Active Directory Security Review (ADSR)

A RICOH Company

The Service

Microsoft Active Directory (AD) has been a critical component of identity and access management for NHS organisations for over 25 years. All computers, servers, desktops, and laptops are connected through AD, making it an immediate target for attackers. Privilege escalation is a common feature of ransomware attacks and often succeeds due to poorly configured and managed AD.

MTI's Active Directory Security Review (ADSR) identifies poor configurations and vulnerabilities. It focuses on detecting misconfigurations that pose the greatest risk of successful attack through AD compromise. Addressing these findings will help you meet the standards of NCSC CAF Principle B2: Identity & Access Control, reduce the risk of ransomware, and significantly improve your overall security posture.

Service Overview

- **Workshop**: Comprehensive assessment of AD security, functionality, and operations, covering domain structure, privileged accounts, password policies, group policies, and security configurations.
- **Discovery & Analysis**: Our consultants use a combination of tools to interrogate the Active Directory and analyse data to produce the report and vulnerability register.
- **Reporting**: Detailed investigation of detected issues, culminating in a report that is prioritised by risk and with pragmatic remediation advice.
- **Strategic Debrief**: Optional meeting to review findings, answer queries, and advise on strategic remediation steps.

Outcomes & Benefits

The key outcomes and benefits of the service and implementing remediation actions are:

Independent Expert Assessment:
Provides an expert, independent view of a critical security component, supporting business cases for investment in your local resilience programme.

Comprehensive Findings Report:
Documents vulnerabilities, operational risks, and actionable recommendations for remediation.

Risk Reduction and Protection:
Implementation of remediation advice significantly reduces risks and protects clinical services and patients from the worst impacts of ransomware attacks.

Regulatory and Compliance Alignment:
Helps achieve NHS CAF Principle B2 and comply with UK legislation, including GDPR and the Network and Information Systems (NIS) regulations.

Vulnerability Register and Remediation Plan:
Tracks critical and high-rated risks and outlines prioritised actions for mitigation.

NHS Cyber and Data Security Services and Resources

NHS organisations can access a wide range of resources to help identify, remediate, and manage cyber security risks to acceptable levels. Those with access to the Cyber Associates Network (CAN) can find a regularly updated list of NHSE and NCSC resources, including those planned for future release. MTI is the delivery partner for one of these services, Technical Remediation, and recommends that all of the services be considered to support local and regional initiatives, cyber resilience programmes, and the development of your local security operating model. Our account managers and security specialists can help you navigate the available services and understand how they might be complemented locally to maximise their impact and benefit.

Why MTI?

MTI is a trusted NHS partner, with over 20 years of cyber security expertise and a proven record of delivering more than 500 risk identification and reduction projects across 98% of NHS Trusts. We understand the operational pressures, compliance requirements, and unique challenges facing NHS organisations.

Our approach is aligned with NHS and national cyber strategies, rooted in a deep knowledge of compliance standards such as DSPT, ISO 27001, and CAF, and strengthened by hands-on experience with the IT and SecOps technologies most widely used across the NHS.

As an award-winning provider of end-to-end infrastructure and cyber services, MTI enables NHS organisations to strengthen resilience and reduce cyber risk with confidence.

Trusted by NHS Organisations

"MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy.

With MTI's expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture. They not only provided valuable insights into the national agenda but also ensured our alignment with it - a luxury we simply couldn't afford to pursue independently. Thus, MTI stepped in, and we are delighted with the results of our collaboration on the cyber strategy.

The feedback from everyone has been overwhelmingly positive, impressed by the accomplishments we have achieved together."

Mark Caines
Associate Director of ICT, Digital & Logistics
East Suffolk and North Essex NHS
Foundation Trust

NHS
East Suffolk and
North Essex
NHS Foundation Trust

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200

Multi-Factor Authentication Review

Multi-Factor Authentication (MFA) is essential because it strengthens security by adding extra layers of protection beyond just passwords. Cybercriminals frequently exploit weak or stolen credentials to gain access, making MFA a critical safeguard. To address this risk, the NHS has introduced a national policy requiring MFA for specific systems and applications.

