Is Microsoft Office 365™ Backup & Recovery Good Enough?
Making a Case for Third-Party Data Protection, Recovery and Archive to Reduce Risk & Exposure

In this issue

The Need for Third-Party Sync and Recover  2
Research from Gartner
Adopt Microsoft Office 365 Backup for Damage Control and Fast Recovery After Malicious Attacks  3
How to Take Action  12
About Us  13
The Need for Third-Party Sync and Recover

Every organization needs to keep data protected and accessible for its users. However, as adoption of Microsoft Office 365™ continues to rise, many are still unaware of the risky protection and recovery gaps within Office 365 when malicious attacks occur or point-in-time recovery is required. Leveraging a third-party archiving tool can automate and simplify the process of recovering your email and other Exchange data. According to Gartner, “Infrastructure and operations leaders using or evaluating Office 365 should consider investing in third-party tools for faster, more-flexible recovery options, as well as reputation damage control after a malicious attack.”

Where does Office 365 fall short? While it does provide adequate infrastructure recovery for the entire email system, it doesn’t offer the same capabilities at the user level. End users expect easy-to-use, self-service recovery and search of email, contacts and calendars without having to involve IT or complete complex training. To achieve advanced protection and recovery, an integrated end-user solution that is intuitive and in sync with Office 365 mailbox changes is required to reduce risk and boost productivity.

Moreover, malicious attacks through email continue to be the primary entry point and challenge for organizations and the effect can greatly impact the integrity of Office 365 email. When malicious attacks occur, or built-in Office 365 policy expirations are not enough to provide adequate end user recovery, customers need an additional layer of protection for resiliency. Limitations with Office 365 deleted items, recoverable items and legal holds make it cumbersome to manage and unreliable in e-discovery or compliance scenarios. Additionally, Office 365 customers are required to configure multiple policies and settings that may conflict with corporate retention policies, further impacting compliance.

The following Gartner research provides background on the adoption of Office 365, limitations on data protection and recovery as well as guidance on how to use third-party solutions in your cloud strategy.

Source: Mimecast
Microsoft O365 offers robust disaster recovery, but limited native backup and recovery. I&O leaders using or evaluating O365 should consider investing in third-party backup and recovery tools for faster, more-flexible recovery options, as well as reputation damage control after a malicious attack.

**Key Findings**

- O365’s native recycle bins and version histories are not true backups, and they don’t allow internal IT organizations to control backup and recovery; this presents potential security risks and slows recovery processes.

- O365 Exchange Online offers robust high availability, but lacks many options for customer-controlled backup and disaster recovery solutions.

- Third-party O365 backup tools provide recovery from internal threats and external attacks, as well as flexible and expanded policies including different backup retention periods.

- Some third-party email archiving tools provide a DR alternative for O365 Exchange Online, in addition to email governance and compliance capabilities.

**Recommendations**

I&O leaders involved in the evaluation of Microsoft O365 initiatives should:
Educate and convince other relevant key stakeholders (such as enterprise architects, security officers, and IT and compliance managers) regarding the potential data loss risks without a third-party backup solution.

Deploy a third-party backup tool to gain faster and more flexible recovery and damage control after serious attacks.

For heavily regulated and litigated organizations, adopt a third-party email archiving tool to recover from potential extended Exchange Online outages.

**Strategic Planning Assumption**

Enterprise adoption of third-party Office 365 backup solutions will increase from less than 25% today to more than 50% by 2020.

**Analysis**

The adoption of Microsoft Office 365 (O365) continues unabated. In an early 2016 Gartner Research Circle survey of 461 participants (see “Implementing Office 365: Gartner Survey Results and Analysis, 2016”), Exchange Online was cited as the top driver for O365 adoption (70%), followed by OneDrive for Business (49%) and SharePoint Online (41%). However, when production data moves to the cloud, many organizations don’t realize that they are still responsible for their data no matter where it’s located. Many are unclear as to whether O365’s native data protection and recovery mechanisms are sufficient, and wonder what their peers are doing.

To address the question, Gartner surveyed attendees at the Gartner Data Center Summit in the U.S. and London in December 2016. Of the 130 responding organizations that use O365 (57% of the total respondents), 48% stated that they use O365 native data protection functions, while 29% use a third-party backup tool. Due to the small sample size and the data center attendee profiles, Gartner believes the actual O365 backup adoption rate could be lower. Details of the results are shown in Figure 1 (refer to the Evidence section for survey details).

