# Thermacell LIV On-Demand Mosquito Repellent System

# Hub Data Usage and Security Overview

**Data Transmitted**

- **Operational device data (via MQTT):** Hub name, LED hue/brightness, Hub temperature, WiFi signal strength (RSSI), system status, error flags, and runtime counters (session, daily, lifetime). For each connected repeller: serial number, temperature, refill/cartridge life, faults, and cap status.
- **Diagnostics (via MQTT):** Memory/heap statistics, WiFi connection quality, error/warning logs.
- **Device identity:** Hub ID, Node ID, and device certificates for TLS authentication.

**Bandwidth per Day**

- The system does not consume a fixed daily bandwidth. Instead, it operates based on throughput, defined as messages per second and payload size. AWS service quotas control and limit that.
- Current throughput is 512 kilobytes per second per connection.

**Data Per Day**

- Each hub sends a maximum of ~3,000 messages per day (ref. https://iot.thermacell.com/home/stats). With message sizes ranging up to 6KB, this results in an estimated data usage of up to 18MB per hub per day, with lower typical usage depending on average payload size.

**Endpoints & Protocols**

- The device communicates with three fixed endpoints, all outbound only:
    - **Primary MQTT** — a1p72mufdu6064-ats.iot.us-east-1.amazonaws.com on port 443 (MQTT over TLS). This carries all operational data, diagnostics and receives commands from the mobile app.
    - **Time Sync** — pool.ntp.org on port 123 (SNTP). Standard network time synchronization.

**Transport Security**

- All data is encrypted with TLS 1.2+ before it leaves the device.
  The connection uses mutual TLS authentication: the device verifies the server using certificate embedded in firmware.
- The server verifies the device using an X.509 client certificate flashed to a secure factory partition during manufacturing. Even on open, unencrypted public WiFi, transmitted data is unreadable by anyone else on the network.

**What the Device Does NOT Do**

- The device does not scan the network.
- Does not open any listening ports.
- Does not access or communicate with any other device on the same network.
- Does not act as a proxy or relay traffic.
- It only makes outbound connections to the 2 fixed hostnames listed above. No location/GPS data, no personal user data, and no audio/video are collected or transmitted.

**Key Security and Privacy Features:**

- Hub and user data are stored or transmitted across multiple AWS services, including Cognito, DynamoDB, and AWS IoT Core. Communication between the hub and the cloud occurs over a secure MQTT channel using public/private key authentication. User-to-cloud communication is handled via HTTPS RESTful APIs, with AWS Cognito managing authentication and authorization. Additionally, Espressif claims to ensure security across four aspects within its architecture (ref. https://rainmaker.espressif.com/en#key-design-principles). Those are:
  - Device Security
  - Network Security
  - Cloud Data Security
  - Security Compliances