Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published December 2018
Sponsored by Trusted Data Solutions

Migrating to the Cloud? It's Not as Simple as it Seems

Executive Summary

The conventional wisdom is that cloud adoption is significant and growing rapidly – and, in this case, the conventional wisdom is right:

- The vast majority of organizations use public and private clouds
- The leading on-premises email platform, Microsoft Exchange, is being migrated to the leading cloud-based email platform, Office 365
- Cloud infrastructure providers are largely replacing on-premises solutions because they offer lower costs and greater efficiencies, and
- The typical larger enterprise uses more than 1,000 cloud applications.

As migration to the cloud continues, so does the need to migrate data from on-premises platforms to the cloud and between cloud providers. However, this is not a trivial undertaking. Consider:

- **Not everything should be migrated to the cloud**
  Migrating everything to the cloud is not only unnecessarily expensive, it also increases the risk that data will somehow be compromised and can consume valuable resources, staff as well as put major strains on your networks and bandwidth. While some decision makers believe that everything should be migrated, it is usually not necessary.
- **There are lots of decisions to be made**
  Decision makers that are contemplating a cloud migration must decide what, how and when to migrate – as well as what not to migrate. Moreover, they must decide how to manage data that is not worth migrating but must be retained.
- **There are lots of problems to solve**
  Organizations that want to migrate data to the cloud must ensure the integrity of the migrated data, decide how they will continue to access data that is not migrated but retained, and understand how they will migrate very large volumes of data reliably and economically.
- **Tape archives must be properly managed**
  The decision about tape migration is an essential one. Most organizations have large quantities of tape storage for backups and long-term archival of strategic information. However, the issue of tape migration is complicated by the fact that some data on tape in some cases may no longer be accessible due to the age or formats of the systems they were stored in, or the tape source may no longer be supported or available.
- **Regulatory issues are critical**
  Regulatory compliance must be maintained when migrating content to the cloud or any other venue, especially while the migration is in process to ensure full chain-of-custody is maintained.
- **Using a single vendor for migration offers benefits**
  A single vendor with expertise across all types of data migration offers a number of advantages compared to using several different point providers that manage only a piece of the migration effort.

Migrating everything to the cloud is not only unnecessarily expensive, it also increases the risk that data will somehow be compromised and can consume valuable resources.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Trusted Data Solutions; information about the company is provided at the end of the paper.

Organizations are Migrating to the Cloud at a Steady Pace

CLOUD ADOPTION IS SIGNIFICANT

Cloud adoption is continuing at a healthy pace as evidenced by the following data points:

- As of late 2017, 97 percent of organizations use public and/or private cloud services, up from 93 percent in 2016[i].
- The number of commercial organizations using Microsoft Office 365 has increased from 60 million in November 2015 to 155 million in September 2018, an increase of 158 percent in just 34 months[ii].
- The adoption of public cloud services increased from 89 percent in 2017 to 92 percent in 2018, while private cloud adoption increased from 72 percent to 75 percent during the same period[iii].
- The typical larger enterprise employed 1,181 cloud services as of early 2018[iv].

Moreover, we are seeing continued growth in the adoption of various cloud services and there are few, if any, signs of a slowdown in adoption. As just one example, average quarterly growth of Amazon Web Services (AWS) during 2017 was 43 percent and during the first three quarters of 2018 it averaged 48 percent[v].

MANY ORGANIZATIONS BELIEVE THAT MIGRATION IS A NATURAL OR SIMPLE CONSEQUENCE OF MOVING TO THE CLOUD

When organizations migrate key services to the cloud, particularly those that are associated with enormous data repositories like email or file stores, there is a mindset that everything needs to be migrated to the cloud. Many are of the opinion that 1) migrating *services* to the cloud means moving *all of their data* to the cloud, and 2) that doing so will be simple and painless.

In most cases, wrong on both counts.

For example, when the decision is made to migrate from an on-premises email solution like Microsoft Exchange to Office 365, many believe that existing archives need to be migrated, as well. While there may be value in doing so for some data, the vast majority of archived data is largely inactive. Migrating it to the cloud would not only be expensive, difficult and expose the organization to issues like losing chain-of-custody, it is largely unnecessary because most of this data will never be accessed anyway. Moving it to the cloud will have virtually no upside and a significant amount of potential downside.

