SECURITY & DATA PROTECTION

Security built in, not bolted on

Yieldly gives you live OEE from any machine without opening up your factory. Production data is encrypted end to end, access is enforced on the server, and the sensor reports out over its own link - so the people who rely on the numbers can trust them, and the people who secure your network can sign off on them.

Encrypted, end to end

Your production data is protected in transit and at rest.

- Encrypted in transit with TLS - on every connection, from the sensor to the app to the API
- Encrypted at rest - the database, file storage and message queues
- The sensor talks to the cloud over a mutually authenticated, certificate-secured channel

Access you control

Strict, server-enforced access so people see only what they should.

- Role-based access plus per-team access groups - granted, not assumed
- Every request is checked on the server; access is enforced at the data layer
- The same controls bind exports, webhooks and integrations - never a wider view

Enterprise identity

Connect your own identity provider and keep your sign-in policy.

- Single sign-on over SAML and OIDC, with multi-factor authentication
- Automated user provisioning and de-provisioning (SCIM)
- OAuth2 for the API, with scoped tokens limited to exactly what each integration needs

Isolated by design

The sensor never touches your machine control network.

- Reports out over its own Wi-Fi or cellular link - not your control network
- No inbound connections to the device, and no open ports to attack
- If the link drops, counts are buffered on the device and back-filled on reconnect - nothing is lost

TLS	SSO + MFA	EU	No inbound
encrypted on every connection	SAML / OIDC, SCIM provisioning	region hosting + data residency	access to the device

HOW IT RUNS

Infrastructure & governance

The platform runs on AWS, with security designed in at every layer - least-privilege access, encryption by default, and automated checks on every change.

Infrastructure & hosting

Cloud	**Runs on AWS, a leading cloud provider**
Region	**Hosted in the EU**
Database	**Managed, encrypted relational database**
Your data	**Isolated and access-controlled by default**
Transport	**HTTPS / TLS enforced on every endpoint**

Least privilege & hardening

IAM	**Resource-scoped permissions - no broad wildcard grants we author**
Storage	**Private by default; public access blocked; SSL enforced**
CI gate	**Automated security checks review every infrastructure change**
Secrets	**Held in managed secret storage, never in code**
Updates	**Devices update over the air with signed firmware**

Governance & data handling

Audit log	**User actions recorded - who did what, and when**
Data handling	**GDPR-aligned, with EU data residency**
Data sharing	**Choose exactly which events leave, and where they go**
Retention	**Operational logs kept to defined retention windows**
Durability	**Raw production data archived in encrypted, durable storage**

IN SHORT

Yieldly is built so that strong security is the default, not an upgrade: every connection encrypted, every user scoped to exactly what they are granted, and every change reviewed before it ships.

PRINCIPLES WE HOLD TO

Least privilege
Every user, token and service gets the minimum access it needs - and no more. Permissions are scoped to the exact resource.

Defence in depth
Access is checked in the app and enforced again at the data layer, so your data stays protected even if one control is misconfigured.

Secure by default
Encryption, private storage and access controls are on out of the box. Nothing leaves the platform unless you turn it on.

Running a security review?
We're happy to walk your IT and security teams through our architecture and controls. Email hello@simple-oee.com.

More detail
simple-oee.com/security