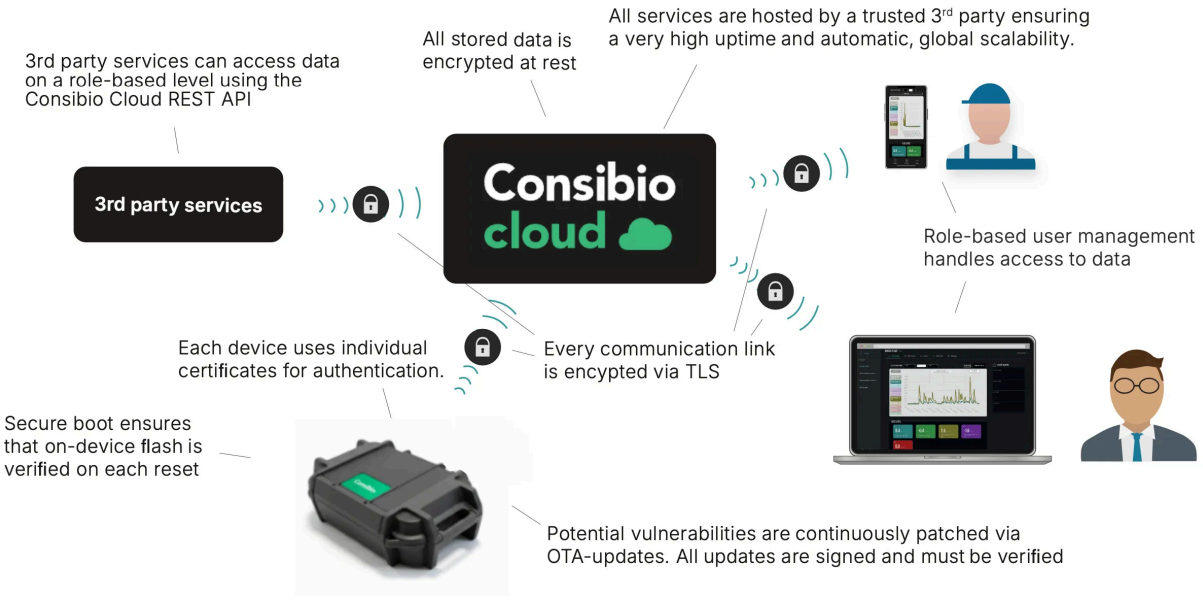
Security in Consibio Cloud

Consibio Cloud collects remote data from IoT dataloggers and handles all data processing, analysis, storage and visualization, alongside the tools needed to manage the dataloggers.

There are three layers in this setup, and the exchange of data between them:

1. **Dataloggers** — sample measurements and send them to the cloud.
2. **Consibio Cloud** — the central hub for storing and managing all data, configurations and analysis.
3. **External accessors** — human users who access Consibio Cloud through the user interface, and service accounts that access data programmatically.

Each layer — and the exchange of data between layers — is protected using industry-standard security practices:



Dataloggers

- Uses a secure boot mechanism to ensure that on-device flash is verified on each reset.
- Potential vulnerabilities are continuously patched via over-the-air (OTA) updates. All updates are signed and must be verified before they execute on the device.

- Communication sessions are always initiated by the device going out to Consibio Cloud, so there are no open services or ports on the device — third parties cannot communicate with the devices directly.
- All communication links are encrypted using TLS v1.3.
- Each device uses individual x509 certificates for authentication.

Consibio Cloud

- All services are hosted by a trusted third party, ensuring high uptime and automatic, global scalability.
- All stored data is encrypted at rest.
- Multiple services continuously scan all activity for vulnerabilities or malicious requests.
- All incoming and outgoing communication channels require strong authentication and TLS encryption.
- All data is divided into sandboxed **projects**. Users are granted role-based access to data at the project level.
- Data backups are performed daily and stored for at least 1 month.

Users and external accessors

- Role-based user management controls access to data.
- Third-party services can access data at a role-based level using the Consibio Cloud REST API.
- All unauthenticated access requests are denied.
- All data requests must be made over a TLS-encrypted link.

Support

Questions about Consibio Cloud’s security? Contact support@consibio.com.