CODE CLIMATE

Velocity Security

We understand that security is critical, and we follow best practices and strict procedures to keep our systems, and your data, safe. We work with respected security firms, like NCCGroup, to perform regular penetration testing and audits of Code Climate and its infrastructure.

Source Code Protection

All access to source code repositories is performed using encrypted connections, either via SSH or TLS. Depending on the version control system, access to private repositories is obtained via an SSH deploy key or a token. Code Climate never writes to repositories.

Velocity does not persist source code files. At the point our system executes code analysis of source code files, it is performed on ephemeral instances and source code content is immediately purged after processing. We only persist file names and metrics to our database.

Velocity Agent

We've developed the Velocity Agent to provide organizations the flexibility to take advantage of all the Velocity features while keeping their software source code in their GitHub Enterprise or BitBucket Server instance, running on their own network.

The Velocity Agent is a lightweight component deployed as a Docker container. The Velocity Agent is in charge of processing the GitHub Enterprise webhooks or BitBucket Server API and transferring aggregated data to the rest of Velocity services hosted by Code Climate.

Velocity only ingests metadata and metrics associated with repositories and projects that have been added within the administrative user interface. For each repository, we extract pull requests, reviews, comments and Git commit metadata.

Velocity Agent never extracts source code files from the GitHub Enterprise or BitBucket Server instance. Extracted data is persisted within our hosted database to support advanced reporting.

Employee Access to Customer Data

When working on a support issue we do our best to respect your privacy as much as possible, we only access the minimum files and settings needed to resolve your issue. Staff do not have direct access to clone your repository.

Employee access is granted according to the principle of least privilege. All privileged access is logged and audited.

Product Security

Single Sign On (SSO)

Velocity supports single sign on (SSO) via GitHub.com, Bitbucket, Gitlab or Google Workspace for authentication. Velocity also supports authentication via SAML.

Permissions

Velocity provides role-based access control for authorization, allowing you to control who can access application settings, billing information and features.

Uptime

Our systems have uptime of 99% or higher, and we proactively post status updates for production incidents. You can check our current and historic status at https://status.codeclimate.com/.