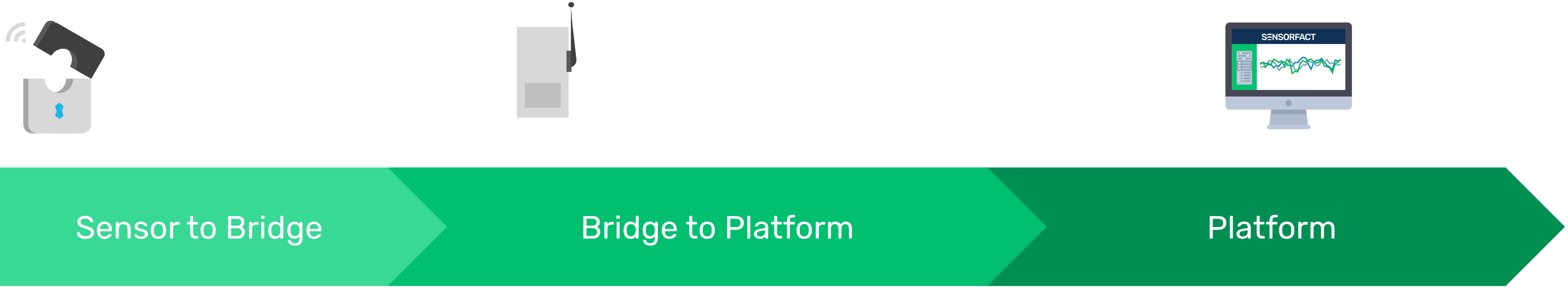
SENSORFACT

Sensorfact Security Overview

Aug 2023



Sensor to Bridge

EnOcean protocol at 868MHz

- Limited range: only accessible with physical proximity
- Wireless data contains no machine or customer information
- No encryption
- Only registered sensors accepted by bridges

Bridge to Platform

Connected via VPN tunnel over public internet, initiated by bridge

- No other outgoing connections necessary
- Sensor data authenticated & encrypted (TLS 1.2)
- Data is buffered on bridge in case of service interruptions
- Security patches and functional upgrades deployed automatically

Platform

Databases and services hosted on AWS Ireland (EU regulations)

- User-facing apps only accessible with login credentials
- Role-based authentication for access to data
- User & customer data separate from sensor data
- All public interfaces encrypted (TLS 1.3)
- Extensive monitoring
- Dedicated DevOps position
- Daily backups

Sensor to Bridge details

EnOcean protocol at 868MHz

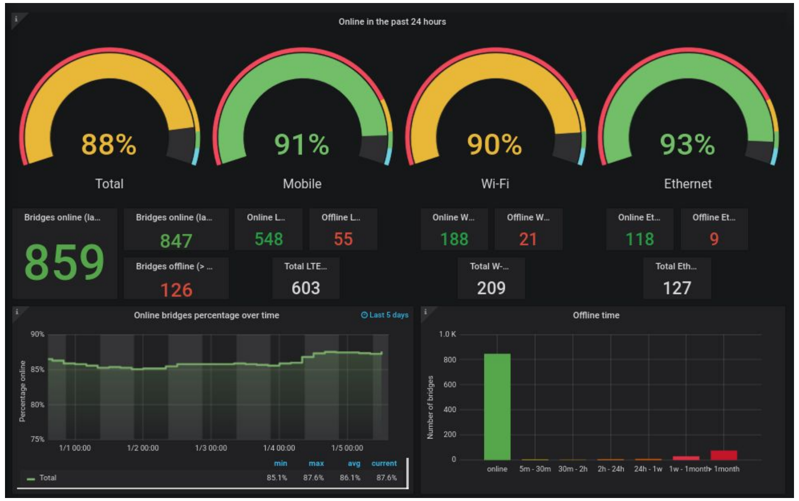
- *Limited range: only accessible with physical proximity*
  Range is 50 meters at most (open field).
- *Wireless data contains no machine or customer information*
  Only a hexadecimal sensor ID and some numbers -- knowledge of the source of the message is needed to successfully interpret the message
- *No encryption*
  This is a possibility with the hardware but we favor ‘plug and play’ ease of access over securing this limited (local, low value) attack surface.
- *Only registered sensors accepted by bridges*
  Configuration is updated hourly over an encrypted and authenticated connection (see Bridge to Platform)

