illumio | GlobalData.

WHITE PAPER

How Network Segmentation Helps Deliver Resilience Against NHS Cyber Threats

Introduction

Since 2013, NHS England has become more involved in the development of strategy and health policy alongside the Department of Health and Social Care (DHSC). The organisation has witnessed major structural changes in recent years, including the formation of forty-two Integrated Care Systems (ICSs), development of the Healthcare Act 2022, a Long-Term Workforce Plan 2023, and a merger with NHS Improvement (NHSX), NHS Digital (NHSD) and Health Education England (HEE). Change is also being driven by several regulations that contribute to updated processes within the authority, such as the Procurement Act 2023, Provider Selection Regime (PSR), Data Protection, and the Digital Information Bill.

"Transforming" technology within the NHS is one of the main strategic goals of the authority. Public Sector IT expenditure grew sharply during the COVID-19 pandemic and has not significantly decreased since it ended. With most technology budget being used by NHS Trusts, followed by centralised organisations (such as DHSC) and Integrated Care Boards (ICBs), the NHS is consistently highlighting that more investment will be put towards digital infrastructure enabling better care for patients. Some targets from the "Plan for Digital Health and Social Care" have already been achieved, such as 90% of Trusts adopting Electronic Patient Record (EPR) systems[1].

But with the organisation spanning 42 ICSs and 229 Trusts in England alone, it continues to be a top target for cyber threat actors, whose motives are financial, political, and service disruption. The substantial amounts of sensitive data in vulnerable systems create an unmissable temptation for criminals.

This report investigates the progress of digitalisation in the UK, the state of NHS cybersecurity solutions today, whilst uncovering emerging threats. It will highlight how health and care organisations can adopt Zero Trust Segmentation (ZTS) to address current security challenges.

Digitalisation in health and care

Emerging technology within health and social care presents tremendous opportunity for the sector. Using digital solutions to assess patient health, provide medical advice, and deliver appropriate services has been identified as a key to help combat threats such as COVID-19. In the UK telehealth played an important role as the first line of defence against the disease. Patients were provided with assessment and advice via tele-communication solutions, such as mobile apps and telephone calls. Artificial Intelligence (AI) software systems with infrared capability were installed in crowded places to monitor population temperature and recognise primary symptoms of the disease. Further waves of the pandemic were predicted from real-time data, using mathematical models. The NHS App was also born from a proven use of the NHS COVID-19 application. It was, therefore, widely recognised that value-based health and care relies on data and analytics for the purpose of measuring patient outcomes and cost drivers. Similar goals in digitalisation of health and care are highlighted by public bodies across all four home nations.

In June 2022 the "Plan for Digital Health and Social Care" in England was published. The main strategy outlined in the document lies in digitalising health services, providing connectivity to support integration across health systems and enabling service transformation[1]. In its Eighth Report of Session 2022-23, published in June 2023, the Health and Social Care Committee further emphasised that all constituent organisations of ICSs should have core digital capability in place, including electronic records, resilience to cyberattacks, and fast connectivity.

Additional targets for NHS England include the presence of an EPR solution in all NHS Trusts by March 2025, increase in usage and availability of the NHS App, and improved digital inclusion and so on[2].

In Scotland, the "Delivery Plan for Care in the Digital Age" strategy was refreshed in June 2023. The plan builds upon the increased use and public acceptance of digital health following the pandemic. Telemonitoring solutions such as Connect Me and Hospital @Home continue to expand, as does the video consulting service Near Me. Some of the key programmes of work include integrated health and social care record development[3].

Similarly, in Wales, the "Digital and Data Strategy for Health and Social Care" emphasises the development of necessary digital skills in the workforce, adoption of needs-specific digital platforms, allowing for real-time service monitoring, and focus on making services digital-first for patients[4].

Across the Irish Sea, Digital Health and Care Northern Ireland (DHCNI) is also looking to empower the Health and Social Care (HSC) system with the necessary skillset to harness the power of technology and improve patient lives. The organisation is focused on ensuring data safety and equipping systems to be joined-up and efficient with informed patient journeys in real-time.

All four home nations have set targets to improve patient experience through digitalisation. The adoption of such technologies presents many opportunities, as well as risks. With large amounts of sensitive data stored, it is crucial for systems to be fundamentally robust by adopting necessary cybersecurity mechanisms.

