

Keepit SaaS backup and recovery

Canonical: <https://agentic.blueapache.com/technical-excellence/keepit/keepit-solutions-with-blueapache/>

Description:

We help you assess and implement Keepit to protect SaaS data and plan how it will be recovered.

Details:

We help organisations assess and implement Keepit for SaaS data protection. We bring our cloud, identity and technology delivery expertise to the decisions that matter: which applications and data to protect, how recovery should work and who will operate the solution.

Moving applications to the cloud changes where they run, but your business still needs a practical way to recover information after deletion, unwanted changes or a security incident. We help you build a recovery approach around those scenarios and the applications your people depend on.

Protect cloud application data independently

Keepit provides backup and recovery for SaaS applications using its own cloud infrastructure. Its Microsoft 365 capability includes data within Exchange Online, OneDrive, SharePoint and Teams. Its wider product portfolio also includes protection for Microsoft Entra ID and other cloud applications.

We start by identifying the connectors and data types relevant to your environment. A Microsoft 365 content requirement and an Entra ID identity-recovery requirement need separate consideration: restoring a document is different from recovering the users, groups or policies that govern access to applications.

Keepit's independent storage and immutable backup architecture are relevant when you want a recovery copy separated from the production SaaS environment. We help you assess how that approach fits your recovery needs, retention requirements and existing protection arrangements.

Design around the recovery you need

We work through the business scenarios before settling the implementation scope. Useful starting points include:

- An employee deleting a document, mailbox item or shared workspace that the business still needs.
- An administrator making an unwanted change across a larger set of data.
- A security incident affecting access to production information.
- A departing employee whose business information must remain recoverable.
- An identity configuration change that disrupts access to cloud services.

For each scenario, we discuss the data to recover, the point in time required, the restore destination and the approvals needed. We also distinguish recovery of stored data from restoration of the SaaS provider's service. Access to a backup does not itself bring an unavailable production application back online.

Connect implementation with day-to-day ownership

A backup deployment needs an operating process around it. Our implementation discussion covers tenant access, connector permissions, the selected users and workloads, retention settings and the people authorised to restore or export information.

We also address how your team will identify failed or incomplete backups and validate representative restores. A successful backup job and a successful business recovery are different checks. Testing the recovery steps helps your team understand what to do when an incident happens.

Where data location matters, we review the available Keepit region and the proposed configuration with you. Region selection, retention and protected workloads are part of the solution design, rather than assumptions based on a general product description.

Work with us on your terms

Our TECHNOLOGY offering gives you a route to product selection and implementation without outsourcing your whole IT function. We can work alongside an internal cloud or infrastructure team, connecting SaaS protection with your broader Microsoft, identity and security environment.

If you need ongoing assistance, we can discuss the operational responsibilities you want us to take on. The engagement should make clear who monitors protection, approves recovery, manages access and reviews coverage as users and applications change.

Questions about Keepit

Can we start with Microsoft 365 and assess other applications later?

Yes. We can scope the initial requirement around your selected Microsoft 365 workloads and separately assess additional connectors. We check the data types and licensing required for each application before adding it to the design.

Is Entra ID backup the same as backing up Microsoft 365 files?

No. Entra ID holds identity objects and policies, while Microsoft 365 includes business content such as mail and documents. We assess both where your recovery plan depends on restoring access as well as information.

Will our team still control restores?

We can design the engagement around your team's operational ownership. Restore permissions, approval steps and our supporting role are agreed during implementation.

Discuss SaaS backup and recovery with our team

Related expertise

- Microsoft cloud, workplace and security
- Veeam backup and recovery