



White Paper

Veeam + Microsoft Combine to Offer Rapid Time to Value for Cloud Data Protection

Sponsored by: Veeam and Microsoft

Phil Goodwin
January 2018

IDC OPINION

Winning organizations in the digital transformation (DX) era will be those that collaborate most effectively between business units and IT. IDC estimates that investors will use platforms/ecosystems, data value, and customer engagement metrics for all enterprises by 2020. This means that organizations that work to transform their IT organization to digital native will have a measurable advantage over those that do not. Thus IT investments will be driven by the ability to create demonstrable business value in a digital economy. Business value will not be measured just by ROI but by the ability to deliver faster application deployment with less human intervention, a better user experience, and simpler operations.

In alignment with digital transformation, we estimate that more than 70% of organizations have a cloud-first application deployment strategy. High among the cloud-first initiatives for many organizations is a transition to Microsoft Office 365 and utilizing public clouds such as Microsoft Azure. However, in this transition, IT leaders are discovering that default data protection schemes are not as robust as they desire. As a result, many are turning to companies such as Veeam to provide the necessary data management and protection policies demanded by the organization.

Because demonstrable business value is so important to digital transformation, Veeam asked IDC to conduct a study of customers using Veeam with Microsoft Office 365 and Azure. The study methodology used in-depth interviews of five organizations of diverse industries, including financial institutions, cloud service providers, and telecom companies. These organizations were also from different geographical regions, including North America and Europe. The advantage of in-depth interviews compared with surveys is that interviews allow broad-ranging exploration of topics that can delve into details. The interviews include a specific set of questions but also allow the respondent to bring up topics, issues, and experiences not otherwise considered.

Key findings from those using Veeam with Microsoft Office 365 include:

- Simple setup with no changes to existing processes
- Near-error-free operation
- Faster mailbox and message recovery
- Periodic maintenance reduced from one to two hours per week to zero

Customer quotes from the interviews are as follows:

"Implementation of Veeam with Office 365 was a very straightforward process. The wizard was simple to use and did not involve any extra complexity." – Darrell Mee, ICT manager, South West Communications Group

"Our restores with Veeam and Office 365 are easier and quicker. The product is simple and just ran." – Financial Company (chose to be anonymous)

Key findings from those using Veeam and Microsoft Azure include:

- Complete elimination of tape for secondary and offsite storage
- Simple-to-use automated tiering
- Sarbanes-Oxley compliance
- Better data control and safety

Customer quotes from the interviews are as follows:

"We were able to completely eliminate tape, tape handling, and offsite transfer. This avoids losing tapes and makes audits easier." – Michael Thorstensen, systems infrastructure consultant, extri:co

"Our people were very happy to be using a new technology that just worked." – Microsystem engineer, ecommerce marketing company (chose to be anonymous)

SITUATION OVERVIEW

By 2020, 60% of organizations will have articulated a digital transformation strategy and will be in the process of implementing it. For many organizations, the entry point for DX is a cloud-first strategy. Commonly, this begins with cloud data protection, such as a cloud backup target, backup as a service, or disaster recovery (DR) as a service. Such implementations utilize public cloud services, and Microsoft Azure is an example of such a service. Many organizations are also transitioning from on-premise Microsoft Exchange to Office 365. Office 365 is an example of software as a service (SaaS), whereby the cloud-based service is offered through subscription.

However, this transition challenges IT organizations to update their data protection strategies as critical organizational data is now outside the traditional datacenter and not automatically protected. Moreover, the service levels offered by cloud and SaaS providers will vary from vendor to vendor. IT organizations must be prepared to take charge of their data protection needs, regardless of data location or service provider. Thus IT leaders will be increasingly looking for data protection tools and schemes that can apply consistent backup policies and achieve required SLAs across the entire data estate.

The advantages of a cloud-based data protection service include:

- Leverages the cloud for data protection, which is one of the most common use cases for cloud computing
- Shows demonstrable economic benefits from on-demand resources and data deduplication
- Inherently (and often automatically) places data copies offsite, eliminating the need for tape
- Easily leverages cloud data repository for disaster recovery or workload availability

Microsoft Office 365 is proving to be one of the most common cloud-based applications IT organizations utilize to transition from an on-premise, license-based model of Exchange to a SaaS model for email applications. For many organizations, this reduces the IT labor associated with managing email servers and may even improve application availability.

However, IT managers are discovering that the default data protection and retention policies of Office 365 are often inconsistent with corporate standards. In addition, in the event of a malicious attack or human error, organizations need to make sure data is protected. Thus many organizations are looking to third-party software vendors to provide the tools needed to upgrade data protection capabilities for Office 365 to corporate standards and to meet data protection needs. Critical functionality includes the ability to retain data for as long as necessary, to quickly restore mailboxes or messages, and to retain data on-premise, if necessary. In fact, many organizations choose to keep an Exchange environment on-premise so that email services can be restored independent of Office 365 services, if for some reason the SaaS environment is not available.

