HORNETSECURITY

FACT SHEET

365 TOTAL BACKUP

365 Total Backup is unique to M365 backup solutions: Besides backing up email, Teams, Planner, OneDrive and SharePoint, it also enables you to back up files on users' Windows-based endpoints.

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

- Back up and restore all Microsoft 365 data
- Easy configuration and multi-tenant management
- Automatic and hassle-free

What is affected?

365 Mailboxes, Teams, Planner, Sharepoint, OneDrive & Windows-based Endpoints

How does 365 Total Backup help you?

Hassle-free with one all-inclusive fee

Unlimited storage, one all-inclusive fee, centralized management, 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.

What improves?

Robust M365 data protection

With Hornetsecurity 365 Total Backup, you automatically back up your user and group Microsoft 365 mailboxes; user and group Team Chats; group plans from Microsoft Planner and any shared files, including recordings of Teams meetings; and files stored within OneDrive, SharePoint Document Libraries and Windows-based endpoints. 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.

HORNETSECURITY

FACT SHEET

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.

Backup of on-premise and roaming endpoints: Any endpoint, whether at the office or anywhere around the world, can be backed up without requiring a VPN.

Group-based endpoint backup policies: Configure settings for large groups of Windows endpoints by setting up policies to define backup directories, storage, frequency and retention.

Set it and forget it - automated backups: M365 backups take place automatically several times per day. For endpoints, backups can be set to take place every 1 to 24 hours.

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, Teams Chats, 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, Teams Chats, 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, Teams, 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.