It’s not surprising that another 12% of respondents were looking for backup solutions that support both O365 Exchange Online and on-premises Exchange implementations, because, based on the Gartner Research Circle survey, many large organizations have hybrid implementations of Exchange (both in the O365 cloud and on-premises). The low percentage of respondents looking for a backup solution that can support all O365 applications is also expected, because not many organizations have adopted all three key components of O365 (Exchange Online, OneDrive for Business and SharePoint Online). A few organizations want to use their idle on-premises data center storage to host backup data, which is consistent with Gartner user client inquiry feedback.

This research analyzes what functions are missing or insufficient to meet business recovery needs in the three key components of O365: Exchange Online, OneDrive for Business and SharePoint Online. It also presents key third-party backup and disaster recovery (DR) options in the market.
What Is Missing in O365 Native Recovery Capabilities?

There are many levels of recovery needs — some are at the infrastructure and application level, and some are at user, mailbox or file level. Infrastructure- and application-level recovery typically involves high availability (HA) and DR. HA handles local data center hardware and software failures for user-transparent, seamless failover and is built into the application with its underlying server and storage platform in the same site. DR handles site disasters that take down the entire site and usually requires remote replicas of hardware and software in a geographically dispersed site, where applications and users can fail over.

With O365, Microsoft does a good job with recovery at the infrastructure and application level (HA and DR). O365 has a financially backed guarantee of 99.9% uptime, which translates into 8.76 hours of downtime a year. In 2016, the published worldwide uptime for Exchange Online ranged from 99.98% to 99.99% per quarter, translating to between 53 minutes and 1.75 hours of downtime per year. These availability statistics have shown a solid availability record and serve most customers’ needs.
However, HA and DR can’t recover all types of data loss and require a backup solution to meet operational recovery needs, such as file corruption, deletion and malicious attacks. Unlike HA and DR, backup must preserve healthy independent recovery points that are not linked to the primary data and must have secure access control. Moreover, backup offers more restore/recovery options than HA and DR, such as restores at different granular levels and restores to different devices and locations.

Unfortunately, O365 doesn’t have native backup and flexible recovery capabilities for user data. Rather, O365 relies on recycle bins and file version histories as recovery mechanisms, which is not true backup functionality. They have many limitations for organizations to recover from serious internal and external attacks or to incur additional costs for data retention. Business units and users who have been conditioned for the flexible recovery options from their on-premises backup solutions are seeking commensurate capabilities in the O365 solution.

**Exchange Online Recovery Limitations**

Gartner has the following observations regarding the native recovery capabilities of O365 Exchange Online:

- Item-level recovery cannot guarantee data retention, requires employees to change behavior, adds exposure to insider threats without the “hold” function, or increases costs and risks with the “hold” function:

  - Although the “Deleted Items” folder can be configured with different retention periods (including “forever”), many users have been trained to manually empty this folder frequently to save quota space with their on-premises solutions and are likely to continue doing so, rendering any retention policy placed by the administrator on this folder a moot point. Employee training to change behaviors will never guarantee a 100% success rate.

  - The “Recoverable Items” folder serves as a second-stage recycle bin and stores deleted content from the “Deleted Items” folder. It has a 14-day default retention period, which can be reconfigured to up to 30 days. After the 30 days, items purged are not recoverable. The 30-day retention is often inadequate when dealing with human error or attacks. End users can manually purge their data from this folder, which poses a risk of an insider threat from disgruntled employees. Such a threat can be significant with mergers and acquisitions (M&As).

  - Microsoft recommends using “In-Place Holds” or “Litigation Hold” to avoid employee purge, and to extend retention or for inactive/departed employees. However, these hold functions have their limitations. Holds are “all or none,” which means all active folders and archived folders will be placed on hold, if enabled. One can’t place only the Recoverable Items folder on hold. This limitation will trigger unnecessary storage sprawl and even additional cost (users without an E3 or E5 plan have to pay $3 per user per month) and increase potential legal risks with too much data placed on hold.
Mailbox recovery may not be adequate with short retention:

- Microsoft retains the deleted mailbox and its content for 30 days, which may not be sufficient for employee turnover and M&As. O365 plans other than E3 and E5 will incur costs to place inactive mailboxes on hold via In-Place Hold or Litigation Hold.

- For many customers, the solid uptime record and geographically dispersed replicas drastically reduce, if not eliminate, the need for third-party DR solutions:

- Exchange Online uses Database Availability Groups (DAGs) to continuously replicate mailboxes to multiple locations in different geographies, in case of hardware or site failures. Data locations are shared with customers.

