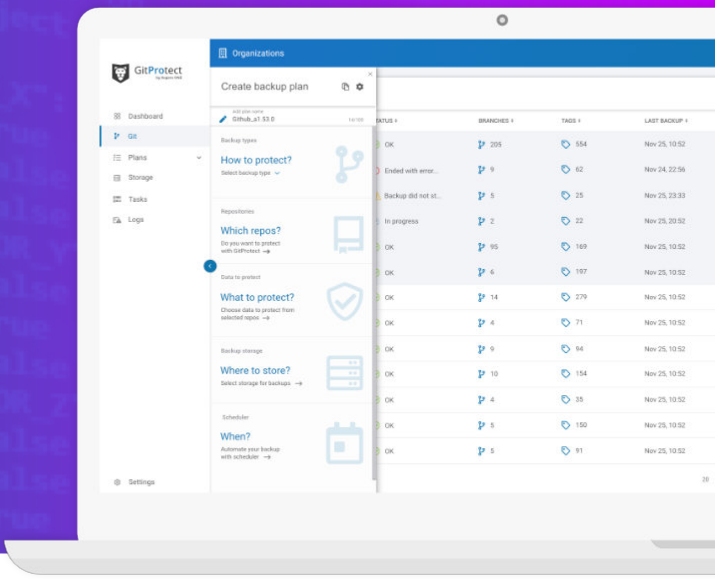
GitProtect
by Xopero ONE

#1 DevOps Backup Platform

Backup repositories and metadata.
Recover with ease. Stay compliant.



Create backup plan

Add plan name: Github_a1.53.0 14/100

Backup types
How to protect?
Select backup type

Repositories
Which repos?
Do you want to protect with GitProtect →

Data to protect
What to protect?
Choose data to protect from selected repos →

Backup storage
Where to store?
Select storage for backups →

Scheduler
When?
Automate your backup with scheduler →

STATUS	BRANCHES	TAGS	LAST BACKUP
OK	205	554	Nov 25, 10:52
Ended with error...	9	62	Nov 24, 22:56
Backup did not st...	5	25	Nov 25, 23:33
In progress	2	22	Nov 25, 20:52
OK	95	169	Nov 25, 10:52
OK	6	197	Nov 25, 10:52
OK	14	279	Nov 25, 10:52
OK	4	71	Nov 25, 10:52
OK	9	94	Nov 25, 10:52
OK	10	154	Nov 25, 10:52
OK	4	35	Nov 25, 10:52
OK	5	150	Nov 25, 10:52
OK	5	91	Nov 25, 10:52

20

GitProtect - professional, manageable GitHub, Bitbucket, GitLab, and Jira 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, Bitbucket, GitLab, and Jira data?

Human and hardware errors

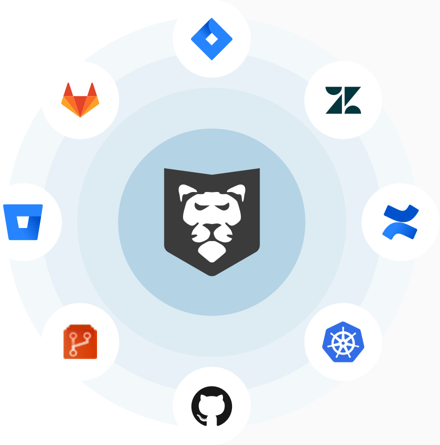
Your developers are not security experts. They make mistakes. **Old repository deletion, HEAD overwrite**, or **branch deletion** - all those situations can wipe your projects and data irreversibly. Or hardware they are working on can be damaged, lost, or stolen...

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

Learn more

All services support

→ GitHub
Bitbucket
GitLab
Jira
Confluence, Kubernetes, Zendesk, Azure Repos, and more coming soon!

Any storage

→ Unlimited Xopero Cloud
Amazon AWS
Wasabi Cloud
Backblaze B2
Google Cloud Storage
Azure Blob Storage
Any storage compatible with S3
NAS: Synology, WD, QNAP, etc.
Files syste: Local, iSCSI, SMB, CIFS, NFS

Still not sure? Checklist!

1. What if something happens to your Git services/your repositories (data wipeout/branch deletion/head overwrite/service unavailability)?
2. What if your Git service account gets hijacked/deleted/blocked?
3. Can you afford to lose your repositories? How much does it cost you?
4. Do you secure your Git repositories in any way? How? Do your copies include repository metadata?
5. Where do you keep your copies? Are these locations secure?
6. How long do you keep copies of your repositories? Do you archive old projects?
7. Do you encrypt your copies? Is the encryption strong and secure?
8. How do you verify a copy of your repository? Do you get notified?
9. How much effort does it take to secure a new repository?
10. What does the repo recovery process look like? How long does it take? How much effort does it require?
11. What is the final cost of losing a repository? How does it impact your business in a long-term?

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

Over **100k protected repos and secured organizations**

Amplience GLADSTONE INSTITUTES NHS Wharton UNIVERSITY of PENNSYLVANIA HEMA

LEAP EV spirent netguru jedox. Ninety One

RED Klar INSHUR smartnumbers