The state of NHS cybersecurity

The DHSC became responsible for regulatory supervision of the NHS Trusts adhering to the NIS Regulations and for compliance with data security standards. NIS Regulations provide legal measures to boost cybersecurity of network and information systems in the UK. At the same time, the Government Communications Headquarters (GCHQ) provides security intelligence to critical sectors within the UK, including healthcare. During the pandemic, the National Cyber Security Centre (NCSC), part of GCHQ, warned of the rise in malicious cyber activity that continues today. Overall, the health and social care organisations remain responsible for their own cybersecurity, with national teams responsible for setting direction and central support. ICSs oversee strengthening security measures across their dedicated areas.

All organisations within the NHS must adhere to Data Security and Protection Toolkit (DSPT) for appropriate management of patient data and clinical systems. Every year NHS organisations undertake self-assessment against the National Data Guardian's ten data security standards. Data security and protection incidents must be reported as part of the assessment. Furthermore, the NCSC's standard for organisations responsible for vitally important services and activities is Cyber Assessment Framework (CAF). The CAF helps national health and social care providers to align their strategy with key risks and priorities, while tracking progress towards cyber resilience.

Despite regulations in place, as well as the integration goals, nowadays, the NHS consists of many different organisations with a variety of solutions.

Emerging threats

Most malware and cyberattacks start by exploiting single points of vulnerability in a network. These can range from something as simple as an intruder guessing or knowing an available password, to complex social engineering scams, where a user is tricked into allowing malicious files into the system. In a single month testing period in 2018, one UK hospital classified 2.2% of all emails received by staff as potential threats, and 2.9% of website actions suspicious[5].

GlobalData predicts that cybersecurity expenditure in the medical device market will continue to grow, at a CAGR of 12.2% from 2022 to 2027, reaching a total market value of $1.1bn by the end of that period[6]. In the healthcare field, cyberattacks can disrupt crucial systems with patient details and processes attached to electronic records, as well as other integrated solutions. The NHS has been found to be vulnerable and not adequately prepared to face such threats, particularly as legacy systems can account for 30 – 50% of all IT services in the authority[7].

The most common goal of cyber criminals is cited as monetary gain. It accounts for around 91% of all data breaches. Patient records contain contact details, personal demographics, sensitive medical information and other tradable information. The approximate cost of a single healthcare record is valued at around $50 on the darknet. Stolen data can often be used by actors to apply for a loan or other financial programmes. State-sponsored cyberattacks, acting through political motivation, are also likely to increase in 2024 with ongoing geopolitical turmoil. It can be very challenging to identify and eliminate such attackers, with many events often going unnoticed. Finally, criminals may introduce ransomware for the sole purpose of financial gain through service disruption, accounting for around 5% of all attacks[5,8].

In 2022 it was estimated in a HIMSS Healthcare Cybersecurity Survey, that financial injury and data loss are the most common consequences that hospitals suffer due to cyber threats. Around 20% of health and care system attacks cause monetary loss and 21% lead to data breaches[9]. In financial costs, hospitals are faced with legal expenses, ransom fees, cybersecurity system replacement costs, and the significant effort of urgently implementing emergency protocols. Equally importantly, the recovery of public trust, whilst non-quantifiable, is another significant, yet unbudgeted expense.

The legacy of WannaCry

In December 2023, the UK's Joint Committee on the National Security Strategy warned that having exploded in 2021, the ransomware threat is still as severe as it has ever been, and the UK is one of the most targeted countries in the world.

The report goes on to specifically cite the potential future impact on the NHS of a major ransomware attack. The health service knows all about that, and with good reason. Those with long memories will remember 2017 when the NHS was the victim of the WannaCry ransomware

attack, which affected over 200,000 computers in more than 150 countries[10]. The health service was not targeted specifically by the attackers but was hit due to software vulnerabilities.

The fallout from the attack had a catastrophic impact on the NHS, affecting at least 34% of Trusts in England. It was estimated to have cost the health service around £92 million through lost services. Thousands of appointments and operations were cancelled, and patients in five areas had to travel to A&E departments elsewhere. No-one would want that level of disruption again.

The NHS was the victim of the age of its IT infrastructure. To access its victims' systems and infect them, WannaCry relied on computers using an old version of the Windows 7 operating system, but did not affect organisations with better defences, such as more modern software with appropriate security 'patching'. Over six years on from the attack, the ransomware threat facing different parts of the NHS, including Trusts, has evolved rapidly, but to a great extent, the defences haven't.

Nowadays, ransomware can do more than lock files and restrict access until a hospital pays a requested sum by hackers. Sensitive documentation can also be extracted, putting private patient information at risk. In May 2021, the Conti cyberattack on the Health Service Executive (HSE) of Ireland encrypted 80% of HSE's IT systems. Furthermore, in August 2022 the Advanced software provider supporting NHS 111 came under ransomware attack, forcing multidisciplinary team members to turn to pen and paper for data collection.

