Beyond Identity

SECURE DEVOPS

> With Secure DevOps, you are actually doing the security verification before the push to repo even happens. We are immunizing the repo rather than treating it with some medicine later
>
> snowflake®

Build pipelines are under attack. SSH keys live outside organizational control, Git author fields are spoofed, and manual GPG signing breaks developer workflows.

Beyond Identity Secure DevOps automates commit signing at the source. GPG keys are generated in the device TPM and bound to legitimate, authorized identities. Every commit is signed automatically. CI/CD pipelines verify identity before code is pushed, providing cryptographic proof between **who**, which **device**, and what **code** they wrote.

- **Prevent malicious code injection:** Stop unauthorized commits to production repos
- **Maximize developer velocity:** Remove onboarding friction and manual key management
- **Simplify compliance:** Meet SLSA requirements without overhauling Git workflows or adding engineering friction
- **Eliminate zombie SSH keys:** Revoke signing keys instantly upon offboarding

Author Verification API

Automatic validation of developer identity and device posture against commit signing key

Unified Policy Enforcement

Centrally control who and which devices can create keys for commit signing. Simple revocation for offboarding developers

Automatic Commit Signing

Developers register a unique GPG once, Beyond Identity automatically signs every commit

Universal Coverage

Integrates with all code repos and DevOps tools including GitHub, Bitbucket, GitLab, CircleCI, Jenkies, Azure Pipelines, Bamboo

PLUG AND PLAY

COMPLIANT WITH