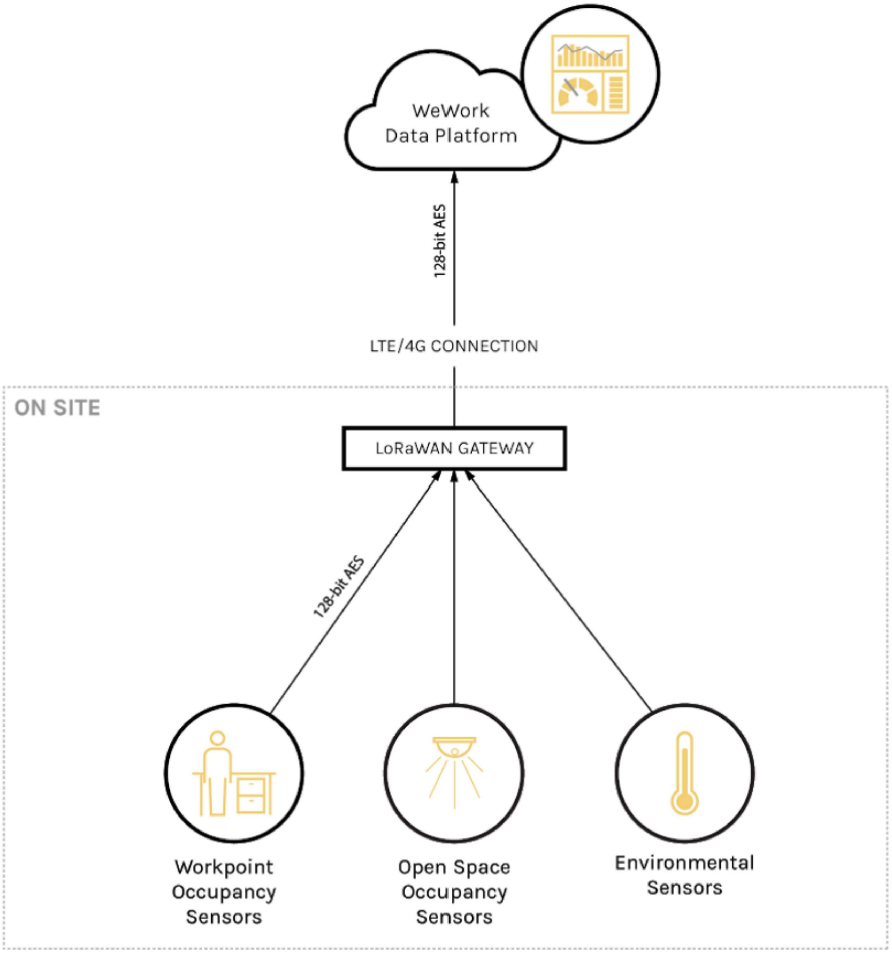
Spatial Insights: Overview

WeWork's Spatial Insights technology helps your organization to understand and optimally utilize workspace. We use lightweight, battery-powered sensors to measure the occupancy of work desks and open spaces, as well as the temperature and lighting conditions in larger workspace environments. Sensors do not collect personal information.

Our sensor system does not use or communicate with your Wifi network; it runs independently using a cellular connection. All communication is secure, and data is stored using cloud technology.

Infrastructure

WeWork's Spatial Insight sensors collect anonymous numerical data using motion and passive infrared technology. Data is transferred wirelessly, using LoRa connectivity, to a locally-installed gateway device. The gateway sends data to our cloud servers using an LTE network.



Privacy Details

WeWork's Spatial Insight sensors do not use or contain cameras. They detect motion and measure space occupancy using passive Infrared technology. Sensors do not uniquely identify individuals or record any personally identifiable information (PII).

Sensor Installation

Sensors are installed in your workspace by WeWork's Spatial Insights deployment team using architectural floor plans and WeWork's own Spatial Insights mobile deployment application. Sensor data is measured and verified during installation in order to ensure successful deployment. Spatial Insights deployments:

- Do not require any work by your organization's IT team (other than providing access to a secure physical location with a dedicated power source for our gateway)
- Do not use any of your internal communications networks or data resources
- Are maintained remotely and patched as necessary by the WeWork Spatial Insights deployment team

Data Collection

All Spatial Insights sensors (desk occupancy sensors, open space occupancy sensors, and environment sensors) are anonymous by default. The sensors collect data but do not store it; they do not contain a physical storage mechanism. Data collected by the sensors is stored on our secure AWS-hosted servers.

The following table shows data collection specifics for each sensor type.

Workpoint Occupancy Sensors	**Open Space Occupancy Sensors**	**Environment Sensors**
Mounted under desks or tables to measure occupancy or vacancy of meeting rooms and desk areas.	Mounted overhead and deployed on a grid to determine utilization of large open spaces.	Wall-mounted to study workplace environment and potential impact on experience and utilization
Data Points: ● Occupied (Boolean) ● Motion Events (Integer) ● Reporting Interval: on status event change and every five minutes ● Coverage area: 20"-40"	Data Points: ● Motion Events (Integer) ● Reporting Interval: On status event change and every five minutes ● Coverage area: 8'x8'	Data Points: ● Temperature (decimal, Celsius) ● Humidity (decimal) ● Light (decimal) ● Reporting interval: five minutes

(depending on mounting location)		

Note: Data reporting intervals are customized based on implementation goals.

Sample Sensor Payload


```
{
  "humidity": 53,
  "irExternalTemperature": 21.3,
  "irInternalTemperature": 22.2,
  "motion": 0,
  "occupancy": 0,
  "temperature": 21.2,
  "vdd": 3537
}
```


Security and Data Integrity

All data is anonymous and contains no personally identifiable information (PII).

- Remote access to the gateway is secured via a 2048-bit SSH-2 RSA key.
- No data is stored on the sensors.
- All data transmitted from the sensor to the cloud is 128-bit AES encrypted end-to-end.
- For devices to transmit data through a gateway, each device must have a unique App EUI and App Key. Devices must also be registered on our network server and management system, preventing rogue device access.
- Access to our management system is secured through SSO.
- Devices are LoRa Alliance Certified.
- Our servers are hosted on the secure Amazon Web Services (AWS) platform.
- AWS Shield protects our AWS infrastructure from attacks.
- Amazon data centers have been accredited under ISO 27001, SOC 1 and SOC 2/SSAE, PCI Level 1, FISMA Moderate, and Sarbanes-Oxley (SOX).
- A Virtual Private Cloud (VPC) is used to isolate network traffic, data, and other resources from other AWS customers.