



FACT  
SHEET

# 365 TOTAL BACKUP

Automated Microsoft 365 data backup, recovery,  
and protection – any time & anywhere

Hornetsecurity 365 Total Backup is a reliable, intuitive, and easy-to-manage backup and recovery solution for Microsoft 365 mailboxes & In-Place Archive mailboxes, OneDrive for Business accounts, SharePoint document libraries, Teams Chats, OneNote and Planner.



Back up and restore  
all Microsoft 365 data



Easy configuration and  
multi-tenant management



Automatic and  
hassle-free

## What is affected?



365 Mailboxes &  
In-Place Archive  
Mailboxes, Teams,  
Planner, OneNote,  
Sharepoint &  
OneDrive



Hassle-free with one  
all-inclusive fee

Unlimited storage, one  
all-inclusive fee,  
centralized manage-  
ment, easy search  
and recovery



Automated  
backups

All files are  
automatically  
backed up multiple  
times per day.



Control over  
data jurisdiction

You decide which  
region you want your  
data to be stored in.



Robust M365 data  
protection

With Hornetsecurity 365 Total Backup, you automatically back up your user and group .Microsoft 365 mailboxes & In-Place Archive mailboxes; notebooks contained in OneNote; user and group Team Chats; group plans from Microsoft Planner and any shared files, including recordings of Teams meetings; and files stored within OneDrive and SharePoint Document Libraries. Mailbox backups include all emails, attachments, calendars and contacts within a user's mailbox. Backup data is encrypted with an individual AES 256 bit key.



# 365 TOTAL BACKUP

## Key features include:

**Multi-Tenancy:** Manage and monitor all your Microsoft 365 backups through Hornetsecurity's centralised, multi-tenant, online management console. You can select individual settings for each organization.

**Backup dashboard:** The user-friendly dashboard provides an overview of all backup and restore activities, including backup status and history of the last restore. In addition, customers can set up backup status email notifications.

**Recover M365 data:** End users can independently recover their own mailbox and In-Place Archive mailboxes, OneNote, and OneDrive data through the „Recover M365 data“ feature accessible through the Hornetsecurity User Panel.

**Set it and forget it - automated backups:** M365 backups take place automatically several times per day.

**Adding users is a breeze:** 365 Total Backup enables you to auto-provision new users to be added to the backup list once they are created.

**M365 versioning and restore:** Any version of the file, conversation, mailbox or plan that exists in the backup can be restored at any time.

**Multiple recovery options:** Microsoft 365 mailboxes & In-Place Archive mailboxes, Teams Chats, OneNote, Planner, OneDrive accounts and Sharepoints can be restored in various ways: to the original account, to a new account for the same user, downloaded as a zip archive or exported as PST.

**Granular recovery of files or email items:** Microsoft 365 mailboxes & In-Place Archive mailboxes, Teams Chats, OneNote, Planner, OneDrive accounts and Sharepoints can be restored in various ways: to the original account, to a new account for the same user, downloaded as a zip archive or exported as PST.

**Audit account activity:** Review a range of actions such as users enabling or disabling mailboxes & In-Place Archive mailboxes, Teams, OneNote, Planner, OneDrive and SharePoint backups; users' data browsing activity; and their restore requests. You can also export your audit if required.

**Custom retention periods:** You have the option to set up custom retention periods, allowing for maximum compliance with your internal policies. This functionality allows for adherence with several frameworks and regulations such as ISO27001 and the GDPR.

**Backups are immutable:** and cannot be deleted or altered by any external parties. Backup Data deletion can only be affected by administrative accounts within 365 Total Backup itself.

**Four-eye approval process:** An additional layer of security that mitigates risks of losing data due to actions of rogue and novice administrators, demanding that sensitivity actions such as deletion of data, changes to company settings, and more, require at least one approval from a selected approving administrator.