exhale.

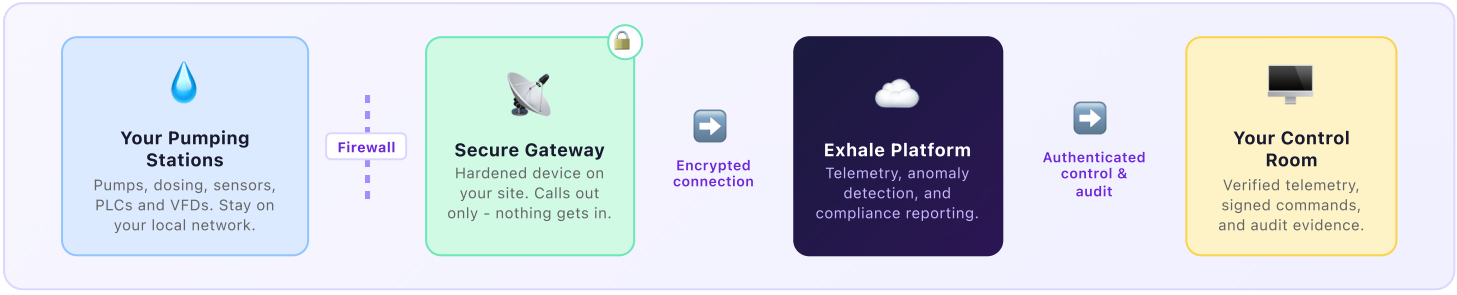
CYBERSECURITY FOR WATER UTILITY OT

Secure Your Pumping Stations
Before someone else controls them

Your pumping stations are now connected - but who else can reach them?

Pumping stations, treatment works, and dosing systems used to be air-gapped. Modernisation programmes have put PLCs and RTUs onto IP networks for telemetry and remote control. The same connectivity that drives efficiency now exposes safety-critical OT to the public internet — and to anyone with a stolen credential.

How We Keep Your Sites Safe



What We Protect Against

Pump & Process Manipulation

Attackers stop pumps to cause flooding or supply outage, or run them at unsafe set-points to cavitate impellers and burst pipes. Our gateway only accepts **signed commands from your authenticated control room** - nothing else reaches the PLC.

Chemical Dosing Tampering

Manipulated chlorine, fluoride, or coagulant set-points create public health incidents that take days to detect. Our gateway enforces **hardware safety envelopes locally** - even a compromised SCADA cannot drive dosing outside safe limits.

Lateral Movement Across Sites

One compromised pumping station becomes a foothold to pivot into the SCADA hub and every other site on the network. Our gateway **isolates each site**, so a breach is contained to a single location and cannot cascade.

How We Protect You

- **Pump-station OT never touches the internet** - PLCs, RTUs, and VFDs sit behind our firewall, talking only to 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** - full audit trail from operator click to PLC ack, evidence-ready for Ofwat, DWI, and NIS Regulations assessors.
- **Each site has unique credentials** - automatically rotated. A compromise at one pumping station gives zero access to any other.
- **Fail safe during outages** - if the link to your control room or our cloud drops, the gateway holds each site at its last known safe state until connectivity returns.

What You Get

Protection without complexity

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

Operational continuity

Pumps stay under your control, not someone else's. Last-known-safe behaviour during outages keeps treatment running and supply flowing while you investigate.

Regulatory confidence

CAF-aligned controls, continuous compliance reporting, and audit logs - ready for Ofwat, DWI, NIS Regulations assessors, or your insurer.

Complete visibility

Live dashboard across every site showing OT health, telemetry, and security events - securely accessible from anywhere, on any device.

> *"Most water companies have been bolting IP connectivity onto pumping stations that were designed before cyber was a consideration. The PLCs work fine, but they have no native authentication and no idea who is talking to them. We put a hardened gateway in front, so modernisation does not open a back door into critical national infrastructure."*
>
> - Gareth Williams, Co-Founder, Exhale

IEC 62443 · NIS2 READY · NCSC CAF · ISO 27001 ALIGNED · UK GDPR · POST-QUANTUM READY

Find out how exposed your pumping stations are
Request a free security assessment of your water-utility OT estate.

hello@exhale.systems
Exhale Systems Ltd · Bristol, UK