



IMPERVA FOR HEALTHCARE

Securing Positive Patient Outcomes

Imperva guards healthcare organizations against the largest, most complex cyber attacks with end-to-end security anywhere, at scale, and with the highest ROI.



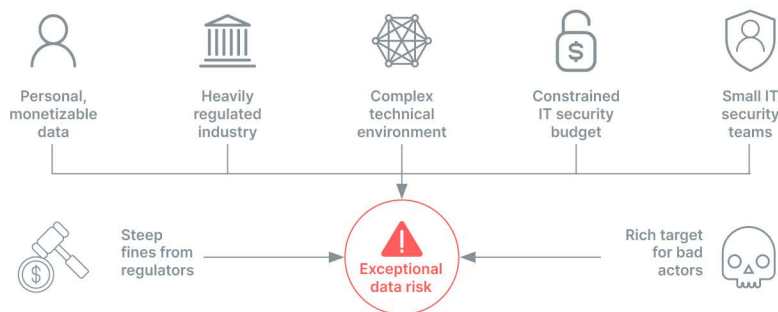
Hospitals, pharmacies, care centers, and other healthcare organizations are prime targets for malicious cyber-criminals. That's because healthcare organizations deal with large amounts of sensitive personal and private data, which are very valuable for cybercriminals.

In 2021, there were several major healthcare-related data breaches, with over 40 million patient records compromised in the United States. This led to several warnings from the FBI about the risk of cybercrime in the healthcare sector.

While many data breaches go completely unreported and are often unknown to the targeted organization, it is believed that healthcare-related data breaches affected over 22.6 million total patients in 2021. The single largest data breach reported in 2021 was Accellion FTA, affecting more than 3 million individuals.

The US government publishes a list of all reported healthcare breaches impacting 500 or more individuals. In total, there were over 600 reported healthcare breaches in the United States in 2021.

Healthcare data produces the perfect storm for cyber risk



\$10.1M

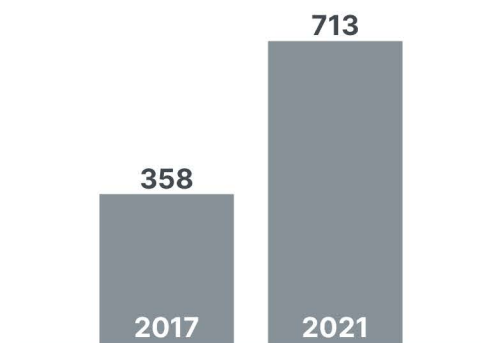
was the average cost for a data breach in the healthcare sector in 2021, 41.6% higher than 2021

40M

patient records were compromised in the United States in 2021

67%

of healthcare data breaches come from hackers or various IT incidents

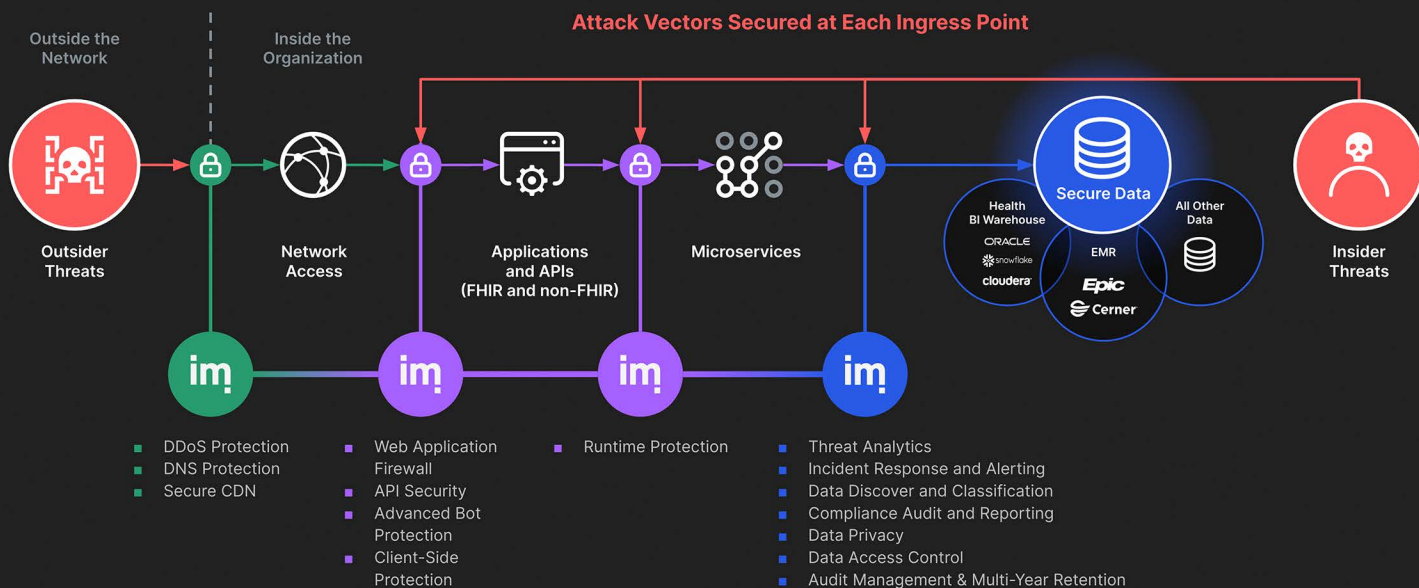


2X

Healthcare data breaches involving >500 records have nearly doubled since 2017

Protecting All Paths to Healthcare Data

Bad actors are innovative and constantly attempting to steal healthcare data. There are many ways to access data in a modern network architecture, each with its own ingress point. Whether someone from outside the network tries to breach perimeter defenses or an insider tries to gain unauthorized access, Imperva provides end-to-end security. With advanced DDoS/DNS protection, web application firewall, API and microservice security, data security, and more, Imperva protects all paths to patient data.



How Imperva Can Safeguard EMR Applications and PHI Data

Protecting sensitive patient data from insider and outsider threats

Imperva Application, Network, and Data Security solutions help safeguard sensitive patient data from unauthorized access, monitoring data activity across a broad range of data stores to identify vulnerabilities and suspicious behavior.

Securing medical applications against denial-of-service attacks and online fraud

EMR software and 3rd party applications are deployed widely within the healthcare sector, creating vulnerable entry points for hackers. Imperva Application Security solutions protect application data from web attacks, DDoS, site scraping, and fraud.

Ensure consistent patient care delivery and system availability

Distributed denial of service (DDoS) attacks cause serious problems for healthcare providers that need network access to provide proper patient care. Imperva DDoS Protection provides cloud-based DDoS security that automatically detects and mitigates all types of DDoS attacks – no matter how large.

Facilitate policy-compliant data handling practices for meeting HIPAA data audit and protection requirements

Imperva Data Security Fabric streamlines data-related compliance processes for assigning policy controls, enforcing separation of duties, retaining audit records, archiving, and reporting. Tasks that formerly required days to complete can be executed in minutes, saving time, shortening audit cycles, and significantly reducing compliance overhead costs.