MTI's MFA Review helps NHS organisations assess their alignment with the national policy and relevant CAF/DSPT assertions. Our consultants will review your existing application estate, policies and process. We will then provide a report on where MFA should be in place and whether existing controls reflect best practice in line with compliance objectives. This report can subsequently be used to develop a plan to close any gaps identified.

The Service

The MFA Review offers a clear review of your organisation's compliance with a Model MFA Policy, based on national policy and best practice guidance. The process includes:

- Workshops and discovery sessions to understand current authentication policies, systems, and business needs.
- An assessment of MFA coverage, controls and alignment with NHSE Policy.
- Analysis of policies and processes to identify gaps or outdated practices.
- Stakeholder interviews to clarify system dependencies, user needs, and challenges.
- Actionable recommendations and a roadmap to guide planning, prioritisation, and future MFA adoption.

Outcomes & Benefits

By engaging MTI's MFA Review, your organisation will achieve the following outcomes:

Risk Reduction:
Once implemented, the remediation action plan with phish resistant MFA solutions, will significantly reduce the risk of successful credential-based attacks.

Authentication Register:
Based on MS Excel, the register will build out your application inventory to show current and expected MFA status for each application.

Modal Authentication and Access Policy:
Provided at the start of the engagement, this policy can be adopted directly or used to refine existing ones. Full adoption supports national policy alignment and CAF compliance.

Gap Analysis Report:
A detailed breakdown of compliance against the NHS MFA standard, including an executive summary, issue matrix, policy review, observations on people, processes and technologies, plus remediation guidance and an action plan.

Patient Safety:
Recent attacks against the NHS have been shown to cause significant harm to patients, including the death of a patient. The MFA Review will help build a robust plan to mitigate many of the most common attack vectors.

NHS Cyber and Data Security Services and Resources

NHS organisations can access a wide range of resources to help identify, remediate, and manage cyber security risks to acceptable levels. Those with access to the Cyber Associates Network (CAN) can find a regularly updated list of NHSE and NCSC resources, including those planned for future release. MTI is the delivery partner for one of these services, Technical Remediation, and recommends that all of the services be considered to support local and regional initiatives, cyber resilience programmes, and the development of your local security operating model. Our account managers and security specialists can help you navigate the available services and understand how they might be complemented locally to maximise their impact and benefit.

Why MTI

MTI is a trusted NHS partner, with over 20 years of cyber security expertise and a proven record of delivering more than 500 risk identification and reduction projects across 98% of NHS Trusts. We understand the operational pressures, compliance requirements, and unique challenges facing NHS organisations.

Our approach is aligned with NHS and national cyber strategies, rooted in a deep knowledge of compliance standards such as DSPT, ISO 27001, and CAF, and strengthened by hands-on experience with the IT and SecOps technologies most widely used across the NHS.

As an award-winning provider of end-to-end infrastructure and cyber services, MTI enables NHS organisations to strengthen resilience and reduce cyber risk with confidence.

Trusted by NHS Organisations

"MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy.

With MTI's expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture. They not only provided valuable insights into the national agenda but also ensured our alignment with it - a luxury we simply couldn't afford to pursue independently. Thus, MTI stepped in, and we are delighted with the results of our collaboration on the cyber strategy.

The feedback from everyone has been overwhelmingly positive, impressed by the accomplishments we have achieved together."

Mark Caines
Associate Director of ICT, Digital & Logistics
East Suffolk and North Essex NHS
Foundation Trust

NHS
East Suffolk and
North Essex
NHS Foundation Trust

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200

Network Segmentation Review

A RICOH Company

The Service

Weak network segmentation leaves NHS organisations vulnerable, with flat networks reducing performance and increasing the impact of a potential breach. A single compromise in a shared or legacy environment can threaten critical services and patient safety.

MTI's Network Segmentation Review assesses networks against NHS England's network segmentation principles, identifying maturity levels and areas for improvement to strengthen cyber resilience and ensure compliance with relevant security guidance.

