Air-Gap & No-Telemetry Statement

Sunbeam Control — AI Workforce Operations Platform

Issued by: Mishki Ltd trading as Sunbeam Control
Version: 1.0
Date: March 2026
Contact: legal@sunbeamcontrol.com

This statement is provided for organisations operating in restricted, classified, or air-gapped environments, and for information security teams that require confirmation of Sunbeam's telemetry posture before deployment.

1. Summary Statement

Confirmed Sunbeam Control can be deployed and operated in a fully air-gapped environment with no internet connectivity. No scan data leaves the machine being scanned in the standard product configuration.	**Confirmed** Sunbeam Control collects zero telemetry, usage statistics, crash reports, or diagnostic data from the Customer's environment in any product mode (Trial, Pro, or Enterprise).
Air-gap compatible	**Zero telemetry**

2. Air-Gap Compatibility

2.1 What Works Without Internet

The following Sunbeam capabilities function fully without any internet connection:

- Network scanner — scans local network; makes no outbound connections to the internet
- Workstation scanner — reads local files only; makes no outbound connections
- Egress scanner — observes existing outbound connections; does not create new ones
- Cloud scanner — uses Customer-provided credentials to call cloud APIs; connection is to the cloud provider, not to Sunbeam
- PDF and CSV report generation — entirely local; no upload
- CLI mode — all flags function without internet
- Licence validation — validated locally in v2.x; no phone-home
- Signed and timestamped evidence (v2.6.0+) — SHA-256 and HMAC operations are local; NTP check is optional
- Change detection (v2.7.0+) — compares against local scan history; no internet required
- Central Server (v2.5.0+) — deployed on Customer infrastructure; network is internal only

2.2 What Requires Internet (Optional Features)

The following two features require internet access but are non-essential and can be disabled:

- Version check: at launch, Sunbeam performs a GET request to check for a newer version. This can be disabled by blocking the URL pub-df3ef38b62634b9286a3dc8a6e2a0853.r2.dev at the network level. The product functions normally if this request fails.
- Fingerprint update: Sunbeam checks for updated AI fingerprints. This can be similarly blocked. The product will continue to use the fingerprints bundled with the installed version.

Neither of these requests transmits Customer data. They are GET requests that contain no payload.

2.3 Deployment in Restricted Environments

For deployment in environments with no internet access:

- Download the installer on an internet-connected machine and transfer via approved media
- The installed product functions fully without internet access
- Fingerprint updates can be obtained by downloading fingerprints.json on an internet-connected machine and copying it to ~/.sunbeamcontrol/fingerprints.json
- Licence keys are validated locally — no activation server is required

3. No-Telemetry Statement

3.1 What Sunbeam Does Not Collect

Sunbeam Control does not collect any of the following from Customer environments, in any product mode, in any version from v2.0.0 onwards:

- Scan findings or any portion thereof
- Machine identifiers, hardware fingerprints, or MAC addresses
- User behaviour within the application (clicks, navigation, feature usage)
- Error reports or crash dumps containing environment information
- Performance metrics or timing data from Customer systems
- IP addresses of scanned machines
- Names of AI agents found during a scan
- Any data from Customer files, processes, or network

3.2 What Sunbeam Does Collect (Limited, Non-Customer Data)

The only outbound requests made by Sunbeam that could be considered data collection are:

- Version check request: the IP address of the machine making the request may be logged by Cloudflare in standard server logs, as with any HTTP request. This is an IP address only — no payload, no Customer data.
- Fingerprint update request: same as above.

These logs are subject to Cloudflare's standard data retention policies and are not used by Sunbeam for any analytical purpose.

3.3 Licence Validation

In v2.x (current), licence keys are validated locally using a regex pattern match. No licence validation request is made to any Sunbeam server. Remote licence validation is planned for a future SaaS tier but is not present in any current version.

4. Verification

Customers who wish to verify these claims independently may:

- Use a network monitoring tool (Wireshark, Little Snitch, or equivalent) to observe all outbound connections made by the Sunbeam scanner process
- Review the open-source egress scanner module, which uses psutil to observe connections rather than create them
- Run the scanner in a sandboxed environment with outbound internet blocked and confirm full functionality
- Request the source code of the scanner module under an NDA for code review

The only outbound connections you should observe are the version check and fingerprint update GET requests to pub-df3ef38b62634b9286a3dc8a6e2a0853.r2.dev, and any Customer-configured integration endpoints (webhook, Splunk, Slack) if those flags are used.

5. Statement of Accuracy

This statement is accurate as of March 2026 for Sunbeam Control versions v2.0.0 through v2.7.0. If Sunbeam's telemetry posture changes in a future version, this statement will be updated and customers with active licences will be notified.

Issued by: Mishki Ltd trading as Sunbeam Control

Contact for technical verification: legal@sunbeamcontrol.com