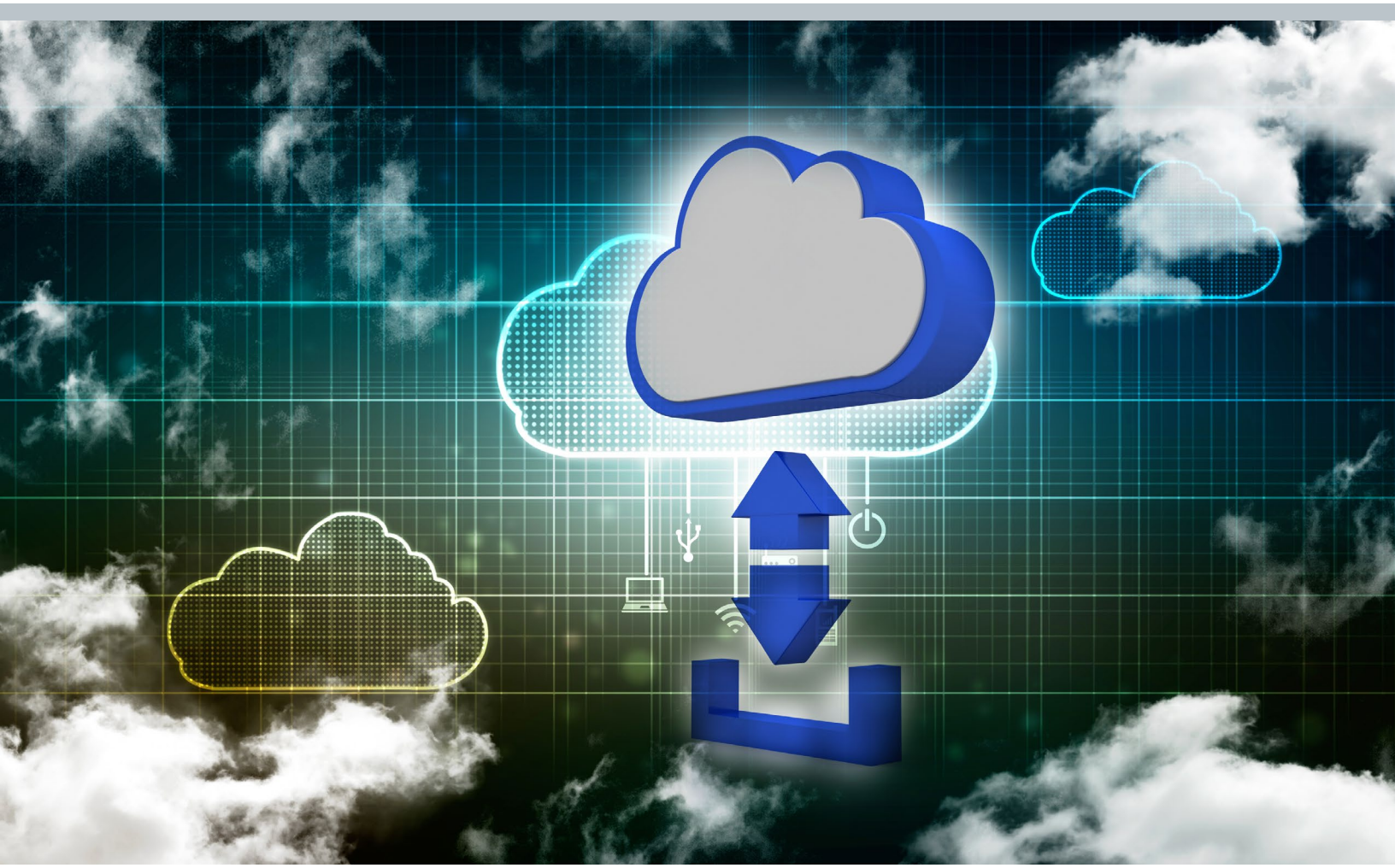
PAPER

Redmond MAGAZINE



PROTECTING OFFICE 365 WITH VEEAM CLOUD BACKUP

By Brien M. Posey

iland®

VEEAM | CSPPARTNER Platinum

www.iland.com

The cloud is well known for its ability to support business agility. In recent years, public cloud providers have even marketed the cloud as something of a panacea. This comes as no surprise, as public clouds can simplify IT operations and allow IT professionals to focus on minimizing OPEX. In spite of its many benefits, the cloud has also introduced some new challenges related to data backups. Public clouds sometimes lure IT professionals into a false sense of well-being.

