PROTECTED HEALTHCARE DATA

There were 686 healthcare data breaches impacting over **44 million** individuals in 2021, reported to HHS U.S. Department of Health and Human Services

$24.1B is expected to be spent on cybersecurity for healthcare organizations by 2026.

$9.23M the average cost of a healthcare data breach in 2021.

39%

39% of healthcare organizations became aware of a breach month after it happened.

TOP 5 HEALTHCARE DATA THREATS IN 2022

IoT Connected Medical Devices
Visibility into each device's security posture, as well as network status, location, and device usage, remains a challenge.

mHealth & Telehealth Technologies
A rising demand that's another external access point your team's don't have control over, but are vulnerable too.

Cures Act & Patient Access
An unprecedented vulnerability in terms of privacy and attack. How do you secure all patients where and whenever they require it?

Understaffed & Underfunded IT Departments
Healthcare staffing issues are not limited to medical departments, while companies spend only 5-7% of the IT budget on cybersecurity.

Lack of Employee Security Training
91% of cyber attacks start with an email, while 24% of physicians can't identify phishing emails.

TOP 5 DATA PROTECTION TRENDS FOR 2022

Fast Healthcare Interoperability Resource Standards
Patient matching issues have plagued the healthcare business for years, and they continue to do so in the absence of national patient identification.

Better Multi-Factor Authentication
Secures the system by ensuring that only authenticated and verified users (patients, employees, and third parties) can access the system at any given time.

Mobile Device Security Strategy
Having remote access to wipe & disable mobile medical devices is a significant security feature that helps you control your device remotely

Isolated & Validated Backups
Moving a backup on remote servers and an isolated network reduce security breaches and increases recovery time.

Integration of Managed Service Teams
Adopt the use of a third party IT and infrastructure service team to streamline compliance and realign internal resources.