Acronis

WHITEPAPER

Six costly data protection gaps in Microsoft 365 and how to close them

MICROSOFT 365 IS A DATA LOSS DISASTER WAITING TO HAPPEN

If your business relies on Microsoft 365, you can expect reliable access to its applications with very high uptime. But many IT professionals are laboring under a dangerous misconception: that Microsoft provides fully-fledged data protection and long-term data retention for Microsoft 365.

The reality is that the emails, attachments, and shared files stored in Microsoft 365 are not protected from the most common and serious data loss issues, ranging from simple accidental deletions to sophisticated malware attacks.

Thus for many organizations, Microsoft 365 represents a major data protection gap, an unhappy surprise waiting to happen. Too late, they may learn that Microsoft provides only limited features to help restore lost, destroyed or damaged Microsoft 365 data, with nowhere near the backup functionality or robustness with which most businesses protect their other critical applications.

> This paper outlines several easy-to-miss limitations of Microsoft's data protection capabilities, and examines how you can address those shortcomings to ensure that you can quickly recover from the many data loss issues to which Microsoft 365 is vulnerable.

6 WEAK SPOTS IN MICROSOFT'S PROTECTION OF MICROSOFT 365 DATA

Microsoft has invested heavily in its data centers' hardware, software, networks, security and operations to ensure high levels of performance, access and uptime for Microsoft 365.

It can quickly detect and recover from many of its own operational errors, site outages, hardware failures and network issues to meet its service-level agreements, which center on application uptime. But these measures do not protect your business from many common Microsoft 365 data loss issues, e.g., the need to restore an email that got deleted by accident, or a OneDrive for Business file that was misplaced, or a library of SharePoint Online content that became corrupted by a malware attack.

> Microsoft offers very limited restoral capabilities for most Microsoft 365 data, and only retains files for a short time (varying from a few weeks to a few months, depending on the application and contract). You may determine that the data residing in a former employee's repository or a long-idle project is suddenly important again, only to find that Microsoft did not retain a copy that you can quickly find and recover.

ACCIDENTAL DELETION ISSUES	INSIDER SECURITY THREATS
MIGRATION FROM PREMISES-BASED MICROSOFT OFFICE	RETENTION POLICY ISSUES
EXTERNAL SECURITY THREATS	LEGAL AND COMPLIANCE ISSUES

MICROSOFT 365 ADMINISTRATORS NEED TO ADDRESS MICROSOFT'S DATA PROTECTION SHORTCOMINGS IN SIX KEY AREAS:

1. Accidental deletion issues

DATA RISK: In the course of their daily work, IT administrators and ordinary employees routinely delete Microsoft 365 user profiles, Exchange Online emails, attachments & files, OneDrive for Business files, and SharePoint Online content. These deletions may be accidental in nature, or intentional but later regretted – most of us have suddenly needed to refer to an email that we deleted only yesterday.

MICROSOFT WEAKNESS: These kind of everyday resource deletions are routinely replicated across the network. The age of the resource exacerbates the problem: older data may be hard-deleted and unrecoverable. More recent deletions of newer resources are slightly less problematic, as soft-deleted files and emails may be recoverable in the short term from the Recycle Bin or Recoverable Items folder.

2. Retention policy issues

DATA RISK: Changing or misaligned priorities in Microsoft 365 data retention policies can result in data being hard-deleted. This can only be partially mitigated by regular review and updating of retention policies.

MICROSOFT WEAKNESS: Microsoft 365 customers have the onus of managing retention policies, but if for whatever reason a hard-deletion occurs due to aging out of the existing retention policy, Microsoft has no ability to recover the deleted resource.

3. Insider security threats

DATA RISK: In addition to routine, non-malicious deletions, Microsoft 365 resources need to be protected against malicious alteration or destruction of data by disgruntled or terminated employees, contractors or partners.

MICROSOFT WEAKNESS: With the exception of relatively recent deletions of relatively new resources, Microsoft does not protect against malicious insider destruction or alteration of Microsoft 365 data.

4. External security threats

DATA RISK: Microsoft 365 data is vulnerable to destruction or alteration by a variety of malware threats, most notably ransomware, which encrypts user data and holds it hostage until an online ransom is paid. These attacks may be mounted by hackers, cybercriminals or hostile state actors.

MICROSOFT WEAKNESS: Microsoft offers very limited protections against malware attacks like ransomware, and limited ability to restore malware-encrypted or -altered files to their pre-attack state.

5. Migration from premises-based Microsoft Office

DATA RISK: The migration from the traditional premises-based Microsoft Office application suite to cloud-based Microsoft 365 services usually involves transitioning from a legacy data protection solution to a new cloud-capable one. The two backup solutions are often incompatible, making it impossible to restore legacy data into the new environment.

