illumio

INDUSTRY BRIEF

Simplifying Segmentation for Healthcare With Zero Trust

Simply achieving network segmentation as recommended by NHS England

Introduction

A 2021 ransomware attack on Ireland's Health Service Executive (HSE) healthcare agency disrupted hospital services across the country and exposed the personal data of more than 100,000 people. It was the country's worst cyberattack ever and one of the most serious on healthcare anywhere in the world.

A probe cited lateral movement in the HSE's mostly unsegmented network as a key factor in the attack's reach. As the report states:

> This network architecture, coupled with a complex and unmapped set of permissions for systems administrators...enabled the Attacker to access a multitude of systems across many organisations and create the large-scale impact that they did.

In response, NHS England published *Network segmentation - An introduction for health and care organisations*. The guide calls for segmenting the systems used in five diagnostic pillars:

- Genomics
- Imaging
- Pathology
- Endoscopy
- Physiological measurement

Within each of these systems, the report urges organizations to segment the following:

- Information technology
- Medical devices
- Operational technology
- Management plane
- Backups

Best practices

NHS England recommends the following actions

Asset inventory
Create and inventory for all assets on the network.

Asset functionality
Identify the main function of each asset.

Asset classification
Classify based on criticality.

Asset communication
Identify which asset it communicates with.

Logical segmentation
Segment assets based on organization defined criteria.

Technologies
Segment by assets such as IT, OT, IoMT

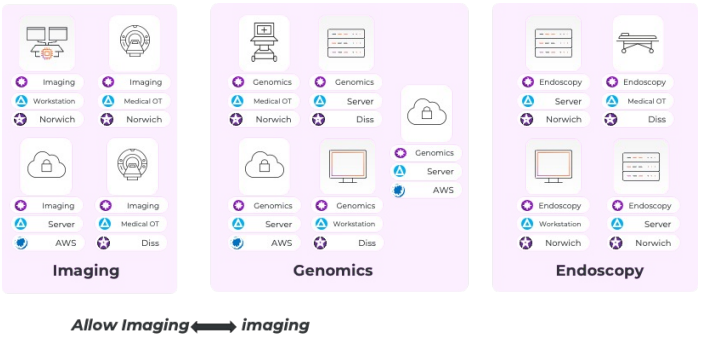
By segmenting these pillars, each process can stay protected if an attack affects one of the other pillars.

One highlighted approach to segmentation is Zero Trust. Here's how the report defines it:

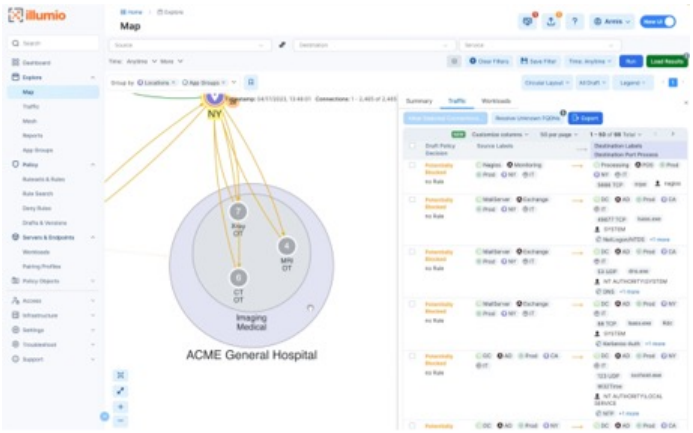
> Zero trust security — Abolishes the concept of a trusted network within an organisation's corporate perimeter and advocates creating micro perimeters of control around critical assets and enforcing strict access controls, network segmentation and identity management.

Zero Trust Segmentation (ZTS)

ZTS is a fundamental pillar of Zero Trust. It creates segments based on identity. Communications are blocked or allowed based on attributes such as risk or port number. Each resource is labelled, so rule-making is simple and granular segmentation is much easier.



Labels apply attributes to each resource, so you can easily see what in the network is communicating with what, and how. These labels show the risk level for each resource and what rules to apply.



Zero Trust Segmentation is enforced on the host, fully independent of the network or location. Creating a segment that spans multiple sites — which switches cannot do — is painless. Membership in a segment is based on its label, and adding to or changing each membership is simple.

In an attack, an infected system can be placed in a quarantine segment until it is cleaned.

The NHS recommends applying segmentation by:

- Environment
- Technology
- Criticality

And east-west traffic should be controlled at these levels:

- Protocol
- Service
- Port
- IP address

In the past, segmentation was a challenge. But Illumio makes it simple. With Zero Trust Segmentation, hospitals around the world protect their critical assets and maintain service delivery — without the complexity or risk.

Learn more about ZTS for healthcare providers

Visit illumio.com/solutions/healthcare

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.