CONNEXONE CASE STUDY

HEALTHCARE

ANY PROTOCOL DATA WHERE

CONNEXITE

INDEX

PROTECTING PATIENT DATA

Healthcare providers need to securely exchange patient data while complying with regulations.

Governments and global authorities are always looking to improve health services, and part of these efforts include collection of sensitive and private data to use for both to keep track of everyone health history and to create a solid base for todays mostly AI driven healthcare researches.

Abundance on data, does not make it anonymous until processed accordingly. All data generated from a patient medical diagnosis belongs to this patient, until approved. Thus moving this data from one repository to another need to have required security measures.

One of the most important security precautions is to protect original datastore from any kind of attack. Data leaving the initial store must not be exposed to any open channel, or create any hole in security chain that would be prone to attack.

This approach ensures patient data to travel integral and keep the infrastructure secure.

CHALLENGE

Secure patient data exchange between hospitals and research centers.

SOLUTION

ConnexOne one-way transfer system for patient records, diagnostic data and research results

OUTCOME

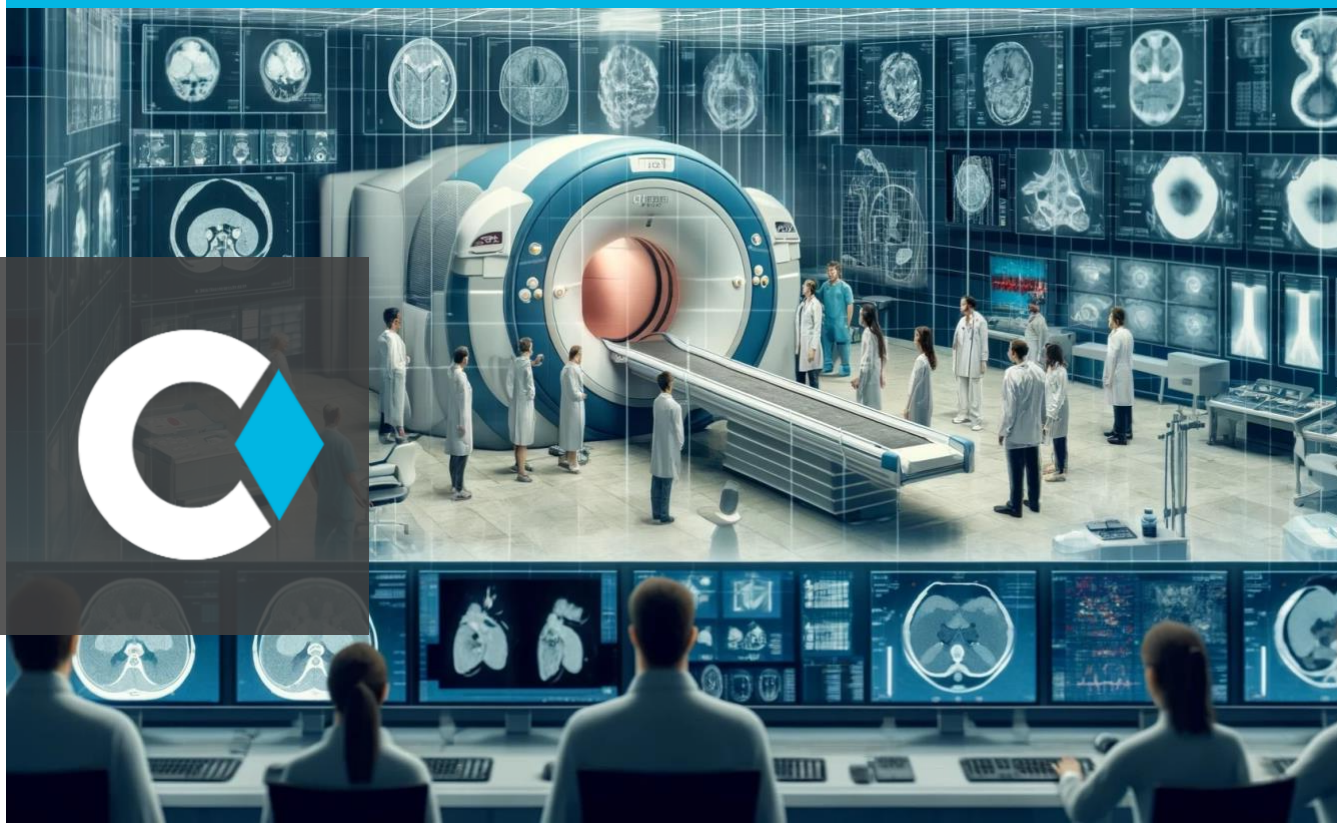
Protecting patient data, compliance with health regulations and keeping healthcare infrastructure not exposed to any external threat while sharing any information with other parties

SOLUTION OVERVIEW

In the healthcare industry, the security and privacy of patient data are of paramount importance. With the increasing digitization of healthcare systems, protecting sensitive information from cyber threats has become crucial. ConnexONE have emerged as a valuable solution for ensuring secure and one-way data transfer in healthcare environments.

