ENDOR LABS

Artifact Signing

Only approved code ever runs in production

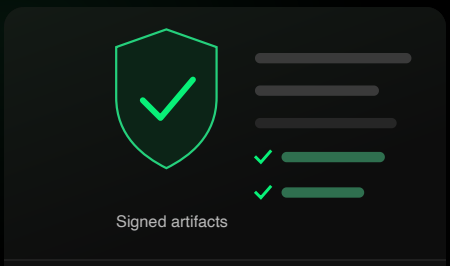
Artifact Signing cryptographically signs container images, binaries, and other build artifacts in the CI pipeline — then verifies them at deployment, so unsigned or tampered code never runs. It is built on the same principles as Sigstore but keeps everything private to your tenant: your existing SSO identities, single-use ephemeral certificates, and a tamper-resistant signature log.

Minutes
to trace a production artifact back to its source commit — not days

Zero
new PKI or identity systems — keyless signing with your existing SSO

Private
signature log in your tenant — no public transparency log

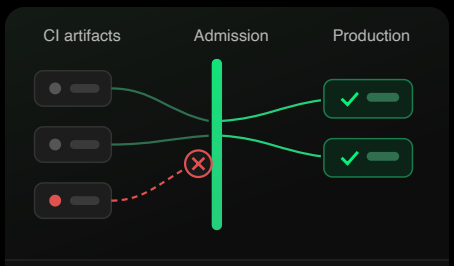
How it works



SIGN

Keyless signing in CI

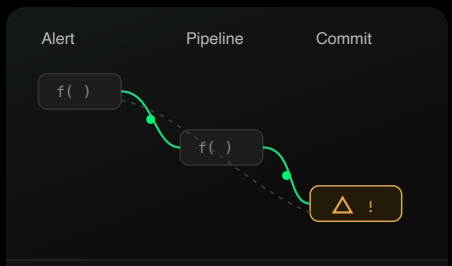
- Sign every container image, binary, or artifact with a single-use ephemeral certificate
- Authenticate with existing SSO — Okta, Azure AD, or Google Workspace
- Drop into GitHub Actions and endorctl workflows without new key infrastructure



VERIFY

Admission control at deployment

- Verify signatures via Kubernetes admission control — block or terminate what fails
- Stop shadow deployments no one approved from ever reaching production
- Prove integrity and provenance, not just that an image survived transit



TRACE

Code-to-cloud in minutes

- Trace a CNAPP or SOC alert to the source commit, build pipeline, and owning team
- Hunt a newly disclosed vulnerability across production using the signature
- Connect every signed artifact to its verified SBOM and VEX for compliance responses

WHY NOW

Hash checks and public logs aren't enough

Hash-only integrity checks confirm an image wasn't altered in transit — not that it came from a trusted build pipeline. Sigstore solves the cryptographic part but forces sensitive provenance metadata into a public transparency log, a non-starter for regulated environments. And after a security alert, incident responders still burn days reverse-engineering which pipeline produced the affected container. Private, keyless signing with provenance closes all three gaps — and gives auditors the evidence that production artifacts were built by approved, traceable pipelines.