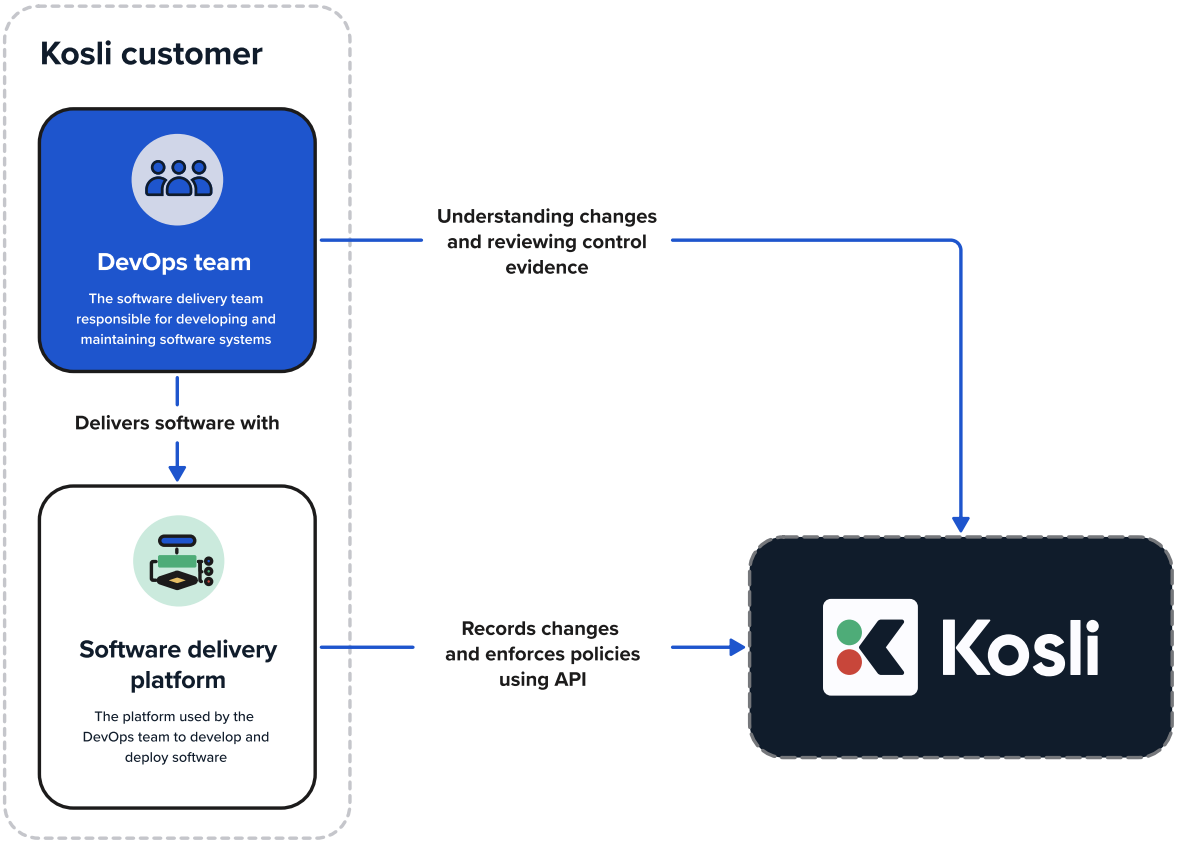
Kosli

RESOURCES

Kosli High Level Architecture

Kosli is a Software as a Service platform to record all of the changes in your software to give you the easy buttons for audit, compliance, security, and incident response. Kosli can be used to implement control gates to enforce policy at the right point in your SW delivery process.

Kosli Attestations



How does Kosli “record” everything? What kind of permissions and access does that require?

Kosli doesn’t require access to your system. Data is sent in one direction only: from your software delivery platform to Kosli.

