MICROSOFT 365 BACKUP: AN INDEPENDENT ADVISORY GUIDE

Your Data, Your Responsibility

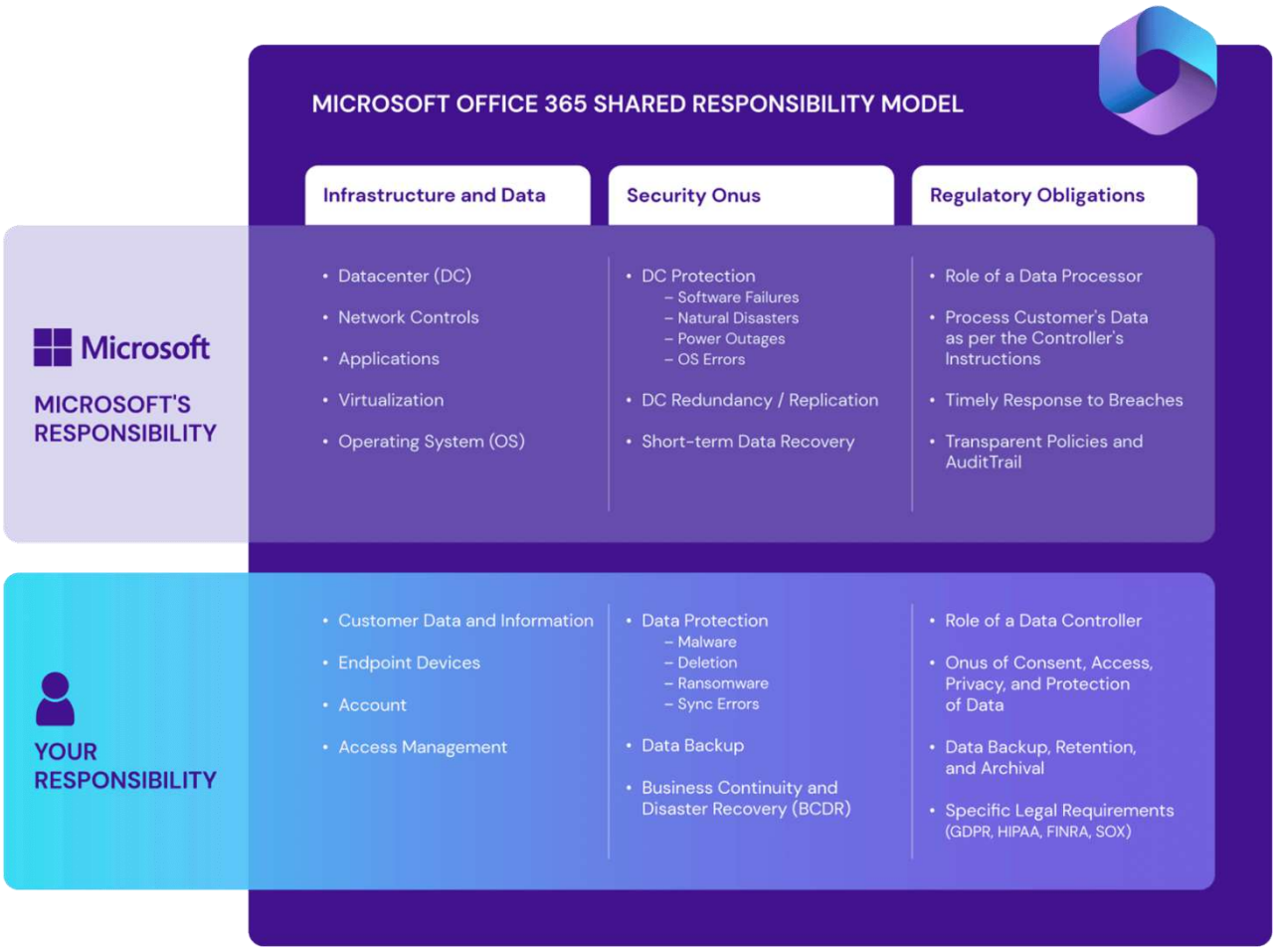
Prepared by ET Works | February 2026

CONTENTS

EXECUTIVE SUMMARY

Microsoft does not back up your data. Under the Shared Responsibility Model, Microsoft ensures platform availability whilst you remain responsible for data protection and recoverability.