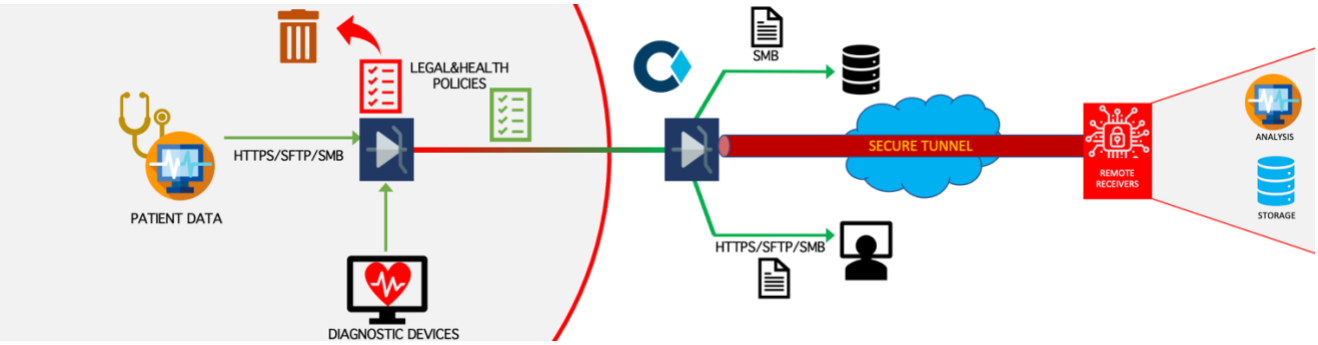
ConnexONE provide essential security measures for healthcare environments, ensuring the protection of patient data, maintaining privacy, enabling secure data exchange, optimizing operational efficiency, and promoting compliance with regulatory standards. By implementing ConnexONE, healthcare organizations can enhance their cybersecurity posture, safeguard patient information, and improve the overall quality of care.

Healthcare organizations are subject to stringent regulatory standards, such as the Health Insurance Portability and Accountability Act (HIPAA). ConnexOne plays a critical role in helping healthcare organizations meet these regulatory requirements



Solution Components

All ConnexOne hardware pairs are capable to transfer any protocols. Special hardware requirements to meet with regulations are optionally possible. It is possible to send received data to more than ConnexOne receiver and destination devices.



Application

ConnexONE, would reside in the boundary of data exchange for healthcare data. ConnexOne Guardian would be the ultimate hop before data would leave the critical healthcare infrastructure. After data leaves Guardian it will travel in lower security zones or untrusted networks. ConnexOne would guarantee no return hit of attack would be possible and data or information integrity will remain while leaving the secure zone.

In case of large file transfer such as file from medical imaging equipment, ConnexOne handles these large files efficiently, by keeping the file structure but removing any external footprints or metadata, and send it securely through its high-speed interfaces up to 10Gbps. Even for files reaching GB size, ConnexOne would be the best solution for secure, fast, reliable transfer.

Any other protocols that may require information sharing with external parties are welcome by ConnexOne. Guardian device listen for requested protocols and parse the payload of the information before sending from its one-way link to pairing Postman device, which ultimately deliver receiving data to any destination via any protocol.

Postman is also capable of sending data to remote destination over wide area links, such as internet, using encrypted tunneling technologies like IPSec, Openvpn and Wireguard

Each protocol would be handled separately and no information exchange between different protocol instance is allowed. Since it is very critical to keep the sensitive information unmodified, ConnexOne does not use any sort of manipulation or filtering on data transferred, guaranteeing that no financial rules are broken.

DISCOVER CONNEXITE SOLUTIONS

connexite.co.uk

CONNEXITE LTD
284 CHASE ROAD A BLOCK 2ND FLOOR
LONDON UNITED KINGDOM N14 6HF

contact@connexite.co.uk