OpsCanvas

SECURITY OVERVIEW · NOVEMBER 2026

SECURITY OVERVIEW: CLOUD ESTATE DATA STAYS LOCAL

How OpsCanvas runs, what it stores, what leaves the machine, and what we share under NDA.

0	0	0
Cloud resource or cost data sent	Credentials collected	Cloud changes it makes

The question: before an AI tool gets context about production, a security team needs to know what it can read, what leaves the machine, and who makes changes. OpsCanvas answers each of those by how it is built, not by policy. It gives the AI tool your team already uses a confirmed map of your cloud, and it runs on the engineer's own machine.

IN THIRTY SECONDS: FOUR FACTS REVIEWERS ASK ABOUT FIRST

WHERE
It runs on your machine

An npm-installed app with a local MCP server. Graph and cost data sit in two local files.

DATA
Cloud estate data stays local

Prompts, resources, cost and credentials stay local. On Pro, published structure syncs to a hosted team workspace.

ACCESS
It never holds your credentials

It reads through identities you approve. One read-only certificate, for your cost export.

CHANGES
Never in the change path

Your AI tool makes changes itself, with your access. OpsCanvas supplies the blast radius first.

1 HOW IT WORKS: THREE PARTIES, ONE CLEAR LINE

YOUR AI TOOL
Claude Code, Codex, Cursor or any MCP client
Its model sees answers, under your agreement.

questions ⇄ answers

OPSCANVAS, LOCAL
MCP server, background service, local files
You confirm what enters the graph in the local app.

read-only →

YOUR CLOUD
AWS, Azure, Google Cloud, Git, Terraform, cost export
Read through identities you approve.

Changes go from your AI tool straight to your cloud, with your access and its approvals. OpsCanvas is not in that path.

2 WHAT LEAVES THE MACHINE: SOFTWARE ADMINISTRATION ONLY

OpsCanvas makes four connections, all to install, update and run the software. None carries cloud estate data.

CONNECTION	USED FOR	CONTROL
packages.opscanvas.io	Program file download, first run and upgrades	Internal mirror supported
registry.npmjs.org	Checking for a newer release	`--no-update-check`
Account service	Registration; pseudonymous telemetry if allowed	Opt out at setup or in the app
app.opscanvas.io	Sign-in; on Pro, the structure you publish	Only for sign-in and Pro

Never sent to OpsCanvas: prompts, answers, cloud resources, cost data, source code or credentials. Optional telemetry is pseudonymous: an install ID, event type, tool and provider names, version and OS.

3 CREDENTIALS AND THE COST SETUP

- **No credential collection:** OpsCanvas uses the identities you approve, such as AWS SSO profiles or an Azure login, in place. Nothing found on the machine is usable until you approve it.
- **One scoped key:** cost setup creates a dedicated IAM role and IAM Roles Anywhere trust anchor. A local certificate gets short-lived access to your export prefix only.
- **Read only:** list and get on the export, plus decrypt for its key if used. No write or delete. You review the template first.

4 AI AND MODELS

- **Your model, your terms:** only the model in your AI tool sees OpsCanvas answers, under your agreement with its provider.
- **No model of our own:** OpsCanvas calls no model. Your AI tool proposes the application structure from your code.
- **You confirm it:** nothing proposed enters the graph until you confirm it. Joins between sources are deterministic.

5 WHERE DATA LIVES, BY EDITION

	OPERATOR	PRO	ENTERPRISE (2027)
Runs	Engineer's machine	Engineers' machines plus your team's Pro account, hosted by OpsCanvas	Your own environment
Credentials, resources, cost	Stay on the machine	Stay on each machine	Stay in your boundary
Sent to servers OpsCanvas hosts	Account details; telemetry if allowed	Plus the confirmed structure engineers publish, synced to your team's workspace: applications, services, environments, repositories and links	Nothing from your cloud

6 DATA AND SOFTWARE INTEGRITY

- **Two SQLite files** in one folder in your user profile, with no credentials or secrets.
- **Verified program file:** checked against a checksum shipped in the npm package `@opscanvas/opscanvas`.
- **Clean removal:** `opscanvas uninstall`, then delete the data folder.

7 CHANGES AND APPROVALS

- **Your AI tool acts:** with your access and its own approval settings. OpsCanvas is never in that path.
- **OpsCanvas writes only its local graph,** and only facts you have confirmed.
- **Agent action controls:** in Enterprise, coming 2027. Design partners now.

8 ENTERPRISE DEPLOYMENT

- **Managed installs:** deploy as a managed MCP server through your AI tool's admin policy, alongside tools such as Intune.
- **Remote wipe:** all OpsCanvas data lives in one known folder an administrator can delete.
- **Restricted networks:** proxies are supported, and the program file can be hosted on an approved internal mirror.
- **Several clients on one workstation:** use a separate OS user or VM per client today.

9 COMPLIANCE AND NEXT STEPS

SOC 2

SOC 2 Type II is planned. Ask us where it stands.

Questionnaires

Send yours. We answer in your format and name any gaps plainly.

Under NDA

A deeper technical review and our security policies.

Contacts

security@opscanvas.ai for vulnerabilities; privacy@opscanvas.ai for privacy.