TRUST AND SECURITY · DATASHEET

Safeguard

Answer the vendor security review before it slows your deal.

How Safeguard is audited, where it runs, who can sign in and how your data is handled.

THE PROBLEM

Before a security tool goes into production, someone has to review the vendor. The questionnaire is long, the answers are scattered, and a vendor who cannot say where data lives, how people sign in or what is audited loses weeks in review.

WHAT IT DOES

Audited

SOC 2 Type I and Type II audited. The report is available on request through the Trust Center at safeguard.sh/security.

Designed for FedRAMP High

The architecture is designed for FedRAMP High requirements.

Regions you can choose

SaaS in US, EU (Frankfurt) and Gov regions, or a private VPC, on-prem or fully air-gapped deployment.

Your data stays yours

No training on customer data. The local runner scans on your machine and sends only encrypted results.

HOW IT WORKS

1. **Ask** — Open the Trust Center at /security
2. **Request** — Ask for the SOC 2 report
3. **Review** — Compare regions, access and data handling
4. **Choose** — SaaS region, VPC, on-prem or air-gapped
5. **Sign in** — SSO with your identity provider

THE REPORT, ON REQUEST

Ask for the SOC 2 report through the Trust Center at safeguard.sh/security.

CAPABILITIES IN DETAIL

Audit	SOC 2 Type I and Type II audited. Reports available on request.
FedRAMP	Designed for FedRAMP High.
Regions	US, EU (Frankfurt) and Gov SaaS regions. Private VPC, on-prem and fully air-gapped options.
Single sign-on	SAML 2.0, OpenID Connect, and Google, Microsoft and GitHub sign-in, with roles and 2FA.
Network posture	No open inbound connections: the architecture polls. Encrypted communication throughout.
Data handling	Tenant isolation, with data scoped to your tenant and organization. No training on customer data.
AI choice	Zero AI mode with no LLM in the loop, bring your own model, or Safeguard models inside your environment.

INPUTS

- A request through the Trust Center
- Your identity provider for SSO
- Your region or deployment choice
- Your own AI model choice

OUTPUTS

- The SOC 2 report, on request
- Answers for your vendor questionnaire
- Role-based access for your team
- Audit logs for your reviewers

INTEGRATIONS AND SURFACES

Trust Center · SAML 2.0 · OpenID Connect · Google · Microsoft · GitHub · Local runner CLI

DEPLOYMENT AND DATA HANDLING

Regions and hosting

SaaS in US, EU (Frankfurt) and Gov regions. Private VPC, on-prem and fully air-gapped deployments are available.

Local runner

The CLI scans on your machine and sends only encrypted results. No open inbound connections; it polls.

Access control

SSO (SAML 2.0, OpenID, Google, Microsoft, GitHub), roles and 2FA.

Model choice

Zero AI mode runs the platform deterministically with no LLM. Or bring your own model (Claude, OpenAI and others), or run Safeguard models inside your environment.

Open the Trust Center

safeguard.sh/security

Scan the code or type the address. Questions: hi@safeguard.sh

Safeguard