Security

Many customers host their Git repositories on internal servers using GitHub Enterprise, GitLab, Atlassian Bitbucket Server, or similar products. GitPrime needs to be able to access these servers to be able to collect the data used to calculate your metrics.

This can be accomplished securely by allowing public access via secure SSH access to internal repositories. This insures that all data transmitted to GitPrime is done over a secure protocol, and allows our customers to maintain strict authentication and access security using SSH keys.

To accomplish this setup, customers must enable network address translation (NAT) of the SSH port on a public IP address to the SSH port of their internal GIT server. For example, if your public IP address is 172.20.54.124 and your internal Bitbucket server exists at 172.45.0.24 using SSH port 7999, the NAT rule introduced to your firewall would forward any traffic 172.20.54.124:7999 to the internal address and port at 172.45.0.24:7999.

Where is my data stored?

GitPrime is built on Amazon's AWS. To find out more information about Amazon's security and infrastructure, please visit their security statement: **https://aws.amazon.com/security/**.

We currently store all persisted data in a Postgres database. All backups of the Postgres database are kept on AWS for a period of 90 days at which point they are deleted permanently.

We do not keep local copies of production data.

How is my data accessed?

Your data can only be accessed via an SSL connection using an authenticated session. We do not provide exports or any form of a

download of your data. It is not possible to access your repos directly.

Who can see my data?

Only people with the username and password you provide can access your data. There is no public access to your data of any kind.

March 21, 2019