

MEETING ROOM OCCUPANCY

3rd PARTY SENSOR SHIELD



PROBLEM

An international legal firm required accurate, real-time data on meeting room usage and attendance to inform future floor space planning.

Without reliable utilisation figures, the firm risked over or under provisioning valuable office space, leading to unnecessary cost or operational inefficiency.

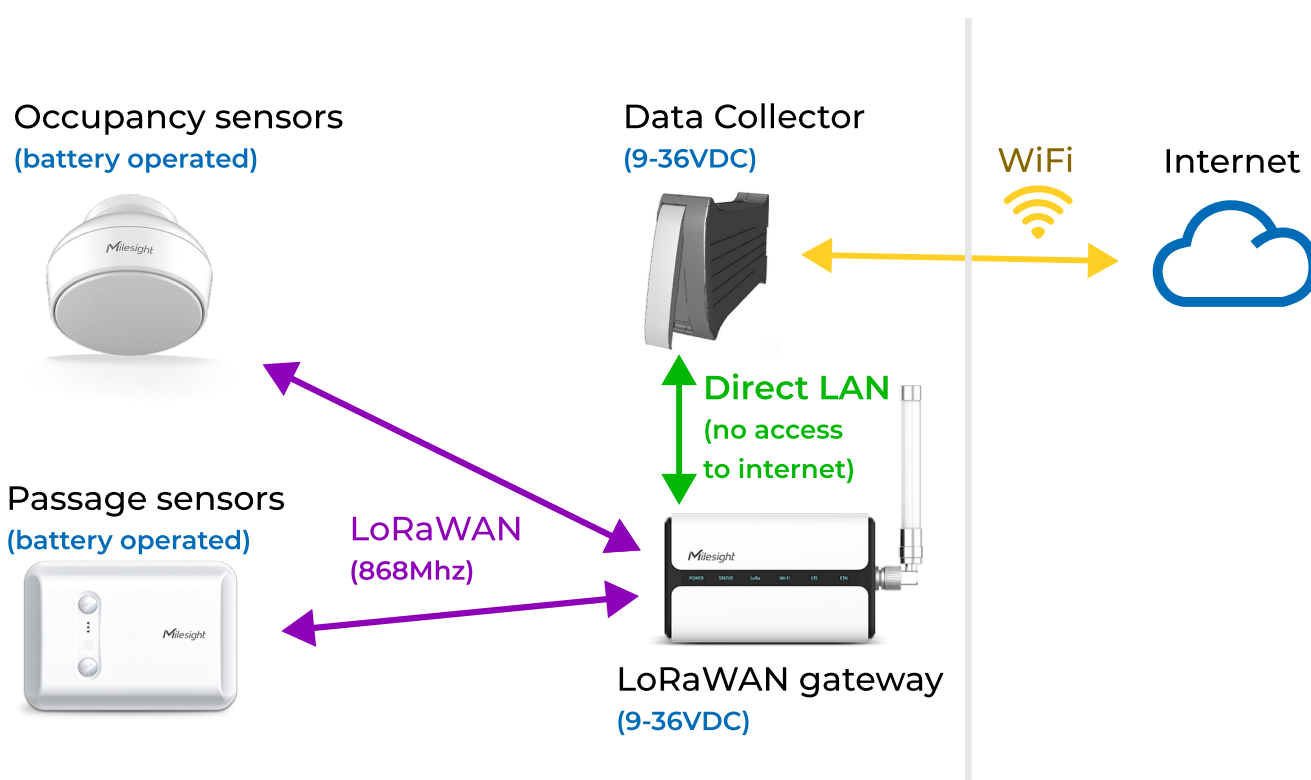
Manual observation was impractical across multiple rooms and floors, and the firm required a scalable, unobtrusive way to capture genuine usage patterns over time.



CHALLENGE

The sensors best suited to detecting room occupancy sent data directly to servers operated by Milesight, with usage figures then returned to the client via an API.

The firm's IT security policy also prohibited any third-party device from connecting to the private corporate Wi-Fi, creating a direct conflict between the operational need for this data and the firm's network security requirements.





SOLUTION

Working with business partner Technik IMS, dbr deployed its Olympus data collection module on site, using BusByte technology to create a secure, isolated collection layer between the sensors and the manufacturer's third-party servers.

This established a physical shield: sensor data was captured and forwarded without ever bridging onto the firm's private network, eliminating the connectivity risk while still delivering the occupancy and attendance data the client needed.



BENEFITS

- Reliable, room-by-room occupancy and attendance data for space planning
- No third-party connectivity to the firm's private network
- Wider choice of sensor hardware, regardless of manufacturer or origin
- Low-disruption deployment, no network reconfiguration required
- Innovation delivered without compromising security standards



CONTACT

mail@dbr.co.uk
+44 1268 442888