Consider for example, Microsoft Office 365. At one time, organizations had little choice but to run Office applications such as Exchange Server and SharePoint Server in their own data centers. At that time, organizations commonly took a laser-focused approach to the backup process. Exchange, SharePoint and other Microsoft Office applications were almost always classified as mission-critical applications, and therefore it was important for organizations to ensure that they had adopted a fully tested and secure backup solution.

Fast forward a few years and Microsoft began offering Exchange, SharePoint and many other applications as part of Office 365. Once Office 365 matured, and was proven to be reliable, organizations migrated to it in droves. After all, Office 365 frees organizations from costly infrastructure and hardware licenses and purchases, while also giving administrators the assurance that all of the various Office 365 applications are configured correctly. Furthermore, using Office 365 instead of an on-premises solution means that organizations are freed from application related maintenance tasks such as patch management and software version upgrades.

One of the unanticipated side effects of the mass migration to Office 365 was that many organizations stopped backing up their Office data. For some organizations, this was because early on no Office 365 backup applications existed. For other organizations, the reason might be tied to an incorrect assumption that Microsoft is backing up their data for them.

WHY ORGANIZATIONS MUST BACK UP OFFICE 365 DATA

In retrospect, the Office 365 service agreement works a little bit differently than one might assume. Microsoft guarantees that the Office 365 applications will remain functional and available according to the terms that it sets forth in its service level agreement (SLA). As such, Microsoft goes to great lengths to protect the Office 365 applications and the underlying infrastructure. Protection of Office 365 data is left up to the

Cover image: ijjomathaidesigners / Shutterstock.com

individual customer. Simply put, Microsoft owns the Office 365 applications, but it is the Office 365 customers that own the data. Because Office 365 customers retain ownership of their own data, they are responsible for protecting that data against loss.

This is not to say that Microsoft leaves you completely unprotected. They don't. Microsoft has built a number of different protective mechanisms into Office 365 in an effort to help customers safeguard their data.

MICROSOFT OWNS THE OFFICE 365 APPLICATIONS, BUT IT IS THE OFFICE 365 CUSTOMERS THAT OWN THE DATA.

The nature and scope of these protective mechanisms vary considerably from one Office 365 application to the next. The one thing that all of these mechanisms have in common is that they all have significant limitations. Take Exchange Online for example. If an administrator deletes a mailbox, then the mailbox doesn't actually disappear. Instead, Exchange Online performs what is known as a "soft delete" of the mailbox (although there are a few circumstances that can result in a hard delete such as using the Remove-Mailbox cmdlet with the -Permanent switch set to True). A mailbox that has been soft deleted still exists, but in an inactive state, and can therefore be recovered at any time over the next 30 days. Once those 30 days pass, the object is permanently removed and cannot be recovered without the aid of a backup.

Similarly, if a user were to delete a file residing on OneDrive for Business, the file is not permanently deleted right away. OneDrive for Business data is protected by a relatively new feature called File Restore. File Restore is a self-service disaster recovery solution that allows an end user to perform point in time disaster recovery on files that have been deleted, encrypted by ransomware, or overwritten with incorrect data. The problem with the OneDrive for Business File Restore feature is that it only provides protection for a period of 30 days. Once 30 days pass, changes or deletions are considered to be permanent and cannot be undone without the aid of a backup.

Since Microsoft puts so many safeguards in place to protect its Office 365 customers against data loss, one must consider why independent backups remain a necessity for protecting data in the Office 365 cloud. There are several reasons why backups are so important.