Moreover, IDC research has found that 78% of organizations are currently using public or private cloud and that 62% of organizations will have more than half of their IT capabilities delivered through some sort of cloud service. Yet we believe that few organizations have fully thought through their cloud data protection strategy and many will be forced to apply ad hoc solutions in a reactive mode. This is often because cloud application deployments are driven by business units independent of standard IT operating procedures. Consequently, data protection may be overlooked as part of the planning process. Instead, leading organizations are setting cloud data protection standards and communicating them with business unit leaders to avoid situations where data is at risk.

In summary, IT organizations need to consider both widely applicable cloud data protection capabilities and application-specific data protection for SaaS and cloud-based applications. Data-driven organizations realize that their data resides in a wide range of platforms, applications, and data types. IT managers must be proactive in specifying and enforcing data protection, retention, and recovery standards. In most cases, business managers are not resistant to these standards – they simply are unaware of them until properly educated.

IN-DEPTH INTERVIEW FINDINGS

Veeam + Microsoft Office 365

As noted previously, Microsoft Office 365 has become one of the largest, most widely used SaaS applications, and organizations are discovering a need for more robust data protection as well as contingency plans in the event Office 365 is not accessible. Uniformly, organizations view email and Office 365 as mission-critical applications. Without them, most organizations acknowledge that a major business disruption would occur.

IDC interviewed leaders of three organizations who have implemented Veeam Backup for Microsoft Office 365. Experience with Veeam Backup for Microsoft Office 365 ranged from nine months to a year, with all the three organizations having several years of experience with other Veeam software. The number of mailboxes managed ranged from several hundred to several thousand, and the number of instances of Office 365 managed ranged from a single instance to multitenant instances.

Findings from our interviews resulted in the following conclusions:

- **Veeam was easy to implement with Office 365:** The time needed to set up Veeam for protecting Office 365 data ranged from 15 minutes to 1 hour for those companies that we interviewed. These companies had prior experience with Veeam but were implementing it with Office 365 for the first time. In all cases, Veeam Backup for Microsoft Office 365 was being implemented simultaneously with Office 365.

According to the people we interviewed, there was no need to change any basic IT processes during the implementation. Backup jobs were scheduled as with other Veeam jobs with the same recovery point objective (RPO) SLA as other applications. In addition, the entire process was transparent to the end user. There was no downtime or loss of application availability during the process. The common theme among all interviewees was: "It just worked."

- **Data backup and restores were simpler and faster with Veeam:** Application availability is a critical factor for all organizations, but outages inevitably occur. IT organizations monitor four critical service levels: recovery point objective, recovery time objective, backup success rate, and restore success rate.

While our interviews were not a quantitative assessment of the customer's data protection operational metrics, we were able to learn about some of the benefits that these organizations realized. For example, when comparing backup of their on-premise Exchange servers with the backup of Office 365, one organization reported a 75% reduction in backup time. Shortened backup windows not only ease operational stresses but also ensure that data is more likely to reach a protected state compared with protracted backup processes that are more prone to interruption or failure.

Of course, restore time and reliability are even more important than backup. Fast, reliable restores ensure that business units can resume normal operations faster and avoid data loss. In our conversations, customers reported 100% restore success rates with Veeam and Office 365. In fact, they reported even better reliability and performance compared with their previous on-premise Exchange environments.

- **Veeam added an extra layer of redundancy and "insurance":** Because Office 365 is offered with a base level of data protection, we were interested to hear from customers the reasons they chose to supplement the base data protection using third-party software such as Veeam.

One customer indicated that Veeam offered an extra layer of "insurance" against data loss. Moreover, the company used Veeam to increase its data retention schedule from 30 days to 1 year, in alignment with the company's normal policies and the policy that had applied to the previous on-premise Exchange environment. This customer also expressed that Veeam Explorer for Microsoft Exchange offered faster and easier searches than Outlook Search.

- **Staff utilization was highly efficient:** Data protection operations are typically considered to be labor intensive, with many organizations having dedicated backup administrators. Among the organizations that we spoke with in this study, one organization had a single person dedicated to backup operations. Another indicated that it could not justify a dedicated resource, with tasks being no more than a part-time effort for one person. All the organizational spokespeople said that their IT staffs were able to spend less time managing backups after implementing Veeam because backup operations were simplified.

Veeam + Microsoft Azure

Microsoft Azure has emerged as a major public cloud provider. Whereas our questions to the aforementioned customers regarding data protection for Office 365 were very application specific, uses for Azure can be very diverse. These uses include storage used to store backup sets, disaster

recovery staging, dev/test "sandbox" environment, and complete application environments, whether software as a service or simply a hosted environment.

In addition, many public cloud providers, including Azure, are the "back-end" physical environment for managed service providers that themselves offer backup as a service or DR as a service. Similarly, single organizations may use public clouds as backup targets or application environments. For this particular study, we spoke with both a cloud service provider that uses Azure as its back-end provider and a direct end-user organization. Key findings from these customer conversations included the following:

- **Eliminate the use of tape:** A primary motivation for both organizations for using Azure was the desire to eliminate tape entirely from their operations. Both organizations expressed the issue that tape handling is both labor intensive and error prone, with lost tapes posing a serious organizational risk. Tape-related labor includes daily effort to manage, eject, and load tapes into tape libraries and manage the movement of tapes to and from an offsite vault.

