Data Map

What Sunbeam Control Collects, Stores, and Transmits

Issued by: Mishki Ltd trading as Sunbeam Control
Version: 1.0
Date: March 2026
Covers: Sunbeam Control v2.2.0 – v2.7.0

This document provides a precise, line-by-line account of every category of data that Sunbeam Control reads, generates, stores, and transmits. It is intended for information security teams, DPOs, and technical evaluators conducting vendor due diligence.

1. Data Read During a Scan

Data Category	Source	What Is Read	What Is Recorded
Local IP addresses	Network interface	Your machine's /24 subnet	IPs with open ports
TCP port state	Network probe	Port open/closed on 60+ ports per host	Open ports only
HTTP response	Network probe	Title, Server header, body snippet (first 512 bytes)	Matched fingerprint only
Outbound connections	psutil net_connections	Remote IP and port of all active connections	Connections matching AI API CIDR ranges only
Browser history	SQLite DB (copied to temp)	URLs visited	Domain names matching 40+ AI domains only
Shell history	~/.zsh_history, .bash_history, fish	Command lines	Lines matching AI CLI patterns only
Environment variables	os.environ	Variable names and values	Names matching 24 AI API key patterns; values never recorded
VS Code extensions	Extension manifest files	Extension identifier and display name	Extensions matching 10 known AI tool signatures
Installed applications	Applications folder / Program Files	Application names	Names matching known AI tool signatures
Application logs	Known log file paths	File existence and last-modified	Existence and timestamp only; content not read

Data Category	Source	What Is Read	What Is Recorded
		timestamp	
Launch agents	LaunchAgents, systemd, Task Scheduler	Service/plist name and program path	Entries matching AI service name keywords
Cloud APIs (if creds present)	AWS/Azure/GCP APIs	Service names, regions, resource identifiers	AI-relevant services only
OS username	os.getlogin(), psutil	Username of process owner or file owner	Username attributed to each finding

2. Data Generated by a Scan

A completed scan produces findings in the following formats, all generated locally:

Output	Contents	Location
PDF report	Cover, executive summary, risk breakdown, findings by surface, compliance mapping, auditor pages	Customer's local filesystem — path chosen by user
CSV export	One row per finding: surface, host, port, service, risk, owner, remediation, compliance frameworks, timestamp	Customer's local filesystem — path chosen by user
JSON output (CLI)	12-field schema: version, timestamp, machine, summary, findings array	stdout or --output FILE — Customer's choice
Signed evidence (v2.6.0+)	SHA-256 hash of findings JSON, HMAC signature, NTP-verified timestamp	Customer's local filesystem — same path as JSON output
Change delta (v2.7.0+)	List of findings added since last scan, list of findings removed	stdout or --output FILE — Customer's choice

3. Data Transmitted

Transmission	Destination	Customer Data Included?	Trigger
Version check	Cloudflare R2 (Sunbeam bucket)	No — GET request only	At launch
Fingerprint update	Cloudflare R2 (Sunbeam bucket)	No — GET request only	At launch if checksum differs

Transmission	Destination	Customer Data Included?	Trigger
Webhook push (--webhook)	Customer-configured URL	Yes — full findings JSON	Customer CLI flag
Splunk push (--splunk-url)	Customer's Splunk instance	Yes — findings as Splunk events	Customer CLI flag
Slack notification (--slack-webhook)	Customer's Slack workspace	Yes — summary + top 5 HIGH findings	Customer CLI flag
Central Server (--central-url)	Customer's self-hosted server	Yes — full findings JSON	Customer CLI flag
Licence check	None in v2.x	Not applicable	Local validation only

4. Data Stored Persistently

Data	Location	Retention
Licence key	~/.sunbeamcontrol/config.json	Until user deletes or reinstalls
Scan history (local)	~/.sunbeamcontrol/history/ (JSON files)	Until user deletes — used for change detection
Output files (PDF/CSV/JSON)	Customer-chosen path	Customer's responsibility
Central Server findings (v2.5.0+)	SQLite on Customer's server	Customer's responsibility
Signed evidence files (v2.6.0+)	Same path as JSON output	Customer's responsibility

5. Data Never Collected

The following are explicitly excluded from all Sunbeam data processing in every product version:

- Environment variable values (API keys, tokens, passwords, secrets)
- File contents of any kind (documents, source code, configuration files)
- Browser history content beyond the domain name
- Shell command arguments beyond the command name pattern
- Email, message, or communication content
- Keystrokes, clipboard, or screen contents
- Audio or video
- Location data
- Data from applications other than those directly related to AI agent detection
- Telemetry, crash reports, or usage statistics from the Customer's environment