tracPulse

SECURITY & DATA PRIVACY — ENTERPRISE Q&A

Your data never leaves your network.

tracPulse is a fully on-premises Health Management Platform for IT Assets. This brief answers the security and compliance due-diligence questions enterprise teams ask — certifications, SOC 2 and ISO 27001 alignment, application security, and data privacy — candidly and specifically.

100% on-premises

All asset data, telemetry and credentials stay on a server you own, inside your network

Zero vendor access

No vendor cloud holds your data; nothing is transmitted outside without explicit admin consent

Signed, fail-closed

Licenses and software updates are Ed25519-signed and verified before use — tampering fails closed

AI stays local

The Ask Pulse assistant runs a local language model on your server — no data sent to any cloud AI

01 · CERTIFICATIONS The SOC 2 / ISO 27001 question, answered honestly

A direct answer — and the context that matters when the software runs entirely inside your own network.

Q **Are you SOC 2 or ISO 27001 certified?**

Not yet — and we won't pretend otherwise. POWERN Automation has not completed a SOC 2 Type II audit or ISO/IEC 27001 certification today. ISO 27001 certification is on our roadmap as the company scales; in the meantime we complete customer security questionnaires candidly and support your own assessment of the product.

OUR POSITION

Those attestations exist to give you assurance about a vendor who *hosts your data*. tracPulse is different: it's deployed entirely inside your network, on your server. We never see, store, or transmit your asset data, so your existing security perimeter and your own certifications continue to govern it. What we can show you instead is exactly how the product is built — and how it produces the evidence *your* SOC 2 and ISO 27001 audits need.

Q Why does on-premises change the compliance picture?

SOC 2 and ISO 27001 primarily attest to a *service organisation's* handling of customer data. With SaaS monitoring tools, your inventory, credentials and telemetry live in the vendor's cloud — so the vendor's certification is essential. With tracPulse:

- The database, the monitoring credentials, and every metric collected live on **your** server.
- There is no vendor account, vendor tunnel, or vendor telemetry pipeline with access to that data.
- Optional product telemetry (crash/health phone-home) is **off until a named administrator accepts a versioned consent** — and a consent-text change stops transmission until re-accepted.

In vendor-risk terms: tracPulse is assessed like deployed software (a data-processing *tool* under your control), not like a data processor holding your records.

02 · COMPLIANCE SUPPORT

How tracPulse supports *your* SOC 2 / ISO 27001 program

tracPulse doesn't just avoid adding compliance risk — it generates the operational evidence your auditors ask for. The mapping below uses ISO/IEC 27001:2022 Annex A and SOC 2 Trust Services Criteria references; it describes how tracPulse supports your program, not a certification claim.

TRACPULSE CAPABILITY	EVIDENCE IT PRODUCES	ISO 27001:2022	SOC 2
Asset inventory & discovery	A complete, continuously refreshed hardware/software register per branch	A.5.9 Inventory of assets	CC6.1
Patch visibility	Missing-update status across the fleet; evidence of a managed vulnerability window	A.8.8 Technical vulnerabilities	CC7.1
Health monitoring, alerts & pulseInsight diagnostics	Continuous monitoring with alert history and investigation trails	A.8.16 Monitoring activities	CC7.2
Admin action audit log	Who did what, when, from which IP — for every privileged/control action in the console	A.8.15 Logging	CC4.1 CC7.2
Approved-software allowlist & unapproved-install alerts	Detection and alerting on unauthorised software appearing on endpoints	A.8.19 Software installation	CC6.8
Endpoint control: USB block, web-access allowlisting, camera/mic disable	Enforced technical controls on removable media and endpoint peripherals, gated per-command and audited	A.8.1 User endpoint devices A.7.10 Storage media	CC6.7
TPM & BitLocker posture reporting	Fleet-wide view of disk-encryption status — flags unencrypted drives	A.8.24 Use of cryptography	CC6.7
Backup, restore & capacity management	Scheduled, integrity-manifested backups with restore verification and retention tiers	A.8.13 Information backup	A1.2 A1.3
Automated remediation scripts with cooldowns & run history	Documented, repeatable operational procedures with execution logs	A.5.37 Operating procedures	CC8.1

03 · APPLICATION SECURITY

How the product itself is secured

Direct answers to the technical due-diligence questions. Every statement below reflects how the shipping code actually works.

Q How do you prevent SQL injection?

