Security and architecture

Where data is collected, what is encrypted and how, exactly what leaves the machine, who else touches it, and which assurances we cannot yet offer. Written for a security reviewer, not a buyer.

1. Summary

ClawMetry collects agent telemetry **locally**, on the machine that produced it. That is true in every deployment mode. What varies between modes is only where the dashboard that reads that data runs, and whether an encrypted copy is transmitted to a service we operate.

The agent-side component makes **outbound connections only**. It listens on no network-facing port, so deploying it requires no inbound firewall exception and gives us no path into your environment.

The product is **read-only by default**. It observes agents and does not alter their behaviour unless an operator explicitly enables enforcement.

2. Components

Collection daemon	A background process running as the same user as the agent. Reads the artefacts the agent already writes and maintains a local store on that machine.
Local dashboard	A web interface bound to `localhost` that reads the local store. Not exposed off the machine unless an operator deliberately exposes it.
Managed cloud	Optional. Receives encrypted snapshots and serves a hosted dashboard that decrypts them in the viewer's browser.
Enforcement layer	Optional and off by default. Applies budget ceilings and tool policy, and can hold an action for human approval.

3. Data categories

What the daemon collects falls into four categories. A security review usually cares about the third and fourth.

CATEGORY	EXAMPLES	SENSITIVITY
Usage and cost	Token counts, model identifiers, request timing, derived cost	Low. No content.
Activity metadata	Which tools were invoked, which repository, session structure, outcomes	Low to moderate. Names of things, not their contents.
Conversation content	Prompts, agent responses, and tool output as recorded by the agent	**High.** This is the material a reviewer should focus on.
Machine identity	Hostname, platform, hardware profile, node identifier	Moderate.

Conversation content is present because the product's audit and replay functions are worth nothing without it — "an agent modified a file" is not an audit trail. It is also why the encryption and retention design below matters, and why self-hosted deployment exists.

Redaction

Events pass a redaction stage before they are written to the local store, exported, or forwarded to a SIEM. Credentials and key-shaped material that appear in agent output are scrubbed at that point, so they do not propagate to any downstream destination. Redaction is not a substitute for secret hygiene in your agents, and we do not present it as one.

4. Encryption

In transit

TLS to every endpoint. In managed cloud mode, snapshot payloads are additionally encrypted before they are handed to the transport, so TLS is not the only thing protecting them.

Snapshot encryption

Algorithm	AES-256-GCM, authenticated encryption.
Nonce	96-bit, randomly generated per payload.
Key derivation	scrypt, when the key is derived from an operator passphrase.
Key custody	Generated and held on your machine. The key is not transmitted to us and is not recoverable by us.
Decryption	Performed in the viewer's browser. The hosted service stores and serves ciphertext.

THE CONSEQUENCE YOU SHOULD WEIGH

Because we cannot decrypt your snapshots, we also cannot recover them if you lose the key. That is the correct trade for this data, but it is a real operational obligation on your side and it belongs in your runbook, not in a footnote.

At rest

The local store sits on your machine under the operating system's own file permissions and inherits whatever full-disk encryption you already run. In managed cloud mode, what we hold at rest is ciphertext, on encrypted infrastructure storage.

---

5. Egress

In managed cloud mode the daemon makes these outbound connections and no others. In self-hosted and air-gapped modes, none of the first row applies.

DESTINATION	PORT	PURPOSE	CONTENTS
ingest.clawmetry.com	443/TCP	Snapshot sync	Client-side encrypted payload
app.clawmetry.com	443/TCP	Single first-run ping	Anonymous install count
pypi.org	443/TCP	Update availability check	Version query. Disableable.

The local dashboard binds to `localhost:8900` by default; the port is configurable. Where container session discovery is enabled, the daemon reads the local Docker socket.

---

6. Audit and tamper evidence

Audit events are hash-chained: each record commits to its predecessor. Removing or modifying a record breaks the chain, and the product reports the break rather than silently reconciling it. This makes tampering *detectable*. It is not an immutability guarantee, and anyone who tells you a local log is immutable is overselling.

Export is by syslog over RFC 5424, framed as CEF or JSON, to Splunk, QRadar, ArcSight, Elastic, or any compliant receiver. The exporter runs on your side, where the plaintext lives, so enabling SIEM export does not require us to hold decrypted data.

---

7. Retention

Retention is configurable and enforced by the product. Enterprise engagements can set it to any period including indefinite; the retention actually in force is reported in generated evidence bundles, so it is auditable rather than assumed.

8. Subprocessors

Applies to managed cloud mode only. Self-hosted and air-gapped deployments involve none of these for your telemetry.

PROVIDER	PURPOSE	WHAT THEY CAN SEE
Google Cloud Platform	Hosting, database, secret storage	Encrypted snapshots and account records
Stripe	Payments and subscription billing	Billing details. We do not handle card data.
Resend	Transactional email	Email address and message content
Anthropic	AI-assisted product features	Only content submitted to those features
Calendly	Scheduling, where a call is booked	Name, email, meeting time

Destinations you configure yourself — a Slack webhook, PagerDuty, your own SIEM — are not subprocessors of ours. They are your systems receiving your data at your direction.

> **BEFORE THIS GOES INTO A DPA**
>
> The list above is published for orientation and is accurate to the best of our knowledge at the date on this document. The list that binds is the one attached to your Data Processing Agreement. Request it and reconcile the two; if they disagree, the DPA governs and we want to hear about the discrepancy.

9. Supply chain

- A CycloneDX software bill of materials is produced for releases.
- Dependencies are audited automatically for known vulnerabilities.
- Build provenance is recorded for published artefacts.
- Vendored dependencies are byte-compared against their published upstream sources.
- Distribution uses PyPI Trusted Publishing. Windows artefacts are code-signed and timestamped.

These controls map onto the four areas of the CISA Secure Software Development Attestation, which we are in a position to complete.

10. Access control

Available	Account authentication, per-organisation data scoping, an owner and member model with a full or limited access flag, and offline licence verification for air-gapped installations. SHIPPING

In development	OIDC-native single sign-on and a four-level role ladder of owner, admin, member, and viewer. SAML is supported through a self-hostable bridge where a contract requires it. IN DEVELOPMENT
Not built	SCIM provisioning. NOT AVAILABLE

If SSO is a hard requirement for your deployment, say so at the first conversation. We would rather lose a quarter of pipeline than discover it during your pilot.

---

11. Certifications and assurance

We are **not SOC 2 certified** and **not ISO 27001 certified**. We do not display badges for either, and we will not describe an unstarted audit as "in progress".

What is available in place of a certificate:

- A CSA CAIQ self-assessment. In preparation; the current draft is available on request.
- This document, and the architecture it describes.
- A Data Processing Agreement with the binding subprocessor list.
- A compliance evidence bundle generated from your own environment during a pilot.
- The source code, which is MIT-licensed and public.

Where a certification is genuinely required, we will scope and commit to it inside the contract that requires it, rather than claim it beforehand.

---

12. Vulnerability disclosure

A security policy with a disclosure address is published in the public repository. We would rather hear about a finding from you than from a customer's incident review, and we do not threaten researchers.

Rangehead is a trading name of Instalabs LLC, Wyoming, United States.
Rangehead is the commercial home of ClawMetry, an open-source project at github.com/vivekchand/clawmetry.
Questions: vivek@rangehead.com · rangehead.com
This document describes the product as at the version and date above. Where it conflicts with a signed agreement, the agreement governs.