Security one-pager

Last updated: April 2026

Overshow is a privacy-first AI assistant that runs on a user's own laptop. Screen frames, meeting audio, OCR text, and transcripts are captured, processed, indexed, and stored locally. Nothing from that capture stream is sent to a cloud service unless the user explicitly enables an integration.

Data boundary (at a glance)

- **Captured data stays on the laptop.** Screen frames, audio, transcripts, OCR text, and embeddings live in a single encrypted SQLite database on disk.
- **AI runs on-device.** WhisperKit transcription, OCR, and semantic embeddings all execute locally; no captured content is sent to a hosted model.
- **Only auth and billing traffic leaves the device by default.** OIDC sign-in and Stripe billing are the sole outbound network paths in the base product. Captured data is never in that path.
- **Integrations are opt-in.** MCP clients and future SaaS integrations (SharePoint, Google Drive, etc.) are off until the user turns them on and authorises them.

Encryption and key management

- **Encryption at rest.** Sensitive text and captured video are encrypted with ChaCha20-Poly1305.
- **Keys in the OS keychain.** Symmetric keys are stored in the platform keychain (Keychain on macOS, Credential Manager on Windows).
- **No cloud replica.** The product does not mirror captures to a server. If the laptop is lost, the data is gone.

Authentication and identity

- **SSO via OIDC** with Google Workspace and Microsoft Entra ID on Enterprise.
- **Single active device per user** on all plans.
- **Session enforcement** at sign-in and on periodic licence checks.

User controls

- **Pause capture.** One switch halts every display and microphone immediately.

- **Ignore list.** Apps, windows, and monitors can be excluded by name; exclusions apply even when the app is in the foreground.
- **Export and delete.** Users can export their own captures and delete them locally at any time.

Admin controls (Enterprise)

- SSO enforcement, device policy, capture policy (which apps may or may not be captured), and AI policy (which models may be used).
- Audit of admin changes and offboarding flow that revokes access and invalidates local stores.

Data retention

- **Captured content.** Free: 7 days rolling. Pro and Enterprise: unlimited, under user control.
- **Account and billing.** Retained for the life of the account plus the statutory retention period.
- **Auth and security logs.** 90 days by default; Enterprise can configure longer.
- **Deletion SLA.** Account deletion requests are completed within 30 days; local stores are wiped on device at offboarding.

Operational practices

- **No telemetry** from the desktop app. Crash reporting is opt-in and scrubbed.
- **Code signing** and notarisation on macOS; Authenticode on Windows.
- **Backups.** Cloud-side backups apply only to account/billing metadata; they do not contain captured content.

Contact

- Security contact: hi@over.show
- Trust Centre: https://over.show/trust-center
- Security overview: https://over.show/security
- Privacy policy: https://over.show/privacy

This document is a summary intended for procurement, IT, and security reviewers. For a formal review package, contact hi@over.show.
