M8 Solutions

DELIVERING TECHNICITY WITH INTEGRITY

PENETRATION TESTING

DAY RATE

2026

M8 Solutions Introduction

M8 Solutions is a specialist UK-based digital services provider delivering expert-led Cyber Security, Automation, Cloud Services, and Digital Transformation solutions directly to NHS organisations. Our business is built on a deep-rooted understanding of the unique pressures and priorities within the UK healthcare system rising demand, constrained budgets, legacy systems, and strict compliance mandates.

We work in close partnership with NHS organisations to solve real-world challenges using a people-first, technology-enabled approach. Whether it's defending against cyber threats, automating labour-intensive admin processes, migrating to secure cloud platforms, or supporting digital maturity assessments, M8 Solutions embeds itself as an extension of the organisations digital team.

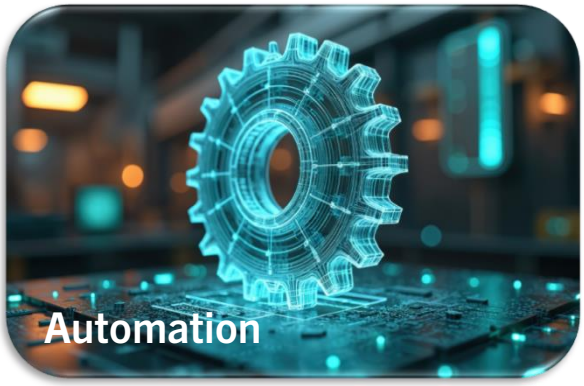
From our flexible consultancy models to our outcome driven service delivery, we focus on high impact, scalable solutions that empower NHS teams to work smarter, faster, and more securely.

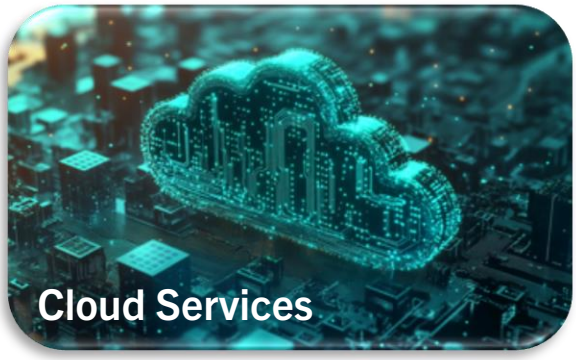
As the NHS faces unprecedented digital demands, M8 Solutions is the partner that helps turn policy into practical progress.

Our Solutions

Cyber Security is far more than a technical requirement, it's the foundation of trust, resilience, and continuity across NHS services. Our consultancy approach is tailored to the unique operational pressures of the NHS, offering strategic guidance and end-to-end security solutions.

We understand the complexity of NHS environments and deliver automation solutions that integrate seamlessly, improve accuracy, and drive measurable results. Whether you're looking to cut costs, reduce admin burdens, or build a smarter, scalable operation, M8 Solutions is your trusted Automation partner.





At M8 Solutions, we enable NHS organisations to fully harness the power of Cloud Services. As an independent, cloud-agnostic consultancy, we design and deliver secure, scalable, and cost-effective solutions tailored to your clinical, operational, and digital priorities.

Digital Transformation in healthcare is about more than technology, it's about reimagining how services work together to deliver safer, faster, and more effective care. At M8 Solutions, we help NHS organisations evolve with purpose, modernising systems, empowering staff, and improving outcomes for patients and communities.

Penetration Testing Day Rate

Penetration testing effort and cost are highly dependent on the scope, complexity, and risk profile of the environment being assessed, which cannot be accurately determined until a formal scoping exercise has been completed. Factors such as the number and type of assets, exposure to the internet, authentication requirements, testing depth, regulatory obligations, and remediation validation all materially affect the level of effort required. To ensure transparency and fairness prior to full scoping, we therefore publish a standard penetration testing day rate of £1,050.00 per day. This provides NHS organisations with cost clarity and flexibility, allowing testing to be appropriately sized and budgeted once the scope and objectives are formally agreed, without compromising the quality or rigour of the assessment.