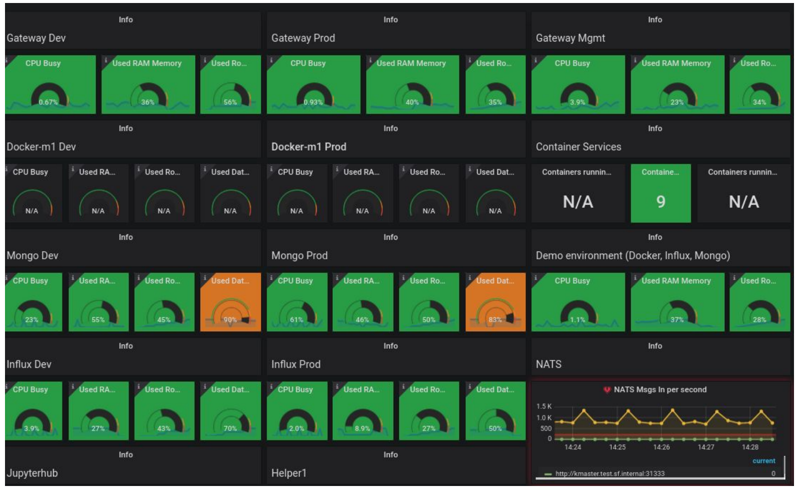
Bridge to Platform details

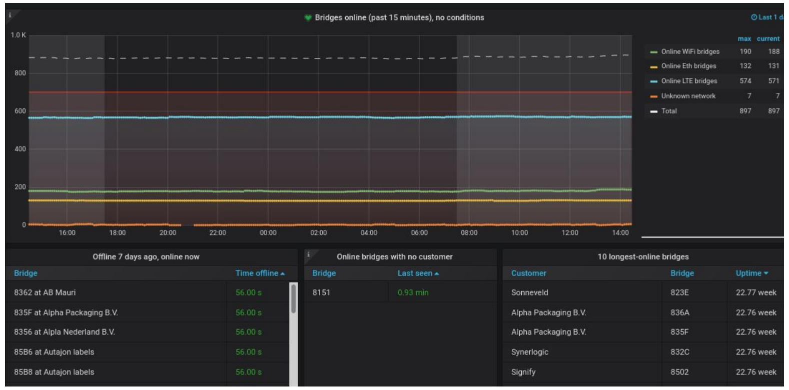
- *Connected via VPN tunnel over public internet, initiated by bridge*
  Each bridge has its own unique certificates, traffic between bridges is not possible.
- *No other outgoing connections necessary*
  All traffic goes over one encrypted and authenticated connection.
- *Sensor data authenticated & encrypted (TLS 1.2)*
  Sensor data is encrypted with TLS another time, to ensure any client sending data to the importer service is known and authentic.
- *Data is buffered on bridge in case of service interruptions*
  Local storage is large enough to potentially store weeks of data
- *Security patches and functional upgrades deployed automatically*
  Software versions are monitored and kept up-to-date

Platform details

- Databases and services all hosted on AWS Ireland (EU regulations)
- Code hosted on private Gitlab repositories
- User-facing apps only accessible with login credentials
- Role-based authentication for access to data
- User & customer data kept separate from sensor data
- All public interfaces encrypted (TLS 1.3)
- Extensive monitoring via Prometheus and Grafana (see examples)
- Dedicated DevOps position
- Full daily backups within AWS
- Separate database instances for inflow and analytics
- Incident evaluation reports when services were interrupted or data was lost, see Incident Reports.
- Production and Development environments on separate VPCs
  All changes are tested in Development first.
- All projects suitably unit tested, end-to-end tests for frontend projects







	max	current
Online WiFi bridges	190	188
Online Eth bridges	132	131
Online LTE bridges	574	571
Unknown network	7	7
Total	897	897

Offline 7 days ago, online now

Bridge	Time offline ▲
8362 at AB Mauri	56.00 s
835F at Alpha Packaging B.V.	56.00 s
8356 at Alpla Nederland B.V.	56.00 s
85B6 at Autajon labels	56.00 s
85B8 at Autajon labels	56.00 s

Online bridges with no customer

Bridge	Last seen ▲
8151	0.93 min

10 longest-online bridges

Customer	Bridge	Uptime ▼
Sonneveld	823E	22.77 week
Alpha Packaging B.V.	836A	22.76 week
Alpha Packaging B.V.	835F	22.76 week
Synerlogic	832C	22.76 week
Signify	8502	22.76 week

SENSORFACT