Containment is the goal; segmentation the means

What has evolved is the thinking around attacks. If an attack can be contained, perhaps to a limited, smaller space, then the ability to detect it and respond is actually much better. The clear goal is being able to contain an attack and be resilient enough to survive it. But that means having the necessary cyber tools to deliver that resilience. A critical factor in being able to achieve that is for the NHS – including specifically NHS Trusts – to have the ability to segment its network.

The current thinking of containment is all about a focus on surviving an attack, through limiting its potency. Stop focusing on everything. That is the legacy of the Colonial Pipeline cyberattack of 2021. The pipeline owners turned the whole thing off. And that's not an acceptable response in an operational environment. The parallel might be: if a hospital comes under attack, they just send their patients somewhere else. The hospital system is congested enough already. So, the narrative is changing. There are so many attacks – just focus on staying in business.

The Zero Trust architecture is considered a "state-of-the-art" solution that helps to identify, isolate, and eliminate technology breaches. The security method eliminates the concept of a trusted network within the organisation's corporate perimeter and groups critical assets within controlled micro-perimeters. It enforces strict access controls, network segmentation, and identity management. All in all, Zero Trust Segmentation (ZTS) allows necessary connections, whilst eliminating the malicious ones.

The NHS cybersecurity landscape: A changing organisation amid developing attacks

Cyberattacks within health and social care are increasing in frequency and sophistication. As the sector relies more on emerging technology, organisations are becoming more susceptible to such incidents. Cyberattackers find the networks of healthcare organisations attractive for three main reasons:

1. They are a rich source of personal confidential data.
2. These networks usually consist of different types of devices and technologies with inadequate security controls.
3. The ageing systems within the NHS offer cyberattackers an incursion opportunity.

There is already clear evidence of risk because a major attack was carried out on the Irish health system in early 2021. The attack was cited in December 2021 when the HSE, which provides all of Ireland's public health services, published the report of an independent review into the ransomware cyberattack on its IT systems. The report identified that the HSE's National Healthcare Network: "is primarily an unsegmented (or undivided) network... 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."

The report made clear the concept of lateral movement was utilised in the attack. This is a technique that cyber threat actors use to gain control of remote systems and thereafter, consolidate their position on the network.

There are three distinct steps in the process, according to the UK's National Cyber Security Centre (NCSC).

1. **Reconnaissance:** "Following the initial compromise of a host, the first step in lateral movement is to perform internal reconnaissance of the network. This gives the attacker an idea of their location within the network, and its overall structure."
2. **Privilege Escalation:** "To solidify their presence and maintain persistence, the attacker will usually try to compromise additional hosts and escalate their privileges, ultimately gaining control of their target (such as a domain controller, a critical system, or sensitive data). Any credentials that the attacker collects will give them (what appears to be) legitimate access to more hosts and servers."
3. **Sabotage:** "Once the goal or target has been reached, data can be exfiltrated, or systems and devices sabotaged."

How the NHS can take the necessary steps to protect itself: The importance of segmentation

This paper reflects and reiterates NHS Digital's positioning of making health and care organisations aware of the need to use network segmentation to improve their security posture and to prevent or mitigate lateral movement across an organisation's network in the event of a cyberattack.

One of the challenges of cybersecurity solutions currently in place in the NHS is that there is a lack of integration and segmentation. That is particularly the case in a lot of NHS Trusts which do not have any network segmentation at all. Many have flat network topologies which are open to greater risk of ransomware attacks allowing a cyber breach to spread through lateral movement. Many Trusts just want to have some segmentation. For those that have no segmentation at all, they are starting from a low base. But even some segmentation is better than none at all.

Organisations can choose from a variety of methods when deciding to implement network segmentation on their complete infrastructure, including cloud capabilities, and local area network (LAN). They can use a **demilitarised zone (DMZ)**, which acts as a perimeter sub-network between the public internet and the organisation's internal network, adding a layer of security to inbound traffic.

1. They can also use a **virtual local area network (VLAN)**, a custom network created from one or more local area networks enabling a group of devices to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN with each network segment an independent logical unit. VLAN segmentation must be accompanied with layer 3 inspection to achieve effective segmentation, and additional controls are required to restrict inter-VLAN traffic.

2. Another option is using a **network access control list (NACL)**. An NACL is an approved list of authorised traffic which can be used to implement segmentation at the network layer ensuring that only approved traffic, contained in the NACL, is allowed to enter a network segment.

