

Your perimeter. Your Sovereign. Not our cloud.

Public AI tools pull company mail and documents into someone else’s platform. A Sovereign does the opposite: computation stays under the owner’s roof. Centurion Limited does not host, proxy, or train on your private world.

THE OBJECTION WE HEAR FROM IT

Teams often assume “AI connected to Microsoft 365 or Google Workspace” means unsafe exfiltration through a vendor cloud. With Sovereign, mail and documents are accessed only under your identity provider’s rules, with tokens kept on the owner’s machine. Centurion Limited never sits in the middle of that traffic.

SECURITY BENEFITS OF THIS MODEL

Owned hardware, owned data The Sovereign lives on customer-owned hardware. Private chat, documents, and mission work stay with the owner — not in a multi-tenant AI product.	Crypto Chat on your network The iPhone companion talks to the Sovereign through Crypto Chat: end-to-end encrypted on the owner’s network. Public chatbots have no equivalent.	Fully offline when policy requires When nothing may leave the room, Sovereign can operate without the public internet. Connectivity is a choice, not a dependency.
No stranger skill store Sovereign does not install skills from unknown vendors. It builds what the owner needs locally, so third-party skills cannot quietly leak mail or documents.	Human approval for consequential steps Serious actions stay under human authority. Default approvals.mode: manual ; hardline blocklist cannot be turned off by YOLO.	We do not train on your content Centurion Limited does not receive private Sovereign inference data to train shared models. Your mail and documents are not our product fuel.

COMPANY EMAIL — BEST PRACTICE

Shared rules Approve the same patterns used for any trusted desktop client: OAuth under your tenant, least privilege, revocable consent, no third-party mail relay. - Mail processed on the Sovereign under the owner’s roof - Centurion Limited does not proxy, store, or train on company mail - IT retains control through the IdP; revoke anytime - Air-gap: leave mail disconnected — Sovereign still works offline	Microsoft 365 Prefer Microsoft Graph with Entra ID — not shared passwords or unmanaged IMAP. - Register an app in your Entra tenant - Delegated access for a named user (app-only only if policy requires) - Least-privilege Graph mail scopes - Admin consent as required - Tokens only on the Sovereign — never in Centurion Limited systems - Revoke/rotate from Entra anytime	Google Workspace Prefer Google OAuth with a Workspace-admin-controlled client — not passwords. - Create an OAuth client under your organisation - Allowlist in Workspace Admin as required - Least-privilege Gmail scopes only - Tokens only on the Sovereign - Revoke from Workspace Admin or the user account - Do not route mail through a Centurion cloud gateway
--	---	---

OS CONTROLS IT CAN VERIFY

Approvals & tools Default manual approval for dangerous commands; configurable toolsets; MCP env filtering strips secrets unless explicitly allowed.	Gateway auth Default-deny messaging access. Empty allowlist = nobody. Pairing and allowlists gate who can talk to the agent.	Memory Horizon / Vault Hot Cache + Session Recall by default. Vault is opt-in encrypted long-term memory — deliberate propose/commit, not transcript dumps.
--	--	---

CONSERVATIVE ROLLOUT (OWNER-FIRST)

Phase 1 Owner / CEO only Dedicated host. Manual approvals. No YOLO. No messaging gateway.	Phase 2 Add Remote Pair that owner’s iPhone only. Review logs and provider traffic.	Phase 3 Optional Vault Init + unlock for sealed long-term memory. Still owner-only.	Phase 4 Expand carefully Allowlists, IdP mail review, then more users; Docker if isolation required.
---	---	---	--

What we do not claim. We do not claim FedRAMP, SOC 2, IL ratings, or military authorisations. Our position is architectural: owner-controlled hardware, encrypted private chat on your network, optional offline operation, and IdP-governed connectors. For a private security questionnaire or architecture review, contact us.