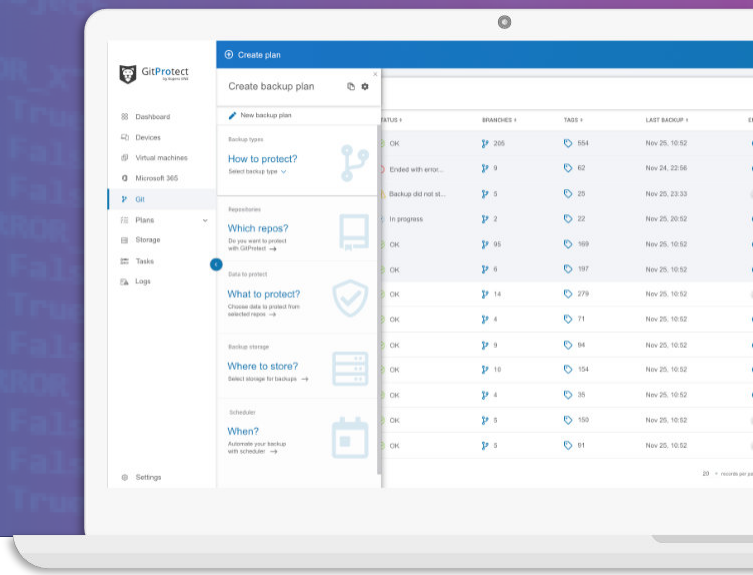
GitProtect
by Xopero ONE

Backup git repositories and **metadata** - set in minutes

Available in SaaS **Available on-Premise**



GitProtect - professional, manageable GitHub and Bitbucket backup that brings you peace of mind and protects your source code, Intellectual Property, hours of work (and money) against any event of failure. Set a backup plan in minutes so it will perform automatically.

Why should I protect
GitHub and Bitbucket repositories?

Human and hardware errors

Your developers are not security experts. They make mistakes. **Old repository deletion, HEAD overwrite**, or **branch deletion** - all those situations can wipe your projects and data irreversibly. Or hardware they are working on can be damaged, lost, or stolen...

Service outages, bugs, and ransomware

GitHub or Bitbucket **accidentally lost your data?** That happened to GitLab before. Major GitHub or Atlassian **outages** that impact your business, cause long-hour downtime, and cost you money? Happen more often than you think. Oh, and **ransomware attack** wiping code and commits from multiple repositories? It happened to GitHub, Atlassian, and GitLab.

Shared Responsibility Models

As most SaaS providers, also GitHub, GitLab, and Atlassian rely on shared responsibility models. Accordingly, service providers are responsible for service accessibility, uptime, and security while you, as a user are responsible for data protection and legal compliance. That's why **GitHub and Atlassian recommend having a third-party backup**.

GitProtect **protects:**

→ Repositories - local and cloud
Metadata (i.e. issues, milestones, pull requests, wikis, releases & more)
Old, unused repositories (archive)
New repositories - automatically added to a backup plan

All services support

→ GitHub
Bitbucket
GitLab (soon)
Azure Repos (soon)
AWS CodeCommit (soon)

Any storage

→ SMB network shares
Local disk resources
Xopero Cloud
Amazon AWS S3
Clouds compatible with S3 (Azure, Google Cloud Storage, Wasabi, Alibaba Cloud)

Still not sure? Checklist!

1. Where do you store your repositories?
2. Do all employees store all repositories, with all branches?
3. Do all employees perform a backup (How often? Every day, once a week...)?
4. How does your company secure cloud repos?
5. How many days could you lose data from? What are your RTO and RPO?
6. How much does it cost you to maintain your script/DIY backup?
7. How long will it take to recover data from a specific day and time?
8. Do you even have a script to recover the data?
9. How do you archive closed projects?
10. If you use scripts how do you verify backup performance?
11. How long does it take to secure every new repository? Do you remember about it?
12. Are your copies encrypted in any way? Is it strong and secure encryption?

Key **features**

Full, incremental, differential copies

Backup plan - predefined or customized

Backup schedule and full automation

Long-term retention, GFS, and FIFO schemes

Restore - fast, point-in-time, granular to other repo or local machine

Cross-over Disaster Recovery and migration (GitHub <-> Bitbucket)

Security: AES encryption, Password Manager, NSPoF

Advanced audit logs, stats, reports, email notifications

Central, multi-level management