Data that is corrupted can be just as harmful as data for which chain-of-custody is lost, since some or all of the data may not migrate properly to the new archive and so will be lost permanently. As a result, it is essential to ensure the integrity of the data before the migration and throughout the entire process so that only authenticated data is moved from the old archive to the new one.

With regard to the migration being simple and painless, that might be the case when migrating a small amount of data. However, for the typical organization that may have a few years of archived emails, files and other content – and that chooses to migrate the data themselves – a migration of this data to the cloud will require significant effort and planning. There are vendors that can make the migration of data to the cloud as simple and painless as possible, but it will still require some level of effort.

When organizations migrate key services to the cloud…there is a mindset that everything needs to be migrated to the cloud.

CLOUD MIGRATION REQUIRES ADDRESSING A NUMBER OF CHALLENGES

When planning a migration of data to the cloud, there are a number of important issues that all relevant stakeholders – IT, business managers, compliance, legal, etc. – must carefully consider:

- **What to migrate**
  First and foremost, decision makers migrating solutions to the cloud must decide what to migrate. There are some obvious choices, such as recent emails for an email system migration, recent files for a file server migration, and so forth. Basically, if a system is to be migrated to the cloud, frequently accessed data associated with that system should also be migrated.

- **How to migrate**
  Another important consideration is how to migrate data to the cloud. To paraphrase a senior executive from Dell at a recent industry conference, "it is easy to store many terabytes of data, but hard to move it." Some organizations will opt for physical migration of data to a cloud provider, sending physical media to the cloud provider's data center on hard disks or DVD-ROMs. For extraordinarily large amounts of data transfer, some providers will provide dedicated and purpose-built systems for the physical transfer of customer data – for example, Amazon Web Services' "Snowmobile" is a 45-foot, ruggedized container that is transported by a semi to customer sites and can store 100 petabytes of data for transfer to either Amazon S3 or Glacier storage[vi].

- **When to migrate**
  The decision about when to migrate is also essential. Should all data be migrated right away? Should it be migrated in blocks by date or by user groups?

- **What not to migrate**
  Also important to consider is what data should not be migrated to the cloud. For example, emails, files, databases and other business records that are older than 12 months, but that must be kept for five years are not a good candidate for migration to the cloud. While legal or compliance may require that the organization retains its data for long periods, this does not mean it has to be migrated to the cloud, since doing so will incur unnecessary levels of cost and risk. While this data should still be readily available in the event it is needed for an eDiscovery effort or a regulatory audit, for example, these requirements can be satisfied in ways other than migrating to the cloud along with the systems that created it.

- **How to manage data that is not worth migrating**
  Finally, how should organizations manage data that is still valuable and essential to keep at the ready, but that does not qualify for migration? We will address this issue in the following pages.

Decision makers migrating solutions to the cloud must decide what to migrate.

Migration Requires Dealing With Multiple Issues

KEY ISSUES TO ADDRESS

When an organization goes through a migration project, it must deal with a number of critical issues:

- It must ensure the integrity of the migrated data not only to guarantee that the data is still usable after the migration, but so that chain-of-custody can be maintained throughout the entire migration process. For example, email data may be successfully migrated from on-premises Exchange to Office 365, but if the organization cannot clearly demonstrate that chain-of-custody was

maintained throughout the entire migration process, the migration process will largely have been a failure. If migrated emails that might be required as part of litigation or for a regulatory audit cannot be proven to be authentic, courts or regulators will typically not allow them to be used as evidence.

- As noted earlier, decision makers must decide what to migrate, since this will have a direct impact on the cost of the migration project and its timing. This is often not an easy decision, since it involves a variety of stakeholder interests, legal requirements, compliance obligations and a host of other factors to ensure data sanctity.

- There are some consequences associated with not migrating some types of data. For example, if emails older than 12 months or data from systems that are no longer in use will not be migrated, there needs to be a way to maintain access to this data for long periods using ancillary solutions.

- Bandwidth is another important issue to consider, since migrating large volumes of data can be time-consuming. For example, a 50 megabit/second broadband connection will require 42 hours 23 minutes to transfer one terabyte of data; an organization with 50 terabytes of data to transfer to the cloud will consume all available bandwidth on a 24x7 basis for 12.6 weeks.

