XY SENSE

Brief

Privacy & Security

XY Sense is private by design.

Here at XY Sense, we know that property teams want to use office utilization data to create awesome workplace experiences, not to invade people's privacy.

That's why we spent 2+ years in R&D developing our sensor hardware and proprietary AI to ensure that we deliver the level of real-time occupancy accuracy today's property teams require without compromising the privacy or information security the people in the space.

XY Sense has been engineered to be both 'private-by-design' and 'secure-by-design'.

This brief explains the privacy-preserving features and security architecture of XY Sense. It is intended for both technical and non-technical audiences.

If you have a question regarding the information presented in this brief, please reach out via info@xysense.com and our team will assist.

100% Anonymous

The sensor only records 100% "X" and "Y" ground point coordinates and anonymous metadata. Not capable of identifying individuals or collecting personal information.

Privacy Compliant

GDPR and CCPA privacy regulation compliant. Sensor does not capture or store personally identifiable information.

Secured Edge Processing

All occupancy data processing is performed 'at the edge' on the sensor itself. Sensor sightings are never sent, stored or retrieved. Even during setup.

Security Best Practices

Information security is part of our DNA. We've architected our solution according to industry best practices and follow strict protocols around the security and protection of customer information. XY Sense is an ISO27001 certified company.

How it works.

100% Anonymous Data Capture.

We're called XY Sense because our advanced sensors leverage the latest developments in machine learning to capture and process the "X" and "Y" occupancy coordinates of people relative to a sensor in real time.

There is no way to identify individuals from XY Sense data. Unlike badge swipes, under-the-desk PIR or device agents, XY Sense captures data passively about the space, never an individual. And with scene processing occurring on each individual sensor device, we've engineered our solution so that images are never sent, stored or retrieved.

Only 100% anonymous (and fully encrypted) occupancy data is made available via our secure analytics platform for workplace reporting and display applications.

Sensor Output Example.

Example of encrypted, anonymized sensor data. (Converted to JSON structure)


```
[
   {
       "Timestamp": "2019-04-16T03:19:26Z",
       "Sightings": [
           {
               "Bbox": [
                   { "X": 615, "Y": 311 },{ "X": 546, "Y": 241 },
                   { "X": 596, "Y": 191 },{ "X": 665, "Y": 260 }
               ],
               "GroundPoint": { "X": 630, "Y": 280 },
               "ReId": null,
               "Score": 0.7373047
           }, ...
       ]
   }
]
```


When we say no images leave the sensor, we mean it.

Raw sensor sightings (images) are never stored, sent or retrievable from XY Sense sensors.

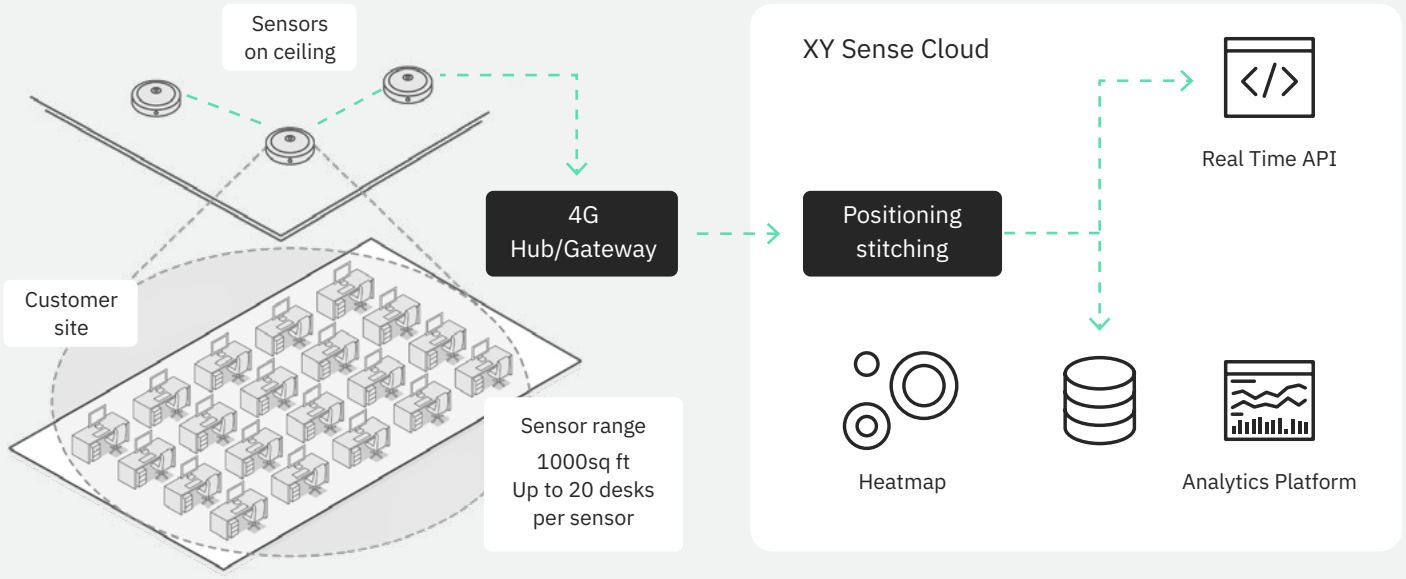
Scene processing happens in real time via our proprietary machine learning algorithm with each device securely processing information independent of other sensors. All data is fully encrypted from the sensor to the cloud using the MQTT protocol and TLS1.2 encryption over port 8883.

