Secure DevOps

BEYOND IDENTITY

Verify every piece of source code was committed from a corporate identity and authorized device to stop software supply chain attacks before they start.

Protect source code from malicious attacks and deter insider threats

Attackers continue to exploit vulnerabilities in modern DevOps environments. Recent attacks ranging from Solarwinds and Kaseya to one of the most expensive in history - NotPetya - have shown the real exposure and massive cost of these attacks.

Companies have moved their agile software development life cycle (SDLC) to the cloud. Today, source code is one of a company's most valuable assets. In distributed cloud-based development environments, engineers can access and update source code anywhere from any device.

The only way to know your source code has not been compromised is to track every source code commit. Who made what changes from what device?

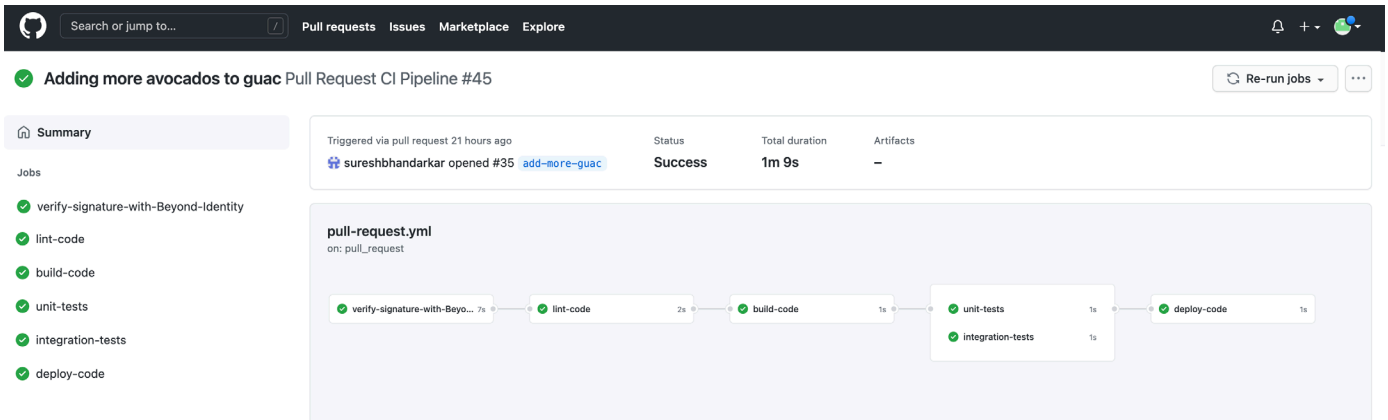
Beyond Identity Secure DevOps is the only product that secures the software supply chain at the developer level. Prevent malicious source code commits by cryptographically binding access and signing keys to a corporate identity and authorized device. Systematically inspect every commit so only source code that is signed by a valid corporate identity is built into the product.

Key Benefits:

- ✓ Eliminate key sprawl and stolen credentials
- ✓ Stop code injection at repo from non-authorized users
- ✓ Protect access to build enviornments, infrastructure, and 3rd party tooling
- ✓ Verifiable source code provenance for auditing and forensics

Verify source code is signed by a valid corporate identity

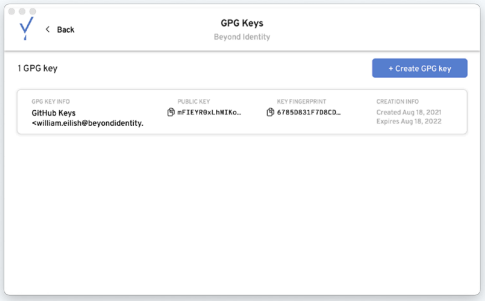
Secure your CI/CD pipeline. Place the Beyond Identity source code provenance check - a Git action or simple API call - at the beginning of your CI/CD pipeline to ensure that only source code that is cryptographically tied to a valid corporate identity makes it into your build.



How It Works

Beyond Identity is the only way to secure the software supply chain at the developer level.

Beyond Identity validates that every Git commit is signed by a verified corporate identity and trusted device. This is done by cryptographically binding a valid corporate identity to the device by minting GPG keys and storing the private keys in the TPM hardware on the developer's authorized device. The private key cannot be moved, and therefore can be trusted. Beyond Identity ensures compliance for all developers. It's an easy one time set up for developers, then Beyond Identity signs all Git Commits in the background without any ceremony to access the private key. Beyond Identity is the only source code signing product thats stops Git Commits from non-authorized devices.

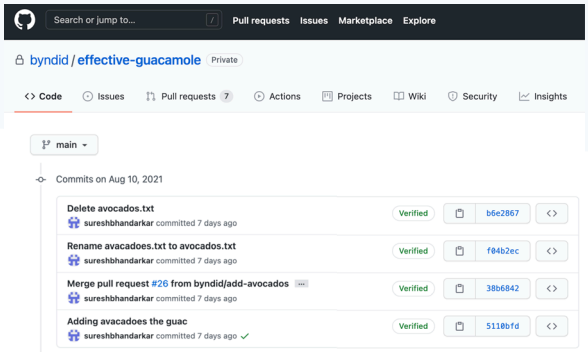


Signing keys are trustworthy

Developers mint their GPG keys using the Beyond Identity Authenticator, private keys are stored in the secure hardware and cannot leave the device. Key revocation is centralized and easy to manage. Beyond Identity's policies control which devices are authorized to create keys.

Restrict source code commit to corporate identites and devices

Only source code that is signed by a corporate identity using Beyond Identity is allowed in the build. There's a 1x set up for developers, then Beyond Identity signs source code behind the scenes for them without the need for a complex signing ceremony which ensures compliance.



GitHub GitLab Bitbucket

Integrates with leading code repositories and CI / CD tools

By integrating your CI automation tool (eg, Jenkins, Bamboo, Circle CI) with Beyond Identity's Identity Verification API, you can show alerts with the CI tool, flag a build or fail a build if there are code commits are not properly signed by a valid corporate identity.