Service Overview

Our Network Segmentation Review focuses on identifying gaps in your current network architecture and practices. We provide a detailed analysis, leveraging NHS England's Network Segmentation Principles and relevant Cyber Assessment Framework (CAF) principles (B4, B5, C1, D1). The structured assessment includes multiple phases to ensure comprehensive coverage of all aspects of your network segmentation.

Scope of Delivery Phases

- **Kick-Off and Information Gathering:** Introduction and requests for key documents like network topology diagrams and policies.
- **Documentation and Policy Review:** Assess existing strategies, access policies, and network controls to identify vulnerabilities.
- **Firewall Configuration Review:** Automated analysis to audit firewall settings for exposures or inconsistencies.
- **Workshop and Analysis:** Collaborative workshops with Subject Matter Experts (SMEs) for in-depth network evaluations.
- **Reporting and Recommendations:** Delivery of a comprehensive summary report detailing risks, findings, and clear remediation steps

Outcomes & Benefits

Partnering with MTI equips your organisation with robust network segmentation and improved cyber resilience. Benefits include:

Improved Cyber Security: Greater protection against lateral movement and breaches, reducing the risks associated with a flat network.

Alignment with National Guidance: Implementing recommendations from the Network Segmentation Review will bring your organisation in line with NHS segmentation guidance and CAF principles.

Comprehensive Gap Analysis Report: Highlights deficiencies against NHS segmentation principles and prioritises identified risks.

Firewall Configuration Audit: Provides detailed results from automated and manual checks, including specific remediation paths for vulnerabilities.

Remediation Action Plan: A structured plan outlining prioritised steps to enhance network segmentation.

Stakeholder Workshop Results: Feedback and alignment on strategic actions delivered through interactive discussions with your team.

NHS Cyber and Data Security Services and Resources

NHS organisations can access a wide range of resources to help identify, remediate, and manage cyber security risks to acceptable levels. Those with access to the Cyber Associates Network (CAN) can find a regularly updated list of NHSE and NCSC resources, including those planned for future release. MTI is the delivery partner for one of these services, Technical Remediation, and recommends that all of the services be considered to support local and regional initiatives, cyber resilience programmes, and the development of your local security operating model. Our account managers and security specialists can help you navigate the available services and understand how they might be complemented locally to maximise their impact and benefit.

Why MTI?

MTI is a trusted NHS partner, with over 20 years of cyber security expertise and a proven record of delivering more than 500 risk identification and reduction projects across 98% of NHS Trusts. We understand the operational pressures, compliance requirements, and unique challenges facing NHS organisations.

Our approach is aligned with NHS and national cyber strategies, rooted in a deep knowledge of compliance standards such as DSPT, ISO 27001, and CAF, and strengthened by hands-on experience with the IT and SecOps technologies most widely used across the NHS.

As an award-winning provider of end-to-end infrastructure and cyber services, MTI enables NHS organisations to strengthen resilience and reduce cyber risk with confidence.

Trusted by NHS Organisations

"MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy.

With MTI's expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture. They not only provided valuable insights into the national agenda but also ensured our alignment with it - a luxury we simply couldn't afford to pursue independently. Thus, MTI stepped in, and we are delighted with the results of our collaboration on the cyber strategy.

The feedback from everyone has been overwhelmingly positive, impressed by the accomplishments we have achieved together."

Mark Caines
Associate Director of ICT, Digital & Logistics
East Suffolk and North Essex NHS
Foundation Trust

NHS
East Suffolk and
North Essex
NHS Foundation Trust

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200

Role-Based Authority (RBA)
Domain and Server Combined

A RICOH Company

The Service

NHS organisations face heightened risks from privileged account misuse and lateral movement within Active Directory, especially given the complexity of healthcare IT environments.

MTI's Role-Based Authority (RBA) aims to implement a Role-Based Authority Architecture, which will remediate vulnerabilities and improve security by implementation of Administrative Zones. Implementing this Role-Based Authority Architecture is a vital component of the Zero-Trust model.

Service Overview

The RBA Domain and Server Combined service delivers targeted improvements to your AD environment, directly addressing weaknesses in account authority, administrative zoning, and access control. Through a series of engagements, MTI ensures your AD is protected against unauthorised privilege elevation and that roles align with your security and operational needs.

