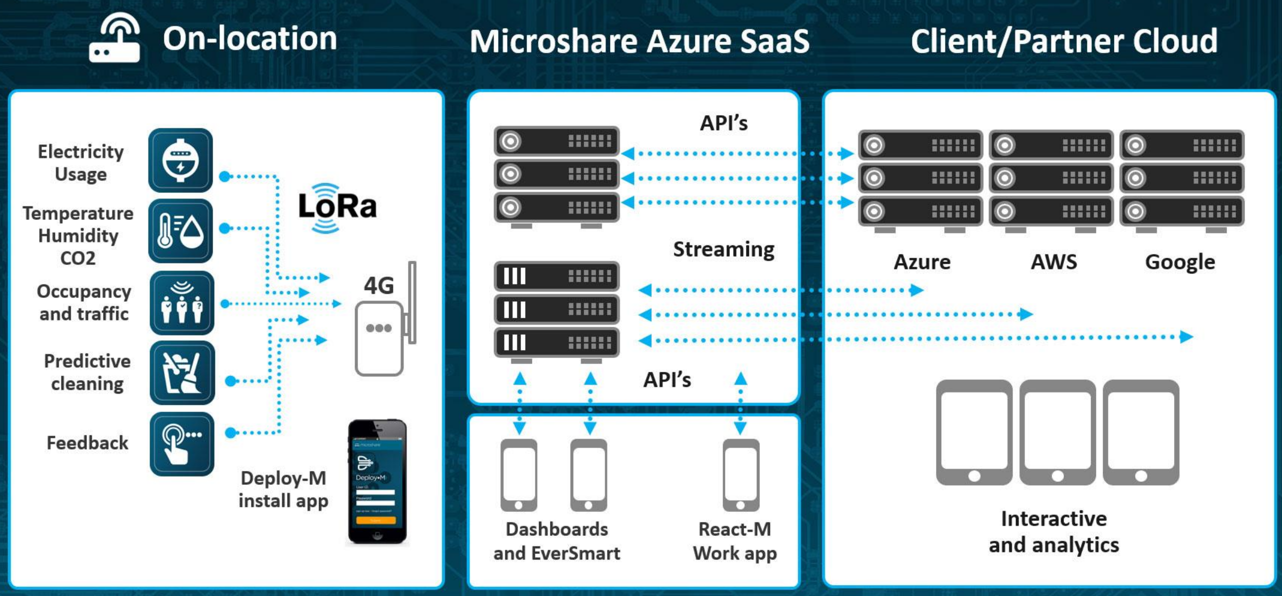
microshare
unleash the data



microshare unleash the data
eversmart™
S Sensing Network

Microshare's platform & infrastructure security overview

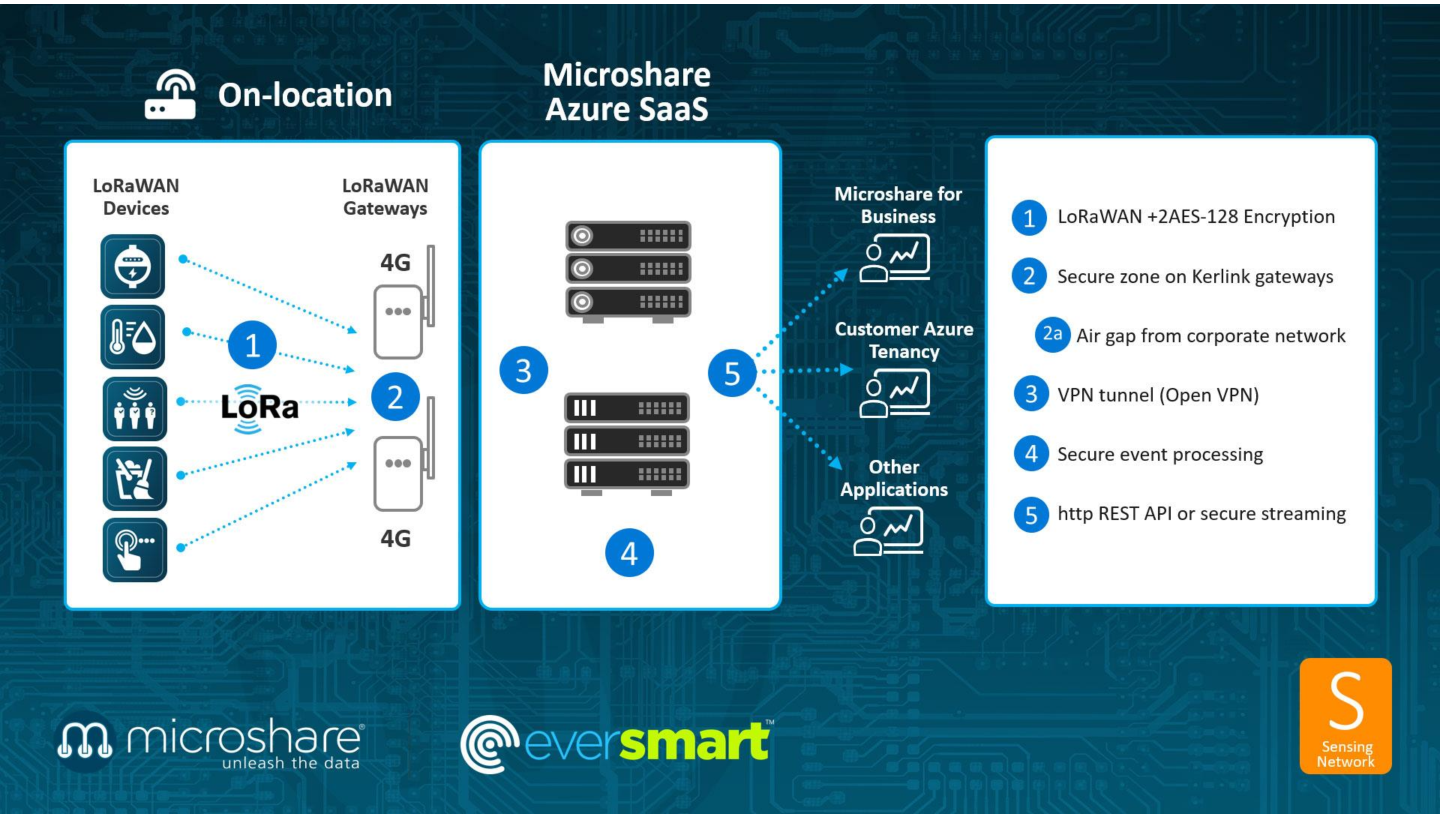
As a trusted provider of Internet of Things (IoT) connected devices to enterprise customers all over the world, **Microshare offers a comprehensive security approach**, based on a combination of proven architecture patterns, our patent-pending data ownership platform and best practice in device implementation. Our SOC 2 compliant approach ensures that data from and to edge devices, such as sensors and actuators is always secured throughout our connectivity layer, our **Microsoft Azure multi-tenant cloud** all the way to our customers' own cloud tenancies or in-house systems.

CYBER ESSENTIALS
AICPA SOC aicpa.org/soc4so SOC for Service Organizations
IASME GDPR

What, how, why?

Our solutions are deployed primarily on a **private network**. We ensure the data integrity at the network level as each device is assigned to our own “NetID”

> *Microshare only uses devices which join the network using **Over The Air Activation** which is more secure than Activation By Personalization (ABP)*



1. LoRaWAN +2AES-128 Encryption
2. Secure zone on Kerlink gateways
   - 2a Air gap from corporate network
3. VPN tunnel (Open VPN)
4. Secure event processing
5. http REST API or secure streaming

We’ve standardized on the gateways provided by **Kerlink**. This has the benefit of **completely isolating the Microshare devices from any corporate network**: Microshare devices **never touch** the Ethernet or Wi-Fi networks in customer locations, so none of the edge devices can be used as a back door to the systems operating within the corporate network.

What, how, why?

An OpenVPN connection is maintained between the on-site gateway and the Microshare cloud platform ensuring the authenticity of the connection and allows the Microshare operations team complete remote control on the devices to maintain performance and patch them with new software required if/when new threats are detected.

Microshare is committed to leading the way to make IoT deployment safe as we scale to a billion devices and beyond!

Hosted on the Microsoft Azure cloud, all data on the Microshare platform is tagged with owner details and digital twinning information so it can be identified in context.

Data shared with trusted external platforms, such as client/partner clouds or apps is always done **using the most secure methods available**.