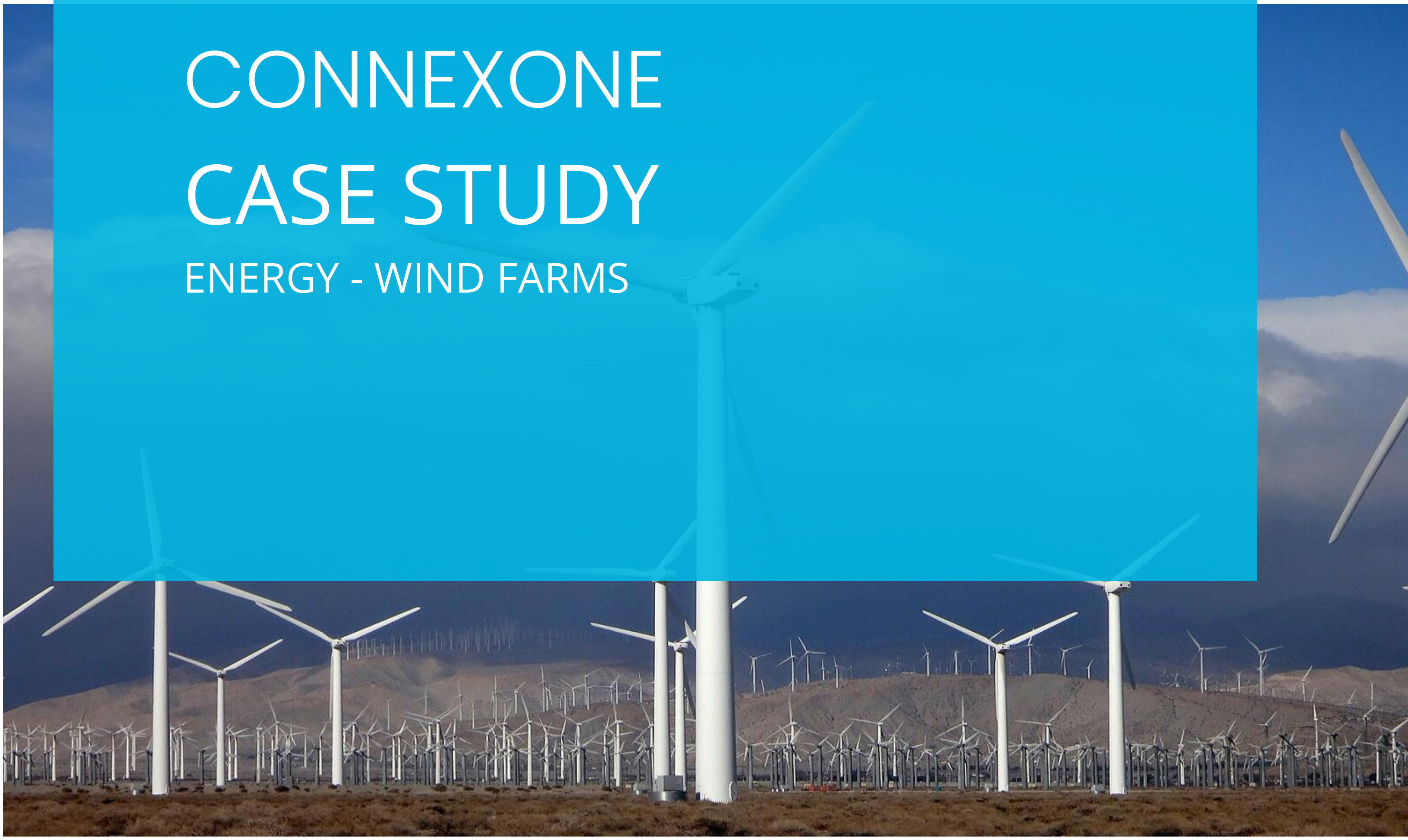
CONNEXITE.CO.UK

PROTECTING WIND FARMS
FROM CYBER THREATS WITH CONNEXONE

# CONNEXONE CASE STUDY

## ENERGY - WIND FARMS

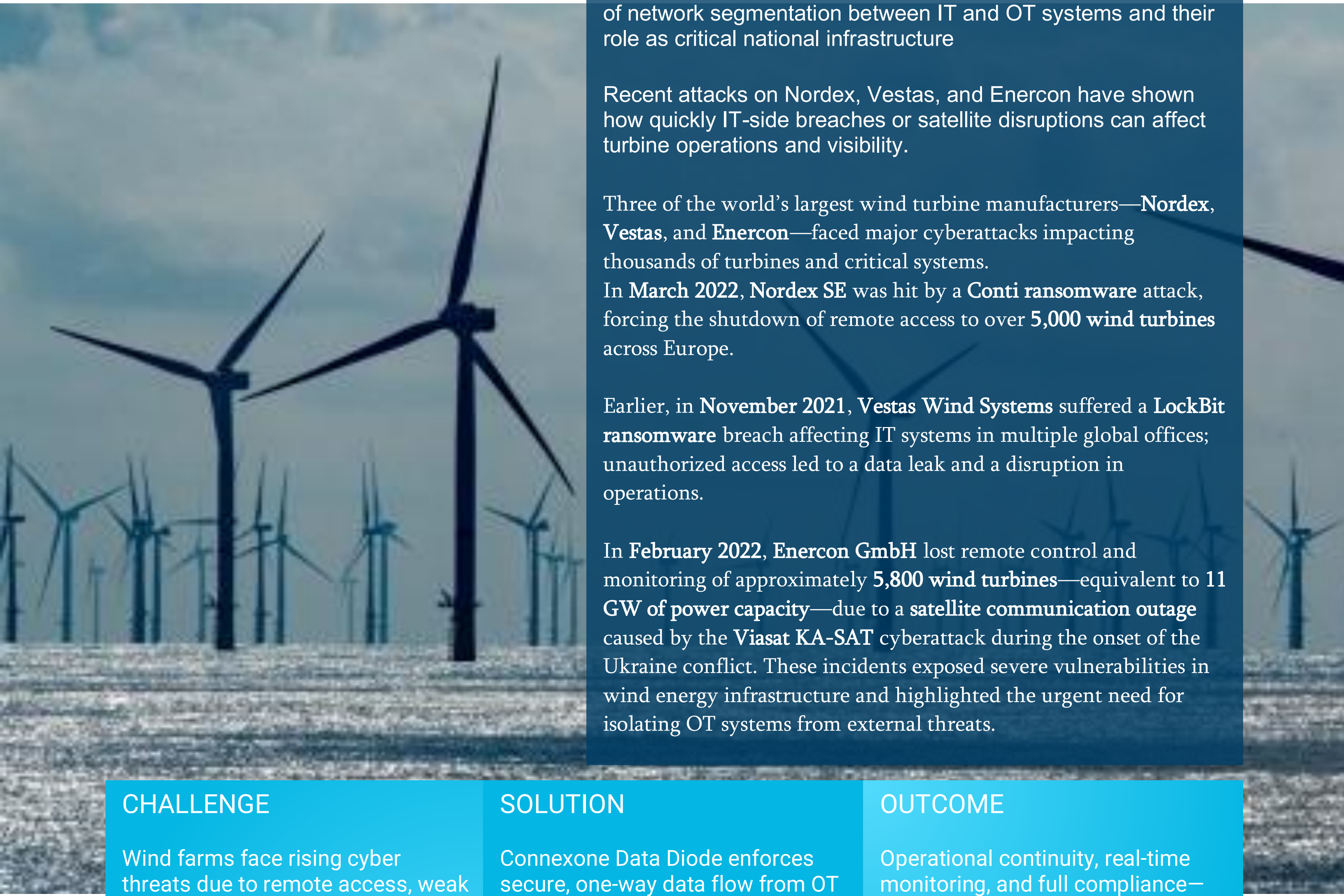


ANY PROTOCOL
DATA
WHERE

CONNEXITE

# INDEX

# HARDWARE ENFORCED SECURITY FOR MODERN ENERGY INFRASTRUCTURE



Wind farms are now prime targets for cyberattacks due to, increased reliance on remote access and third-party systems, use of legacy SCADA protocols with little or no encryption, lack of network segmentation between IT and OT systems and their role as critical national infrastructure

Recent attacks on Nordex, Vestas, and Enercon have shown how quickly IT-side breaches or satellite disruptions can affect turbine operations and visibility.

Three of the world's largest wind turbine manufacturers—**Nordex**, **Vestas**, and **Enercon**—faced major cyberattacks impacting thousands of turbines and critical systems.
In **March 2022**, **Nordex SE** was hit by a **Conti ransomware** attack, forcing the shutdown of remote access to over **5,000 wind turbines** across Europe.

