oneAdvanced

Cloud security in the healthcare sector

5 data points every CISO needs to know.

1 Prevalence of cyber attacks

Beyond numbers, each breach can **disrupt care, delay treatments, or compromise patient confidentiality**. The growing volume of incidents signals an urgent need for **stronger digital safeguards** and **dedicated cybersecurity expertise** to protect both data integrity and patient wellbeing.

(Source: **IT Brief**)

The UK health sector self-reported

3820

data breaches between 2023 and Q1 2025.

The cost of a cybersecurity incident in the healthcare sector averages

US $9.8M

more than double the average across other industries.

2 Cost of inaction

Cyberattacks are extremely costly for healthcare organisations. With such high financial stakes, delays in implementing robust cybersecurity measures or relying on fragmented tools can result in **multimillion-dollar losses per incident** diverting funds away from **vital healthcare services, patient care, and medical innovation**.

(Source: **Deloitte UK**)

3 Tool sprawl complexity

Cybersecurity tool sprawl is costly and complex. Managing dozens of disparate tools can overwhelm teams, create integration gaps, and reduce overall effectiveness. Rationalising and consolidating tools help organisations **strengthen their security posture, optimise spend, and reduce operational risk.**

(Source: **Deloitte UK**)

The average healthcare organisation uses

43

cybersecurity tools, with 5% operating more than 100 tools.

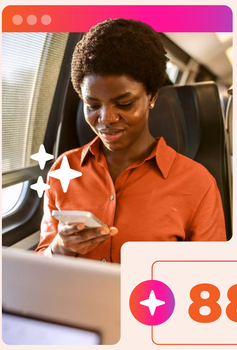
70%

of organisations are classified as either Formative or Beginner in cybersecurity readiness, indicating a significant need for external expertise.

4 Growing reliance on MSSPs

The lack of mature cybersecurity capabilities across many UK organisations, particularly in healthcare, underscores the importance of partnering with MSSPs or IT providers to **strengthen defences, monitor threats, and maintain compliance** to protect patient data and critical systems.

(Source: **Cisco**)



5 AI & the future of cybersecurity

This gap between policy and staff awareness is a serious risk: when staff are unaware of AI governance or how to use AI-enabled cybersecurity tools correctly, the deployment of these technologies can inadvertently **increase exposure to cyberattacks, data breaches, and operational disruption.**

(Source: **Security Brief**)

88% of healthcare cyber risk owners state they have AI related policies, 50% of healthcare workers are unsure whether such policies exist or know nothing about them.

Stay in Ctrl.

Don't let cloud security complexities hold you back.

Discover how **OneAdvanced IT Services** can help you protect your complex environments with our expert managed cloud security solutions.

Learn more

Microsoft Solutions Partner

bsi ISO/IEC 27001 Information Security Management

ISO 9001:2015

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

computing CLOUD EXCELLENCE AWARDS 2025 WINNER Best Cloud Support Provider OneAdvanced – Managed IT Services