First and foremost, as previously noted, Microsoft's built-in protective mechanisms generally come with an expiration date. If a user overwrites or deletes important data, but doesn't notice until the next month, then that data is probably going to be unrecoverable through

any of the tools that are built into Office 365. The only option at that point, will be to restore a backup that you have created yourself.

Another reason why it is so important to backup Office 365 is that not all of the protective mechanisms that Microsoft gives you allow for point in time recovery capabilities. Your users can perform point in time recovery of OneDrive for business files, but there is no easy way to roll an Exchange mailbox back to a previous state.

ONCE AN ORGANIZATION HAS DETERMINED THAT IT NEEDS TO PROTECT ITS OFFICE 365 DATA, THE NEXT QUESTION IS HOW BEST TO ACHIEVE THAT PROTECTION.

If a situation were to occur that warranted a point in time recovery of one or more Exchange Online mailboxes, it might be tempting to go to Microsoft for help. Being that Microsoft is responsible for the integrity and functionality of the Office 365 cloud, the company does, of course, create backups. However, these backups only serve to recover the Office 365 service following a major data loss event. Microsoft does not typically restore files or objects on behalf of individual Office 365 subscribers.

Yet another compelling reason to create your own Office 365 backups is that most organizations have compliance requirements or internal business requirements that must be met. For example, an organization might be required to retain all deleted data for two years as a part of a regulatory requirement. Needless to say, the safeguards that Microsoft has baked into Office 365 are not going to satisfy such a requirement.

Arguably, the best reason of all for creating your own Office 365 backups is self-preservation. Taking the initiative to create your own Office 365 backups may one day save your job. After all, nobody wants to tell their boss that they have lost important company data because they simply did not feel the need to back that data up.

When organizations suffer data loss, they are impacted by more than just lost sales or lost information. Reputation, trust, reliability all become tarnished in the eyes of a customer. It is a must to have every mechanism in place to provide comprehensive data protection.

Of course, backing up Office 365 data is not just a matter of why, but also of how. Once an organization has determined that it needs to protect its Office 365 data, the next question is how best to achieve that protection.

CONSIDERATIONS FOR PROTECTING OFFICE 365 DATA

Presently, the market is flooded with Office 365 backup products ranging from those offered by large, well known backup vendors to niche solutions from compa-

nies that you might have never heard of.

As you begin to evaluate the available solutions, there are some important things to consider. Many of these considerations are obvious, but there are at least two things that warrant special attention.

First, you must consider what the backup product is actually protecting. Many of the early Office 365 backup products only protected Exchange Online, and nothing else. Today's Office 365 backup tools tend to be more capable than those early tools, but even now the protection of Office 365 data is sometimes lacking. This can be especially true for SharePoint Online. As such, it is extremely important to make sure that the backup product that you choose is actually capable of protecting all of your Office 365 data. More specifically, a good Office 365 backup solution needs to be able to protect Exchange Online, SharePoint Online and OneDrive for Business.

As you are no doubt aware, we live in an increasingly cloud centric world. Because so many applications, and even infrastructure components live in the cloud, Internet bandwidth is becoming increasingly congested. Backing up cloud data to your own data center only serves to further increase that bandwidth congestion. Conversely, backing up the data to another cloud keeps that traffic stream off of your network. Furthermore, backing up to the cloud frees your organization from the cost and hassle of having to maintain a backup server in your own data center.

A second reason why it makes sense to backup your Office 365 data to the cloud, is because cloud backups offer better overall protection.

Veeam touts the 3-2-1 rule. The basis of this rule is that if data is to be truly protected, there needs to be three copies of the data—the original copy and two backup copies. One of these backup copies is typically kept on-premises (for easy access), while the other is stored off-site. Having an off-site copy of the backup ensures that the organization's data will survive in the event that the data center is destroyed.

A GOOD OFFICE 365 BACKUP SOLUTION NEEDS TO BE ABLE TO PROTECT EXCHANGE ONLINE, SHAREPOINT ONLINE AND ONEDRIVE FOR BUSINESS.

A second critical consideration is the location of the backup target. Many of the backup solutions that are available for Office 365 are designed to stream backups from the Office 365 cloud to a backup server residing in your own data center. Although this approach works, it isn't ideal.