MICROSOFT WEAKNESS: Microsoft offers no solution to address data loss issues during Office to Microsoft 365 migration. Few third-party data protection solutions integrate backup functionality for Office and Microsoft 365: they usually do one or the other but not both.

6. Legal and compliance issues

DATA RISK: Compliance requirements (like the European Union's GDPR regulations) and legal issues can exacerbate the business costs of the unprotected data losses described above. Unrecoverable Microsoft 365 data loss can expose the business to government or industry-specific regulatory fines, legal penalties (e.g., damages or lost lawsuits stemming from failure to meet e-discovery or evidentiary requirements), revenue and stock price losses, loss of customer trust, and damage to the company brand.

MICROSOFT WEAKNESS: With all of the associated data loss risks described above, Microsoft can do little to protect organizations using Microsoft 365 against a variety of compliance and legal exposures. For example, after a ransomware attack, a business storing its EU-based customers' personal data in SharePoint Online might be unable to honor requests for copies of that data, thereby violating GDPR requirements.

THE BOTTOM LINE

Once you understand the various soft spots in Microsoft's ability to protect Microsoft 365 data, you can start looking at data protection solutions that address those gaps. We all know the stakes are high: failure to defend an Microsoft 365 data loss can be career-limiting.

ACRONIS DELIVERS COMPLETE, GRANULAR BACKUP FOR MICROSOFT 365 WITH ENHANCED SEARCH FEATURES

Acronis Cyber Backup protects your Microsoft 365 data with direct, agentless backup from most Microsoft data centers to the Acronis global network of data centers. It offers a welter of enhanced features that make it easy to find and restore a variety of Microsoft 365 resources in Microsoft Exchange Online, OneDrive for Business, and SharePoint Online at a very granular level. Acronis Cyber Backup licensing entails no upfront investments and no ongoing maintenance costs. Table 1 shows the feature breadth and flexibility of Acronis Cyber Backup for Microsoft 365:

ACRONIS CYBER BACKUP FOR MICROSOFT 365 FEATURE	EXCHANGE ONLINE	ONEDRIVE FOR BUSINESS	SHAREPOINT ONLINE
Data backed up	Emails, archived mailboxes, calendars, contacts, tasks	Files and folders	Sites, sub-sites, document libraries, lists, page libraries
Granular point-in-time recovery	Yes	Yes	Yes
Search through backup	Search mailboxes items	Search files	Search site items
Cross-user and cross-organization recovery	Yes	Yes	Yes
Restore to custom folder via live browsing	Yes	Yes	–
Preview email content	Yes	–	–
Download from backup	Yes for attachments	Yes for files	Yes for files
Send email from backup	Yes	–	–
Permissions recovery	–	Yes	Yes

Table 1. Acronis Cyber Backup for Microsoft 365 Features

> These highly granular search and restoral features make it possible to download a required file directly from the backup, to download any of multiple versions of documents (not only the most recent one), to send emails directly from the backup without having to restore them to your Exchange Online mailbox first, and to restore any data element to its original location or a new destination.

ACRONIS PROTECTS YOUR ENTIRE MICROSOFT ENVIRONMENT (AND EVERYTHING ELSE, TOO)

Acronis Cyber Backup is a **single data protection solution for your entire Microsoft environment**, whether your workloads are premises-based, hosted in private or public clouds, and/or hosted by Microsoft.

It also protects your **Microsoft virtual machines running on Hyper-V** and your Windows servers, desktops and mobile devices. It also protects a **broad range of non-Microsoft platforms**, including physical, virtual and cloud environments, plus servers running other popular operating systems and hypervisors, a variety of popular databases, and desktop OSes like macOS and mobile OSes like iOS and Android.

A single data protection platform for your entire IT environment eliminates the mutual incompatibility of standalone premises-only and cloud-only backup solutions. It also reduces the cost of licensing, education and integration. Figure 1 shows the 20+ platforms protected by **Acronis Cyber Backup.**

Further, the Acronis Cyber Backup user interface is simple enough to be run by IT generalists, allowing you to ramp up new data protection staffers quickly, save on daily operations costs, improve the service levels you deliver, and allow you to focus on higher-priority projects.

