datto | SAAS PROTECTION

SaaS Protection for Google Workspace Technical Overview

Technical Backup Features

Services Covered	Google Workspace's Gmail, Calendar, Contacts, Drive files (including non-native file formats) and Shared Drives
Automated Backup	Automated daily point-in-time backups begin after initial ingest
Backup Frequency	3X Daily
On-Demand Backup	Able to initiate anytime on service level; will not interrupt regularly scheduled backups
Automatic New User Detection	Ability to set backup to specific organisational units (OUs). Able to add all current users and back up new users automatically; nightly job detects status of services in Google Workspace environment
Automated Archive	Nightly job detects status of services in Google Workspace environment, then archives those services that are archived in Google Workspace
Licenses Supported	Basic, Business, Enterprise
Storage Locations	Stored in Datto's private cloud located in US, EMEA, AUS, CAN; built-in redundancy; geo replication; ZFS file storage; SOC 2 Type II audited; data encrypted in transit and at rest
Restore Function	To original user or alternative user in original file format
Restore Granularity	File level, folder level with hierarchy in tact; file and folder level permissions maintained; option to restore files without attached permissions
Export Format	MBOX for Mail, ICS for Calendar, VCF for Contacts, Original MS format for native Google Apps files; original format for non-native file types (PDF, MOV, etc.)
Search	Search across multiple users; metadata search
Administrative Roles	Manage your accounts using roles such as Super Admin and General Admin roles.
Audit Logging	Available under "Reporting" in UI
Data Retention	Set to infinite retention by default. ICR - Backup snapshots are retained in the Datto Cloud indefinitely, TBR - Backup snapshots are retained for up to 1 year in the Datto Cloud
Data Pruning	3X daily user backups are retained for 30 days; after 30 days, one daily backup is saved per user; after 90 days, one weekly backup is saved per user; after 1 year, one monthly backup is saved per user.
Daily backup success report	Granular reporting to confirm the health and status of your backup snapshots per client and application

SaaS Protection for Google Workspace

Businesses depending on Google Workspace for collaboration are at risk for potential data loss. Although data is stored in Google servers, Google does not take responsibility for data created by the end users of their service.

An independent backup separated from Google is necessary to recover quickly from the most common data loss pitfalls such as:

- Accidental deletion or data overwrites
- Malicious end-user activity
- Lost data due to deprovisioned Google Workspace licenses
- Ransomware attacks
- External app errors (data corruption via syncing or overwriting)

Security Overview

Ransomware Recovery

Companies need to consider a multi-layered approach when it comes to security against ransomware and other cyber attacks. Without sufficient backup, companies stand to risk losing all of their files. With point-in-time backups, you can restore individual files or an entire application's data from a backup snapshot taken prior to an attack such as, last Friday at 8PM.

Certifications

Datto SaaS Protection has completed a SOC 2 Type II audit against the AICPA Service Organisation Control Trust Services Principles, Criteria, and Illustrations for Security, Availability and Confidentiality. The audit firm concluded that controls were suitably designed and operating effectively to provide reasonable assurance that control objectives would be achieved. SaaS Protection data is also stored in leading co-location facilities compliant with HIPAA. The SaaS Protection app also helps support GDPR compliance with built-in data controls and deletion tools.

Encryption

When it comes to encryption, Datto deploys the highest level of security for customer data. At rest, data is encrypted using industry standard 256 bit (AES-256) encryption. All data written for the user is encrypted prior to storage. In transit, Datto employs TLS 1.2 encryption.

OAuth Token

When setting up SaaS Protection, the authorisation of the backup is captured through the app's UI and uses Oauth tokens, so there is no need to store sensitive user credentials in Datto's database. The app's connection with Google Workspace will not be lost with admin password changes, as the Oauth token will maintain the authorisation with the SaaS Protection app.

Getting Started

For more information on SaaS Protection Security, see dat.to/SaaS-Security

datto
101 Merritt 7, Norwalk, CT 06851
partners@datto.com
www.datto.com

USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 406 504 556
Singapore: +65-31586291