Canon

CYBERGUARD SECURITY FOR THE HEALTH SECTOR

Cyber security services to reinforce your defences and provide the 24/7 coverage your organisation needs.

SECURE YOUR BUSINESS WITH CYBERGUARD

CONTENTS

INTRODUCTION

The UK's health sector is vast and diverse, encompassing a wide range of organisations, from small GP practices to large NHS Trusts, private hospitals, and individual healthcare practitioners. These organisations are entrusted with highly sensitive patient data, including medical records, personal information, and financial details, making them attractive targets for cybercriminals.

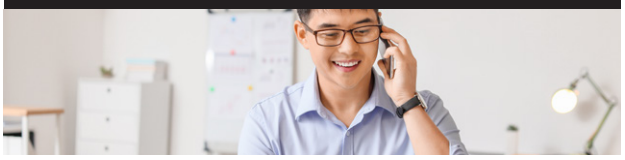
The increasing reliance on digital technologies, such as telehealth and electronic health records, has revolutionised healthcare delivery. However, it has also expanded the attack surface, exposing the sector to more sophisticated cyber threats. The rise of remote working and the use of personal devices further exacerbate these risks.

Reports indicate a concerning increase in cyberattacks targeting the health sector. Attackers are not only interested in large hospitals but also smaller clinics and individual practitioners, as the sensitive data they hold is highly valuable. Worryingly, a significant percentage of healthcare organisations lack comprehensive cybersecurity strategies, leaving them vulnerable to attacks.

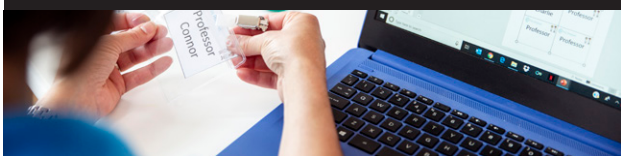
Key concerns for the health sector include patient safety and wellbeing, data breaches, reputational damage, and financial losses due to operational disruptions. It is crucial for healthcare professionals to be trained in cybersecurity best practices and comply with stringent data protection regulations, such as the General Data Protection Regulation (GDPR) and the Data Security and Protection Toolkit, to ensure the safety and privacy of patient information.

THE CYBER SECURITY MIX

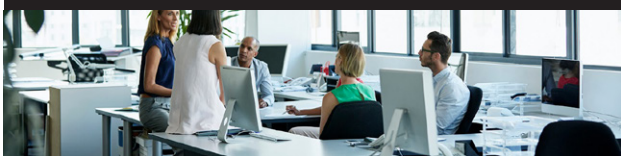
Managed Detection & Response



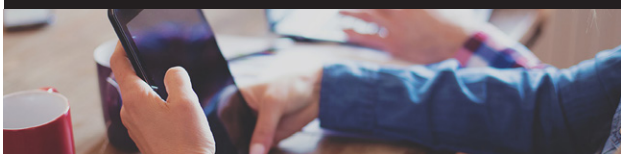
Pen Testing



Incident Response

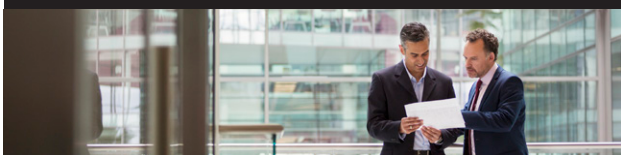


Training & Certification



Security Posture Review

Managed Firewall



The challenge is to continually monitor your security posture and act quickly when a problem is found.

Canon CyberGuard Security Services

Canon's cybersecurity services are tailored to the specific needs of the UK health sector, offering robust defence against evolving cyber threats. We provide comprehensive solutions, including intrusion testing to identify vulnerabilities and incident response to manage and mitigate breaches, both critical in safeguarding patient data and maintaining operational continuity. Our team of certified experts can also develop strategic security plans and roadmaps aligned with NHS Digital guidelines, conduct thorough risk assessments, and even provide a virtual CISO (vCISO) to bolster your internal capabilities. Recognising the importance of a well-informed workforce, we offer security awareness training tailored to the healthcare environment and assist with achieving essential certifications and accreditations.