In 2025, 30.2% of organisations lost data within M365, up from 17.2% the previous year driven by accidental deletions, misconfigured policies, ransomware and internal threats. Microsoft's native retention windows are limited, and once data is permanently deleted or overwritten, recovery without an independent backup is not possible.



- *Figure 1: Microsoft Office 365 Shared Responsibility Model, reproduced from HYCU.com*

Critically **replication is not backup.** Microsoft's geo-redundant infrastructure protects against hardware failure but not logical data loss. When a user deletes a file or ransomware encrypts a library, that change replicates instantly across all copies. Independent backup adhering to the 3-2-1 rule (three copies, two media types, one offsite) is essential. Microsoft's native tools alone do not satisfy this principle.

Pricing models: Per-user pricing offers predictability and suits data-heavy environments. Per-capacity (per-GB) pricing can escalate as backups accumulate. Model both scenarios against actual user count and data footprint before deciding.

Email archive is distinct from backup: Archive serves compliance, eDiscovery and long-term immutable retention captured in real-time at the gateway. Check Point Harmony Email,

Barracuda and Mimecast offer add-on archiving alongside email security. Cryoserver and MailStore provide standalone archive platforms.

Entra ID is also at risk: Microsoft's 30-day recycle bin does not cover the full scope of identity objects. Users, groups, roles, conditional access policies and app registrations all require independent protection, and coverage varies significantly across vendors.

Migration risk: Historical backup data typically cannot be migrated between vendors. Run platforms in parallel, export critical data and do not cancel outgoing contracts prematurely. Inactive mailboxes may require temporary Microsoft 365 licence reactivation to migrate data.

*Based on direct evaluations and structured bake-offs, ET Works' primary recommendations are **Keepit** and **AvePoint** for the majority of M365 environments, and **HYCU** or **Rubrik** for organisations with multi-platform requirements, existing Nutanix infrastructure or broader cyber recovery strategies.*

THE INDEPENDENT BACKUP MARKET LANDSCAPE

Beyond Microsoft's own offering, the independent M365 backup market is substantial and growing. Analyst coverage from both **Gartner** and **IDC** confirms this is a mature, competitive space, though neither framework exclusively covers the pure-play M365 backup segment, both encompass broader enterprise backup and SaaS data protection markets.

The most relevant analyst reference point for organisations evaluating dedicated cloud-to-cloud protection is the **IDC MarketScape for Worldwide SaaS Data Protection 2025–2026**, which specifically assesses vendors on their ability to protect M365 and broader SaaS application stacks.

The **Gartner Magic Quadrant for Backup and Data Protection Platforms** (2025) covers the wider enterprise infrastructure market and is a useful secondary reference, particularly for organisations with hybrid or on-premises workloads to consider alongside M365.

Analyst Report	Leaders	Major Players / Visionaries	Primary Focus
IDC SaaS Data Protection 2025-2026	Keepit, HYCU	Rubrik, Cohesity, Commvault, Rewind	Cloud-to-cloud, SaaS-native
Gartner Backup & Data Protection 2025	Commvault, Veeam, Druva, Rubrik	HYCU (Visionary), Veritas, Dell	Enterprise hybrid and multi-cloud

Table 1: Key vendor positioning in relevant analyst reports

The key takeaway from reading these two reports together is that the vendors best positioned for **pure SaaS and M365 protection** are not always the same as those dominating the broader enterprise backup market. An organisation selecting a Gartner Leader primarily for its enterprise infrastructure credentials may find it is investing in significant complexity and cost for a requirement that a SaaS-specialist could fulfil more efficiently.

With over **30 M365 backup providers** now active in the market, the practical challenge is less about finding a solution and more about identifying the right balance of simplicity, coverage, pricing model and commercial terms for each organisation requirement.

PRICING MODELS: PER-USER VS PER-CAPACITY

One of the most commercially consequential decisions when selecting an M365 backup solution is choosing between a **per-user** and **per-capacity (per-GB)** pricing model. Each carries distinct advantages depending on the organisation's profile, and the right answer is rarely obvious without modelling both scenarios against an organisation's actual environment.

PER-USER PRICING

Under a per-user model, pricing is tied to the number of licensed or active users, typically including unlimited or unmetered storage as part of the subscription. This model is widely favoured for its **predictability and simplicity**.