We also monitor all sensors in real time to alert on any abnormal behaviors or connection issues to make sure your sensor continue to work as intended.

Even if you were to pull down a sensor and physically open it up, you would not find any images on it, or any other information relevant to the surroundings or customer.

How it works.

Anonymous Data Processing.



1. Real-time, anonymous data capture

When installed and in active mode, the sensor works continuously to capture raw sightings within the wide-range sensor zone (1,000sqft/ 95m2) every 2 seconds.

Each sighting is processed in real time, locally on the 'edge of the device' and converted into 100% anonymous 'X' and 'Y' coordinates of people moving in the sensor coverage range.

The raw sighting is simultaneously destroyed after processing. This means that the sensor only ever records 100% anonymous scene coordinates. Raw sightings are never recorded, stored, sent or retrievable. Even during setup.

2. Data processing at the edge

Processed data is then transmitted via an encrypted MQTT connection to XY Sense's cloud platform through an on-premise 4G hub. Customers have the option to configure the sensors to use their corporate network and firewall. XY Sense's unique sensor daisy-chaining capabilities allows for multiple sensors to connect to one 4G hub.

3. AI powered position stitching

Encrypted, anonymous sensor data is then processed by proprietary algorithms on the XY Cloud Platform to deliver accurate positional stitching between sensor sightings. This enables full floor plan coverage without duplicates.

4. Real-time updates to analytics & booking integrations

Having stitched real-time sightings together and normalized against the mapped floor plan, sensor data is then pushed to both our real-time API feed and XY customer analytics platform to update dashboards, wireless e-labels and smart booking systems.

This processing happens in near real-time with updates delivered to XY customer analytics platform every 2 seconds. This means that end-user tools such as kiosk views of floorplans with available seats are updated in real-time.

How it works.

Encrypted Data Flow.

The diagram below highlights the flow of data between the components. Sensors connect to the cloud via the XY Sense Hub connecting directly to our IOT platform. This is via HTTPS / Encrypted MQTT over 4G.

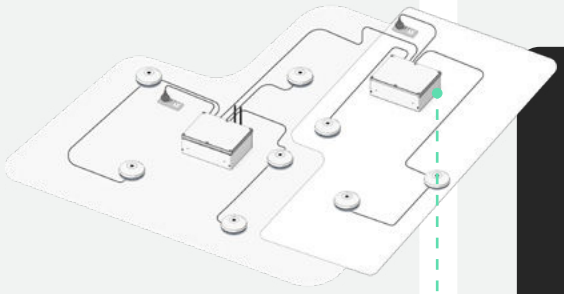
More detail on our platform architecture can be provided upon request.

Customer's Network

No connectivity unless required.

Customer Location

Example, floor 5.



Sensors installed in ceiling, connected byCat5e or above delivering power and data. Connected to an XY Sense 4GHub/Gateway.

Data Over Ethernet

- Anonymous X,Y coordinates
- Anonymous person vector

Authentication

- Shared certificates

HTTPS/ Encrypted MQTT over 4G

XY Sense Web Platform

- End user application
- Users access reports, analytics
- Admins can manage configuration & access

Data

Real Time API

- Websocket-based stream of data, real time, per floor. Secured with web tokens.
- Customers control access. E.g. mobile apps, live display kiosks, BI, IWMS or other integrations

XY Sense Cloud Tracker & Processing Pipeline

Processes data from all customer's floors/sites. Analytics engines produce speciality reports and dashboards.

XY Sense IOT Platform

Customer IWMS / Workplace Apps

XY Sense can source floor plans or space type data from existing tools.

E.g. FM Systems, Serraview, CadM,iOffice etc

XY Sense Platform.

What Data Do We Capture?

XY Sense captures the minimum required identification and contact data for users of the XY Sense platform (name, email, title, company) to support authorized platform access.

Some basic workplace information (floorplans, team space allocations) is also required to support the effective translation of captured XY coordinate data into utilization or occupancy information.

All data collected is subject to strict technical and organizational data security measures.

<user name>

<email>

<company>

We take your data security seriously.

XY Sense technology has been designed and engineered using industry best practices for data protection and security.

Every element of our solution - XY Sense hardware, on-site networking technology, cloud-hosted infrastructure and software, as well as our APIs - have been designed to ensure that data is captured,processed, transmitted and stored in a secure manner.

- All data is encrypted from the sensor to the cloud using the MQTT protocol and TLS1.2 encryption over port 8883.
- Sensors are actively monitored. If we stop receiving data, either because of malicious activity or a fault,we are notified and start an investigation. We actively monitor the amount and pattern of data we are receiving from the sensors including memory, CPU and other signs of activity on all sensors.
- Our application is secured via HTTPS/TLS 1.2 over port 443.
- Our application supports, O Auth enabled single-sign on as well as 2-factor authentication.
- We provide regular over-the-air firmware upgrades and security enhancements.
- Our solution (hardware and application) is penetration tested and validated by third parties at minimum on annual basis.
- XY Sense is ISO27001 Certified.

Have a question about privacy or data security?

Our team is here to help, just email info@xysense.com

www.xysense.com