CHALLENGES TO OVERCOME

RANSOMWARE ATTACKS

These attacks are increasing in both sophistication and frequency. They involve the use of malicious software to encrypt critical data, rendering it inaccessible until a ransom is paid. Healthcare organisations, with their reliance on patient data, are prime targets.

A successful cyber attack can lead to the disruption of essential services, such as emergency care and surgeries, potentially endangering patients' lives. Moreover, the loss of sensitive patient data can erode trust and lead to legal repercussions.

PHISHING AND SOCIAL ENGINEERING

These attacks exploit human vulnerabilities like trust, helpfulness, fear, or urgency. Cybercriminals use deceptive emails, messages, or phone calls to manipulate staff into divulging sensitive information, such as login credentials or patient data, or to click on malicious links that can install malware or grant unauthorised access to systems.

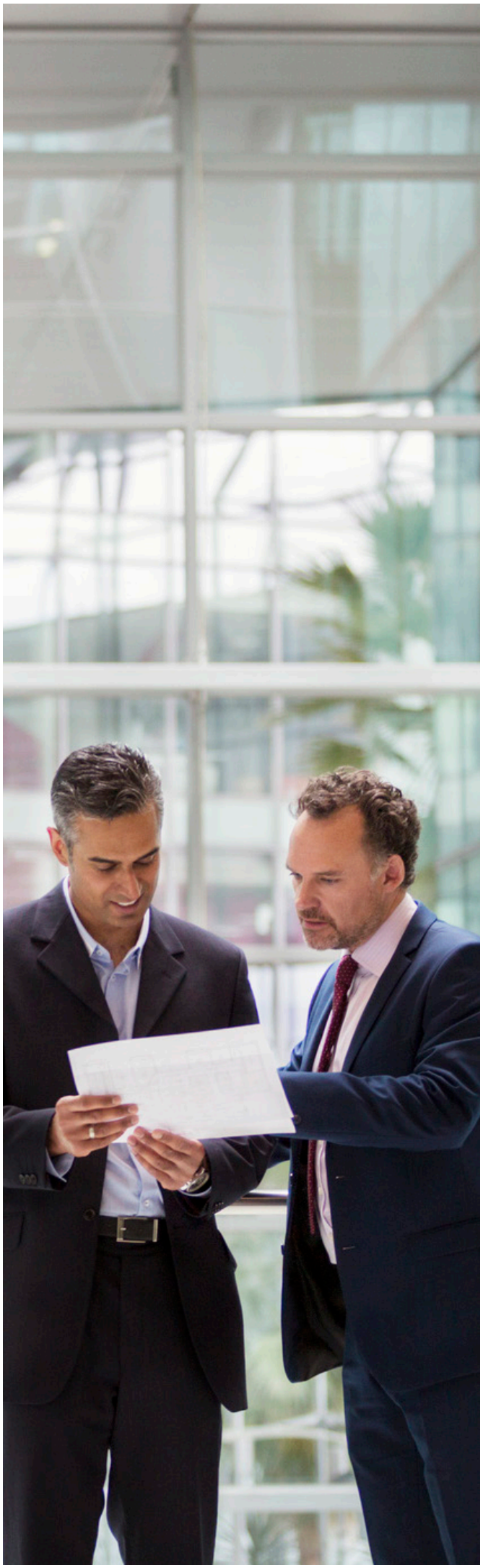
For example, a staff member might receive an email seemingly from their supervisor requesting immediate access to patient records, or a message posing as a patient needing urgent assistance. The consequences can be severe, ranging from compromised systems and data breaches to financial losses and reputational damage.

INSIDER THREATS

Insider threats pose a significant risk to healthcare organisations, as individuals with legitimate access to sensitive data can compromise cybersecurity either intentionally or unintentionally. This includes employees, contractors, and third-party vendors who may inadvertently cause data leakage or deliberately engage in unauthorised access or system disruption.

The consequences of such threats can be severe, ranging from the breach of patient confidentiality to the disruption of critical healthcare services.

