

Microsoft 365 Backup, powered by Veeam

YOUR DATA. YOUR RESPONSIBILITY.



Challenge

Microsoft 365 is among the most widely adopted SaaS platforms in the enterprise — and one of the most widely misunderstood when it comes to data protection. Microsoft operates a shared responsibility model: Microsoft guarantees the availability of the service, while the customer remains responsible for the data inside it.

Native retention policies, litigation hold, and the recycle bin are governance and availability features. They are not backup. They do not reliably address deletion discovered months later, malicious insider activity, ransomware propagating through OneDrive sync, or a departed employee whose mailbox was purged when the license was reclaimed.

Summit's Microsoft 365 Backup as a Service delivers fully managed, independent protection for Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams — built on Veeam, operated by Summit, and stored in secure data centers worldwide.

How We Do It

COMPLETE CONTROL



Microsoft 365 data is captured into storage Summit operates independently of your tenant, so a compromise, lockout, or licensing change on the production side does not take the recovery copy with it.

FLEXIBLE RECOVERY



Restore a single email, a document version, a full SharePoint site, or an entire user account — back to the original location, to an alternate target, or as an export — without opening a Microsoft support case.

FULLY MANAGED OPERATIONS



Summit owns policy configuration, monitoring, failure remediation, backup-window planning, and capacity management. Your team requests restores; ours performs them.

Deployment Models

Both models deliver the same underlying service. The difference is isolation and how the platform is managed.

MULTI-TENANT



Your tenant is protected on Summit's shared VB365 platform. Summit operates the backup servers, proxies, and object-storage repositories, and handles platform patching and upgrades.

PRIVATE BACKUP SERVER



A dedicated VB365 deployment for a single customer and tenant, with the proxy integrated into the deployment. Suited to customers with isolation or configuration requirements the shared platform cannot meet.

Key Capabilities



EXCHANGE ONLINE

Primary and archive mailboxes, folders, and individual items including calendar entries, contacts, and tasks.



SHAREPOINT ONLINE

Sites, subsites, document libraries, lists and list items, with version history and permissions preserved.



ONEDRIVE FOR BUSINESS

User drives, folder structures, files, and previous file versions across the tenant.



MICROSOFT TEAMS

Teams, channels, channel posts, tabs, and the Teams-connected SharePoint and OneDrive content behind them. Teams chats are available as optional scope.

GRANULAR RECOVERY



Browse and search restore points, then recover a single item without staging a full-scale restore first.

POINT-IN-TIME RESTORE



Roll back to a specific restore point rather than only the most recent copy – critical when corruption is discovered late.

POLICY-BASED RETENTION



One year of retention by default, extendable to seven years or indefinitely with the archive tier, with GFS weekly, monthly, and yearly tiers for regulatory hold.

IMMUTABLE STORAGE



Backups written to Summit S3-compatible object storage with immutability enabled and a 30-day lock, so retained copies cannot be altered or deleted inside that window.

ENCRYPTED END TO END



TLS 1.2 or higher in transit and AES-256 at rest, applied by the Veeam proxy before data is written to Summit-operated object storage.

COMPLIANCE SUPPORT



Locate items across restore points to support audit, legal hold, and internal compliance inquiries.

MONITORING AND REPORTING



Continuous job-health monitoring by Summit operations, with success and capacity reporting, plus a quarterly health review covering job trends, restore tests, capacity, and licensing.

CROSS-REGION COPY



Optional backup copy to a bucket in a second Summit region for customers with geographic separation requirements.

DURABLE OBJECT STORAGE



Summit S3-compatible object storage with eleven nines of durability, with an optional archive tier for long-horizon retention.

Your Business Data

DATA PROTECTION AND MANAGEMENT SOLUTIONS



Microsoft 365

BACKUP

RESTORE

SUMMIT™

What gets protected:

- Mailboxes and archives
- Files and documents
- SharePoint sites and libraries
- Teams, channels, and posts
- Calendars, contacts, and tasks
- Permissions and metadata

Benefits

MANAGED PROTECTION ON A PLATFORM INDEPENDENT OF YOUR MICROSOFT TENANT

- | | | |
|----|---|---|
| 01 | MEET REAL RETENTION REQUIREMENTS | Set RPO and retention to what the business and its regulators actually require, rather than to what native Microsoft 365 tooling happens to allow. |
| 02 | RECOVER WITHOUT A SUPPORT CASE | Restore from accidental deletion, malicious change, or ransomware propagation on your own timeline, from a copy that lives outside the tenant. |
| 03 | REMOVE THE OPERATIONAL BURDEN | Backup operations, capacity planning, throttling management, and failure remediation shift to Summit — no additional headcount, no additional tooling to learn. |

Service Details

PROTECTED WORKLOADS:

Exchange Online including mailboxes, calendars, and contacts; SharePoint Online sites, libraries, and lists; OneDrive for Business; Microsoft Teams channel content

OPTIONAL SCOPE:

Teams chats, SharePoint site Web Parts, and Public Folders. Each requires additional setup time, and Public Folders requires additional service account permissions.

DEPLOYMENT MODELS:

Multi-tenant on Summit's shared VB365 platform, or a dedicated private backup server. Same underlying service in both.

BACKUP FREQUENCY AND RPO:

Daily by default, and tunable to the customer's requirement.

RETENTION:

One year by default. Extendable to seven years, or indefinite with the archive tier. GFS weekly, monthly, and yearly tiers available for compliance or regulatory hold.

STORAGE:

Summit S3-compatible object storage with immutability enabled on a 30-day lock and eleven nines of durability. Optional backup copy to a bucket in a second Summit region.

ENCRYPTION:

TLS 1.2 or higher in transit; AES-256 at rest, applied by the Veeam proxy before data is written to object storage.

REPORTING:

Continuous job-health monitoring by Summit operations, with success and capacity reporting. Quarterly health review covering job-success trends, restore tests performed, capacity trends, licensing reconciliation, and ticket history.

ONBOARDING:

Approximately two business weeks from order to first completed full backup, including configuration and initial seed. The customer provisions a service account and assists Summit with the Entra ID app registration; the temporary Global Admin role is removed once registration and admin consent are complete.

SUPPORT MODEL:

24x7x365 incident response through the Summit NOC for priority incidents. Change requests, scope adjustments, and non-urgent configuration changes are handled during business hours. Escalation runs through Summit support and engineering, with Summit opening vendor cases on the customer's behalf where required.

COMPLIANCE:

SOC 2 Type II across Summit data centers and processes. HIPAA BAA available on request.

Related Summit Services

ENTRA ID BACKUP



Protect the identity layer alongside the data layer — users, groups, roles, and configuration.

SALESFORCE BACKUP



The same managed SaaS protection model applied to Salesforce data and metadata.

MANAGED BACKUP AND DRAAS



Extend a single data protection strategy across SaaS, virtualized, and physical workloads.