Scoping

During the scoping phase, the client will work closely with **a** senior CREST-accredited penetration tester to ensure the engagement is precisely defined and that all technical, business, and regulatory requirements are more than adequately addressed. This collaborative process confirms the systems in scope, testing methodology, depth of assessment, constraints, and success criteria, ensuring alignment with both risk appetite and compliance obligations. Based on the agreed scope, size, and estimated effort, the required number of testing days will be formally defined and quoted. Pricing is calculated transparently using a flat day rate multiplied by the total number of days required to deliver the engagement to the agreed standard, ensuring clarity, consistency, and assurance of a high-quality penetration testing outcome.

Example Test Details

Penetration Test Services	Days	Day Rate	Total
External Infrastructure Assessment	3	**£1050.00**	£3,150.00
N365/SharePoint Assessment	4	**£1050.00**	£4,200.00
Azure Assessment	3	**£1050.00**	£3,150.00
Server Build Review	3	**£1050.00**	£3,150.00
		Total	**£32,550.00**

Please note this table is provided as an illustrative example only and excludes VAT. The number of days required will vary depending on the scale, scope, and complexity of your cloud-based assets, and will be confirmed following the formal scoping exercise.

Terms and Conditions

These Terms and Conditions apply to all professional services provided by M8 Solutions Limited a company registered in England and Wales, with registered number 12702481 and having its registered office at Highfield House Congleton Road, Scholar Green, Stoke-On-Trent, Staffordshire, England, ST7 3SY (hereinafter referred to as "M8 Solutions");

1. COMPANY'S DUTIES

1.1. The Company shall perform the Security Testing for the Client using reasonable skill and care and in a professional, timely manner. Time for provision or completion of the Security Testing or any part of it shall not be of the essence.

1.2. Where a Test Report is required, it shall, unless otherwise agreed, be produced by the Consultant within five (5) working days or as agreed with the Client on completion of the Security Testing and sent to the Client.

1.3. Whilst the Company will use reasonable endeavours to ensure that the same Consultant will continue throughout the Security Testing, it reserves the right to replace that Consultant, if necessary, at its reasonable discretion by notifying the Client.

1.4. The Company shall, where the Consultant is present on the Client's premises, ensure that the Consultant complies with such reasonable site rules and procedures as are prior notified to the Company.

2. THE CLIENT AGREES

2.1. To obtain appropriate consent from its ISP (Internet Service Provider), only where the ISP is hosting services on behalf of the Client and any other relevant third party supplier of the System, only where the third party supplier is hosting services on behalf of the Client for the Security Testing to be carried out and, when requested by the Company, to provide evidence of such consent and to notify relevant employees that the Security Testing has been scheduled and that they may be monitored;

2.2. To arrange a mutually convenient time with the Company for the performance of the Security Testing and to inform any relevant parties such as the ISP of the date agreed with Company in accordance 3.1.

2.3. To make appropriate backups of the System prior to the commencement of the Security Testing.

2.4. That, where the Security Testing is to take place on the Client's premises, the Client shall ensure that suitable accommodation is provided for the Consultant which shall include network access and, where necessary, access to data centres, server rooms and/or switch rooms.

2.5. That, by signing the Penetration Test Authorisation Form, the Client consents, for itself and on behalf of all group companies, to the Company performing the Security Testing and that it has procured, where necessary, the consent of all its (and its group companies) employees, agents and sub-contractors that the Company shall be permitted to carry out the Security Testing. The Company will be carrying out the Security Testing in the belief that it has all appropriate consents, permits and permissions from the Client and its group companies (and their employees, agent and sub-contractors);

2.6. That, whilst the Company will conduct all Security Testing in line with accepted best practice and make all reasonable efforts to avoid disruption of the Client's network, the tools and techniques used may cause disruption to the Client's Systems and/or possible loss of or corruption to data and the Client agrees to take such backups and provide such redundant systems as are prudent in the circumstances. The Company will notify the Client in the event where activity would lead to loss of service or data before proceeding where this is known to the Company.

2.7. To notify the Company immediately if there are any periods during Security Testing when the Company should stop work due to critical business processes (such as batch runs) or if any part of the System is business critical so that the Company can, if needs be and with the Client's consent, modify its testing approach.

2.8. That, during the performance of the Security Testing and for a period of 6 months after completion of the Security Testing, it will not recruit any employees or personnel of the Company which it met or was introduced to through its relationship under this Contract without the prior written consent of the Company.

