A zero-trust model *for healthcare*

BLOCK

Introduction

Critical infrastructure is a prime target for cyber criminals, hacktivists and bad actors. This includes the healthcare sector, with attempts to disrupt the processes that protect millions of ill and injured people.

Last year, the healthcare sector suffered more attacks than any other sector, [1] and potentially devastating examples continue to make headlines.[2]

In 2022, Russian hacking group Killnet threatened to seize control of hospital ventilators. In 2023, the private medical details of more than a million NHS patients were compromised in a cyber-attack.[3] And, in 2024, a cyber-attack on pathology laboratory Synnovis led to NHS London cancelling more than 1,500 vital operations and appointments.[4]

The risk from cyber-attacks to life-saving infrastructure cahnnot be underestimated. Understandably, healthcare providers want:

- To increase resilience.
- To protect devices and operational tech.
- To achieve easy integration.

In light of this, an enhanced network security posture is clearly needed — but how to go about it?

[1] www.ft.com

[2] www.verdict.co.uk

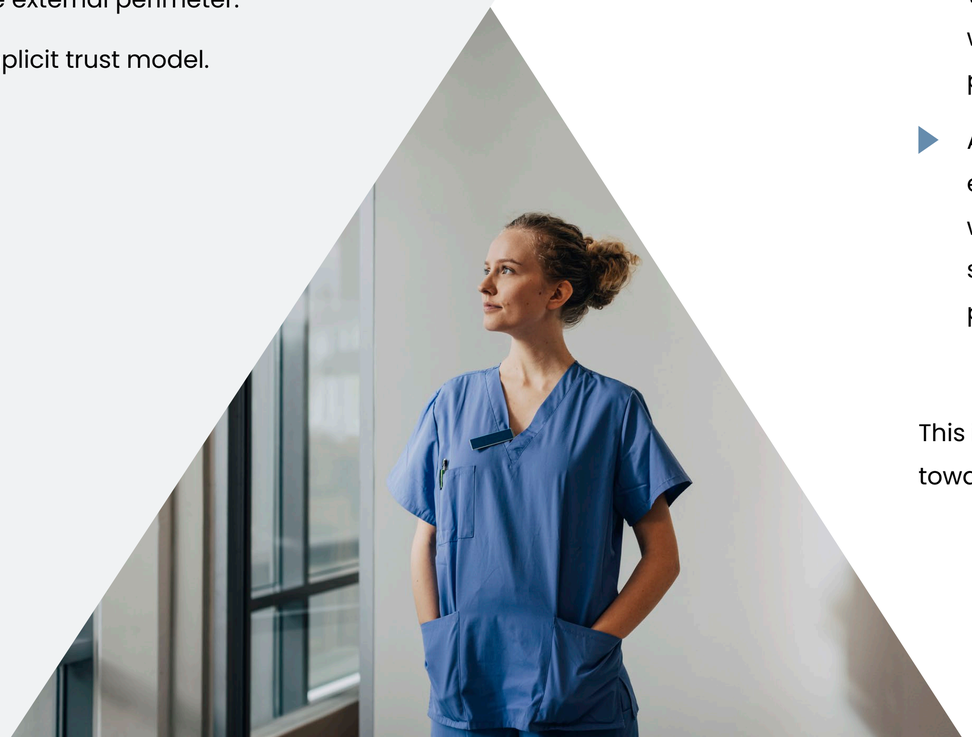
[3] www.verdict.co.uk

[4] https://www.bbc.co.uk/news

Securing the healthcare network: a zero-trust model approach

Imagine this scenario: An employee goes to work at their office, they swipe into the employ carpark and through the external doors to get into the building, but once inside are - by and large - trusted to act and roam freely without much scrutiny, as all focus is on the external perimeter.

This sums up the implicit trust model.



The implicit trust model sees all users, devices and systems within a network trusted by default once they have gained access to the network. External actors are considered untrustworthy. The security efforts are focused on the perimeter and those attempting to cross it, whilst those on the inside have a certain amount of freedom to access whatever they wish to.

The limitations of the implicit trust model include:

- Insider threats are difficult to prevent.
- Advanced Persistent Threats (APTs), with attackers operating undetected within the network for prolonged periods of time.
- An increased attack surface due to excessive network access privileges, which make it easier for attackers to successfully pivot from an initial entry point to higher value targets.

This is why healthcare is rightly moving towards a zero-trust model.