When per-user is the better fit:

- Organisations with consistent headcount and manageable off-boarding volumes
- Environments where users store large volumes of data in OneDrive, SharePoint or Exchange, as heavy data per user makes per-capacity expensive
- Organisations where budget certainty and auditable billing are a priority
- Mid-market and enterprise organisations where per-user costs can be negotiated favourably at volume

PER-CAPACITY PRICING

Under a per-capacity model, organisations pay for the volume of backup storage consumed, similar to Microsoft's own $0.15/GB/month approach. This can appear attractive at the outset, particularly for organisations with a small number of users and lean data volumes.

When per-capacity may suit:

- Large enterprises with many licensed users but low or well-controlled data footprints
- Organisations with high staff turnover who do not wish to carry seat licences for former employees
- Environments where granular cost attribution per workload is commercially required

WHY MODELLING BOTH SCENARIOS MATTERS

The assumption that per-capacity pricing is cheaper for large organisations is often misleading. As modern environments accumulate data through Teams recordings and large SharePoint libraries, most reach a break-even threshold where per-user pricing becomes the more cost-effective option. Capacity costs grow indefinitely with data accumulation; per-user costs remain fixed regardless of storage volume.

Key variables ET Works models with organisations include:

- **Data accumulation** — the rate at which historical backups drive up capacity costs over time
- **Volume discounts** — negotiated per-user rates available at larger headcount
- **Inactive users** — whether former employees are backed up for free or charged as active seats

In many cases, a negotiated per-user rate delivers a lower total cost for large data estates than a per-capacity model.

ET Works' approach is to identify the most cost-effective model for each organisation's specific circumstances rather than defaulting to one pricing structure. Where the numbers are close, per-user pricing is generally preferred for its predictability and simplicity.

VENDOR OVERVIEW: WHAT WE HAVE SEEN IN THE MARKET

The Microsoft 365 backup market has matured significantly, shifting from basic data duplication to comprehensive cyber-resilience and governance platforms.

As organisations increasingly recognise that Microsoft's Shared Responsibility Model places the burden of data protection squarely on the customer, demand for independent backup has accelerated and the market has consolidated around a recognisable group of vendors that appear consistently across organisation evaluations, analyst reports and competitive bake-offs.

With over 30 providers now active in this space, the challenge is rarely finding a solution but identifying the right fit. Feature parity across leading solutions is closer than many expect; the meaningful differences lie in pricing architecture, storage independence and the vendor's long-term ability to support migration, compliance and retention at scale. The market is consolidating around cloud-native SaaS-delivered platforms, with continuous backup, AI-assisted anomaly detection and rapid rollback becoming standard expectations rather than premium features.

The vendors below represent the strongest performers in the current landscape, selected for their proven ability to handle complex recovery scenarios, large-scale data migrations and regulatory requirements across a range of organisation sizes and complexity levels.

Primary recommendations:

- Keepit — *IDC SaaS Data Protection Leader*. Best for simplicity and independent cloud storage with transparent per-user pricing that includes unlimited retention.
- AvePoint — *Microsoft 365 Backup Storage Partner*. Best for organisations requiring governance, migration capabilities or Microsoft-aligned assurances.
- HYCU — *IDC SaaS Data Protection Leader*. Best for multi-SaaS environments and Nutanix users, offering "bring-your-own-storage" flexibility.
- Rubrik — *Gartner Quadrant Leader & Microsoft 365 Backup Storage Partner*. Best for enterprise-grade cyber recovery and security integration.

	Microsoft Backup Storage Partner	Storage Logic	Pricing Models	Delivery Options
Keepit	Standard Integration	Independent Cloud	Per-User (Unlimited)	Managed Service / Subscription
AvePoint	Preferred Partner	Azure-Hosted / Pooled	Per-User & Per-Capacity	Managed Service / Subscription
HYCU	Standard Integration	BYO Storage (Azure/AWS/S3)	Per-User & Per-Capacity	Managed Service / Subscription
Rubrik	Preferred Partner	Security Cloud / Hybrid	Per-User & Per-Capacity	Managed Service / Subscription

Table 2: Primary vendor comparison: storage, pricing and delivery

EMAIL ARCHIVE: A DISTINCT BUT ADJACENT CONSIDERATION

Email archive is frequently conflated with email backup, but they serve fundamentally different purposes.

Microsoft 365 includes some native archiving capability (In-Place Archive and Litigation Hold) within E3 and E5 licensing tiers, though coverage is not universal and management can be cumbersome.