Cloud services, such as Office 365, change this model. The 3-2-1 rule does

not really make sense when it comes to data that is born in the cloud. While there is still something to be said for having three copies of the data, keeping a backup copy on-premises may not be the best option, because bandwidth constraints would make for excessively long restore times. A better solution would be to create two backup copies in the cloud, with each copy residing in a different region. This approach would allow for relatively fast restore operations, and insulation against regional disasters.

CHOOSING THE RIGHT SOLUTION

You can't exaggerate how much organizations rely on Office 365. Office 365 includes the heart of an organization's data: valuable contacts, vital messages and sensitive attachments—email contains some of the most important data in any organization. Unfortunately, protecting that data is an increasing challenge.

Microsoft Office 365 is a robust and capable Software as a Service platform that meets many organization's needs. However, despite Microsoft Office 365's robust capabilities, there are five pitfalls when relying on them for data protection:

- Accidental deletion
- Retention policy gaps and confusion
- Internal security threats
- External security threats
- Legal and compliance requirements

When considering a solution for data protection, it is critical to choose one that can address each of these challenges. Partnering with Veeam, iland now offers iland Secure Cloud Backup for Microsoft Office 365 that provides complete backup and recovery for an organization's Office 365 data. With this offering, an organization's Office 365 data is automatically backed up daily to iland's secure cloud along with unlimited storage quota and an unrestricted retention policy. If an organization requires a specific time for the backup jobs to run, the IT administrator can work with the iland support team during the onboarding process to establish the time across all Office 365 users.

Veeam backup for Microsoft Office 365 works with your existing Veeam infrastructure by backing up virtual machines and data, and adds the additional protection of your Office 365 data. With Veeam Cloud Connect and iland Secure Cloud Backup, an end to end encrypted, reliable and efficient tunnel is created and your data is safely backed up to the iland repository. From within the Veeam interface you can create your protection strategies and schedules and use the iland cloud for short-term backup and long-term archival.

With easy-to-use, granular recovery, Veeam Backup for Office 365 can facilitate finding the right data and restoring it as quickly as you need it. iland provides the iland Secure Cloud Console, a single pane of glass management UI that can give anyone administering their backups full visibility into their cloud utilization. With the ability to monitor historical trending and allocate additional space on the fly, you can be assured that backups of mission-critical data will never stall while you wait to implement more capacity.

FOR THE THIRD CONSECUTIVE YEAR, GARTNER RECOGNIZED ILAND AS A LEADER IN THE 2018 MAGIC QUADRANT FOR DISASTER RECOVERY AS A SERVICE.

When evaluating a solution, choose a vendor that has reputation and experience with backup and disaster recovery. For the third consecutive year, Gartner recognized iland as a Leader in the 2018 Magic Quadrant for Disaster Recovery as a Service. What's more, iland was positioned at the highest ability to execute in the Leader's quadrant.

In addition, iland offers security and compliance that redefines the standard. iland offers access to its in-house, certified compliance team that is skilled and prepared to ensure organizations have the necessary documentation they need to fulfill their audit requirements in the US, EMEA and APAC. In fact, iland is one of only two organization's to have earned a gold star certification from the Cloud Security Alliance (CSA). The CSA's certification program is technology neutral, and subjects cloud providers to a rigorous assessment of its security controls therefore attributing a gold star as the highest rating awarded by the CSA.

So, what are you waiting for? Contact iland today to backup your Office 365 data.

Brien Posey is a 17-time Microsoft MVP with decades of IT experience. As a freelance writer, Posey has written thousands of articles and contributed to several dozen books on a wide variety of IT topics. Prior to going freelance, Posey was a CIO for a national chain of hospitals and health care facilities. He has also served as a network administrator for some of the country's largest insurance companies and for the Department of Defense at Fort Knox. In addition to Posey's ongoing work in IT, he has spent the last several years training as a commercial Scientist-Astronaut candidate in preparation to fly on a mission to study polar mesospheric clouds from space.

Find out more:
https://www.iland.com/contact/

iland®

VEEAM | CSPPARTNER Platinum