A managed SOC assumes the pivotal role of overseeing your security landscape. It's at the forefront, persistently monitoring for threats and ensuring prompt actions against cyber-attacks.



THE SOLUTION

Canon's CyberGuard solution provides the very latest in cyber security services. With so many variations of threats and the potential of multiple security gaps within health organisations, CyberGuard gives peace of mind that your security is in good, experienced hands.

Don't let the threat of cyber crime get the better of you. With the right experts at hand, and with proper preparation, you can mitigate risk. And, if the worst does happen, you can recover. We offer a range of services to help you strengthen your security from all angles.

We protect our customers from end-to-end through:

- Security Testing
- Managed Detect & Respond Services
- Security Awareness Training
- Cyber Certification.

We provide reassurance in the event of an attack through fast and effective Cyber Incident Response, built upon sound threat intelligence gathered by our own team of cyber analysts coupled with intel from various global sources.

OUR CYBERSECURITY SERVICES GIVE YOU:

- Peace of mind with UK-based, 24/7 monitoring and response
- Intelligence-based analysis for better visibility of threats
- A proactive approach to security
- Help from trusted CREST and CHECK
- Compliance with data protection regulations

BENEFITS:

- Improve visibility with our Threat Intelligence
- Proactively monitor your infrastructure
- 24/7 UK Security Operations Centre (SOC)
- Support from a cyber security incident response team (CSIRT)

We work with leading technology providers in the cyber security sector, including:

Microsoft Security

paloalto NETWORKS

Qualys.

KnowBe4 Human error. Conquered.

CROWDSTRIKE

OUR SERVICES

At the heart of our cyber security efforts lies our UK-based Security Operations Centre (SOC), operational 24/7. This dedicated team comprises seasoned and accredited cyber security experts, diligently sifting through a multitude of alerts from various sources.

Choosing our SOC brings many advantages for the health sector. Foremost among them is the capability to detect and counteract security threats in real-time, curtailing their potential to inflict substantive damage or result in financial losses. With vigilant eyes on networks, systems, and applications, our SOC ensures that deviations and questionable activities are swiftly detected and addressed.

This real-time monitoring is crucial for healthcare organisations to protect patient data and ensure business continuity.

FEATURES AND BENEFITS:

- **Threat Detection and Response**
- **Incident Management**
- **Proactive Threat Hunting**
- **Enhanced Incident Response Time**
- **Better Visibility**
- **Reduced Costs**

OUR SOC DELIVERS THE FOLLOWING MDR SERVICES

MANAGED SIEM

Our state-of-the-art SIEM solutions, powered by Microsoft Sentinel, ensures a comprehensive view of your security landscape. Through intelligent log analysis and event correlation, we spotlight unusual patterns and behaviours, facilitating quicker incident response and better threat visibility.

MANAGED EDR

We recognise the need for a layered defence strategy. By integrating industry leaders such as Microsoft Defender and CrowdStrike, our Endpoint Detection and Response (EDR) service offers unmatched precision in pinpointing and neutralising threats at the endpoint level, well before they can proliferate.

MANAGED XDR

Extended Detection and Response (XDR) is a unified defence against incidents that span endpoints, identities, email, collaboration tools and cloud applications. By monitoring diverse attack surfaces and analysing the overall threat landscape, XDR provides a higher level of protection against emerging and sophisticated threats to the health sector.

MANAGED NDR

Network Detection and Response (NDR) platforms capture network metadata, enrich it with machine learning derived security intelligence, and apply it to your detection and response use-cases. NDR continuously analyses network traffic and behaviour, enabling security teams to respond quickly and prevent potential breaches or damage.

MANAGED FIREWALLS

A robust perimeter is fundamental to cyber security. Our managed firewalls not only act as your organisation's first line of defence against intruders but are also continually updated and fine-tuned to adapt to evolving threat patterns, ensuring that your network boundaries remain impregnable.

