Trust365 BUSINESS

Harnessing Cybersecurity

for Healthcare Organisations

trust365.com

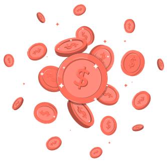
Holistic Cybersecurity for Healthcare Organisations

The Cybersecurity Challenge Healthcare Organisations are Facing

Hospitals and other healthcare facilities are becoming increasingly reliant on technology for many aspects of their operations, from record keeping and patient scheduling to medical imaging and surgical procedures. While this has helped to streamline many processes and improve patient care, it has also opened up these institutions to cybersecurity threats.

89% of healthcare organisations

reported an average of **43 cyber** attacks per year



£16,400 per hour to as much

as **£34,900 per hour** is the average cost of a cyber attack

95% of all identity theft

incidents come from **stolen healthcare records**

Common Cybersecurity Threats Targeting the Healthcare Organisations

Phishing

Phishing attacks involve fraudulent emails and websites that trick employees into disclosing login credentials, financial information, or downloading malicious attachments which leads to unauthorized access to sensitive data, financial losses, and damaged reputation.

Ransomware

Ransomware encrypts vital data and demands ransom for its release, while malware infiltrates networks and systems, stealing or destroying sensitive information and resulting in operational disruptions, loss of data, financial burdens, and legal ramifications.

Data Loss

Data loss can occur due to hardware failure, accidental deletion, or cyber-attacks aimed at destroying or stealing information resulting in disrupted operations, customer dissatisfaction, lost intellectual property, legal liabilities, and even business closure.

User Risk

Cybersecurity incidents are often caused by human errors such as weak passwords, and clicking on malicious links. Inadequate security practices put sensitive data at risk, leading to financial losses, damaged reputation, and loss of competitive advantage.

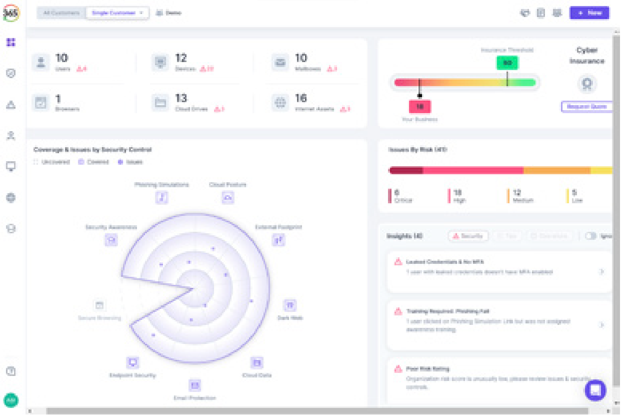
Holistic Protection. Hassle-Free. Cost-Effective.

Bridging Cybersecurity Gaps in Healthcare

Trust365 BUSINESS

Enhance Your Healthcare Security

- ✓ Prevent disruption of medical services, patient safety, and overall operations.
- ✓ Build trust in data security for patients, staff, and administrators.
- ✓ Mitigate the financial risk of being sued or paying fines in case of a breach.
- ✓ Secure patient records, cloud services, medical devices, maintain HIPAA compliance.



Leaked Credentials & No MFA

1 user with leaked credentials doesn't have MFA enabled

Training Required: Phishing Fail

1 user clicked on Phishing Simulation Link but was not assigned awareness training

Poor Risk Rating

Organization risk score is unusually low, please review issues & security controls.

The Key to Robust Cybersecurity in Healthcare

Healthcare Staff

Healthcare professionals have relatively high turnover rates due to the intense working conditions and therefore require a comprehensive security solution that factors in both old and new employees. It s crucial to maintain rigorous cybersecurity practices including real-time protection, regular access reviews and continual security training to ensure the safety of sensitive data and system integrity.

Patients

Given their reliance on health systems for their well-being and the sensitivity of their personal health information, patients form an essential demographic in healthcare cybersecurity. A robust security solution should prioritize safeguarding patient data in real-time, consistently reviewing and controlling access levels, and maintaining continuous system integrity to ensure dependable patient care and confidentiality.

Non-Staff Care Providers

Third-party healthcare personnel present unique cybersecurity challenges in healthcare due to their necessary yet conditional access to critical systems. Their security strategy must incorporate real-time safeguards, meticulous access control, and ongoing system protection to manage the distinctive risks they pose while maintaining operational efficiency and data confidentiality.

Email Security

Stay ahead of potential email threats by leveraging a userfriendly API-based active protection.

Cloud Data

Enable cloud data protection to achieve a safe and secure data collaboration with external users.

Awareness Training

Equip employees to be the first line of defense against the evolving landscape of cyber threats.

External Risk

Gain actionable insights on external threats by scanning digital footprint and exposed vulnerabilities.

Endpoint Security

Protect laptops, and desktops from cyber threats such as malware, and ransomware.

Secure Browsing

Keep your browser secure with the Trust365 extension for protection against viruses and malicious sites.

Phishing Simulation

Continually simulating cyber attacks like phishing emails to highlight weak spots.

Cyber Insurance

We include insurance cover in your subscription from Day-1 for total peace of mind.

Schedule a Meeting Today Protect & Your Business.

Trust365
BUSINESS

Trustify Ltd,
5 South Charlotte Street,
Edinburgh,
EH2 4AN UK

Telephone: 0800 634 3365

Website: www.trust365.com