OpsPocket security overview

SSH, server monitoring and AI agents for Android (iPhone coming) · by Mt7 Private Limited · November 2026

Built so you don’t have to trust us with your servers. OpsPocket is an SSH client, server monitor and AI coding agent chat for the Linux servers you run. It has no account and no cloud: your servers, keys, passwords, commands, files and chats never reach Mt7.

Architecture

- **Plain SSH, phone to server.** No agent is installed on your servers; it uses your existing SSH accounts, keys, permissions and network (VPN, Tailscale, WireGuard and others). The optional alerts-with-the-app-closed feature adds one small helper you can remove from the app.
- **No analytics, advertising, tracking or crash-reporting code.** An automated test fails the build if any is added.
- **What does reach Mt7:** the Pro check (store purchase proof, a random install ID, and Google Play or Apple proof that the app is genuine), AI-answer reports you choose to send, and optional alerts that are encrypted on your server with a key made on your phone, which our relay cannot read. Never server data.

On the phone

- Secrets in the iPhone Keychain or encrypted with an Android Keystore key; left out of the phone’s cloud backups.
- App lock with Face ID, fingerprint or passcode; locks again after a minute away.
- Keys expire after the idle time you choose, and this phone’s key line on your servers gets an end date.
- Waits after 5 failed unlocks; after 10, removes its own key from your servers and erases the phone (can be turned off).
- Key and password screens kept out of screenshots and recordings; lock-screen alerts say only the kind of alert.

On the connection

- Strict host key checking: no connection if a server’s key changes. Ed25519 keys and modern SSH algorithms only.
- End-to-end encryption through jump servers; optional **from=** limit on where this phone’s key works.

Changes to your servers

- Every change and every suggested command is risk-rated and shown in full first; destructive ones need typed CONFIRM plus biometrics.
- AI agent changes wait for approval with your fingerprint or screen lock, unless the agent’s own settings already allow them.
- Read-only servers; private keys, .env files and AI sign-in files locked; a hash-chained audit log signed with Ed25519.

Transparency

- **Network activity** lists every connection the app makes. **Strict privacy** stops everything except SSH to your servers, store purchases and the Pro check, and fails closed.

Certifications

OpsPocket and Mt7 Private Limited don’t hold SOC 2 or ISO 27001 certification today. We offer the design above, and straight answers to your security questionnaire.

Contact

Security questions and questionnaires: **developer@mt7.in**. Report a vulnerability: the same address, with “Security” in the subject; we answer within 2 working days. Details: **opspocket.app/security** and **opspocket.app/privacy**.

Mt7 Private Limited, Bengaluru and Bahraich, India. CIN U68200UP2025PTC233604. This summary describes OpsPocket as of November 2026. No app can be perfectly secure; keep your phone’s screen lock on and its system up to date.