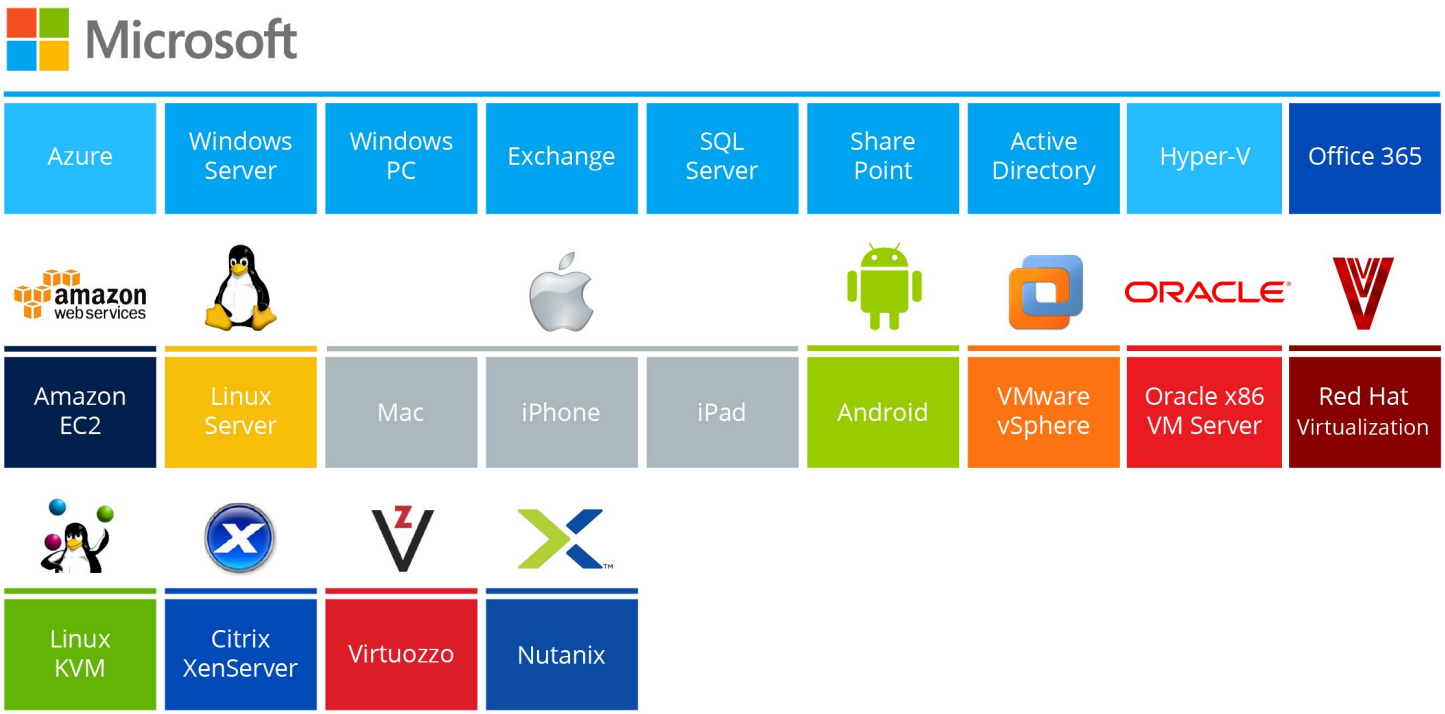

Figure 1. Platforms Protected by Acronis Cyber Backup

ACRONIS USES SIMPLE, EFFICIENT, AGENTLESS BACKUP

The backup agent component of **Acronis Cyber Backup for Microsoft 365** runs in the secure Acronis Cloud instead of on your premises, which streamlines and simplifies the process of configuration and maintenance.

ACRONIS BACKS UP YOUR MICROSOFT 365 DATA TO THE HIGHLY SECURE ACRONIS CLOUD

Acronis backs up Microsoft 365 data **directly from Microsoft data centers to the Acronis Cloud**, a global network of data centers secured via a comprehensive information security and compliance program that includes administrative, physical and technical controls based on ongoing risk assessment.

Our information security policies and processes are based on **broadly accepted international security standards** such as ISO 27001 and the National Institute of Standards and Technology (NIST), and take into account the requirements of related local regulation frameworks such as Europe's General Data Protection Regulation (GDPR) and the United States' Health Insurance Portability and Accountability Act (HIPAA).

