Patient data at risk

Understanding the current state of healthcare security.

Healthcare organizations are vulnerable to a wide range of attacks, whether it's collecting a past-due payment for services, fulfilling an order for medical devices, or a simple gesture of sending flowers to a loved one's bedside, making it a vulnerable industry compared to others.

Patients

40% of American customers stopped doing business just after **ONE** poor customer service experience.

40%

96% of consumers say that customer service is an essential fact that affects their choices.

83% of consumers in the US claim they will immediately stop spending after a security breach & **21%** will never return to that organization.

Contact Center

One in four data breaches come from lost or stolen devices — a problem that will persist with the increase in remote and hybrid workers.

1:4

95% of data breaches are caused by human error.

43% of all breaches are insider threats within the organization.

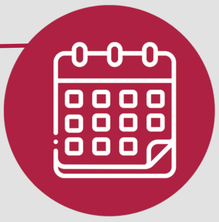
Organization

Only **5%** of an organizations' data is properly protected & **54%** of companies say their IT department are not prepared enough to handle a cyberattack.

$10.1

A data breach in the healthcare industry costs **$10.1 million** dollars on average.

On average, it takes **4.5 days** of a ransomware to be detected & **75 days** to contain a data breach.



The ideal vendor

What to look for when partnering with a payment security provider.

- Flexibility
- Scalability
- Frictionless patient journey
- Secure
- Compliant
- Security across all communication channels
- Future-proof technology

Patients today have choices

Patients today have choices regarding their healthcare options. Give patients the confidence to choose your organization by partnering with a vendor that prioritizes secure engagements and protects their sensitive personal data.

Eckoh