EXHALE

CYBERSECURITY FOR BATTERY STORAGE

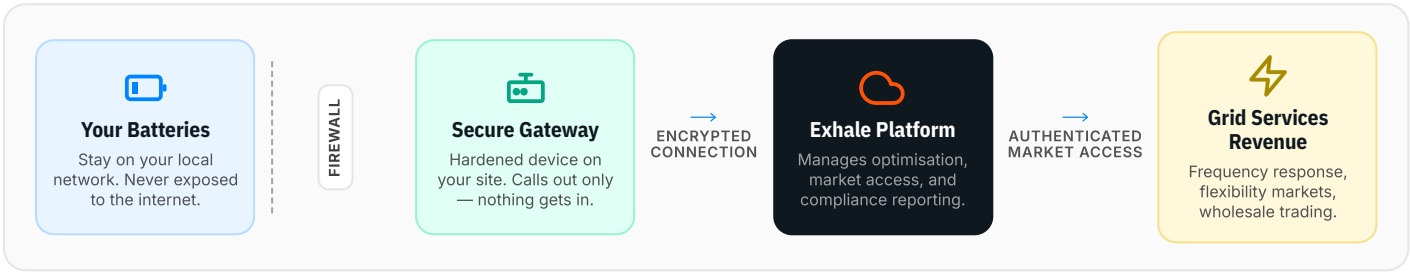
Secure Your Connected Assets

Before a bad actor takes control

Your batteries are remotely managed, but are they secure?

Grid-connected batteries can be charged, discharged, or damaged through their internet-facing control interfaces. A single breached credential could destabilise your site's grid connection or destroy cells through over-charge attacks.

How We Keep Your Batteries Safe



What We Protect Against

Remote Takeover

Attackers exploit internet-facing inverter APIs to seize control of your battery fleet. Our gateway ensures batteries are **never directly reachable** from outside your site.

Equipment Damage

Malicious commands push batteries beyond safe limits. Our gateway enforces **hardware safety limits locally** — even if the connection to the Exhale platform fails.

Grid Disruption

Coordinated attacks use batteries to destabilise local grid infrastructure. Every command is **independently verified** through our platform before being passed to your equipment.

How We Protect You

- **Batteries never touch the internet** — they sit behind our firewall, communicating only with the on-site gateway.
- **The gateway only calls out** — no inbound connections are accepted. Even if someone knows it exists, they cannot connect to it.
- **Every command is signed and logged** — a complete audit trail from instruction to battery response, traceable end to end.
- **Each site has unique credentials** — automatically rotated. A compromise at one site gives zero access to any other.
- **Fail safe during outages** — if the internet or cloud goes down, the gateway holds your batteries in a safe state until connectivity returns.

What You Get

Protection without complexity

We handle the security architecture. You get a hardened, auto-updating gateway device, installed on site, with nothing to configure or maintain.

Revenue from secured assets

Your batteries earn from grid frequency services and flexibility markets — securely, automatically, and with full transparency.

Regulatory confidence

Continuous compliance reporting, performance monitoring, and audit logs — ready for any regulator or insurer who asks.

Complete visibility

Live dashboard showing asset status and security events — securely accessible from anywhere, on any device.

> *"Most battery owners don't realise their assets can be remotely controlled by anyone with stolen API credentials. We built Exhale so that even if credentials are compromised, the physical equipment remains protected by hardware-enforced limits at the edge."*
>
> — Gareth Williams, Co-Founder, Exhale

IEC 62443 · NIS2 READY · NESO COMPLIANT · ZERO TRUST · UK GDPR · POST-QUANTUM READY

Find out how exposed your batteries are

Request a free security assessment of your storage portfolio.

hello@exhale.systems

Exhale Systems Limited · Bristol, UK · Co. no. 16808856