USE CASE

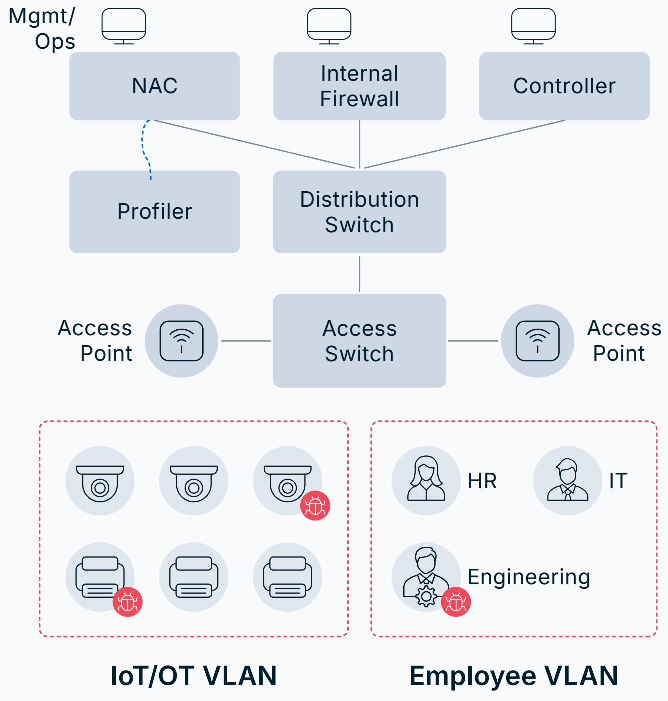
IoT/OT Security

A Zero Trust approach to securing unmanaged devices

Legacy Networks Are Challenged By IoT/OT Devices

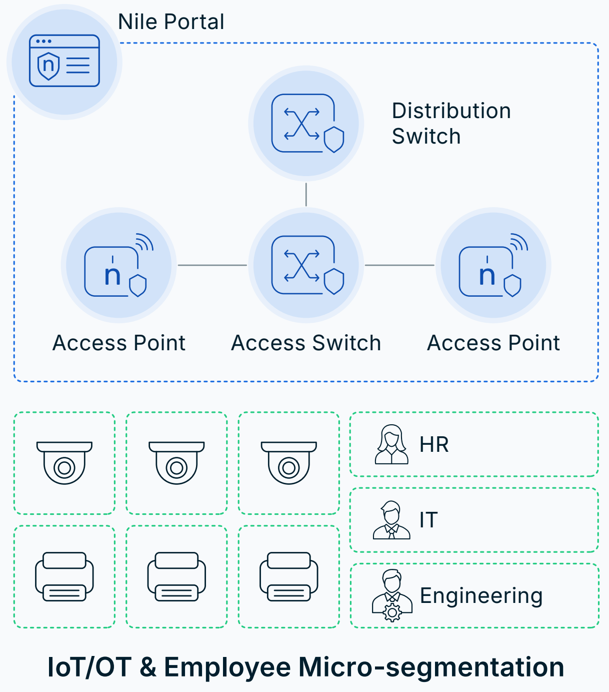
Traditional architectures rely on VLAN segmentation, external NAC systems, and manual operations, which were not designed for massive IoT device use and their limited security capabilities.

Traditional VLAN-based IoT/OT Security



- Implied trust creates threat exposure
- One-time Identity verification

Nile Zero Trust Fabric IoT/OT Security



- ✓ Explicit trust with Segment-of-1 isolation
- ✓ Continuous identity verification

Nile's Leading-Edge Differentiation

Only VLAN-free wireless and wired network to deliver Zero Trust security on Day 1, without complex add-ons.

Industry-only LAN with default per-device isolation, eliminating lateral movement and potential risk.

All IoT and IP-based OT communication requires explicit intent-based "allow" privileges

1. Granular Zero Trust Security For IoT/OT Devices
2. Reduced Attack Surface Through Default Segment-of-1 Isolation
3. Improved IT Controls While Exceeding Legacy Compliance Demands

Nile Makes Securing IoT Easy

Simple By Design

Streamlined operations via built-in device profiling, default isolation and automated controls eliminate the need for complex NAC appliances.

Zero Trust Security On Day 1

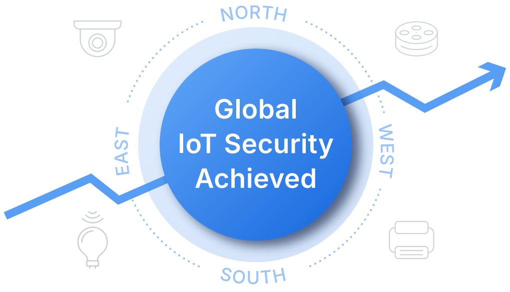
IoT and IP-based OT are never placed in coarse and vulnerable VLAN segments that lead to breaches and attacks.

Reduced IT Burden and Cost

Reduction in IT overhead with turnkey, secure NaaS that eliminates ongoing integration and maintenance costs.

Nile Customer Secures IoT for $1M Savings

- ✓ Multi-vendor network led to two separate NAC solutions
- ✓ A single solution amounted to nearly $1M annually in licensing
- ✓ Elimination of legacy NAC solutions covered cost of upgrade to Nile's secure NaaS



Nile Brings IoT/OT Security Into The Modern Era

Challenges	Nile Secure NaaS Approach
Complicated VLAN segmentation	VLAN-free, Segment-of-1 isolation by default
Creation of separate rules per IoT type	Automated rule creation and policy enforcement
Bolted-on and complex NAC that stays stagnant	Built-in access for simplicity and speed
High operational overhead	Autonomous operations
Visibility of unmanaged devices	Unparalleled visibility and containment

Ready to Get Started?

Let's Talk ↗