3. FEES AND PAYMENT

3.1. Subject to 3.2 below and unless otherwise agreed, the Fees payable under this Contract shall be invoiced on delivery of the Test Report or, if none is to be provided, on completion of the Security Testing. Invoices are due for payment within 30 days of the date of the invoice. All payments due under this Contract shall become due immediately upon termination of this Contract despite any other provision in this Contract. All payments due under this Contract shall be made without any deduction by way of set off, counterclaim, discount or abatement or otherwise.

3.2. All sums under the Contract are unless otherwise stated, exclusive of VAT. Any VAT payable in respect of such sums shall be payable in addition to such sums and shall be payable in addition to such sums, at the rate from time to time prescribed by law on delivery of a valid VAT invoice.

4. CONFIDENTIALITY

4.1. Each party will not disclose or permit its employees, agents and sub-contractors to disclose any Confidential Information entrusted to it by the other party provided always that this restriction shall not apply to information already in the receiving party's possession, or which comes into the public domain other than by breach of this obligation by the receiving party or its employees, agents and sub-contractors, or which is disclosed to the receiving party or which is required to be disclosed pursuant to any law or regulation or by the rules of any stock exchange or by a court of competent jurisdiction. If Confidential Information is required to be disclosed pursuant to any law or regulation or by the rules of any stock exchange or by a court of competent jurisdiction then the Receiving Party shall notify the Disclosing Party prior to any disclosure.

5. INTELLECTUAL PROPERTY RIGHT

5.1. Ownership of all Intellectual Property Rights in the System remains at all times with the Client and/or its ISP or other third-party supplier. For the avoidance of doubt, all Intellectual Property Rights in the materials used by the Company to carry out the Security Testing remain vested in the Company or any relevant third-party owners.

5.2. All Intellectual Property Rights in the results of the testing shall belong to the Client.

5.3. Copyright in the Test Report shall also remain with the Company, but the Client is hereby granted a non-exclusive, non-transferable licence to copy and use the Test Report for its own internal purposes only. The Client will need prior agreement to be sent in any form to any 3rd party. In any event this will not be given to the forwarding of a Test Report to a Penetration Testing company or entity.

6. LIABILITY

6.1. Nothing in this clause 7 excludes or limits the liability of the Company for fraudulent misrepresentation or for death or personal injury caused by the Company's negligence. Save as aforesaid the following provisions set out the entire financial liability of the Company (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Client, its ISP or any third-party supplier of the System to the Client.

6.2. The Company shall not be liable for any loss, damage, costs, expenses or other claims for compensation arising from any material or instruction supplied by the Client which are incomplete, incorrect, inaccurate, illegible or defective in any other way. The Company should highlight to the Client any known errors.

6.3. The Company shall not be liable for any loss or damage caused to either the Client, its ISP or other third party supplier of the System either jointly or severally except to the extent that such loss or damage is caused by the negligent acts or omissions of or a breach of any contractual duty by the Company, its employees, agents or sub-contractors in performing the Security Testing.

6.4. The Company's total liability in respect of all claims arising under or by virtue of this Contract or in connection with the performance of this Contract shall not exceed £1,000,000 in aggregate.

6.5. The Client's total liability in respect of all claims arising under or by virtue of this Contract or in connection with the performance of this Contract shall not exceed the amount £1,000,000 in aggregate.

6.6. The Company and the Client shall not be liable to each other for any indirect or consequential loss or damage whether for loss of profit, loss of business, depletion of goodwill or otherwise whatsoever or howsoever caused which arise out of or in connection with this Contract even if such loss was reasonably foreseeable

7. TERMINATION

7.1. Either party may (without limiting any other remedy) at any time terminate the Contract by giving written notice to the other if the other commits any material breach of these Conditions and (if capable of remedy) fails to remedy the breach within thirty (30) days after being required by written notice from the other Party to do so, or in an Event of Insolvency.

8. DATA PROTECTION

8.1. In the course of providing the Security Testing, the Company may obtain Personal Data from the Client. The Client confirms that it has obtained all consents required from data subjects to enable such Personal Data to be disclosed to the Company and

made all necessary registrations and notifications in accordance with applicable Data Protection Laws to enable the Company to carry out the Security Testing and the Client will ensure the same are kept accurate and up to date.

