

Cybersecurity in Healthcare:

The diagnosis and the antidote

As healthcare data breaches increase, what does it take to stay ahead of threats?



\$10.93M

The average cost of a data breach in healthcare **continues to increase.**

[2023 IBM & Ponemon Institute Report](#)

13 Years

Healthcare has had the highest industry cost of a breach for **13 consecutive years.**

[2023 IBM & Ponemon Institute Report](#)

53.3%

Since 2020, healthcare data breach costs have increased **53.3%.**

[2023 IBM & Ponemon Institute Report](#)

Healthcare organizations need security solutions to stay ahead of the targeted threats.

40m

Nearly **40M** health records breached or stolen in 2022

[US HHS OCR Breach Portal Data](#)

Why?

- ✓ Expanded Attack Surface
- ✓ Lack of cybersecurity staff and budget
- ✓ Lack of data inventory (knowing what kind of data we have & where)
- ✓ Lack of data classification (e.g., PHI, PII, IP, etc.)

These 4 key steps can help your healthcare organization reduce cyber risk with a more business-driven approach:

1

Take a risk-based approach to security

2

Timely detection to help minimize the impact of data breaches

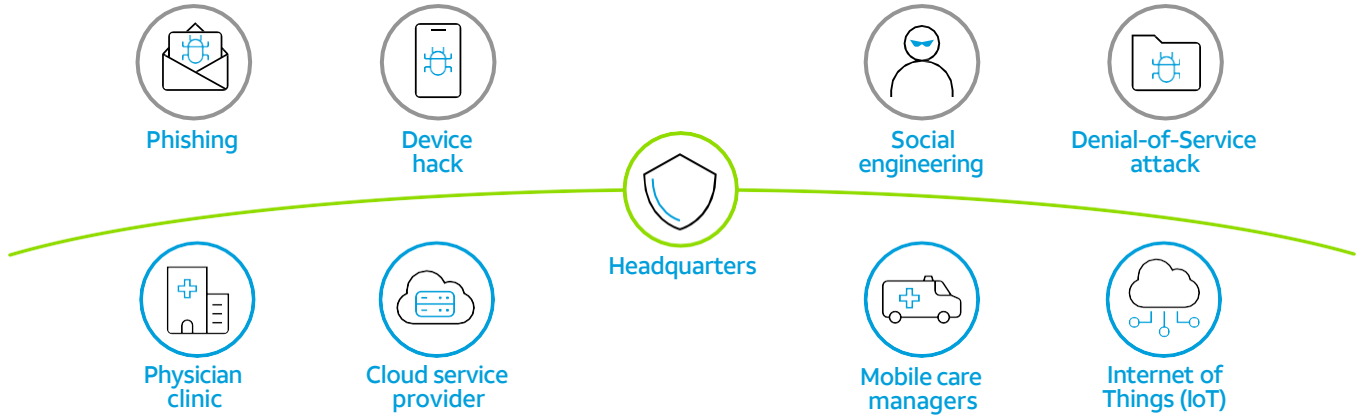
3

Effective vulnerability management

4

A well-formed incident response team and plan to help withstand a data breach

Secure patient data and improve patient care.



Current healthcare challenges	AT&T security solutions
Adoption of healthcare industry-specific standard of HITRUST Common Security Framework (CSF)	<ul style="list-style-type: none"> • HITRUST CSF workshops, readiness, remediation, and validated assessments with certification
Security awareness training	<ul style="list-style-type: none"> • Security awareness training • Social engineering / phishing
Proactive incident response reporting processes	<ul style="list-style-type: none"> • Incident response tabletop exercise • Incident response retainer • Pre and Post Breach Services
Achieve and sustain compliance with HIPAA/HITECH regulations	<ul style="list-style-type: none"> • HIPAA/HITECH compliance assessment • Healthcare risk assessments • Compliance as a Service
Manage patient data in a highly secure manner	<ul style="list-style-type: none"> • SASE solutions • Zero Trust • Vulnerability, Threat and Fraud Management
Optimize security efforts for third-party vendors	<ul style="list-style-type: none"> • Third-party risk management
Protect healthcare operations	<ul style="list-style-type: none"> • MDR • Cyber SOC Design and Build • DDoS defense
Emerging technology and innovation	<ul style="list-style-type: none"> • Cloud security, OT Security • Emerging Technology Risk and Innovation Strategy

To learn more about AT&T Cybersecurity Consulting, [visit www.att.com/security-consulting](http://www.att.com/security-consulting).

© 2023 AT&T Intellectual Property. All rights reserved. AT&T, AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. All other trademarks are the property of their owners. Actual results and your experience may vary from those described in this case study. Information and offers subject to change. Please contact your sales representative for additional information. | 356803-101821