Build a Zero Trust network



NHS organisations are strengthening security through continuous verification and least-privilege access.

Healthcare networks are more connected than ever. Clinical systems, cloud platforms, medical devices, remote users, and third parties all need secure access.

Access complexity has grown and so has the challenge of securing it. Traditional security assumes that once a user or device has been authenticated, it can be trusted.

Zero Trust takes a different approach

Verify every user and device

Authenticate and authorise every identity and endpoint before network access is granted. Trust is continually assessed throughout the session, helping prevent compromised or non-compliant devices from accessing critical resources.

Segment the network

Separate clinical systems, corporate services, medical devices and guest networks into controlled environments. Segmentation limits lateral movement and helps contain threats before they spread.

Make context-aware access decisions

Evaluate every access request using factors such as identity, device posture, location, network context, and risk, rather than credentials alone.

Apply least-privilege access

Only grant the permissions needed for a specific role or task. Access can be adapted or revoked as users, devices, and levels of risk change.

2x

fewer security incidents

Complete Zero Trust implementations halve the likelihood of security incidents.

30%

more resilient

Mature Zero Trust organisations report significantly stronger resilience.

11%

lower ransomware risk

Strong identity controls reduce the likelihood of ransomware attacks.

Source: *Cisco, Security Outcomes for Zero Trust: Adoption, Access, and Automation Trends*, 2023.

Getting started

A Zero Trust approach doesn't require a complete network replacement. Most NHS organisations introduce it as part of their existing infrastructure roadmap, aligning identity, segmentation, and policy with planned refresh cycles.

The result is a more resilient network, where access decisions are driven by identity, context, and risk, rather than assumption.