If we revisit the scenario above, our employee in the office building will find every door locked until they can provide verification that they have the necessary approval to enter. Until then, all doors are sealed shut and what lies behind them is kept safe.

The benefits of the zero-trust model include:

- Every access request is continuously verified.
- Users and devices are granted the minimum level of access necessary.
- Micro-segmentation limits the ability of attackers to move laterally.

Building the zero-trust model: the four essentials

1. Network access control

Network Access Control (NAC) is the foundational component in building a zero-trust security model. NAC ensures that only authenticated and authorised users and devices can access network resources, thereby enhancing overall network security.

Functions

- Authentication and authorisation for users, devices on the least privilege principle when gaining network access.
- Real-time monitoring to detect anomalies in the behaviour of both users and connected devices.
- Enforce control over the devices permitted to access the network, removing risks from shadow IT and unauthorised devices.
- Administer session based network access, allowing segmentation and contextual access capabilities to be added and providing the means to revoke access when devices are no longer authorised, for example the device is retired, lost, stolen and/or compromised.

2. Segmentation

Segmentation involves dividing a network into smaller, isolated segments, each with its own set of security policies and controls. By limiting the potential for lateral movement by attackers, security is enhanced, and potential breaches are contained.

Functions

- Granular division of segments divides the network right down to the level of individual workloads, applications and devices.
- Access control policies enforce strict access controls for each segment, so that only authorised users and devices can access specific resources, whilst also remaining adaptable to user behaviours and threat intelligence.
- Isolated network zones can be created, allowing development, testing and production environments to be separated, for example.
- Detailed data analytics and monitoring spot anomalies and signs of a security threat.

3. Contextual access

Contextual access refers to granting or denying access to resources based on a comprehensive evaluation of multiple factors, taking into account the broader context behind an access request—rather than relying solely on static credentials such as someone's username and password.

Functions

- Robust authentication methods, including multi-factor authentication (MFA), help to verify a user's identity, as well as assess whether they have the appropriate permissions.
- Devices' security postures are evaluated, looking at whether they have suitable encryption in place, for example, and if they are a personal or business device.
- Environments are scrutinised, including the geographical location throwing up potential red flags as well as the type of public or corporate network a user is on.
- Behaviour is monitored, flagging suspicious activity such as logging in at unusual times of day, spikes in data traffic and being out of sync with historical data.

4. Zero trust access

Zero trust access implements strict access controls and continuous verification of every access request, no matter whether it comes from inside or outside the network. In short, no user or device is trusted by default.

Functions

- Assessment of users' trustworthiness in real time, with dynamic and continuous authentication.
- Least privilege access granting only what is needed to perform their tasks safely and securely, supported by Role-Based Access Control (RBAC) to help manage permissions.
- Risk assessments and changing contexts inform access controls to be adaptive.
- Endpoint security solutions monitor and protect devices from threats, and ensure the devices meet security requirements before network access is given.

With these four essentials in place healthcare can have the reassurance and resilience of an enhanced network security posture.

Key considerations for healthcare when transitioning to a zero-trust model

Stakeholders

Ensure you have stakeholder engagement. Buy-in to the zero-trust model and a commitment to reducing the risk profile is critical to momentum and success.

Planning

Consider where you want to get to by implementing this model and new technologies, and weigh up your current appetite for investment and innovation and what phase, or phases, are suitable for now.

Infrastructure

Understand your infrastructure's current limitations and map them into your refresh plans. This will aid sensible buying decisions and the development of your business capabilities.

BAU change

Have the agility and flexibility to accommodate new devices and updates over time, embedding them into your procurement process and solution selection, onboarding and operations.

Operations

Anticipate a potential initial increase in support tickets as people and processes adapt to change, so a service model needs to be in place to support and empower your teams.

Securing the healthcare network: watch the on-demand webinar

Block's Lead Security Architect Paul Yarwood explores how Block works with our NHS clients to adopt an enhanced network security posture.

Learn about:

- Reducing cyber risk and increasing cyber resilience in healthcare.
- Protecting and securing BYOD, medical devices and IoT.
- Ensuring ease of management.
- Tools and techniques for a smooth transition journey to a zero-trust model.
- Challenges and considerations to keep in mind.

The on-demand webinar is available to watch now here.

Get in touch

Find out more about how we can help you improve your security posture and achieve the full benefits of digitalisation.

email: hello@block.co.uk

visit: www.block.co.uk

tel: 0344 967 1644

BLOCK