WHITE PAPER

Post-Migration Risks of Office 365

By Nick Cavalancia

mimecast®
unified email management

TABLE OF CONTENTS

mimecast®
unified email management

You are likely already aware of some limitations around Exchange Online and have legitimate concerns around security and availability of data and services.

You have to admit it – it's tantalizing to say the least: trading in the headache of implementing, managing, supporting and updating Exchange on-premises for the lure of simplicity that Office 365 and Exchange Online brings sounds like a no-brainer.

But, when you make the move, will the reality match the hype? It's an important question IT needs to really think about. After all, when problems with the security of email, access to archived content, or the availability of Exchange Online arise, IT will be the ones under scrutiny for making the decision to move to Exchange Online in the first place. Which means you should only move email to Office 365 once you have a proper understanding of what you do and don't get with your monthly subscription.

You are likely already aware of some limitations around Exchange Online and have legitimate concerns around security and availability of data and services. So let's start with a simple question.

What should you expect, then, once you move to Office 365?

To answer the question, let's first take a look at where you are today. Your on-premises Exchange implementation comes with a lot of functionality – but even Exchange has shortcomings. In fact, if you consider everything that makes up your Exchange environment, you'll quickly realize that you historically have gone well beyond just the Exchange solution itself and purchased whatever you needed – antivirus, backup, archiving, eDiscovery, etc. – to make up for where Exchange either didn't provide an adequate solution for your situation, or where you simply wanted to augment and use a layered approach.

Whether you're going to Exchange Online for simplification of pricing, ease of use, or anytime, anywhere accessibility to email, recognize what you needed with on-premises Exchange, you still need now with Exchange Online. So, as you think about making the move to Exchange Online, know there will be some trade-offs. What you gain in ease of use and simplicity of administration, you may give up in management fine tuning, control over security and availability, and an ability to personally address any issues that arise with Exchange Online.

To put some perspective around your needs, let's look at 3 different expectations for Exchange Online that you likely have after years of working with on-premises Exchange. See how Exchange Online measures up in an effort to see past the hype and move to Office 365 with your eyes wide open.

Expectation #1: Securing Exchange Online

Email continues to be the easiest way for someone external to the organization to gain entry. What started as a broad-stroke shotgun blast of emails with malware-laden attachments or requests to verify personal credentials has grown into something far more sinister – spear-phishing.

Spear-phishing is much like it sounds – a far more targeted form of phishing, where emails are designed to infiltrate a specific company or set of users within the company.

Spear-phishing is much like it sounds - a far more targeted form of phishing, where emails are designed to infiltrate a specific company or set of users within the company. The sender establishes trust by appearing legitimate, maybe even from within the organization, and the email looks genuine. The methodology is the same as phishing – embed an attachment or URL with malicious code in an effort to get that code to run locally, giving the attacker access or control to an endpoint. In addition, the goal of spear-phishing is far more malicious – the attacker is less concerned about the target's credentials, and more concerned with what those credentials can access. Cases of data extraction, manipulation, ransom, and destruction have all started with spear-phishing attacks.

Because spear phishing is designed to take advantage of an unsuspecting employee, it is in essence the modern day version of social engineering. While users can be trained to look for phishing emails and to not click links or attachments, it's very difficult, if not impossible, to educate users on how to spot spear-phishing emails well enough to rest the defense of your organization solely on their judgment. The spear-phishing email can look 100% legitimate, making this threat problematic to identify.

When you migrate, you're going to need solid technology to address this growing problem. So just how protected will you be with Exchange Online?

The bad guys are continuing to develop new ways to attack organizations and email is one of the most accessible ways in.

The Hype

Email-based threats are an ever-changing landscape with increasingly more sophisticated attacks, so Microsoft is working on addressing this. In their defense, Microsoft has had quite a lot on their plate. If you were to roll back the clock a year or so ago, spear phishing wasn't such an issue, so Microsoft stayed focused on making Office 365 a better product. There is, after all, quite a bit to what makes up Office 365 and it's more than just Exchange - Yammer, SharePoint, OneDrive, and more all need to work together online.

Now that spear phishing has become a top security concern, Microsoft announced a preview release of their new Advanced Threat Protection for Exchange Online which includes time of click protection to guard users from clicking through to malicious URLs.

