

Patronum Backup for Google Workspace Service Definition

TABLE OF CONTENTS

1. PATRONUM BACKUP FOR GOOGLE WORKSPACE	3
2. KEY PRODUCT FEATURES	4
2.1 Automated Full Fidelity Backups	4
2.2 Backup Administration	4
2.3 Search and Flexible Recovery	4
2.4 AI-based Automation	4
2.5 Intelligent Ransomware Protection	5
2.6 Access Control and Security	5
3. SERVICE OVERVIEW	6
3.1 Operations	6
3.2 Privacy and Data Protection	6
3.3 Access and 14-day Free Trial	7
3.4 Deinstallation	7
4. PATRONUM BACKUP LICENSING	8
5. ABOUT BESPIN LABS AND AFI TECHNOLOGIES	9
6. FULL FEATURE LIST	10
6.1 Backup Content Support	10
6.2 Backup Functionality	10
6.3 Security & Anti-ransomware	10
6.4 Export, Recovery & Admin	10
6.5 Reporting	11
6.6 Service	11

1. PATRONUM BACKUP FOR GOOGLE WORKSPACE

As Google Workspace grows within an organisation it accumulates increasingly sensitive and business-critical information. This data must remain available, secure, and compliant at all times.

To avoid exposing an organisation to risks such as ransomware attacks, accidental data deletion, insider attacks, data loss, compliance issues, and data retention breaches, a data protection strategy is essential.

Patronum Google Workspace Backup is a proven dedicated backup solution. Afi Technologies provide backup solutions to thousands of clients worldwide and a number of these have over 100,000 users each and petabytes of data.

2. KEY PRODUCT FEATURES

The main features of Patronum Google Workspace Cloud Backup are summarised below.

2.1 Automated Full Fidelity Backups

- Automated weekly, daily or high-frequency (up to 24) backups per day.
- Regular fully automated backup runs, resilient to Google API errors.
- Drive, Shared Drive and document sharing permissions backup.
- Document IDs, file metadata including dates and author.
- Full structure of email, labels and nested labels, folders and threads.

2.2 Backup Administration

- SLA policy-based backup, automated re-scheduling to avoid failures
- Actionable backup reporting in web dashboard or email - clear status/error messages that keep administrators informed.
- Automated archiving of deleted Workspace users. This saves on licensing costs as backup archived users are free and retained forever.
- On-demand backups can be triggered by Admin for all users.
- Unlimited retention at one or multiple Google data centres, selected by customer, in United States, United Kingdom, Netherlands, Canada and Australia

2.3 Search and Flexible Recovery

- Keywords and phrase search in Google Workspace email backups using full-text search across all contents, not limited by the standard metadata search fields.
- Granular item-level or whole user instant account restore.
- Data restoration to the same / other accounts, in-place or to a new folder.
- Point in time restore and versioning with unlimited number of recovery points and file versioning (both native and external formats).
- Browse and restore any prior versions of Google Workspace data without a time limit.
- Instant online preview and export to MBOX, EML and PST formats.

2.4 AI-based Automation

- Backup schedules automatically adjusted based on the protection levels (SLAs) assigned by the admin for OUs or single users.
- Google Workspace users and Drives are automatically discovered and protected.

- Shared Drives or users deleted from Google Workspace account are automatically archived and available for restore and export at any time.
- Google Workspace API errors are handled by a prediction engine to avoid Google Workspace API calls limit.
- Parallel execution, automatic reschedules, reconfiguration and retries of problematic backup runs.
- Instant email alerts for administrators in addition to configurable regular status updates via email

2.5 Intelligent Ransomware Protection

- Early ransomware attack detection with instant admin email notifications.
- Instant pre-emptive backups help to preserve Google Workspace data when ransomware hits.
- Auto-labelling of recovery points to define the last clean snapshot unaffected by attacks.
- Immutable backup storage - past recovery points can't be affected by cyber attacks

2.6 Access Control and Security

- Native support of Google 2FA for administrators and users.
- Detailed audit log with WAN IP addresses, session details, Admin actions and system events.
- Custom backup operator roles for admins, support team or users, enabling restore operations without data access rights to email or file contents.
- Self-service via web portal for end-users to let them recover lost items themselves, including Shared Drive data.
- Data at rest is encrypted with AES256 and TLS 1.2 for data in transit.