THERE ARE EVEN BIGGER ISSUES TO ADDRESS

Migrating to a new platform, especially one in the cloud, is problematic. The ideal approach is often to migrate existing data into the new system, but that approach comes with a number of challenges as noted above, not the least of which involves migration costs and often incompatible data formats between older and newer systems. There are many situations when a new solution offers significant functionality improvements over current tools, but the cost and complexity involved in moving away from the current system negate much of the business value of doing so.

The issue of migration becomes more important in a cloud environment.

For example, the traditional model of deploying email archiving using on-premises systems requires a certain amount of trust – trust in the technology that is offered by the vendors of the on-premises solution, trust in the quality of how these technologies have been implemented, trust in the responsiveness of the vendor's support when things go awry, trust in the patches and upgrades that are offered, and trust in third party providers.

Moreover, for those in charge of managing solutions in the cloud, more trust is required from the providers offering these services because that data is now in the hands of a third party over which the organization exercises less control than it does over its own IT department. Not only must decision makers trust the quality of the hardware and software deployed in the cloud providers' data centers, the ways their technologies have been implemented, the responsiveness of support staff, etc., but now trust must be placed in a variety of other attributes of the provider(s). These include the quality of the technical team managing the data center, the overall financial health of the provider's business, the quality of the management team that runs the business, their integrity in managing sensitive and confidential customer data, and their responsiveness in migrating data back on-premises or to another cloud provider. The issue is further complicated by the fact that most organizations have a lack of expertise at migrating all data types and formats from multiple systems. This is particularly problematic for organizations that go through acquisitions, where multiple IT infrastructures must be consolidated.

As a result, the issue of migration becomes more important in a cloud environment. Due diligence is very important in selecting cloud providers because of the high stakes involved. For example, they must be vetted on a number of parameters, such as their business model, financial health, uptime, backup strategies and redundant capabilities. While due diligence is important when selecting on-premise solutions, an order of magnitude more care must be applied when vetting cloud providers.

To complete a full migration, multiple vendors may be required, particularly if moving disparate solutions to the cloud. This increases costs and increases the likelihood that there will be problems like data integrity issues, chain-of-custody issues and the potential for variation in the quality of service delivery. Ideally, only a single vendor can be used for the entire migration process.

TAPE MIGRATION IS A CRITICAL ISSUE FOR MOST ORGANIZATIONS

It is important to note that tape is by no means a "dying" technology. For example, LTO tape shipments grew 12.9 percent in 2017 over the previous year and total tape capacity sold in 2017 equaled almost 109 petabytes[vii]. Tape continues to represent the lowest cost option for long-term retention. Moreover, tape is not hackable and not subject to things like ransomware in other types of more accessible storage.

The decision about tape migration is an essential one because most organizations have large quantities of tape storage for backups and long-term archival of strategic information. However, the issue of tape migration is complicated by the fact that some of that data was created by systems that are no longer supported. In some cases, the systems that created this data are no longer available and so the tapes cannot be read.

However, not all data stored on tape should be managed the same way. For example, analytics must be performed to ensure that data can be classified and managed appropriately: old, useless data must be decommissioned properly and defensible deletion policies must be created and followed. While this sounds conceptually simple, it is not as easy as it sounds. While many decision makers understand the value in defensibly deleting older data that no longer needs to be retained (and that could pose a risk to the organization if not deleted), the practice often runs into roadblocks from decision makers who fear the consequences of deleting data that might eventually be required for litigation or other compliance purposes.

Not all data stored on tape should be managed the same way.

SATISFYING REGULATORY COMPLIANCE IS ESSENTIAL WHEN MIGRATING

One of the key issues in any migration is ensuring that regulatory compliance is satisfied when migrating content to the cloud or any other venue, especially while the migration is in process. For example:

- Financial services firms must maintain compliance with the various rules from the Securities and Exchange Commission (SEC), Financial Industry Authority (FINRA) and other regulatory bodies around the world when migrating data. For example, FINRA oversees archiving requirements for broker-dealers, investment advisers and others – archives that are migrated must maintain the integrity of the data that is being migrated.

- Organizations that must comply with the European Union's (EU) General Data Protection Regulation (GDPR) must protect any data it possesses or controls on residents of the EU. This includes ensuring that all third parties they work with are also GDPR-compliant and that they will satisfy GDPR requirements while migrating or performing other options on their data.

