The security review, **on one page.**

Verillian keeps your own record of each request it captures, on servers your agency runs, and never receives your prompts, responses or records.

What runs where, and who holds the keys?

The Verillian software on each device, the admin server and the sealed record all run on devices and servers you operate. Content is encrypted to your organization's key, created in your administrator's browser. Verillian never receives that key.

What does Verillian never receive?

Your prompts, responses, and tool calls are never sent to us, from any deployment, for any reason. Enforcement and the record run inside your network, with no Verillian service in the request path.

How is each record signed?

Each entry is signed on the device, and your own admin server flags any entry that fails to verify when it arrives.

Who signs in to the console?

Through your own identity provider over OIDC, so there are no local passwords to manage. Roles are assigned in the console, and MFA stays whatever your identity provider enforces.

For procurement:	The system of record for your AI use, on your own infrastructure.
Trust and security overview:	How Verillian is designed for trust
Architecture and data flow:	Architecture and data flow
On the site:	Security overview for your review

hello@verillian.ai