	Email Backup	Email Archive
Primary purpose	Recovery from data loss or corruption	Long-term retention, eDiscovery and compliance
Data capture	Scheduled point-in-time snapshots	Real-time in-flight capture at the gateway
Storage	Point-in-time restorable copies	WORM (Write Once Read Many) immutable storage
Retention	Typically 1 to 7 years, point-in-time	Often 7 to 10+ years, immutable
Access	IT-led restore on request	End-user and legal/compliance access
Search capability	Item-level restore	Full-text eDiscovery and legal hold
Compliance driver	Business continuity	Regulatory (FCA, GDPR, FINRA, HIPAA)

Table 3: Backup versus archive: functional and compliance distinctions

For organisations requiring a dedicated archive solution, particularly in regulated sectors, the following approaches are worth considering:

ADD-ON TO AN EMAIL SECURITY SOLUTION

Several email security vendors (including Check Point, Mimecast, Barracuda) offer email archiving as an integrated module alongside their core security services, making this a commercially efficient route for organisations who are already invested in a security platform.

STANDALONE ARCHIVE PLATFORMS

Where email archiving is a first-class compliance requirement rather than an add-on consideration, a dedicated platform (such as Cryoserver, MailStore, Smarsh, Global Relay or Veritas Enterprise Vault) may be the more appropriate route.

WHY MANY ORGANISATIONS NEED BOTH

Backup and archive are not interchangeable — backup protects against data loss and ensures operational recovery, whilst archive satisfies the immutable, long-term retention requirements demanded by regulators such as the FCA, GDPR and HIPAA.

For organisations in financial services, legal, healthcare or any sector with formal data retention obligations, both capabilities should be in place and are best evaluated together rather than as separate procurement decisions.

BACKING UP MICROSOFT ENTRA ID

Microsoft Entra ID (formerly Azure Active Directory) is the identity backbone of your Microsoft 365 environment. It controls who can access what, across every application, device and service your organisation relies on. Despite this, it is one of the most commonly overlooked components when organisations plan their M365 backup strategy.

Entra ID stores users, groups, roles, app registrations, conditional access policies, administrative units and directory configurations. If any of these are accidentally deleted, maliciously modified or corrupted, the downstream impact extends far beyond a lost file. Without a restore point, rebuilding an identity environment manually is a significant and time-consuming undertaking, and certain configurations may not be fully recoverable at all.

What an Entra ID backup should cover:

- User accounts, including attributes and group memberships
- Security and Microsoft 365 groups
- Conditional access policies
- App registrations and enterprise application configurations
- Roles and administrative assignments
- Administrative units and directory settings

	Microsoft Native Tools	Independent Backup
Deleted users and groups	30-day recycle bin only	Full restore to any point in time
Security and Microsoft 365 groups	30-day recycle bin only	Full restore to any point in time
Conditional access policies	No native backup or versioning	Policy versioning and restore
App registrations	No native backup	Captured and restorable
Role assignments	No native backup	Captured and restorable
Administrative units	No native backup	Captured and restorable
Directory configuration	No native backup	Captured and restorable

As organisations deepen their reliance on Entra ID for single sign-on, Zero Trust frameworks and device management through Intune, the blast radius of an identity incident grows considerably. Entra ID coverage varies significantly across vendors and should be included as a scored criterion in any structured evaluation.

MIGRATING BETWEEN BACKUP PROVIDERS

Switching backup providers is more complex than it first appears. The single most important thing to understand is that **historical backup data almost never transfers between vendors** — all snapshots, version history and point-in-time restores held by the outgoing provider become inaccessible once the contract ends.

What you lose when you switch

- **Historical data** — previous restore points are gone once the old contract ends; there is no import mechanism between platforms
- **Retention continuity** — if regulatory obligations require retention back to a specific date, a migration creates a gap unless the outgoing contract is extended through the transition
- **Metadata integrity** — manual data exports can lose critical attributes such as Created By dates, Modified timestamps and original sharing permissions
- **Configuration** — backup schedules, retention policies, user mappings and exclusions must all be rebuilt from scratch on the new platform

Licensing and identity considerations

- Inactive or departed users whose Microsoft 365 licences have been removed may need to be **temporarily reactivated** to allow the new platform to ingest their historical data — an unexpected cost if not planned for
- Verify that **User Principal Names (UPNs)** match across both platforms before cutover; mismatches will cause data attribution failures

How to minimise risk

1. **Run both platforms in parallel** for 30 to 90 days to retain access to historical restores during the transition
2. **Export critical data** in portable formats such as PST or CSV before decommissioning the old platform
3. **Test restores** across Exchange, SharePoint, OneDrive, Teams and Entra ID on the new platform before going live
4. **Don't cancel the outgoing contract prematurely** — treat the overlap cost as a necessary insurance premium

***The single most common mistake** is cancelling the old service the moment the new platform goes live — leaving the organisation with no way to recover any data from before the migration date.*

Expect 1–3 months of dual-platform subscription costs during transition; this is normal and should be treated as insurance against data loss.