8.2. In respect of any Personal Data held or processed by the Company as a result of or pursuant to these Conditions, the Company represents to the Client that it has made all necessary registrations and notifications in accordance with applicable Data Protection Laws and that it will ensure that the same are kept accurate and up to date during the term of the agreement.

8.3. In addition to and notwithstanding any other right or obligation arising under these Conditions, the Company (and shall ensure that its Personnel shall):

8.3.1. implement appropriate technical and organisational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "Security Incident").

b) use the Personal Data obtained as a result of these Conditions only for the purposes of fulfilling its obligations under these Conditions and not disclose Personal Data without the written authority of the Client.

c) comply with the express instructions or directions of the Client from time to time in connection with the use of such Personal Data and the requirements of any Data Protection Laws and such Personal Data shall be treated as Confidential Information of the Client for the purposes of these Conditions.

d) not do or omit to do anything which causes the Client to breach any Data Protection Laws or contravene the terms of any registration, notification or authorisation under any Data Protection Laws of the Client; and

e) not transfer Personal Data which has been obtained by or made available to the Company to any country outside the European Economic Area without the prior written consent of the Client.

10.4. The Company shall not subcontract any processing of the Personal Data to a third-party subcontractor without the prior written consent of the Client. If the Client refuses to consent to the Company's appointment of a third-party subcontractor on reasonable grounds relating to the protection of the Personal Data, then the Company will not appoint the subcontractor.

8.3.2. The Company shall not be in breach of this Clause 10 if it acts on the instructions of the Client.

8.3.3. If the Company believes or becomes aware that its processing of the Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform the Client as soon as reasonably practicable and provide the Client with all such reasonable assistance at the Client's cost as the Client may reasonably require in order to conduct a data protection impact assessment.

8.3.4. The Company will (and will ensure that its Personnel will) without undue delay notify the Client if it becomes aware of a Security Incident or if lawfully able that a disclosure of Personal Data may be required by law, or if it receives a request from an individual to access their Personal Data or to cease or not begin processing (or to rectify, block, erase or destroy Personal Data), or if it receives any communication from the Office of the Information Commissioner or similar authority relating to the Personal Data. The Company shall provide all such timely information and cooperation as the Client may reasonably require in order for the Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Laws. The Company shall further take all such measures and actions as are technically practicable and within its control to remedy or mitigate the effects of the Security Incident and shall keep the Client up to date about all developments in connection with the Security Incident.

9. FORCE MAJEURE

9.1. Neither party to the Contract shall be deemed to be in breach of these conditions or otherwise liable to the other party in any manner whatsoever for any failure or delay in performing its obligations to the extent that the same is caused by Force Majeure. In the event the Force Majeure continues for a continuous period in excess of thirty (30) working days, either party shall be entitled to give notice in writing to the other party.

SPECIFIC TERMS - PENETRATION TESTING

The terms in this section are in addition to the General Terms and apply only to Agreements that cover the provision of Penetration Testing.

(a) Penetration testing and vulnerability assessments will be limited to conducting an agreed set of tests on the devices, systems, infrastructure and applications that are defined in the Statement of Work within the Agreement.

(b) The Company's Penetration Testing methodology is in line with the guidance of the Open Web Application Security Project (OWASP) and Penetration Testing execution standard (PTES). Testing is a combination of automated and manual testing, with manual testing designed to exploit any vulnerabilities identified by the automated testing. All tests look for exploitable vulnerabilities within the identified scope. Penetration Tests do not include a review of the actual code of any website applications.

(c) All other tests and systems are out of scope and will not be tested without a signed amendment to the Agreement.

(d) Test IP Address: the Company's testing is carried out from a dedicated Penetration Testing network, and the Company will supply the Client with the relevant IP address so that the Client can add it to any IPS/IDS or filtering system to allow testing to be completed. Log files may record ping sweeps and port sweeps from the Company's test IP address in addition to other activity that may be suspicious to any SEM or SIEM deployed on the systems and applications under test.

(e) The Company's testers will take care not to cause Denial of Service (DOS) conditions or anything that would affect the performance of the systems under test.

(f) The Company's testers will take care not to perform testing that will result in breaking any of the devices we identify nor will we attempt to exploit any vulnerability where we think that doing so may cause damage, nor will we intentionally damage any information or information systems during testing.