- Legal requirements are another form of compliance obligation with which all organizations must comply. As noted earlier, operation data integrity must be maintained during any migration so that chain-of-custody is not violated, which would render the data useless for legal purposes.

Taking a Holistic View of Migration

When considering the choice of a specialist migration vendor, it is important to note that the use of a single vendor with expertise across all types of data migration offers a number of advantages:

- Potentially lower cost, since a single vendor will enjoy economies of scale that the use of multiple vendors will not allow.
- A vendor that has expertise in various types of data migrations can use a standardized approach and potentially offer a greater quality of migration. This is because they can understand the interdependencies across data types that will be involved in the migration effort and can gain visibility into how a problem in migrating one type of data might impact another.
- There is the potential for encountering fewer problems in migrating multiple data types if a single vendor is used, if only because a single approach to the entire migration process lends itself to greater efficiencies than if multiple vendor relationships and timing must be established.
- Using one vendor instead of multiple, point providers for a migration project enables the application of the holistic provider's expertise across the breadth of data types, data formats and systems that created the data. This can result in less time required for the migration, greater support for defensible deletion, and less impact on end users during the migration. Moreover, there is potentially greater security during the migration process since only a single vendor will be managing all data types instead of parceling out different types of data to multiple vendors.

A vendor that has expertise in various types of data migrations can use a standard-ized approach and potentially offer a greater quality of migration.

Next Steps and Conclusions

Osterman Research recommends four steps in considering a migration project and choosing the appropriate vendor for it:

- **Data analysis**
  It is essential to conduct a thorough data inventory across the organization to understand what data the organization has, where it is located, and how it is currently managed. This will enable decision makers to know what to migrate, what not to migrate, what data can be deleted defensibly, and how the remaining data should be managed.

  Once the data to be migrated has been determined, the next decision is the way in which this migration will be accomplished. If the migration is to be managed internally, decision makers need to determine the impact on IT staff resources, their learning curve in developing expertise for the migration process, the potential delay on other projects, and other issues. Decision makers need to understand if they really should manage the migration internally versus using a third party for the project.
- **Vendor selection**
  There are a number of capable vendors that can properly manage a migration project, but fewer that can migrate every data type that an organization might have. The vendor should be able to manage tape migrations and manage on-premises, tape-based data stores properly if the organization has large tape libraries that should be analyzed.
- **Budget allocation**
  Decision makers need to understand how much the migration effort will cost and if they are willing to fully fund a properly managed migration. That might sound

obvious, but migration is not the place to cut corners given the negative consequences that can result from an underfunded migration project.

- **Implementation plan**
  Finally, develop a migration plan that will take into account not only the mechanics of the migration steps, but also the impact on user productivity and access to essential corporate data during the migration.

About Trusted Data

Trusted Data Solutions (TDS) is the foremost expert in managing legacy data from backup tape, email, and voice systems. TDS sets the standard in compliantly transforming the management and accessibility of legacy data and electronically stored information alike. For over two-decades, TDS has been the preferred choice of corporations, regulated institutions, eDiscovery specialists, government agencies and law firms that require an expert for their compliant data transformation initiatives. TDS's leadership is demonstrated by their continued commitment to innovate and advance their services globally.

With its North America Headquarters in New York City, and two international headquarters in the United Kingdom and Singapore, TDS maintains the most expansive global restoration assurance facilities footprint in the market, with locations in New York, New Jersey, California, Canada, England, Wales, Germany, the Netherlands, Norway, Switzerland, Australia, Hong Kong, and Singapore. Within this footprint TDS manages millions of customer tapes, equating to over 500 petabytes of data, across more than 37 thousand successfully delivered projects.

www.trusteddata.com

marketing@trusteddata.com

North America
+1 212 679 7600

Europe
+44 (0) 20 3794 7600

Asia Pacific
+ 65 6262 5622

REFERENCES

[i] Source: McAfee, *Navigating a Cloudy Sky*

[ii] Source: Microsoft published data

[iii] https://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2018-state-cloud-survey

[iv] Source: Netskope Cloud Report, Winter 2018

[v] https://www.statista.com/statistics/422273/yoy-quarterly-growth-aws-revenues/

[vi] https://aws.amazon.com/snowmobile/

[vii] https://www.networkworld.com/article/3263452/backup-recovery/theres-still-a-lot-of-life-left-in-tape-backup.html