A GREAT BACKUP BAKE-OFF

Choosing an M365 backup platform is rarely as simple as comparing datasheets. Through direct vendor evaluations and pricing comparisons across multiple providers, ET Works has developed informed preferences across the leading platforms.

Where requirements are complex, budgets are constrained, or an organisation wants to validate a recommendation against their own specific recovery and compliance scenarios, a bake-off offers a structured way to put a shortlist of providers through their paces side by side — a head-to-head evaluation against an agreed set of technical, commercial and operational criteria.

HOW A BAKE-OFF WORKS IN PRACTICE

A meaningful bake-off requires planning and coordination. As a guide, allow around an hour per vendor for an initial demonstration and Q&A — a shortlist of three to five providers typically equates to a full day of effort, though in practice this is best spread across several days.

ET Works manages the evaluation end to end, covering:

- Evaluation criteria — defined around the organisation's specific requirements rather than a generic checklist
- Scoring guidance — how to score what matters most, recognising that priorities differ by organisation
- Vendor briefing — each provider receives a consistent brief covering the environment, data volumes and compliance requirements
- Scheduling — coordinating availability across multiple vendors and keeping the process to a workable timeline
- Normalised pricing — different commercial models are mapped to a like-for-like comparison to support a confident decision

In some cases a full bake-off is not required. ET Works will also run a pricing-focused comparison across multiple vendors to find the most appropriate balance of functionality and cost.

THE PROOF IS IN THE TASTING

The following are anonymised examples of recent engagements:

UK University — With M365 backup not yet formalised across the institution, there was a need for a solution that could protect both staff and student data without creating a management overhead for the IT team. ET Works coordinated vendor demonstrations, managed all commercial discussions and negotiated pricing, allowing the internal team to focus on evaluating each platform on its own merits. A solution was selected and implemented within budget.

NHS Trust — Rising storage costs under a per-capacity model prompted a review of per-seat pricing for better long-term cost control. ET Works worked through the options with relevant vendors, supporting an expansion of retention policies and improvements to governance and management. The transition to a per-seat model provided a more predictable and sustainable commercial framework aligned to the Trust's long-term data protection requirements.

HOW ET WORKS CAN HELP

Every organisation's M365 environment is different and whilst Microsoft 365 is often seen as the most critical platform, it may not be your only SaaS platform. If your business runs Salesforce, Atlassian (Jira/Confluence), ServiceNow or similar platforms, the same data loss risks that apply to M365 apply equally there.

ET Works can help you to assess your data footprint, model pricing scenarios and identify the solution best suited to your requirements. We work with multiple vendors in this space and are not tied to any single platform — our only obligation is to the outcome that is right for your organisation.

Whether you need a straightforward recommendation or a structured bake-off across the leading platforms, we can help you decide with confidence.

Get in touch to arrange a no-obligation conversation.

E: hello@etworks.co.uk
W: etworks.co.uk

DISCLAIMER & METHODOLOGY

This document is prepared for advisory and consultative use, developed through formal vendor evaluations, direct engagements and ongoing market analysis. ET Works maintains partnerships with selected vendors in the M365 backup and data protection market; however, vendor inclusion reflects an independent assessment of market relevance, solution capability and suitability rather than commercial relationship alone. Pricing and product features are subject to change, and all figures should be validated with vendors prior to any formal proposal.

This guide uses publicly available information from Microsoft, IDC, Gartner and leading vendor product documentation, combined with ET Works' direct experience from formal evaluations and structured vendor bake-offs. Analyst references include the IDC MarketScape for Worldwide SaaS Data Protection 2025–2026 and the Gartner Magic Quadrant for Backup and Data Protection Platforms 2025. All feature descriptions and pricing models reflect vendor documentation validated as of February 2026.