3. Application and microsegmentation can also be used. **Application segmentation** refers to the method of segmenting applications from the rest of the network. **Microsegmentation** is a technique used to divide a network into secure zones allowing the isolation of workloads by applying security policies at a granular level. Each microsegment is responsible for ensuring that only authorised endpoints can access the applications and data housed on its segments.

4. The final element is **Zero Trust security**, which 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 security is being adopted by many organisations worldwide to protect their networks. The NHS does not rely completely on the Zero Trust approach but recommends that organisations choose from a variety of the above methods when deciding to implement network segmentation on their local area network (LAN).

These alternatives listed above are taken from NHS Digital guidance and assurance providing possible options for segmenting the network[11].

The importance of these segmentation measures in limiting the impact on the public cannot be overstated. A cyberattack on a local NHS trust could mean cancelled appointments and an unspecified delay in the delivery of treatment.

Compounding the problem today for NHS organisations is the impact on cybersecurity defences of artificial intelligence (AI) and particularly, generative AI. Using generative AI's writing capabilities, bad actors, especially those looking to launch ransomware attacks, can now strike faster with greater accuracy, as the typical spelling errors and grammar issues in phishing emails are more easily eliminated, making attacks more evasive and convincing.

Getting the security fundamentals right

Designing, implementing and maintaining a fully comprehensive cybersecurity defence is beyond the capacity and means of NHS institutions. What is important is to identify the points of highest risk, those that are most likely to be attacked and which will have the biggest impact on the NHS. By protecting those first and then working their way down, those responsible for services are giving themselves a chance of being able to maintain them. If, for example, as an NHS trust, you take that risk-based approach, the chances of you being more resilient increase.

It is questionable why the NHS cybersecurity strategy doesn't simply follow a Zero Trust route, but the reality is that the current NHS approach is more nuanced. What is imperative is that a cyberattack is contained. This means the likely spread of attack is lower and the recovery much quicker. Perhaps most importantly, the total cost of that breach is much lower.

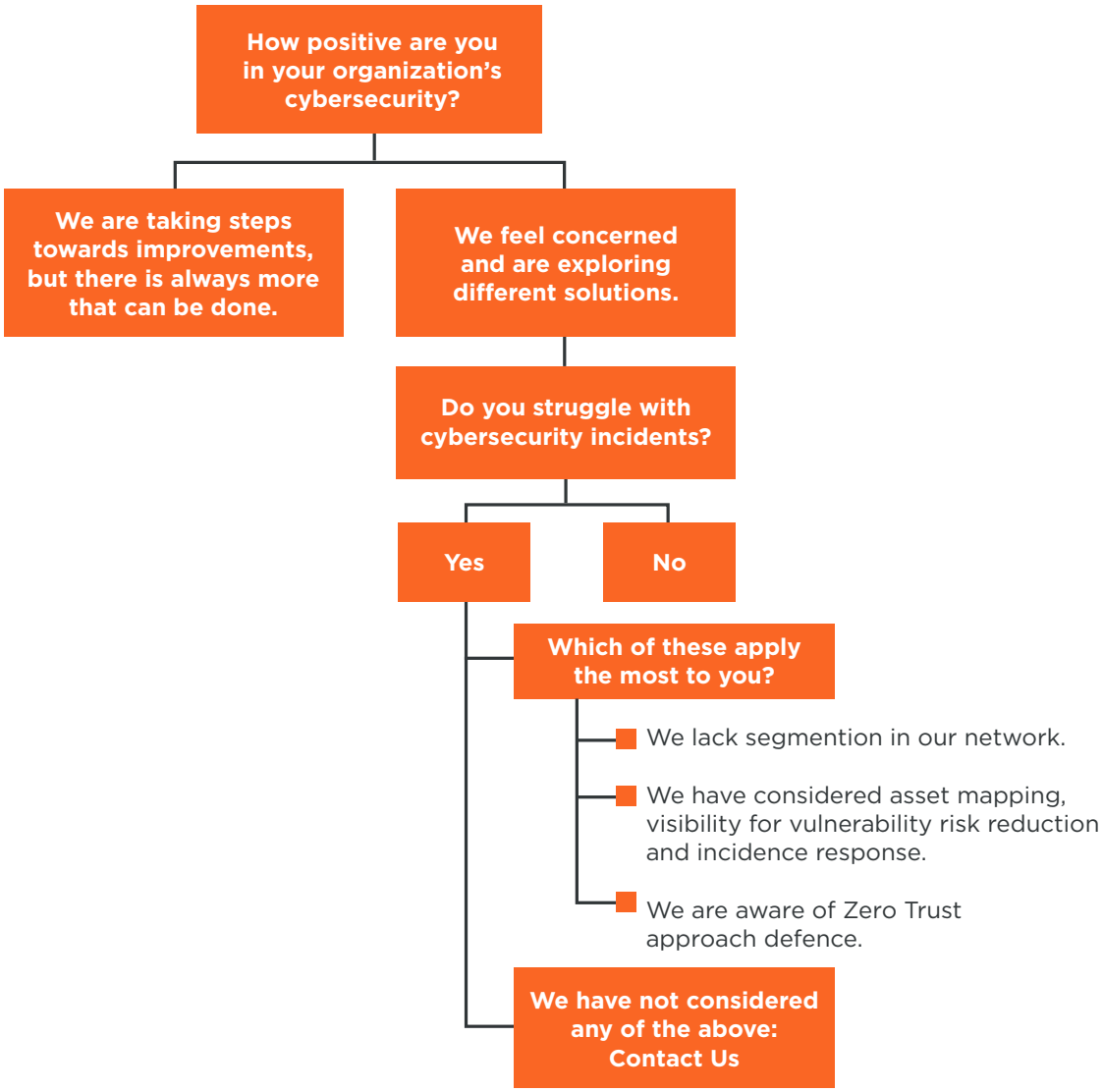
There are a number of Zero Trust use cases which are directly relevant to the NHS and which provide segmentation, which a lot of hospitals lack. The use cases are outlined below.

