GUARDIAN PLUS

The security questionnaire, answered in advance

Hosting, encryption, access control, audit, AI, the agent, and what Guardian Plus does not do.

Security teams have to verify claims, and vague ones cost everybody a week. This pack answers the questions a questionnaire usually asks, in the order it usually asks them, plainly enough that you can rule us in or out before you book a call. Where the honest answer is a limitation, it is here too.

Hosting and tenancy

- Single-tenant per customer, always. There is no multi-tenant mode.
- Self-hosted on your servers (OS installers or container images) or hosted by us on infrastructure dedicated to your organisation.
- Nothing phones home except a daily licence check.
- Your Suite pairs only with your own product instances and your own secrets.

Encryption

- In transit: every connection is TLS, including the agent’s outbound socket, the browser, and the relay between them.
- At rest: credentials, documents, ticket contents and integration secrets use AES-256-GCM with a fresh initialisation vector per record. A tampered record fails to decrypt rather than returning garbage.
- A key per scope: derived per company, and per person for private vaults. One company’s key can never open another’s data.
- Refuses to start blind: on boot the service proves it can decrypt with the key it was handed, and exits if it cannot.
- Secrets never in the browser: credentials injected into a remote session are resolved server-side.

Terminal and desktop sessions are relayed through the platform: TLS-protected end to end, but not end-to-end encrypted in the cryptographic sense. Shared credentials are decryptable server-side by design, because injection, break-glass and recovery depend on it.

Identity and access control

- Single sign-on across every module with multi-factor authentication (time-based codes, policy and grace periods you control).
- Federation to Microsoft Entra or Okta over OpenID Connect; user sync from Active Directory over LDAPS with deprovisioning and group mapping. SAML is not supported.
- Permissions by action, not by page: dozens of individually grantable actions, assigned through groups, with grants that can carry an expiry date.
- Fails closed: if a permission check errors, access is denied.
- Deactivate someone once and every product session ends immediately.
- A person’s private vault cannot be opened by any administrator, including a super admin, and the attempt is recorded.

Audit and logging

- Every sign-in and every failure is written to an authentication log that cannot be edited or deleted through any interface.
- Service desk history is append-only, enforced by the database rather than by application code.
- Every credential reveal records who, when, from where, and which permission allowed it, including administrator overrides.
- Every suppressed alert records the reason it was withheld.

The audit trail is append-only, not hash-chained. We will not call it tamper-proof.

The AI

- No third-party AI vendor: open-weight models on infrastructure we operate, or on your own if nothing may leave your network.
- It asks before it acts: approve every step, approve the plan once, or unattended; destructive commands stop for a human regardless.
- It inherits your permissions: every tool it calls re-derives the permissions of whoever asked.
- Write actions are hidden from it entirely; your most sensitive documents are never fed to a model.

The agent and the network

- Outbound TLS only: one authenticated socket, dialled out and kept alive. No listener on a managed endpoint.
- Signed installers per platform, each bundling its own runtime.
- Optional, scoped listeners only where you choose them: a collector for agentless devices, an SNMP trap receiver, loopback screen sharing on macOS and Linux.
- Three documented network postures, including an isolated management plane behind a single closable inbound rule.

What Guardian Plus does not do

- We are not SOC 2 certified. A workflow collects SOC 2 control evidence from your estate; that is a tool for your audit, not a certification of ours.
- Encryption is not zero-knowledge. An operator with the master key and database access can decrypt shared items.
- The audit trail is append-only, not tamper-proof.
- Our AI service is ours by default; host the models yourself if the requirement is that nothing leaves your network.

Send us the actual questionnaire

We would rather answer it early than at the end. Deployment documentation, the threat model and the network posture guides are available during evaluation, not after signature. Write to support@guardianplus.ai or book a technical deep-dive at https://get.guardianplus.ai/demo.