ABOUT THE AUTHOR

Marcus Evans is an industry veteran with over 30 years of experience supporting and advising organisations on Managed IT Services, Infrastructure, End-User Computing, Security, Networking and Business Applications. A nomadic British-Australian dual citizen who has lived and worked across seven countries, Marcus brings a uniquely global perspective to the challenges facing IT leaders and service providers today. As the Commercial Manager at ET Works he writes on the topics of cloud services, data protection and the evolving managed services landscape. Outside of work, he is on a long-running quest to reach a single-figure golf handicap (progress ongoing).

APPENDIX: M365 BACKUP MARKET — VENDORS OF NOTE

The following is a non-exhaustive list of providers active in the M365 backup and SaaS data protection market as of early 2026. This list is provided for reference only and does not constitute a recommendation.

Primary Recommendations

- AvePoint ⭐ — Microsoft 365 Backup Storage Preferred Partner; strong governance, migration and compliance capabilities
- HYCU R-Cloud ⭐ — IDC SaaS Data Protection Leader; bring-your-own-storage flexibility with 80+ SaaS application coverage
- Keepit ⭐ — IDC SaaS Data Protection Leader; fully independent cloud storage with transparent per-user pricing and unlimited retention
- Rubrik Security Cloud ⭐ — Gartner Magic Quadrant Leader and Microsoft Preferred Partner; enterprise-grade cyber recovery and security integration

Notable Managed Service Option

- ConnectWise SaaS Backup (powered by Keepit) ⭐ — This provides the "IDC Leader" technology of Keepit delivered as a fully managed service via the ConnectWise platform

All Other Vendors (alphabetical)

- Acronis Cyber Protect Cloud — Combined backup and cyber protection platform popular in the MSP channel
- Afi.ai — Cloud-native SaaS backup focused on Google Workspace and M365
- Altaro (Hornetsecurity) — MSP-focused backup with strong Office 365 coverage under the Hornetsecurity umbrella
- Arcserve — Established enterprise backup vendor with SaaS and hybrid coverage
- Asigra Tigris — Channel-delivered, agentless backup with strong security and compliance features
- Axcient x360Cloud — MSP-focused platform combining backup, business continuity and cloud recovery
- Backupify (Kaseya) — SaaS-native M365 and Google Workspace backup, part of the Kaseya stack
- Bacula Enterprise — Open-source-based enterprise backup with broad workload support
- Barracuda Cloud-to-Cloud — M365 backup with integrated email security and archiving options
- CloudAlly — Straightforward SaaS backup for M365 and Google Workspace
- Cohesity DataProtect — Enterprise data management platform with SaaS protection capabilities
- Commvault Cloud — Enterprise-grade platform with broad hybrid and SaaS workload coverage

- ConnectWise Cloud Backup (formerly SkyKick) — Now a core ConnectWise product following the 2024 acquisition; primarily focused on MSP-led M365 migrations and standard protection
- Cove Data Protection (N-able) — MSP-delivered backup with cloud-first architecture
- CrashPlan — Endpoint and cloud backup with a focus on remote workforce protection
- Datto (Kaseya) — MSP-focused backup and business continuity platform
- Druva — Cloud-native data protection with strong compliance and eDiscovery features
- IBM — Enterprise data protection within broader IBM storage and security portfolio
- Metallic (Commvault) — SaaS-delivered version of Commvault targeting mid-market and enterprise
- Microsoft 365 Backup (Native) — Microsoft's high-speed recovery tool; excellent for rapid restoration but lacks long-term offsite independence (does not satisfy the 3-2-1 rule on its own)
- MSP360 — Affordable cloud backup platform popular with smaller MSPs
- NAKIVO — Cost-effective backup for virtual, physical and cloud environments including M365
- NinjaOne SaaS Backup — RMM-integrated backup leveraging Dropsuite's M365 capabilities
- Redstor — Cloud-native backup with AI-powered recovery, popular in the UK market
- Spanning (Kaseya) — SaaS backup for M365 and Google Workspace within the Kaseya ecosystem
- SpinOne — SaaS security and backup platform with ransomware protection focus
- SysTools — Backup and migration toolset, primarily SME-focused
- Veeam Data Cloud — The market share leader's SaaS-native evolution, providing the familiar Veeam recovery power without the infrastructure overhead
- Veritas Alta SaaS Protection — Enterprise-grade SaaS data protection within the Veritas portfolio
- Zerto (HPE) — Continuous data protection and disaster recovery, primarily enterprise hybrid environments

⭐ ET Works primary recommendation. *This list is not exhaustive — additional vendors may exist as white-label offerings, reseller-branded services or regional variants built on the platforms above.*