datto | SAAS PROTECTION

SaaS Protection for Microsoft 365 Technical Overview

Technical Backup Features

Services Covered	Microsoft 365's Exchange Online, Calendar, Contacts, Tasks, all OneDrive file types, OneNote data in Sharepoint and OneDrive Document libraries, Sharepoint Sites, Custom Site Collections, Microsoft Teams Content (team sites, files, documents), Public channel conversations, Calendar Meetings
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 and Share-Point Site Detection	Able to add all current users or SharePoint sites and back up new users or sites automatically; nightly job detects status of services in Microsoft 365 environment
Microsoft 365 Licenses Supported	E1, E3, E5, Exchange Only 1 and 2, Sharepoint only 1 and 2, Business Essentials, Business Premium, EDU, GOV, NPO
Storage Locations	Stored in Datto's private cloud located in US, EMEA, AUS, CAN; built-in redundancy; geo replicated within geographical region; ZFS file storage; SOC 2 Type II audited; built-in encryption
Restore Function	To original user or alternative user in original file format
Restore Granularity	File level, folder level with nested hierarchy and file permissions intact
Export Format	MBOX for Mail, ICS for Calendar, VCF for Contacts, Original MS format for OneDrive
Search	Discovery search within and 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 Microsoft 365

With more and more MSPs moving clients to Microsoft 365 for collaboration and business operations, the risk of potential data loss is impossible to ignore. Although data is stored in Microsoft servers, they don't take responsibility for data loss that occurs on the client's side.

An independent backup separated from the app itself is necessary to avoid the most common data loss pitfalls such as:

- Accidental deletion or data overwrites
- Malicious end-user activity
- Lost data due to deprovisioned Microsoft 365 licenses
- Ransomware attacks
- External app errors (data corruption via syncing or overwriting)

Security Overview

Ransomware Recovery

MSPs need to consider a multi-layered approach when it comes to security against ransomware and other cyber attacks - especially with cloud attacks on the rise. Without sufficient backup, your clients stand to risk losing all of their files. With point-in-time backups, MSPs 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 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 supports GDPR compliance and data is also stored in leading co-location facilities compliant with HIPAA.

Encryption

When it comes to encryption, SaaS Protection 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, SaaS Protection 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 Microsoft 365 will not be lost with admin password changes, as the Oauth token will maintain the authorisation with SaaS Protection.

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