Backup Everything

TECHNICAL DATASHEET

Device Protect365

Overview

Deep Dive into the main Features

Device Protect365 supports a wide range of operating systems however to summarize what the solution can do, we have categorised as follows:

- Backup Sets
- Security
- General

Data loss can be down to human error, hardware failures, software issues, malware and even natural disasters. Accidental deletion of files, incorrect storage device formatting, or improper shutdowns are common issues.

We aim to go into the main features and explain what they are and the benefits of how they can help you in your backup strategy to protect you from any such situation that may occur.

Backup Sets

Flexible, Configurable and Efficient

Multi-Platform Compatibility

Device Protect365 supports a wide range of operating systems, including Windows, macOS, Linux and others. This cross-platform support allows you to protect your entire IT infrastructure—workstations, laptops, and servers—regardless of the operating system being used.

We support all major operating systems and popular NAS devices including:

- Microsoft Windows Desktops
- Microsoft Windows Servers
- macOS
- Linux
- Databases
- VMware
- Hyper-V
- Synology
- QNAP

Data Compression

Before data is uploaded to the cloud, it is compressed at the source. This minimizes the amount of data transferred and stored, helping businesses save on bandwidth costs and storage space while speeding up the backup process.

Data Deduplication

The backup engine detects and removes duplicate data, reducing backup storage requirements and increasing performance. This is especially useful in environments where multiple systems generate redundant or similar data sets.

How much Space can be saved?

- 10-20% for regular files (exc PDF's, Videos, Photos)
- 50%+ for databases (MS SQL, MySQL, etc.)
- 50%+ for Hyper-V and VMware

File Filtering

Administrators can define granular rules to include or exclude specific file types or paths from backup. This ensures that only relevant data is captured, improving performance and avoiding unnecessary storage of temp files, caches, or non-essential media.

Bandwith Throttling

Customizable bandwidth control allows you to limit the amount of network traffic used during backups. This prevents congestion during working hours and ensures critical business operations aren't impacted by data transfer loads.

Backup Scheduling

Create scheduled backup jobs to run at specified intervals —hourly, daily, weekly, or monthly. You can also set multiple schedules for different backup sets, ensuring critical data is protected in line with business policies.

Data Retention Policies

Set policies to retain different versions of files for a specific period or number of days. This allows for recovery from accidental deletion, overwrites, or ransomware attacks by restoring older clean versions.

Open File Backup (VSS)

Supports backing up files even when they are in use, using Microsoft's Volume Shadow Copy Service (VSS). This is critical for businesses using documents that are constantly being accessed or edited.

Security

Enterprise-Grade Protection

Multi-Factor Authentication (MFA)

Adds an extra layer of login security to protect against unauthorized access. Users must verify their identity via an authentication app or code in addition to their password, making credential theft far less effective.

End-to-End Data Encryption

All data is encrypted using AES 256-bit encryption before it leaves the device. It remains encrypted during transfer and storage. Only the customer has the encryption key, ensuring complete confidentiality and compliance with GDPR and other data protection standards.

Restore Drill (Backup Verification)

Perform test restores without affecting live data to confirm that backups are complete and recoverable. This proactive feature helps ensure you'll be able to restore successfully in the event of real data loss.

Data Integrity Check

During backup and restore operations, integrity checks are run to verify the accuracy of each file. This guarantees that corrupted or incomplete files are flagged and helps maintain the reliability of the backup system.

There are many ways to ensure the integrity of the backup data.

- Post-backup check is to verify that all the data transferred to the backup destination is correct. Check the email reports and what has been uploaded and do a test restore.

- Periodic data integrity checks, the system does a health check to verify all data on the backup destination is correct.

- Manual Data integrity check, the user can perform a health check to verify all data on the backup destination is correct at anytime.

General Functionality

Tools for Visibility and Management

Backup Notifications

Receive alerts via email for job success, failure or warnings. This helps IT teams monitor and respond to backup activity proactively and avoid downtime or missed backups.

Custom Script Support

Allows integration of pre- and post- backup scripts. Automate actions such to give more control over the system.

Quota Restriction

Control the storage for every account by setting a limit. If the limit is reached then the backups will stop. This allows flexibility on agreed storage between all parties without storage costs increasing and errors if folders are accidently selected for backup.

Technical Summary

Feature	Description
Platforms Supported	Windows, macOS, Linux, Databases, VMware, Hyper-V, Synology and QNAP
Backup Types	Full then Incremental
Storage Locations	Our Storage or your own S3 Storage
Compression & Deduplication	Source-side file compression and block-level deduplication
Encryption	AES 256-bit (in-transit and at-rest)
Authentication	Username + Account Password + Encryption Password + MFA + Timeout
File Versioning	Define how long you want to keep the data to restore back from
Bandwidth Management	Custom bandwidth throttling per backup schedule if needed
Notifications	Email alerts and logs for backup statuses
Automation Support	Custom scripting for pre/post jobs

Never Lose your Data again

Device Protect365 is your peace of mind in a world full of data threats. Whether it's accidental deletion, hardware failure, or a ransomware attack—we've got your back.

Ready to protect your devices?

Visit: www.backupeverything.co.uk

or call us on +44 (0)345 055 9207

Backup Everything