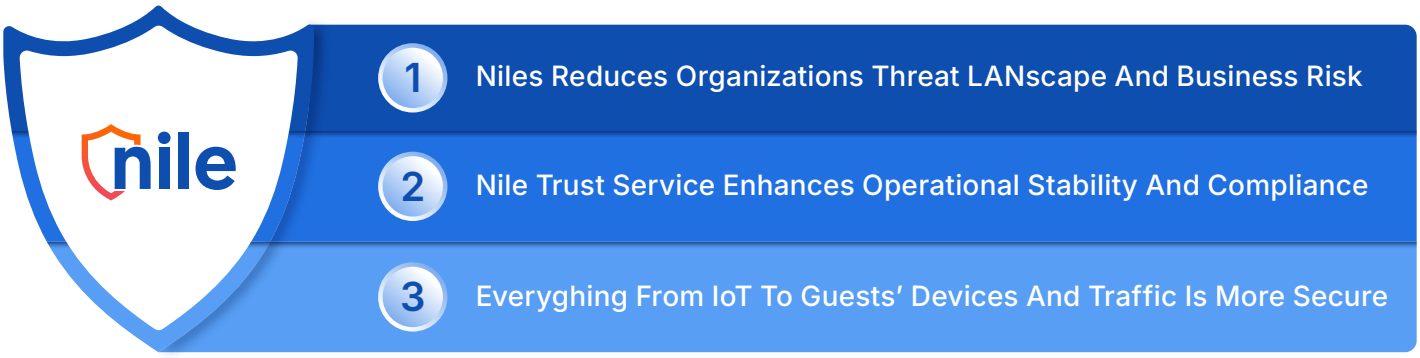
- Deterministic containment
- Per-device isolation, no VLAN exposure

Nile's Leading-Edge Differentiation

Identity-based polices and containment with continuous enforcement maps to evolving Zero Trust requirements.

Automated segment-of-1 isolation eliminates lateral movement and limits a potential blast radius.

Industry-first embedded Zero Trust allows any organization to achieve Zero Trust compliance.



Nile Makes Threat Containment Easy

Microsegmenatation By Default

All devices are placed into "segment-of-1" isolation without complex integration projects and cost.

No VLAN-Based Complexity

VLAN-based imitated threats and intricate network changes are replaced with native Zero Trust

Enhanced Compliance By

Organizations instantly gain measurable network and per-device security outcomes without IT or user burden.

Simplified Quarantine And Containment

For a financial services customer, real-time threat containment is not a nice-to-have; it is a requirement. For any device not in compliance, Nile isolates, enforces a per-device policy, and only allows access to a specific remediation service by default.

No complex VLAN assignment, timing dependency, and operational complexity.

Breach And Threat Containment Shouldn't Be Difficult

Legacy Upgrade Approach	Nile Secure NaaS Approach
Broad VLAN-based segmentation open to additional exposure	Per-device isolation with least-privilege access
Non-deterministic remediation based on complex network changes	Deterministic policy-based model without complexity
Complex and expensive NAC integration	No legacy NAC solutions required
High operational overhead	Simplified model that leverages built-in Trust Service capabilities
Unpredictible, with hidden costs	Predictable NaaS model - with built-in support

Ready to Get Started?

Let's Talk ↗