**Bottom Line**

Gartner believes that Exchange Online’s limited backup/recovery functions are inadequate to handle serious attacks. Organizations sharing the same concerns should invest in a third-party Exchange Online backup tool. The few organizations that Gartner has heard from that are still concerned with DR and business continuity (BC) in case of a catastrophic event that brings down the entire Exchange Online service will have to invest in a third-party email archiving solution that can also serve as a DR solution.

**OneDrive for Business and SharePoint Online Recovery Limitations**

Like other enterprise file sync and share (EFSS) products, OneDrive for Business can quickly propagate malware, such as ransomware, via its real-time sync capability. Therefore, it cannot be used as a backup solution (see “Debunking the Myth of Using EFSS for Backup”).

OneDrive for Business and SharePoint Online share the same storage infrastructure and the recovery mechanisms. Microsoft performs robust application backup, including continuous transaction-log backup and, at the database level, daily incremental backups and weekly full backups with a remote copy. Application backup is retained for 14 days for Microsoft data center DR of site collections or subsites, not for granular restores of individual user accounts, folders and files. Gartner believes 14-day retention for DR purposes is sufficient in many cases. Unlike the case with Exchange Online, which is mission-critical, Gartner doesn’t typically encounter clients asking for third-party DR solutions for OneDrive for Business or SharePoint Online.

However, for SharePoint Online, restoring from a Microsoft’s native site collection backup means overwriting the same URL for the site collection without the ability to roll back if something goes wrong. Backup can solve this issue by restoring to an alternative location, rather than the original location. Moreover, some Gartner clients have complained that Microsoft-assisted recovery for customers took too long (sometimes as long as 30 days) or was unsuccessful.
For granular restores of user files and SharePoint objects, OneDrive for Business and SharePoint Online rely on the “Recycle Bin” for user self-service restores. When versioning is turned on for OneDrive and SharePoint documents, older versions can be used for recovery purpose by the users themselves, if the versions have not been purged permanently.

However, recycle bins and version histories do not equate to backup, because they don’t have the security characteristics of backup, such as deletion access control, isolation and immutability. Specifically:

- **Recycle bins are prone to insider attacks** — O365 doesn’t have secure deletion access control for recycle bins, because it allows users to permanently purge content from their recycle bins, even with the second-stage bins. This could pose serious security risks with disgruntled employees, especially in the case of M&As.

- Retention of the Recycle Bin can’t prevent users’ manual deletion and can’t guarantee 100% compliance from users when asked not to delete files from this bin.

- To restore files and items from the second-stage Site Collection Recycle Bin, administrators have to configure each user account to allow them to access, which is time-consuming and hard to scale.

- Similar to the Recoverable Items folder in Exchange Online, the 30-day retention of the second-stage recycle bins is typically too short for unstructured user files, because on-premises file server backups are usually retained for at least a year to cater to unpredictable human behaviors.

- **File versions are not immutable, nor isolated, recovery points** — File versions fail the immutability and isolation test of true backup. Older versions are tightly linked to the active file; they are not isolated, independent recovery points, resulting in undesirable recovery scenarios. For example:

  - If an active file is deleted, all of the older versions of the file are deleted as well. If they are deleted permanently from the recycle bin, then there are no versions left for recovery points by end users.

  - User cannot choose to restore only a particular version. If both an earlier version and the current version of a file are deleted, then the current version has to be restored first before an earlier version can be restored.

- **File-version-based recovery will be slow after ransomware attacks** — File versions don’t have consistent recovery points across files, folders and users; it would be extremely time-consuming to discover the proper restore points for thousands or tens of thousands of files after a ransomware attack and then to restore each file one by one.

Because recycle bin and file version storage counts against the total user storage quota, deleted objects in recycle bins and old versions could consume usable storage quickly, especially with a long-retention period. This situation is made worse by the lack of
version control capabilities. Separating backup from the recycle bins and versions to a different location outside of O365 is more advantageous than an ongoing challenge to balance the ratio between usable storage and recycle bin and version storage.

**Bottom Line**

Gartner recommends investment in a third-party backup tool for OneDrive for Business and SharePoint Online to provide more-secure protection against insider threats and offer consistent recovery points for easier, faster and more flexible recovery options. Gartner believes that O365’s native DR functions are sufficient for OneDrive for Business or SharePoint Online customers.

**Deploying Third-Party Backup Tools for Fast, Flexible Recovery and Damage Control**

Office 365 is a suite that comprises many products with different management consoles, policies and APIs. The lack of a coherent data architecture (see “Devising an Office 365 Data Strategy”) in the O365 suite makes it challenging to manage production data, as well as backup data. Exchange Online has its own data storage, whereas OneDrive for Business and SharePoint Online share the same storage in a different repository than Exchange Online.