Scope of Delivery Phases

- **Kick-Off and Discovery**: Initial coordination and review of existing AD architecture, accounts, and policies.
- **Analysis and Design**: In-depth analysis of privilege assignments and development of a tailored role-based architecture, including zoning boundaries.
- **Implementation**: Deployment of RBA controls, remediation of rogue or excessive privileges, and realignment of admin roles.
- **Reporting and Recommendations**: Final report detailing changes, metrics, and a clear path to ongoing management.

Outcomes & Benefits

With MTI's RBA Domain and Server Combined service, organisations benefit from:

- **Reduced Privilege Risks:** Secure, enforceable segregation of high-privilege roles.
- **Regulatory Alignment:** Meets requirements of frameworks including CAF and MITRE ATT&CK.
- **Operational Clarity:** Fewer unnecessary admin accounts, simplifying management and accountability.
- **Improved Cyber Resilience:** Makes it harder for attackers to escalate privileges or persist in your AD.
- **Clear Role-Based Authority Architecture:** Well-defined authority sets for AD object/data management and Windows server/client administration.
- **Remediated Access Controls:** Rogue permissions addressed across system containers, DNS containers, organisational units, and group policies.
- **Segmented Higher Authority Groups:** Limits the scope of high-level privileges.
- **Domain and Server Boundaries:** Authorisation pathways clearly defined.
- **Sustained Adoption:** Knowledge transfer and documentation support stakeholders in maintaining the new model.

NHS Cyber and Data Security Services and Resources

NHS organisations can access a wide range of resources to help identify, remediate, and manage cyber security risks to acceptable levels. Those with access to the Cyber Associates Network (CAN) can find a regularly updated list of NHSE and NCSC resources, including those planned for future release. MTI is the delivery partner for one of these services, Technical Remediation, and recommends that all of the services be considered to support local and regional initiatives, cyber resilience programmes, and the development of your local security operating model. Our account managers and security specialists can help you navigate the available services and understand how they might be complemented locally to maximise their impact and benefit.

Why MTI?

MTI is a trusted NHS partner, with over 20 years of cyber security expertise and a proven record of delivering more than 500 risk identification and reduction projects across 98% of NHS Trusts. We understand the operational pressures, compliance requirements, and unique challenges facing NHS organisations.

Our approach is aligned with NHS and national cyber strategies, rooted in a deep knowledge of compliance standards such as DSPT, ISO 27001, and CAF, and strengthened by hands-on experience with the IT and SecOps technologies most widely used across the NHS.

As an award-winning provider of end-to-end infrastructure and cyber services, MTI enables NHS organisations to strengthen resilience and reduce cyber risk with confidence.

Trusted by NHS Organisations

"MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy.

With MTI's expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture. They not only provided valuable insights into the national agenda but also ensured our alignment with it - a luxury we simply couldn't afford to pursue independently. Thus, MTI stepped in, and we are delighted with the results of our collaboration on the cyber strategy.

The feedback from everyone has been overwhelmingly positive, impressed by the accomplishments we have achieved together."

Mark Caines
Associate Director of ICT, Digital & Logistics
East Suffolk and North Essex NHS
Foundation Trust

NHS
East Suffolk and
North Essex
NHS Foundation Trust

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200

Secure Backup Reassessment (SBRe)

The Service

Healthcare organisations are increasingly targeted by ransomware and malware attacks designed to compromise backup solutions and encrypt or destroy backup data as a precursor to a larger-scale ransomware attack. Attackers aim to make recovery difficult in order to increase disruption or pressure organisations into paying a ransom.

MTI's Secure Backup Reassessment (SBRe) service is specifically designed for NHS organisations seeking to validate and enhance the effectiveness of remediation implemented since their initial review. Aligned with National Cyber Security Centre (NCSC) principles, this structured engagement reassesses your backup solution to confirm that risks have been addressed, ensure continued compliance, and support trusted clinical operations.

