Safeguarding At-Risk Medical Devices and Clinical Networks

Healthcare organizations have long relied on traditional wired and wireless networks to support medical devices due to a combination of cost, regulation, and operational dependency. In short, these devices lead to:

- Outdated software
- 7–15+ year lifecycles
- Persistent security gaps

Challenge

To mitigate risks, IT teams attempt to implement Zero Trust network segmentation, least-privilege access, and behavioral monitoring. While these measures can limit exposure, reduce lateral movement, and enforce containment, the expertise required and architectural limitations make this very cumbersome.

- Legacy Limitations: VLANs, ACLs, and NAC created operational friction
- Poor Enforcement: Numerous gaps, increased risk and lateral movement
- High Cost: Zero Trust has required add-ons and deep expertise

Solution

Nile delivers a uniquely redesigned, cloud-native network architecture with Zero Trust built directly into the fabric. Per-device isolation and granular micro-segmentation limits access, isolates unsupported devices, and simplifies policy enforcement reducing operational burden while improving network enforcement capabilities across environments.

- Isolation by default: all wired and wireless devices
- No lateral movement: threats contained (e.g., malware, MitM attacks)
- Extended IoT lifecycle: of any vulnerable / unsupported devices

Case Study

$2.5M of Orphaned X-Ray Systems Secured, Deferring Immediate Replacement

A large dental specialty organization (DSO) was recently informed that 50 Panoramic X-ray systems in use across its network of dental offices would no longer receive software/security updates from the vendor. This end-of-life status introduced unexpected vulnerabilities, escalating the need to isolate these devices from critical business systems.

- Outdated Windows XP on these devices was already a vulnerability
- High replacement cost of $50K per unit was prohibitive
- Re-engineering the legacy network was very disruptive and IT intensive

Because they were in the process of trialing Nile's secure NaaS to replace their outdated legacy network infrastructure, the team avoided a costly network rearchitecture. Instead of new VLANs, IP re-addressing, and complex NAC and firewall changes, Nile's VLAN-free Zero Trust Fabric provided isolation of each device by default.

Using Layer 3 enforcement to eliminate the limitations of flat Layer 2 networks and a single firewall rule restricted what the X-ray systems could communicate with, and if compromised, their blast radius.

The End Result

Securing vulnerable IoT devices became simpler with a security-first architecture that embeds Zero Trust into the network by default, without expensive add-ons and operational complexity.

- No network re-architecture required
- 50 high-risk devices isolated
- $2.5M in replacement costs deferred