Earlier, in **November 2021**, **Vestas Wind Systems** suffered a **LockBit ransomware** breach affecting IT systems in multiple global offices; unauthorized access led to a data leak and a disruption in operations.

In **February 2022**, **Enercon GmbH** lost remote control and monitoring of approximately **5,800 wind turbines**—equivalent to **11 GW of power capacity**—due to a **satellite communication outage** caused by the **Viasat KA-SAT** cyberattack during the onset of the Ukraine conflict. These incidents exposed severe vulnerabilities in wind energy infrastructure and highlighted the urgent need for isolating OT systems from external threats.

## CHALLENGE

Wind farms face rising cyber threats due to remote access, weak segmentation, and outdated SCADA protocols.

## SOLUTION

Connexone Data Diode enforces secure, one-way data flow from OT to IT—eliminating all inbound cyber risk.

## OUTCOME

Operational continuity, real-time monitoring, and full compliance—without exposing turbine control systems. Keeping the energy production highly effective

# SOLUTION OVERVIEW

Connexone is a plug-and-play device that protects wind farm control systems by allowing data to flow out—but never in. This means operators can safely monitor turbine performance, send reports, and meet compliance standards without risking a cyberattack entering through the connection. It's a simple yet powerful way to protect critical infrastructure and keep energy flowing.

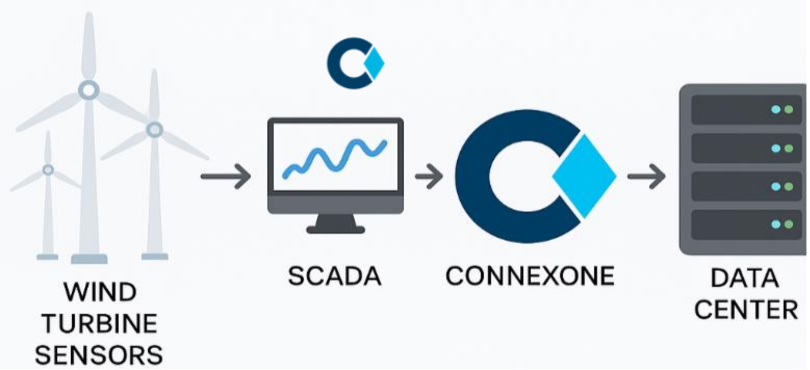
Connexone Data Diode is a hardware-based cybersecurity solution that enforces unidirectional data flow from wind farm operational technology (OT) systems—such as SCADA and turbine controllers—to external IT networks and monitoring centers.

Unlike firewalls or software-based gateways, Connexone operates at the physical layer, ensuring that no commands, malware, or unauthorized traffic can ever flow back into critical systems. This approach eliminates entire classes of cyber threats while enabling safe, real-time data export for performance monitoring, diagnostics, and compliance reporting.

Connexone seamlessly integrates into existing wind farm infrastructure without requiring changes to firmware, protocols, or workflows.

## Solution Components

All ConnexOne hardware pairs are capable to transfer data from logical controllers, or SCADA applications.



## Application

ConnexONE enables secure, policy-driven data transfer from wind farm control systems to external networks—ensuring critical SCADA data, turbine telemetry, and performance reports are shared without exposing operational systems to cyber risk. Data from turbines and control units is collected via standard protocols and passed through a unidirectional flow enforced by the ConnexONE Data Diode. Connexone can collect data directly from wind turbine controller unit or from a SCADA application, practically using any protocol including MODBUS, Profinet, OPC-UA, MQTT etc.

There are different hardware flavors to be used, from a single data collection point support to thousands, for different deployment scenarios. Data can be sent to local data center, or any cloud driven analytic and storage systems.

| ASPECT | BEFORE | AFTER CONNEXONE |
|---|---|---|
| Data Direction | Bidirectional, open to abuse | Unidirectional, physically enforced |
| Malware Entry Risk | Software filters only | Hardware-isolated, no entry path |
| Remote Vendor Exposure | High via VPNs and remote tools | Fully blocked |
| Compliance | Complex to validate | NIS2 / IEC 62443-ready |

# DISCOVER CONNEXITE SOLUTIONS

→ connexite.co.uk

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

contact@connexite.co.uk