Third-party backup tools are available primarily from two types of vendors. Type I vendors offer backup as a service (BaaS), with unlimited storage for backup copies to be stored in a cloud provider’s data center, rather than Microsoft O365, such as Amazon, Azure or the BaaS provider’s own cloud. With BaaS solutions, organizations avoid the hassle of managing software and hardware refreshes and upgrade cycles. Type I vendors include Barracuda Networks, Datto, Druva, Spanning Cloud Apps and Unitrends.

Type II vendors offer O365 backup as part of their backup software solutions, often with separate software licenses that don’t include storage. The purchase of storage, which can be on-premises or in the cloud, is typically a separate decision, similar to other on-premises backup software solutions. With these solutions, the IT organization acquires backup software and has full control of the entire backup policy management stack with many flexible options; however, it is also responsible for backup software and hardware upgrades (unless hardware is in the public cloud). Type II vendors include Arcserve, Commvault and Veeam Software. These vendors are fairly recent with their O365 support, with Veeam supporting only Exchange Online today.

Gartner recently surveyed both Type I and Type II vendors. The key findings are as follows:

- Although most vendors started out by supporting Exchange Online only, many have pledged to add OneDrive for Business and/or SharePoint Online support by the end of 2017. However, vendors’ plans do change.

- All O365 backup products allow customers to configure their retention up to infinite and have various levels of restore granularity and restore locations.

- Type II vendors can back up both Exchange Online and Exchange on-premises with different agents. Those that can offer a single, unified
The restore/recovery console can reduce management complexity.

- Of the eight vendors, three (Barracuda Networks, Datto and Unitrends) offer a single backup solution with a single license for all three key O365 components: Exchange Online, OneDrive for Business and SharePoint Online. All three products are Type I cloud-to-cloud backup.

- Pricing varies greatly because of the different pricing models and capabilities. Type I vendors’ pricing includes unlimited storage and could go as low as less than $2 per user per month for Exchange Online only. Type II vendors’ pricing doesn’t include storage and could also go below $2 per user per month, after volume discounts for Exchange Online. Some vendors’ pricing can be higher, because a single license may include backup of OneDrive for Business and SharePoint Online or even other SaaS applications, such as G Suite. Some solutions may have data governance and compliance functionality as well.

- All products allow centralized management. Large organizations should look for process automation, such as group policies for initial deployment, auto retries if backup fails and user self-service restores. Microsoft’s plan to enable Azure Active-Directory-based Dynamic Security Group will streamline the license management process.

Heavily Regulated and Litigated Organizations Should Adopt a Third-Party Email Archiving Tool to Also Gain DR for Exchange Online

Microsoft O365 has a solid record of infrastructure HA; therefore, organizations do not usually need a third-party solution for DR. However, there are always exceptions. For organizations that require an email DR solution controlled by its own IT, and can justify investment in the additional protection, a few email cloud archiving solutions also offer email BC services because they run a live Exchange Server in their cloud data center. Examples include Barracuda, Mimecast, Proofpoint and Veritas. In the event of an outage, planned or otherwise, email continuity services enable users to send, receive, compose and forward emails when email services are unavailable and maintain productivity. Ideally, a user shouldn’t recognize an outage. Mimecast, for example, operates within Outlook for Windows. Continuity products offer numerous benefits and capabilities, such as reducing the recovery point objective (RPO) and the recovery time objective (RTO), mailbox synchronization and enabling communication between end users and IT.

However, investment in a third-party email archiving solution is more easily justifiable for heavily regulated and litigated organizations, because the same solution can satisfy both email compliance/governance/e-discovery needs and the DR requirement (see “When to Use Microsoft’s Native Capabilities for Archiving and E-Discovery” for scenarios in which a third-party archiving tool is needed). Other important observations regarding third-party email archiving solutions are described in the sections that follow.

Putting Email Continuity in Perspective

Most providers of email continuity also offer archiving and email gateways services to guard against phishing and provide spam filtering. If your enterprise is heavily litigated against, regulated or plans on retaining emails for longer retention periods, it makes sense to invest in Exchange Online archiving regardless of continuity planning. Archiving is a foundational
activity that preserves email according to retention schedule and serves as a mechanism for responding to governance events. Email gateways have a daily impact on email quality, productivity and security. Continuity purchases are almost always part of a portfolio investment consisting of these services; thus, enterprises should grade and evaluate across the board, not just continuity services.