Acronis Cloud security features include:

- **Enterprise-wide access control** based on unique user IDs and strong passwords, secure authentication protocols (LDAP, Kerberos, SSH certificates), two-factor authentication, and the use of web application firewalls
- **Multi-layered, zone-based data security** buttressed by real-time data encryption in transit and at rest, secure data transfer over HTTPS (TLS), enterprise-grade AES-256 encryption for customer data, and Acronis CloudRAID technology for maximal data availability
- **Rigorous, high-fences physical security** with access controlled by biometric hand-geometry scans and proximity key cards, video surveillance backed up by 90-day archiving, and staffed by security personnel 24x7x365
- **Highly available, redundant data center** infrastructure protected by UPS and backup diesel-generators, redundant HVAC, network and UPS, VESDA air sampling and dual zone pre-action (dry pipe) sprinkler systems, plus temperature and humidity monitoring

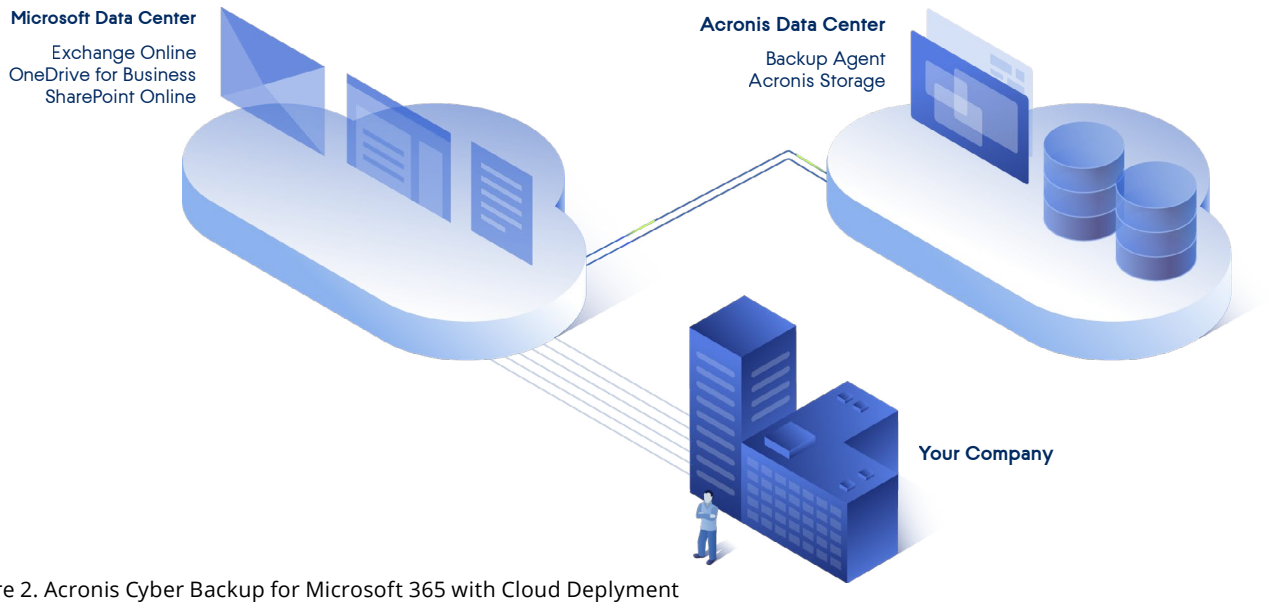

Figure 2. Acronis Cyber Backup for Microsoft 365 with Cloud Deplyment

ACRONIS PROVIDES ENHANCED PRIVACY

Acronis Cyber Backup protects data privacy against prying eyes with **multi-level backup encryption** reinforced by data transfers over the network with TLS encryption, data-center storage with high-grade disk-level encryption, and per-archive encryption using AES-256.

ACRONIS PROVIDES AUTOMATIC PROTECTION OF NEW MICROSOFT 365 USERS, GROUPS AND SITES

Once an initial Acronis backup plan has been configured and enabled for an Microsoft 365 environment, IT staff does not have to worry having to modify it every time a new Microsoft 365 user, group or site is added. **Acronis Cyber Backup automatically detects** when new users, groups or sites have been added and adds them to the backup plan.

ACRONIS SUPPORTS MICROSOFT AUTHENTICATION

Acronis supports Microsoft Multi-Factor Authentication (MFA) to enable the use of additional authentication measures like trusted devices or fingerprints.

ACRONIS PROVIDES POWERFUL REPORTING AND STATUS MONITORING TOOLS

Acronis provides **advanced reporting and backup status monitoring capabilities** to help IT staffers improve their efficiency and responsiveness. The Acronis management portal contain compact, easy-to-understand widgets containing all statistics for backup and restoral as well as reports, notifications and alerts for critical events.

CONCLUSION

If your business relies on Microsoft 365, you need to complement Microsoft's rudimentary data protection with Acronis Cyber Backup, the most reliable and easy-to-use backup for businesses of all sizes.

To learn more about **how Acronis Cyber Backup can greatly improve,** simplify and reduce the cost of protecting your Microsoft 365 data, get a complimentary 30-day trial here, or find an Acronis reseller here.

Acronis

For more information visit **www.acronis.com**