Service Overview

The Secure Backup Reassessment provides a comprehensive analysis of your backup environment and actionable recommendations for improvement. It builds on findings from previous reviews to evaluate implemented changes and address any remaining gaps or vulnerabilities.

Scope of Delivery Phases

- **Kick-Off and Discovery:** Review existing backup architecture, updates since the prior assessment, and risk mitigation strategies.
- **Analysis:** Examine backup processes, technologies, and risk areas against NCSC 3-2-1 principles and new implementation guidance.
- **Validation:** Assess whether deployed changes meet resilience requirements, including air-gapping, immutability, and access controls.
- **Reporting and Recommendations:** Deliver updated findings and tailored recommendations as an addendum to the previous assessment report.

For Customers Who Have Already Had an SBR

The SBR reassessment service incorporates both the original NCSC principles and the new principles introduced in the latest guidance, as outlined below:

- Backup Isolations
- Patching and Updates
- Resilience to Destructive Actions
- Point-in-Time Recoverability
- Key Management and Encryption
- Alert Management and Observability

Outcomes & Benefits

This service ensures your backup and recovery strategy meets the stringent requirements of NHS operations:

- **Clinical Continuity:** Reduces the risk of significant and sustained disruption to healthcare services, which can take months to restore and cause widespread harm to patients.
- **Improved Cyber Resilience:** Strengthens defences against ransomware and protects backup services from unauthorised access.
- **Clear Roadmap:** Provides practical, prioritised guidance to close identified gaps and reduce business risk.
- **Enhanced Visibility:** Offers a clear understanding of what data is protected and where vulnerabilities may exist.
- **Comprehensive Assessment Report:** Presents detailed findings on the current backup environment, including coverage analysis, compliance with NCSC principles, and any identified shortfalls.
- **Remediation Register & Actionable Recommendations:** Outlines priority remediation actions, investment required, and steps to address outstanding risks, improve resilience, and align with best practices.
- **Backup Solution Validation:** Confirms that backup practices, including air-gapping and encryption, align with NCSC principles.
- **Updated Report Addendum:** Provides documented findings appended to the original assessment for a complete audit trail.

NHS Cyber and Data Security Services and Resources

NHS organisations can access a wide range of resources to help identify, remediate, and manage cyber security risks to acceptable levels. Those with access to the Cyber Associates Network (CAN) can find a regularly updated list of NHSE and NCSC resources, including those planned for future release. MTI is the delivery partner for one of these services, Technical Remediation, and recommends that all of the services be considered to support local and regional initiatives, cyber resilience programmes, and the development of your local security operating model. Our account managers and security specialists can help you navigate the available services and understand how they might be complemented locally to maximise their impact and benefit.

> "
>
> MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy. With their expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture.
>
> Mark Caines
> Associate Director of ICT, Digital & Logistics
> **NHS Foundation Trust**

Why MTI?

MTI is a trusted NHS partner, with over 20 years of cyber security expertise and a proven record of delivering more than 500 risk identification and reduction projects across 98% of NHS Trusts. We understand the operational pressures, compliance requirements, and unique challenges facing NHS organisations.

Our approach is aligned with NHS and national cyber strategies, rooted in a deep knowledge of compliance standards such as DSPT, ISO 27001, and CAF, and strengthened by hands-on experience with the IT and SecOps technologies most widely used across the NHS.

As an award-winning provider of end-to-end infrastructure and cyber services, MTI enables NHS organisations to strengthen resilience and reduce cyber risk with confidence.

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200

Vulnerability Management Maturity Assessment (VMMA)

A RICOH Company

The Service

NHS organisations face significant challenges in vulnerability management due to a rapidly changing threat landscape, complex infrastructure, and limited resources. This makes developing a strong vulnerability management process essential for reducing risks to patient safety. Attackers often exploit vulnerabilities soon after they are disclosed, increasing the need for patching and remediation to be carried out as quickly as possible.

The Vulnerability Management Maturity Assessment (VMMA) reviews existing vulnerability patching, the tools in use, automated and manual processes, and how the overall vulnerability management process is risk managed. The review is conducted against the NCSC Cyber Assessment Framework (CAF), aligned to the NHS Baseline, and delivers a formal report with detailed findings and recommendations for improvement.