(g) The Company's testers will immediately report any critical risk vulnerability that we might identify to the Client contact.

(h) The Company will require explicit authorisation to proceed from you and from any additional parties involved in hosting the infrastructure or application that is in scope before the start of any test work.

The Company will not:

(a) Disclose test results or related information to third parties without your prior permission, unless otherwise required by law;

(b) Allow anyone, other than on a need-to-know basis, access to your test information.

(c) Exchange information in relation to the tests and test results other than by using encrypted email.

The Client will identify and disclose to the Company any third parties that may conceivably be affected by the Company's testing activities in relation to this Project, and any damages and/or loss of service caused by the Client's failure to identify and/or disclose such third parties shall remain the sole responsibility of the Client and the Client therefore agrees that the company cannot be held responsible for any costs or damages howsoever arising from such activities.

The Client's authorisation to commence testing activities is deemed to include confirmation that any relevant client-internal or external parties have been appropriately notified and that all necessary permissions from such parties for the Company to commence testing have been provided to the Company.

The Company will only identify vulnerabilities that are already known at the date on which any tests are carried out, and which are capable of being exposed by the range of testing tools deployed by the Company. The Client accepts that it is in the nature of technical security testing that there may be flaws which will be uncovered in the future or by the use of alternative tools and attack methodologies, none of which could normally be identified at the time of testing, and therefore agrees that it will not, now or in the future, hold the Company to account for any such matters.

The Company shall accept no liability for damages caused to the Client by any automated or nonautomated attacks on the Client's internet-facing infrastructure or its applications, irrespective of whether or not the Company's security testing activity carried out under this Agreement did, did not, or could have but did not, identify any vulnerability exploited or which might in future be exploited by any such attack.

The Company will identify vulnerabilities that its testing has exposed; wherever possible, it will identify by reference to commonly available and published information the appropriate patches and fixes that are recommended to deal with the identified vulnerability but it will be entirely the Client's responsibility to formally identify and deploy an appropriate solution to the vulnerabilities identified by the Company's security testing.

M8 Solutions

DELIVERING TECHNICITY WITH INTEGRITY

M8 Solutions Limited

Highfield House, Congelton Road,

Stoke-on-Trent, Staffordshire,

ST7 3SY

T: 01782 634 993

E: info@m8solutions.co.uk

www.m8solutions.co.uk

Company Reg: 12702481

M8 Solutions

technicity with integrity

In today's rapidly evolving digital landscape, cyber security isn't just a necessity - it's a cornerstone of trust and resilience. At M8 Solutions, we specialise in safeguarding NHS organisations from sophisticated cyber threats, delivering tailored security solutions designed specifically for healthcare's unique demands. Our team of cyber security experts understand the critical importance of protecting sensitive patient data and ensuring the integrity of NHS operations. Our practices are designed to provide a robust, proactive defence that protects patient data, supports operational resilience, and builds trust across the healthcare landscape.

PROTECTING NHS SYSTEMS WITH TAILORED CYBER SECURITY SOLUTIONS

1 CHIEF INFORMATION SECURITY OFFICER-AS-A-SERVICE (CISOAAS)

- Delivering remote CISOaaS or CISO on-demand, providing cost-effective strategic cyber security leadership tailored for the NHS.
- Providing expertise in security operations, and cyber strategies.
- Acting as a trusted advisor, with expert consultancy aligned with NHS goals.
- Supporting governance, risk and compliance initiatives.

2 CYBER SECURITY STRATEGIES AND POLICY DEVELOPMENT

- Developing and refining long-term cyber security strategies for the NHS.
- Producing security policies to enhance resilience and compliance.
- Supporting digital transformation projects with robust frameworks.
- Conducting risk assessments to inform investment in technologies and processes.
- Providing ongoing advisory services aligned to your cyber goals.

3 OUTSOURCED CYBER SECURITY OPERATIONS CENTER (CSOC) SOLUTIONS

- Cyber threat intelligence and analysis.
- Security information and event management (SIEM) implementation.
- Advanced threat detection and response solutions.
- Security orchestration, automation, and response (SOAR) solutions.
- Providing detailed performance metrics and security health reports.
- Forensic analysis and investigation cool-off services.

