CONNEXITE.CO.UK

Government Agencies RemoteData Transfer
Use Case Document with ConnexONE

CONNEXONE

CASE STUDY

GOVERNMENT

ANY PROTOCOL DATA WHERE

CONNEXITE

INDEX

SECURE CONFIDENTIAL GOVERNMENT DATA

Government data usually consist of highly confidential information related with public safety, which needs to be protected at all cost.

The nature of critical data makes it a common target for attackers. Keeping it safe yet accessible for sharing within the country or sometimes within an international alliance, requires a guaranteed security precautions that many firewalls or intrusion system can not offer.

Today's data is not only generated in word processors, but also on big data engines , digital cameras, IoT devices and with many more technological endpoints. This makes delivery methods different for each protocol, and together with remote transfer requirements, more sophisticated approaches are now needed.

Keeping data secure and integral, away from any possible attack, and being able to transfer it when necessary is the most challenging part of today's information driven world.

CHALLENGE

Keeping any data, primarily government files, safe, protecting from external attackers to change, delete or steal, but also being able to move data to less secure zones to share with other parties

SOLUTION

ConnexOne ensures one-way secure and reliable transfer for any data exchange, including files, video and databases, disabling return path physically to make sure no external traffic that may be harmful reaches to secured data

OUTCOME

Absolute protection of data against external threats, eliminating risk of data loss that may arise public safety risks and cause loss of confidence and reputation

SOLUTION OVERVIEW

Government agencies require secure data transfer to remote destinations while keeping data integrity. Traditional data transfer methods may create flaws that may lead data loss.

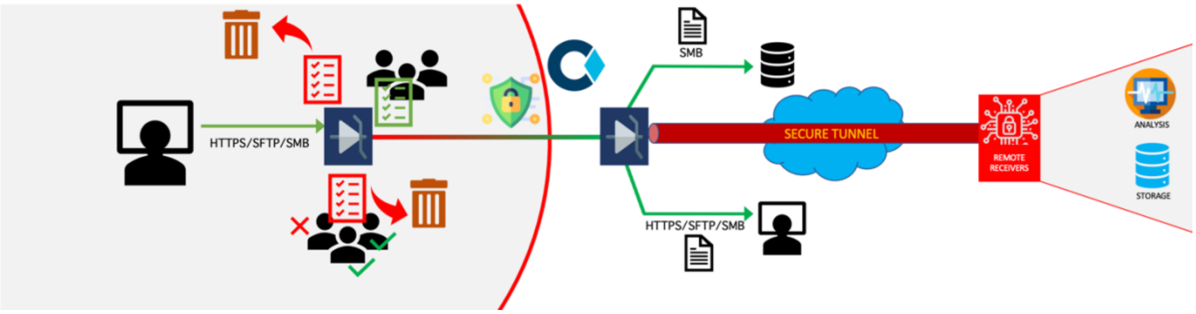
ConnexOne supports any protocol to be transferred using a single way hardware-based communication. It allows required protocols to share data with it, encapsulate this information, securely encrypt and deliver to low security zone to deliver any destination using the protocol needed. Using its built-in tunnelling functionalities, transferred data can easily sent through internet or any WAN connection

There is no protocol limitation on receiving side or delivering to destination. That makes ConnexOne solution, would not require any architectural change and integrate with current environment without any interruption or any sort of resource requirements. It supports all tunneling technologies from IPSec to Wireguard and does not require any special hardware or technology on connecting remote end.

ConnexOne is a long-term investment that provides secure transfer for today’s architecture and also ready to support any future protocol requirements.

Solution Components

All ConnexOne hardware pairs are capable to transfer any protocols. It is possible to send received data to more than one ConnexOne receiver and destination devices.



Application

ConnexONE, provides listeners for any protocol that needs to cross the boundaries of secured zone. Upon receiving data, ConnexOne decides how to process based on the admin configured rules. In case of a file transfer, it is possible to send the file for approvals to many users, clear metadata and even share it with a third-party security solution for detailed corporate policy checks. Once the file is allowed for transfer, it is sent to receiving pair device.
Receiving end also supports many options. Users can download the files from a web interface, the file can be sent to a storage area via any file transfer protocol including NFS, SMB and SFTP. Most important option in this zone, is to send the file to remote destination a via secure tunnels. This is especially critical to share data with other government agencies, embassies or international authorities.

Data transfer is not limited with file protocols. Basically, any protocol data can be carried over data diode. 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 legal 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