

Paxvian Security Whitepaper

How the assurance service works, and the safety discipline it enforces

Paxvian is an owner-authorized, evidence-first security assurance service. It shows a customer what is exposed about the assets they own and how an attacker could combine that exposure. The assessment is conditional and evidence-backed, and nothing is ever executed. This paper is for a security or procurement reviewer. It describes what the service does; it is not a certification or a guarantee.

Evidence-first method

Every finding separates five things: the observed evidence Paxvian actually collected; the attacker objective being evaluated; the conditions that would still have to be true for that objective to succeed; the potential impact if they were; and the chain-breaker control that reduces the risk.

“Incomplete” and “unassessed” are first-class outcomes. Missing evidence never becomes a clean result, and a missing control never becomes proof of compromise. A candidate with insufficient evidence is marked ambiguous or excluded. It is never silently promoted to verified.

Nothing is executed

Paxvian performs no offensive or active security testing. It does not scan, exploit, test credentials, establish persistence, evade controls, cause denial of service, or touch any system the customer does not own and has not verified.

Reachability and attack paths are computed deterministically over the declared topology and owner-supplied configuration. Attacker's-eye output is always conditional and clearly marked as not executed. Paxvian never produces a “how to compromise” playbook.

Owner authorization and scope

Technical checks are owner-authorized and non-exploitative only: passive public evidence plus configuration checks on assets the customer has verified they own. Every engagement records the authorized scope and that nothing was executed.

Inputs are pseudonymous by design. The topology intake rejects IP/CIDR-looking and secret-looking labels, and a personal recovery phone number is stored only as an owner-scoped alias, never as a real number.

Data handling and durability

Customer state is held in per-purpose SQLite databases and replicated continuously off-host with Litestream to an S3-compatible object store. A non-destructive restore drill (paxvian-verify-persistence) verifies every replica and SQLite integrity before a pilot begins.

Retention is bounded and account deletion is honored end-to-end: erasing an account removes its records across every store. Assessment topology for the sample and demo flows is not persisted.

Access control and audit

Business access is role-scoped: Owner, Security administrator, Analyst and Executive viewer, each with least-privilege rights over members, projects, evidence, reports and the access audit. Only the owner may grant owner-only roles.

Invitation bearer tokens are returned once and stored only as a SHA-256 digest. Organization members share the license owner's tenant; the browser never supplies the authoritative tenant or license-owner identifiers. A hash-chained audit ledger records role and membership transitions and can be exported; it never contains account email addresses or bearer tokens.

Regulatory alignment (KVKK / GDPR)

The service is built around data minimization, owner authorization, bounded retention and honored erasure: the operational properties a KVKK/GDPR reviewer checks. Paxvian maps findings to control frameworks (e.g. ISO 27001, NIST CSF, IEC 62443) for context; it is an assurance evidence register, not a statement of compliance or a certificate.

Generated with Paxvian