MANAGED VULNERABILITY SCANNING

To be forewarned is to be forearmed. Our proactive vulnerability scanning solution delves into your systems, networks, and applications, identifying potential weak points. This ensures you can act pre-emptively, fortifying vulnerabilities before they can be exploited.

INCIDENT RESPONSE

When faced with a cyber incident, time is of the essence. Canon's Cyber Security Incident Response (CSIR) service is CREST-approved, a testament to our unparalleled expertise in the field. In the aftermath of a cyber attack, our primary focus is on swift containment, recovery, and ensuring minimal disruption for your patients and staff.

OUR CSIR SERVICE ENCOMPASSES:

- Rapid Response: Efficiently addressing security incidents to prevent further damage.
- Expert Analysis: Identifying the nature and scope of the breach, ensuring informed decisions at every step.
- Recovery and Restoration: Re-establishing the integrity of your systems and getting your operations back on track.
- Post-Incident Review: Analysing the incident to provide actionable insights, bolstering your defences for the future.

IR RETAINER SERVICES

For health organisations seeking added peace of mind, we offer our IR Retainer Services. With this, you're not only prepared for potential incidents but also assured of priority response, ensuring even swifter action and mitigation in the event of an unforeseen breach.

FEATURES AND BENEFITS:

- **CREST Accredited**
- **Incident Management**
- **Proactive Threat Hunting**
- **Enhanced Incident Response Time**
- **Service Excellence**

PENETRATION TESTING SERVICES

Penetration Testing, also known as “Pen Testing”, is a simulated cyber-attack carried out by in-house experts to assess the security of a computer system. By simulating real-world attack scenarios, our Crest-accredited team can identify weaknesses in the system’s defences, such as misconfiguration, outdated software or insecure network settings.

They can then create an efficient defence plan against hacking attempts.

- Infrastructure Assessment
- Mobile and Web Application Security
- Red Team Assessment
- PCI DSS Assessment
- Stolen Device Assessment
- Physical Security Assessment
- GDPR Assessments

CHECK
IT Health Check Service

CREST

FEATURES AND BENEFITS:

Identify Potential Vulnerabilities

Compliance and Regulations

Proactive Security

Incident Response Planning

Risk Mitigation

Stakeholder Confidence

BUILD BUSINESS RESILIENCE AND IMPROVE YOUR SECURITY STRATEGY WITH CANON

CANON'S RANGE OF IT SERVICES ARE POWERED BY OUR PARTNER WAVENET

Wavenet is a respected, multi-award-winning provider of cybersecurity, telecoms and technology solutions to thousands of businesses and enterprises across the UK.

WHY HAS CANON PARTNERED WITH WAVENET?

After an extensive market research exercise followed by rigorous due diligence of numerous IT service providers in the UK, we chose to partner with Wavenet, unlocking access to an extensive range of IT services that could be incorporated into the Canon strategic partnership.

Through this partnership, we combine Wavenet's expertise in technology with Canon's experience in delivering managed print services to deliver 'gold standard' IT solutions to our clients.

GET STARTED

CyberGuard Technologies is the security division of our partner Wavenet. We provide a suite of fully managed end-to-end security services from a 24/7 UK security operations centre. Our cyber defences protect against the potential devastation of an attack from cyber-criminals including defending your finances, identity, reputation, data and your customers' confidential information.

We provide cybersecurity, communications and technology-managed services that grow with your business – no matter what the future holds.

We focus on finding the right cybersecurity solutions so you can focus on what matters most to your business – for today and tomorrow. Always thinking ahead, give you the confidence that when you work with us, we'll future proof your business.

Networking & Connectivity

IT, Cloud & Technology

CyberGuard

TeamsLink & Collaboration

Unified Comms & Voice

Mobile Solutions & IoT

Contact Centre

POWERED BY wavenet

Call us on **01895 691330** or email **IT-Services@cuk.canon.co.uk** to enquire about the full range of IT services from Canon.

Canon (UK) Ltd
4 Roundwood Avenue
Stockley Park
Uxbridge
Middlesex
United Kingdom UB11 1AF

Tel: 01895 691330
Email: IT-Services@cuk.canon.co.uk

Canon