Service Overview

MTI's VMMA service conducts a comprehensive assessment of your vulnerability management program, evaluating its maturity across core areas like policy, processes, and technology. By benchmarking against the Cyber Assessment Framework (CAF) and NHS Vulnerability Management guidance, VMMA identifies weaknesses, highlights areas for growth, and delivers practical recommendations for improvement.

Scope of Delivery Phases

- **Kick-Off and Information Gathering:** Initial meeting to outline goals, collect policies, system configurations, and other documentation.
- **Workshop and Analysis:** Facilitate structured workshops with stakeholders to review end-to-end vulnerability management processes.
- **Assessment:** Detailed evaluation of gathered data across 12 VMMA focus areas, mapping to best practices and CAF principles.
- **Reporting and Recommendations:** Delivery of a formal report with executive summary, maturity scores, and prioritised improvement actions.

Outcomes & Benefits

By partnering with MTI for VMMA, your organisation achieves measurable improvements in vulnerability management maturity. Key benefits include:

Enhanced Risk Mitigation: Reduce the likelihood of cyber-attacks by addressing critical vulnerabilities effectively.

Improved Compliance and Reporting: Align processes with CAF and NHS standards to streamline regulatory adherence.

Actionable Strategy: Receive a focused plan for ongoing improvements, enabling optimised resource allocation.

Bolstered Cybersecurity Resilience: Achieve long-term confidence in protecting essential systems and data.

Detailed Assessment Report: Highlights risks, compliance gaps, and maturity levels across 12 VMMA areas.

Vulnerability Improvement Plan: A clear roadmap for addressing deficiencies and advancing maturity levels.

Visual Maturity Modelling: RAG-rated dashboards and radar diagrams that illustrate your organisation's security posture.

Customised Recommendations: Strategically prioritised actions tailored to your operational context and regulatory obligations.

NHS Cyber and Data Security Services and Resources

NHS organisations can access a wide range of resources to help identify, remediate, and manage cyber security risks to acceptable levels. Those with access to the Cyber Associates Network (CAN) can find a regularly updated list of NHSE and NCSC resources, including those planned for future release. MTI is the delivery partner for one of these services, Technical Remediation, and recommends that all of the services be considered to support local and regional initiatives, cyber resilience programmes, and the development of your local security operating model. Our account managers and security specialists can help you navigate the available services and understand how they might be complemented locally to maximise their impact and benefit.

Why MTI?

MTI is a trusted NHS partner, with over 20 years of cyber security expertise and a proven record of delivering more than 500 risk identification and reduction projects across 98% of NHS Trusts. We understand the operational pressures, compliance requirements, and unique challenges facing NHS organisations.

Our approach is aligned with NHS and national cyber strategies, rooted in a deep knowledge of compliance standards such as DSPT, ISO 27001, and CAF, and strengthened by hands-on experience with the IT and SecOps technologies most widely used across the NHS.

As an award-winning provider of end-to-end infrastructure and cyber services, MTI enables NHS organisations to strengthen resilience and reduce cyber risk with confidence.

Trusted by NHS Organisations

"MTI has played a crucial role in shaping our Cyber Security Strategy, previously we felt we were being reactive. With the volume of work coming in and the ever-evolving threat landscape, we recognised the urgent need for a more structured and comprehensive strategy.

With MTI's expertise and guidance, the MTI team brought a panoramic view of the NHS, enabling us to grasp the bigger picture. They not only provided valuable insights into the national agenda but also ensured our alignment with it - a luxury we simply couldn't afford to pursue independently. Thus, MTI stepped in, and we are delighted with the results of our collaboration on the cyber strategy.

The feedback from everyone has been overwhelmingly positive, impressed by the accomplishments we have achieved together."

Mark Caines
Associate Director of ICT, Digital & Logistics
East Suffolk and North Essex NHS
Foundation Trust

NHS
East Suffolk and
North Essex
NHS Foundation Trust

ukmarketing@mti.com
mti.com
+44 (0) 1483 520 200