ZTS use cases and their use within the NHS:

Zero Trust Use Cases	NHS Need
Ransomware Containment	With ransomware quoted as the number one cybersecurity threat for patient data in the NHS[5,8], the issue needs to be addressed fast in the incidence management process. The WannaCry attack is one of the most crucial examples demonstrating why ransomware containment needs to be targeted by organisations.
Asset Mapping and Visibility	To deliver fully integrated and scaled solutions within health and care systems, connectivity of medical devices is necessary. It is delivered through tools such as Electronic Patient Records, digital applications and so on. Therefore, it is important to consistently review inventory of all assets connected to the clinical network. Mapping assets within their logical groups provides better organisational resilience and helps identify the risk of an attack.
Vulnerability Risk Reduction	With legacy systems within the NHS accounting for approximately 30-50% of all solutions, it is not surprising that current regulations highlight that authorities must have vulnerability management mechanisms. Health and care organisations need to ensure appropriate risk reduction is in place for vulnerable systems.
Incident Response & Recovery	In the case of an incident, health and care organisations must work fast to eliminate security breaches and report what they have done in response. ZTS helps identify, contain, and eliminate potential threats.
Critical Asset Protection	Overall, the protection of NHS assets and services is crucial. ZTS can immediately shrink an attack surface by automating necessary workflows.

Conclusion

Overall, the progressive digitalisation process in the health and care sector creates many opportunities as well as threats for the sector. Key NHS opinion leaders continuously highlight the need for simple, yet effective, cybersecurity measures, following several serious threats met by the sector. Despite the new regulations created and listed system goals across all four nations, cybersecurity measures remain unaligned within organisations such as constituent NHS Trusts. This white paper highlights the importance of segmentation with an example of Zero Trust that ensures hospital facility network security, through incidence identification, containment, response and recovery. The paper will help readers in trusts to assess whether their current approach to cybersecurity measures is resilient to potential threats.



References:

1. "A Plan for Digital Health and Social Care", Department of Health and Social Care, June 2023.
2. "Eighth Report - Digital transformation in the NHS", Inquiry Digital transformation in the NHS, Health and Social Care Committee, June 2023.
3. "Care in the Digital Age: Delivery Plan 2023-24", Scottish Government, Digital Health and Care Directorate, August 2023.
4. "Digital and data strategy for health and social care in Wales", Welsh Government, July 2023.
5. "Phishing in healthcare organisations: threats, mitigation and approaches", Priestman W et.al., BMJ Health Care Inform, Sep 2019, doi: 10.1136/bmjhci-2019-100031.
6. "Hospital 2040: how healthcare cybercrime is predicted to escalate", GlobalData Plc., Medical Devices DECODED, Jan 2024.
7. "Cyberattacks are one of the biggest threats facing healthcare systems", Khalaf R, Financial Times, Jan 2024.
8. "Hospital cybersecurity risks and gaps", Wasserman L, Front Digit Health, Aug 2022, doi: 10.3389/fdgth.2022.862221.
9. "Healthcare Cybersecurity Survey Report", Healthcare Information and Management Systems Society, 2022.
10. "A hostage to fortune: ransomware and UK national security", Joint Committee on the National Security Strategy, Dec 2023.
11. "Network segmentation - An introduction for health and care organisations", NHS England Digital, Nov 2023.