CONNEXONE
CASE STUDY

TOURISM

ANY
PROTOCOL
DATA
WHERE

CONNEXITE

INDEX

STRESS FREE LEISURE SERVICES

Ultimate goal for any tourism related service is to provide a smooth and positive service to make people happy and feel them more precious

Today any service to end customers requires not only quality at the service delivery time, but also processes that support this delivery. As all of the supporting business systems are now digitally driven, protecting the generated data can never be ignored on any business vertical.

User privacy is perhaps the most important aspect of tourism industry. It is now backed by legal regulations and treated as a corporate asset once it is processed under user consent.

Video Surveillance and remote monitoring of tourist attractions such as natural reserves, historical monuments, or theme parks is an integral part of todays security. Keeping it secure and accessible is another challenge.

All booking subsystems, infrastructure telemetries, critical operation security also need to be taken care, to provide a perfect service to customers.

These challenges need to be handled sensitively without compromising the service quality.

CHALLENGE

Secure customer and infrastructure data, remotely monitor touristic attractions and sharing data to external parties

SOLUTION

ConnexOne one-way transfer system for customer records and surveillance video provide data integrity and prevent data disruption while allowing remote transfer

OUTCOME

Customer data would be protected against any external threat, keeping it confidential. Any premise would be remotely controlled with video transfer. Data transfer, to third parties and legal entities allow smooth business operations

SOLUTION OVERVIEW

Data diodes would enhance cybersecurity in the tourism industry by enabling one-way data transfer, protecting critical systems from external threats.

They secure payment gateways, customer data, and internal networks in hotels, resorts, and airports. In smart tourism infrastructure, data diodes isolate operational systems while allowing telemetry data to be securely monitored.

They protect sensitive data in tourism data centers, ensuring compliance with privacy regulations like GDPR.

Also, data diodes enable safe remote monitoring for tourist attractions and secure marketing and analytics systems. By enforcing unidirectional data flow, data diodes safeguard tourism businesses from cyberattacks while allowing critical information to be transmitted securely for operational efficiency and compliance.

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.
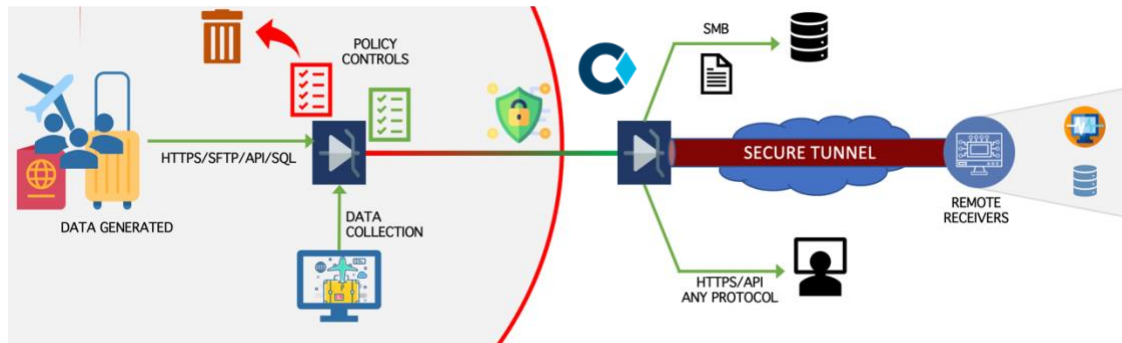
Application

ConnexONE, would reside in the boundary of data exchange for relevant data. ConnexOne Guardian would be the ultimate hop before data would leave the critical 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 reservation/hotel/airport systems, 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