All user-supplied values are passed to the database as **bound parameters** (prepared-statement placeholders) — never concatenated into SQL text. Dynamic SQL fragments are limited to code-controlled identifiers (table/column names from fixed internal lists used by schema migrations), which are not reachable from user input.

Q How are passwords and sessions handled?

- Console passwords are stored only as **salted, iterated hashes** (Werkzeug PBKDF2) — never in plaintext or reversible form.
- Access is role-based: **Admin / Support / Management** roles are enforced server-side on every route; operational (write) actions are limited to operator roles.
- Browser sessions are signed with a per-installation random key, carried in an HttpOnly, SameSite cookie, and every state-changing request is **CSRF-protected** with a session-bound token.
- Mobile app access uses short-lived **bearer tokens generated from a cryptographic RNG**; only their SHA-256 hashes are stored, so a database leak does not expose usable tokens. Tokens support refresh and server-side revocation.

Q How are monitoring credentials protected?

The domain credentials used to reach endpoints are **encrypted at rest** (Fernet: AES-CBC with HMAC authentication). The encryption key is a separate file outside the database with restricted permissions — so a leaked database file or backup does not expose credentials. Backups record a key fingerprint, and a restore against the wrong key is detected rather than silently accepted. For deployments that require it, the key can be relocated via configuration to a protected path or secrets-management mount.

Q How do you secure the software supply chain — licenses and updates?

- **Licenses** are Ed25519-signed entitlement blobs issued by the licensing server. The deployed product holds only the *public* key: it can verify but never mint or alter a license. Any local tampering breaks the signature and fails closed.
- **Updates** ship with an Ed25519-signed manifest; every downloaded component is verified against its SHA-256 hash before installation, and a failed update **rolls back automatically**.
- **Endpoint agents** authenticate the server through a vendor-signed server certificate chain (mutual trust), so an agent won't take commands from an impostor server.

Q Is every remote action accountable?

Yes. Every control command (service restart, USB block, shutdown, script run, and so on) is **individually enable/disabled by an administrator** in Settings → Control Commands, and every execution is written to the audit log with username, role, action, target asset, result, and source IP. Detective features are on by default; intrusive ones are opt-in.

Q What about the AI assistant — does it send our data to a cloud LLM?

No. Ask Pulse runs a **local language model on your tracPulse server** (llama.cpp). Questions, asset names and metrics are processed entirely on-box; there is no API call to any external AI provider, and the feature works with no internet connection at all.

04 · DATA PRIVACY What is collected, where it lives, who controls it

DATA RESIDENCY

Everything stays on your server

The tracPulse database, credentials, telemetry history, reports and AI models all reside on the server you deploy — typically inside your LAN with no inbound internet exposure. Retention and downsampling are admin-configurable, so you decide how long history is kept.

DATA MINIMISATION

Device data, not personal content

tracPulse collects machine operational data: hardware inventory, OS and patch state, performance metrics, service and software lists, event indicators. It does not read user documents, e-mail, browsing history or file contents. Personal data is limited to identifiers such as usernames and hostnames.

REGULATORY ROLES

You remain the data controller

Because POWERN Automation has no access to the data, the customer remains the data fiduciary/controller under India's DPDP Act 2023 (and controller under GDPR where applicable). tracPulse functions as an on-premises tool under your governance — no cross-border transfer is introduced by the product.

VENDOR TELEMETRY

Phone-home is consent-gated

Optional product-health telemetry to the vendor is disabled until a named administrator accepts a versioned consent notice that states exactly what is sent. If the notice ever changes, transmission stops until the new version is accepted. Declining never degrades the product.

05 · DUE DILIGENCE What we welcome from your security team

Q Can we run our own security assessment?

Yes — and we encourage it. Because the product deploys in your environment, your team can evaluate it directly rather than relying on a vendor report:

- **Vulnerability assessment / penetration test** of your tracPulse deployment — we support the exercise and remediate what it finds.
- **Security questionnaires** (SIG, CAIQ, or your internal format) — we will complete them candidly.
- **Deployment hardening review** with our team: HTTPS termination via your reverse proxy, network segmentation of the monitoring server, least-privilege service accounts for endpoint access, and OS-level protection of the credential key file.

> **OUR POSITION**
>
> Rather than a certificate about our cloud, you get the software inside your perimeter where your team can test it, firewall it, and audit it. We'll support your assessment and fix what you find — a stronger assurance position for you than a report about someone else's data centre.

POWERN Automation · contact@powernsolutions.in