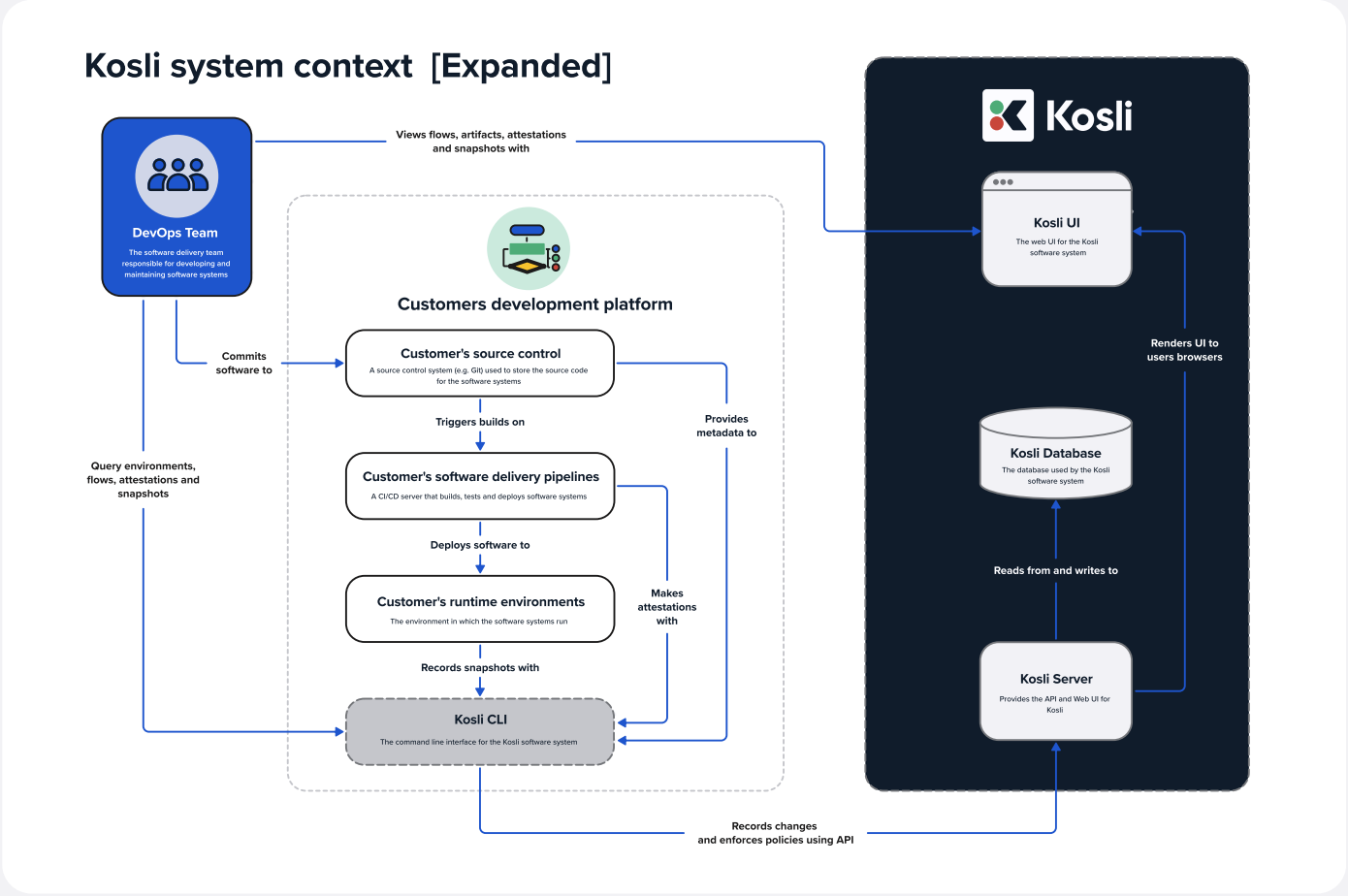
Kosli doesn’t access or record your sensitive data or secrets. We only record data that you send to us, which is typically low sensitivity data such as timestamps, cryptographic fingerprints for running artifacts, metadata for builds, tests, pull requests, etc.

Kosli is SOC 2 Type 2 compliant. We take the security and availability of your data seriously.

SaaS setup

Kosli is a SaaS platform that can be delivered in multi-tenant, or single-tenant, depending on customer needs.

- **Multi-tenant** is hosted by AWS in EU central (Frankfurt), with EU west (London) for failover and disaster recovery.
- **Single-tenant** can be hosted in any AWS region, as requested by the customer.



How does Kosli fit into your environment

Kosli records changes in your runtime environment, and the facts of how those changes are made from your delivery pipelines and source code repositories. These changes and facts are pushed to Kosli. Kosli never has access to your environments, pipelines, or source code.

Data stored in Kosli

Kosli records data needed for audit, security and compliance. The customers decide what data they want to store. Typical information include:

- Git commit information
- Built artifacts
- Pull requests
- Test runs and results
- Approvals
- Links to Jira or other ticketing systems
- SW artifact metadata from runtime environments

User data stored by Kosli:

- Email address
- GitHub ID - where GitHub social logins are used
- Name
- Hashed API keys

For security reasons customers can also decide to store information at their own location and record a URL in Kosli. This can for instance be used to store test result files.

Access to Kosli

Kosli provides a web interface and a REST API. **All connections are encrypted using HTTPS.**

- Access control is provided by:
- **Web UI login** controlled through Single Sign-On or GitHub Social Login
- **REST API** access controlled via API key
    - Kosli API keys can be either personal or belong to a service account.

Access to Kosli can be done with the API directly or by using the open source kosli-cli tool https://github.com/kosli-dev/cli

A security FAQ is available at https://www.kosli.com/security