4 CYBER SECURITY AUDITS AND ASSESSMENTS

- Conducting assessments through M8 Solutions Cyber Security Diagnostic programme.
- Comprehensive audits of DSPT/CAF compliance and identifying areas for improvement.
- Delivering detailed gap analysis and practical recommendations for remediation.

5 THREAT MONITORING AND INCIDENT RESPONSE

- Threat modelling and risk analysis.
- Real-time threat detection and response to mitigate breaches and disruptions.
- NHS Cyber Alert (formerly CareCert) management, providing guidance to ensure swift and effective responses to emerging threats.
- Incident investigation and root cause analysis, including detailed post-incident reporting.

6 NETWORK AND INFRASTRUCTURE SECURITY SOLUTIONS

- Security architecture review and enhancement.
- Implementing and optimising firewalls, intrusion detection, and prevention systems.
- Securing NHS network infrastructure and medical devices against unauthorised access.
- Zero Trust security model architecture and implementation.
- Ensuring compliance with NHS network security policies.

7 ENDPOINT AND DEVICE SECURITY

- Comprehensive endpoint protection, including Internet of Medical Things (IoMT) devices.
- Deploying Endpoint Detection and Response (EDR) solutions to monitor and protect devices.
- Deploying Mobile Device Management (MDM) solutions to securely manage NHS-issued mobile devices.

8 STAFF AWARENESS AND TRAINING

- Tailored cyber security training programmes (Cyber Academy) for NHS staff at all levels.
- Simulated phishing campaigns to strengthen awareness and preparedness.
- Promoting a culture of vigilance and security best practices across all teams and staff.

9 VULNERABILITY/EXPOSURE MANAGEMENT

- Conducting regular vulnerability scans to identify and address potential risks within NHS systems.
- Produce and implement comprehensive remediation plans and strategies to address and rectify identified vulnerabilities.
- Providing ongoing advisory services to enhance cyber defence measures as part of a cycle of continuous improvement.

10 PENETRATION TESTING

- Performing penetration testing, simulating cyber threats to uncover vulnerabilities in infrastructure and applications.
- Red teaming and ethical hacking services.
- Developing tailored remediation strategies to address identified cyber weaknesses.
- Providing ongoing advisory services, ensuring continuous improvement of cyber defences.

11 DATA STORAGE, BACKUP, AND RECOVERY SOLUTIONS

- Disaster recovery and business continuity planning to ensure uninterrupted patient care.
- Designing and implementing secure data backup solutions.
- Encryption and key management.
- Mitigating the risks of ransomware attacks and data breaches.

12 COMPLIANCE AND REGULATORY SUPPORT

- Ensuring adherence to GDPR, DSPT, and NHS England's digital guidelines.
- Supporting NHS organisations through audits and certifications.
- Providing ongoing compliance monitoring and advisory services.

13 SECURE CLOUD AND HYBRID SOLUTIONS

- Offering expert guidance secure cloud and hybrid infrastructure architecture, tailored to NHS requirements.
- Enabling scalability and efficiency without compromising data security.
- Encryption and key management.
- Delivering solutions to maintain compliance with NHS guidelines and best practices.

14 IDENTITY AND ACCESS MANAGEMENT (IAM) SOLUTIONS

- Analysing current access controls to identify and address security gaps.
- Designing and implementing robust IAM frameworks tailored to organisational needs, ensuring secure access controls.
- Managing privileged accounts.
- Providing continuous monitoring and support to ensure compliance and security.

15 THIRD-PARTY VENDOR RISK MANAGEMENT

- Assessing and managing risks associated with external vendors and suppliers.
- Ensuring third-party compliance with NHS cyber security frameworks e.g. CAF.
- Implementing vendor monitoring and reporting solutions.

16 CYBER SECURITY BRIEFINGS AND REPORTING

- Delivering regular briefings to NHS leadership on emerging threats and cyber trends.
- Providing detailed cyber performance metrics and security health reports.
- Offering strategic advice to support informed decision-making.

With a deep understanding of NHS-specific challenges, we provide tailored cyber security solutions that prioritise compliance, resilience, and operational continuity. Let us help you secure your systems, protect sensitive data, and ensure uninterrupted patient care.

01782 634 993 INFO@M8SOLUTIONS.CO.UK WWW.M8SOLUTIONS.CO.UK