

Security and compliance

Kestra runs on your infrastructure, under your rules. Self-hosted, on-prem or air-gapped, with no vendor access to your data.

Kestra Enterprise Edition, self-hosted • Updated September 2026



SOC 2 Type 2

Security, Availability and Confidentiality. Independently audited, report on request

GDPR Article 5

Covered by the same SOC 2 audit. DPA on request

Air-gapped ready

Docker, Kubernetes or directly on a VM. No outbound internet connectivity required

Secrets stay in your vault

Vault, CyberArk, Delinea, AWS, Azure, Google and more

✓ Compliance

Kestra Technologies is SOC 2 Type 2 audited for Security, Availability and Confidentiality, together with GDPR Article 5, by an independent auditor.

The audit covers how we build the software and how we operate as a vendor: secure development, code review, vulnerability management, access control, incident response and change management. Your self-hosted deployment runs in your infrastructure and stays under your control. The [hardening guide](#) and the [deployment architecture](#) documentation cover that side.

The full report, our policies and live control monitoring are available at kestra.io/trust.

📁 Deployment

Self-hosted

Runs entirely inside your infrastructure on Docker, Kubernetes or directly on a VM. Your Postgres, your object storage, your network.

Air-gapped

Workers run inside air-gapped zones, connecting outbound to the control plane only, never to the internet. Where policy requires it, the control plane can also run inside the zone, installed from a private registry.

📁 Where your data lives

Workflow definitions, execution history, logs and secrets stay in your database, your object storage and your network. Kestra has no access to your environment. Anonymous usage reporting, in-product documentation and hosted blueprints are the only components that call out to Kestra, and air-gapped mode disables them.

Workers are the only component that reaches your private systems: hypervisors and vCenter, on-prem databases, ITSM, internal APIs, and equipment inside restricted OT environments. They connect outbound to the control plane over a single authenticated channel, hold no database credentials, and need no inbound firewall rule where they run.





Security controls

Identity and access

SSO over OIDC with Google, Microsoft Entra ID, Okta, Keycloak and authentik, plus LDAP.

Secrets

Credentials never sit in flow definitions. Flows reference a key and the value resolves at runtime from your vault.

Audit and change control

Audit logs record every create, update and delete, with actor, timestamp and a before-and-after diff.

Directory sync

SCIM 2.0 provisioning, deprovisioning and group sync from Okta, Entra ID, Keycloak and authentik.

Read-only vault access

Your vault stays the source of truth. Kestra reads but cannot create, edit or delete. Set globally, per tenant or per namespace.

SIEM export

Ship audit logs to Datadog, Elastic, OpenTelemetry, Syslog CEF and other destinations.

RBAC

Roles bound to users, groups and service accounts, scoped per namespace and inherited by child namespaces.

Tenant isolation

Multi-tenancy separates flows, secrets, files and access between teams.

Version control

Every flow is versioned YAML with Git as the source of truth, and full execution history with inputs, outputs and logs.

Machine access

Service accounts and API tokens, separate from user accounts. Account lockout after repeated failed logins for basic auth and LDAP users.

Execution isolation

Policies force script tasks into container isolation across every tenant. Worker file-system restrictions and plugin allow-lists by prefix or regex.

Transport

TLS on the UI and API. One-way or mutual TLS between the control plane and workers, with authenticated, revocable worker registration.

How the software is built

- Source code in version control with a documented code review process, covered by our SOC 2 Type 2 audit.
- Vulnerability scanning across code and container images with GitHub Security, SonarCloud and Trivy, under a documented vulnerability management policy you can download from kestra.io/trust.
- Fixes ship in the latest release. Security advisories are published at github.com/kestra-io/kestra/security/advisories.
- Continuous control monitoring through Drata, with live status published at kestra.io/trust.

What to send your security reviewer

- 1 Trust center**, kestra.io/trust. The SOC 2 and GDPR Type 2 report, live control monitoring, the subprocessor list, and downloadable policies: Information Security, Vulnerability Management, System Access Control, Risk Assessment, Incident Response Plan, Encryption, Data Protection, Data Classification, Privacy, Data Retention, Asset Management, Business Continuity Plan, Software Development Life Cycle, Code of Conduct.
- 2 Security hardening guide**, kestra.io/docs/administrator-guide/security-hardening. Network isolation, container sandboxing, host permissions, plugin restriction and CI/CD validation for your own deployment.
- 3 Deployment architecture overview**, on request. Components, network posture and air-gapped installation.