3. SERVICE OVERVIEW

3.1 Operations

Solution Provider

Bespin Labs Ltd, Bates Mill, Colne Road, Huddersfield, HD1 3AG United Kingdom.

Service Operator

Afi Technologies Inc. 210 N University Drive #303, Coral Springs, FL 33071, United States

Service Access

Patronum Google Workspace Backup is a subscription based software as a service product installed within a customer's Google Workspace domain by a Super Admin via the Google Workspace Marketplace. Customers are also given an Afi backup online account.

Support Services

Support is available within Patronum Google Workspace Backup service.

Help is available from within Patronum Google Workspace Backup service.

Hosting and Location

Customers select which Google Cloud Platform's data centres located in the United States, United Kingdom, Netherlands, Canada and Australia store their data.

Service Security

As specified in "Google Workspace Cloud Backup via Bespin Labs" Government Digital Marketplace entry.

3.2 Privacy and Data Protection

As specified in "Google Workspace Cloud Backup via Bespin Labs" Government Digital Marketplace entry.

Patronum Google Workspace Backup access is based on the permissions set and controlled by the customer's IT and security teams and Bespin Labs and Afi personnel cannot access the content of customer documents or emails.

3.3 Access and 14-day Free Trial

Register for a trial at <https://bespinlabs.com> for a 14-day free trial (multiple users, unlimited data) of Patronum Google Workspace Backup. After submitting a short form you will be emailed details about how to install some software on your domain and access to an online Afi account. You will need Super Admin privileges to install Patronum Google Workspace Backup on your organisation's domain.

3.4 Deinstallation

Patronum Google Workspace Backup must be removed by a Google Workspace domain Super Admin.

After Patronum Google Workspace Backup has been fully deinstalled we will permanently delete any trial backup data within 30 days.

4. PATRONUM BACKUP LICENSING

For pricing details please refer to the Patronum Pricing Plan. The minimum subscription period is one year with a Monthly billing option.

A protected user requires one licence covering up to 50Gb of storage, pooled across protected users.

- There are no charges for Shared Drives.
- There is no minimum number of licences.
- There is no minimum % of domain users that need to be licensed.

To extend the storage limit per user (50Gb) you can add an Additional Storage Unit of 100Gb, which is also pooled across protected users.

5. ABOUT BESPIN LABS AND AFI TECHNOLOGIES

Bespin Labs Limited is a UK Google Cloud solutions provider. It became an Official Google Cloud Partner in 2018 and launched its first product, Patronum in 2019.

Bespin Labs runs in a transparent, collaborative, and engaging community way for our team, partners and our customers. The customer first approach is at the heart of everything the company does, from features requests to pricing strategies.

Afi is a SaaS backup provider focused on Google Workspace and Microsoft 365 data protection typically for midsize to large enterprises with 5,000+ users.

6. FULL FEATURE LIST

6.1 Backup Content Support

- Google Workspace
- Gmail
- Google Drive
- Shared Drives
- Contacts
- Calendars
- Hangouts (chats)
- Google Sites
- Google Drive's Computers folder

6.2 Backup Functionality

- SLA-based protection
- Automated backups
- Backup data retention

6.3 Security & Anti-ransomware

- Data & metadata encryption
- At rest encrypted using AES-256, in transit secured using TLS
- Immutable backup data versioning
- 2 Factor Authentication
- AI-based ransomware detection & preemptive backups
- Automatic critical recovery points labelling
- OKTA SAML
- Bring your own encryption

6.4 Export, Recovery & Admin

- Full text search
- Instant content preview
- Email export in PST format
- Full Drive contents export
- Granular audit log
- Role-based access management
- Configurable admin access to sensitive data
- User self-service recovery portal
- User self-service recovery portal for Shared Drives

6.5 Reporting

Daily, weekly or monthly email reports

Instant email alerts

Instant Slack notifications

6.6 Service

24/7 email support

Support ticketing system

Emergency admin phone support