In this case, both companies use Veeam to transfer data from onsite application infrastructure to Azure. In doing so, they eliminated the use of tape while still ensuring that data is moved offsite in the event of an onsite disaster. It was also noted in our conversations that this offsite effort provided an "air gap" between the primary data and secondary backup copies to protect against ransomware attacks. These offsite copies also satisfied the organizations' Sarbanes-Oxley regulations for disaster resilience and improved the companies' security audits.

- **Hybrid cloud data protection:** As IT organizations drive toward digital transformation, many find hybrid cloud configurations (i.e., on-premise private cloud connected with off-premise public or managed cloud) as a natural way to take advantage of on-demand cloud resources and economics. As we have noted, cloud data protection is often the first step in this transitional effort.

In our discussions with Veeam and Azure customers, we found that one of the organizations uses Veeam to back up to a Microsoft StorSimple appliance onsite and then replicate to the cloud and another uses Data Domain appliances in a similar configuration. Our research has found this onsite purpose-built backup appliance (PBBA) combined with cloud replication to be a common configuration in the industry. As the participants in our discussions expressed, the onsite PBBA retains backup data for rapid restore, while offsite cloud replication ensures that data is protected at a remote location. For example, one of the study participants uses the PBBA to store data locally for 35 days, with data retained in Azure for 1 year.

Other benefits discussed by participants included DR enablement by virtue of data stored in Azure and the ability to access on-demand resources for workload restoration. Participants felt that this PBBA-to-cloud scenario provided better data safety. To reduce the network load, one participant moves incremental changes to Azure on a daily basis, with a full backup transfer weekly.

- **Build a virtual lab:** One of the participants in our study discussed the implementation of a virtual lab using Veeam On-Demand Sandbox and Microsoft Azure. This virtual lab is used as a proof-of-concept test bed for virtual machine (VM) restores in Azure, migrating VMs to Azure and performing DR testing. According to this user, Veeam On-Demand Sandbox in Azure was easy to set up and tear down as testing requirements demanded.
- **Better reliability:** The organizations participating in our study using Veeam and Azure reported faster restores as well as more reliable and granular backups when compared with their previous environment. These prior environments were on-premise backup/restore with a product other than Veeam and without a separate cloud repository. Respondents stated that

they had fewer backup failures. Both the cloud service provider and the direct end-user organization reported 98% success on backup jobs, which is within the 97% success guideline that IDC uses to describe best practice operations.

- **Positive impact on staff:** Given that data protection operations have historically been labor intensive, reductions in effort are welcome developments to IT managers. As with our Veeam and Office 365 study participants, Veeam and Azure participants reported positive impacts on their staffs after implementing Veeam with Azure. These companies reported that new staffs came up to speed faster and required less training than they did for their previous backup environments. In addition, one company reported that its staff members were proud to use a technology that works and allows them to demonstrate to management and the organization the success of their operations.

CHALLENGES/OPPORTUNITIES

The feedback from the customers interviewed for this study was almost overwhelmingly positive, but they did have suggestions for other organizations considering implementing Veeam with the Microsoft cloud:

- **Ensure that a relevant Office 365 admin account is established at the outset of implementation.** In this situation, the customer had not established an Office 365 admin account related to the backup environment and could not complete the configuration until doing so.
- **Bandwidth for data transfer to/from the cloud is the biggest issue.** In a scenario where data was being transferred from an on-premise PBBA to Azure, respondents reported long data transfer times due to data volumes and bandwidth constraints. While this is not directly related to either Veeam or Azure, if data needs to be retrieved from the cloud, IT organizations should understand the data transfer time involved for their situation when planning RTO requirements. In addition, one user, who used the Microsoft StorSimple virtual appliance, reported the need to clear the appliance before every data transfer to avoid error conditions.
- **Large data sets may take days to upload/download from the web.**

In addition, these organizations collectively experienced two technical support incidents during implementation; both were reportedly resolved quickly, without finger-pointing and to the customers' satisfaction.

CONCLUSION

Data protection in the cloud is a natural use of cloud capabilities where the inherent offsite nature of a cloud deployment and on-demand resource pricing models create compelling data protection options at affordable prices. However, adding cloud to an organization's infrastructure model changes the way data is protected, especially for cloud-based applications.

Office 365 is regarded as a mission-critical application by many organizations, and IT managers are quickly discovering that default data protection schemes may not meet corporate data management and retention requirements. In addition, IT managers must specifically address data for any cloud-based application. Veeam and Microsoft provide solutions to meet the growing needs of organizations in these two areas.

Based on our conversations with Veeam customers, we found that IT organizations have successfully used Veeam for protecting Microsoft Office 365 data and leveraging Microsoft Azure. These organizations reported the following general results:

- Simple implementation and operation
- Better service-level delivery
- Reduced labor associated with data protection
- Elimination of the use of tape for backup/recovery
- Safe and secure storage of data offsite

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2017 IDC. Reproduction without written permission is completely forbidden.