Evaluating Vendors’ Continuity Life Cycle Processes

The email continuity life cycle consists of the event (the outage), the continuity response and failover technology, and the restoration of the active mail environment (end of the outage). In considering third-party email continuity options, buyers should question how the service detects restoration and shifts coverage back to the primary Exchange Online server. Microsoft identifies this potential problem as “split brain” syndrome, in which it’s unclear which mail database is to be mounted, and there is a failure in reconciliation. Third-party vendor responses to how this is achieved can vary. For example, Proofpoint takes an “always on” approach, in which external inbound mail intended for Exchange is delivered with a copy of the mail stored in Proofpoint Continuity. Internal and outbound messages are received as journal copies and deduplicated in Proofpoint Continuity.

During outages, Proofpoint will continue to queue up external inbound mail intended for Microsoft Exchange in their system, but journal copies are not received. When Exchange comes back online, Proofpoint will deliver the queued external messages to Exchange, and the delayed journal reports for these will be received and continue to be deduplicated in the Continuity system. Other vendors will take an end user or administrative user approach, meaning they will be responsible for initiating a continuity event and deciding how to access their email (Outlook plug-in, web portal, etc.). When a continuity event is ended by either the admin or the user, the primary mail server is again responsible for sending and receiving mail. Deduplication then occurs at the application level — Outlook plug-in, portal or mobile application.

Evidence

The results presented in Figure 1 are based on a Gartner study conducted at the Real Time Research Kiosk during the Gartner Data Center Conference in Las Vegas, 5 December to 8 December 2016. Additional responses were collected online from 12 December to 16 December 2016 among attendees of the Gartner Data Center Summit, which was held in London, U.K.

In all, 230 qualified respondents participated in the study.

Respondents were required to be members of their organization’s IT staff or department or to serve in an IT function. In addition, they were required to be personally knowledgeable about their organization’s storage technologies, architectures and policies.

The survey was developed collaboratively by a team of Gartner analysts who follow data center storage issues and was reviewed, tested and administered by Gartner’s Research Data Analytics team.

Source: Gartner Research Note G00322135, Pushan Rinnen, Garth Landers, 26 May 2017
How to Take Action

After reading the Gartner research, you may be considering leveraging a third-party archiving tool to supplement the limitations within Office 365. Educating cross-functional stakeholders regarding the potential data loss risks without a third-party solution may be required. Start a dialogue on your organization’s risk profile as well as how you can team together to help users get more value from their email system. Enabling end-user search and recovery will likely top the list, in hopes to remove the administrative burden from IT while making users more productive.

Mimecast Sync & Recover for Exchange and Office 365 gives organizations a simple, streamlined way to quickly recover deleted or corrupted email, calendar, and contacts by leveraging archive data while eradicating the need for an independent backup product. It offers true protection and recovery that enhances the end user experience and provides enhanced security from malicious attacks. Delivered from a single, unified platform and administration console, integrated archiving and recovery means less risk and stronger resiliency.

Source: Mimecast
Is Microsoft Office 365™ Backup & Recovery Good Enough? is published by Mimecast. Editorial content supplied by Mimecast is independent of Gartner analysis. All Gartner research is used with Gartner’s permission, and was originally published as part of Gartner’s syndicated research service available to all entitled Gartner clients. © 2017 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner’s endorsement of Mimecast’s products and/or strategies. Reproduction or distribution of this publication in any form without Gartner’s prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner’s Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see “Guiding Principles on Independence and Objectivity” on its website.

About Us

Mimecast makes business email and data safer for more than 26,400 customers and their millions of employees worldwide. Founded in 2003, the company’s next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management in a single, fully-integrated subscription service.

Mimecast reduces email risk and the complexity and cost of managing the array of point solutions traditionally used to protect email and its data.

For customers that have migrated to cloud services like Microsoft Office 365™, Mimecast mitigates single vendor exposure by strengthening security coverage, combating downtime and improving archiving.

Mimecast Email Security protects against malware, spam, advanced phishing and other emerging attacks, while preventing data leaks. Mimecast Mailbox Continuity enables employees to continue using email during planned and unplanned outages.

Mimecast Enterprise Information Archiving unifies email, file and instant messaging data to support e-discovery and give employees fast access to their personal archive via PC, Mac and mobile apps.

Contact us

www.mimecast.com

For more information call:
Europe: +44 (0)20 7847 8700
North America: +1 617 393 7050
South Africa: +27 (0) 105 009 950
Australia: +61 3 9017 5101