Microsoft's existing offering – Exchange Online Protection (EOP) provides some protection against malware and viruses, as well as protection against phishing attacks. Its new unreleased product adds on protection from spear phishing and better protection from attachment-based threats.

The Reality

Unfortunately the bad guys are continuing to develop new ways to attack organizations and email is one of the most accessible ways in.

To keep up with threats, you may need to consider extending Exchange Online in the same way you do with your on-premises Exchange. Even when ATP for EOL is released, using a single-vendor approach to security can often leave gaps. But by taking a layered approach, you will provide a better defense against phishing-based attacks, as well as against other kinds of threats, such as a denial of service attack. Layered security helps ensure evolving threats do not get a foothold within your Exchange Online environment.

While threats are an on-going concern, you have a more business-centric issue to address before you move – what are you going to do about archiving?

Expectation #2: Archiving

Archiving is a critical part of Exchange for those organizations that are subject to compliance standards, playing a major role in organizations where eDiscovery is necessary to assist with addressing legal and HR issues. Whether you are subject to compliance standards or are concerned about eDiscovery, just because you put your email up into the cloud, doesn't mean those same compliance, HR, or legal requirements have been met.

So what's available for you with Exchange Online?

While using either in-place or litigation holds has the tendency to bloat your storage, Exchange Online quickly addresses this by allowing customers to purchase additional storage.

The Hype

While it's not an area Microsoft claims to have a true solution for, there are still features such as journaling, litigation holds, and in-place holds that can be of value. If you're not familiar with these, journaling creates a record of sent and received email by placing a copy of messages into a specified mailbox for later retrieval. Exchange supports two variants – standard and premium journaling that provide different levels of granular selection of messages to be journaled. This is often the basis for an Archiving solution, which will extract the journaled messages and organize them within an archive. A litigation hold can hold all mailbox content indefinitely. An in-place hold provides granularity around what to hold and how long to hold it for. In either case, even if a user "deletes" a message, it is still available, just not to the user.

There are some benefits to using these features with Exchange Online. While using either in-place or litigation holds has the tendency to bloat your storage, Exchange Online quickly addresses this by allowing customers to purchase additional storage for an extra monthly fee. Additionally, in-place holds have impressive granularity. Flexible retention durations on messages to be held can be set using query-based selection.

For some of you, this basic set of functionality may cover your needs, but if you're looking for a true archiving solution, this isn't for you.

The Reality

All of the features in Exchange Online related to archiving are more the basis for an actual archiving solution than a solution themselves.

Cloud-based solutions utilize simple changes in MX records to alter the flow of email.

Journaling is the process that makes a copy of messages, but provides little management granularity. Holds provide that granular definition of what is deemed important within Exchange Online and, therefore, should be retained. But that's where their value stops.

A true archiving solution will go beyond just selecting what should be retained and additionally provide protection against deletion through comprehensive read-only archiving, an ability for users to easily access and search archived messages, storage management of attachments, availability when Exchange Online is down, and the portability of archived email separate from your chosen email solution.

Some of you may also be trying to figure out how to use your existing on-premises solution with Exchange Online. It's more than likely that whatever you're currently using won't work with Exchange Online. Some on-premises solutions are trying to address this by either funneling email flow through the archiving solution first (and then pushing to Exchange Online) or by sucking email out from Exchange Online and archiving it after the fact.

But, does using on-premises archiving with cloud-based email even make sense?

Cloud-based solutions utilize simple changes in MX records to alter the flow of email. Also, there is something to be said for using a solution (archiving included) that is built from the ground up for use in the cloud versus an on-premises patchwork solution. And since you're already looking to get rid of a very large part of your on-premises infrastructure (namely, your Exchange servers), why would you want to use an on-premises archive solution?

For some, Exchange Online's Journaling and Holds might be good enough from both an archive and compliance perspective. But for those organizations who want to ensure data integrity and auditability, and are looking to more easily and effectively take advantage of the email archived, a 3rd party alternative may provide better control, an interactive experience, and archive portability.

We live in the world of three, four, five, or even six 9's of availability, each one getting us closer to being up all the time.

While both archiving and security need to be a part of your plan to move to Exchange Online in order to mitigate risk and ensure compliance, your highest expectation revolves around minimizing the greatest risk to your organization's operations: an Exchange Online outage.

Expectation #3: High Availability

One of the promoted features in most every cloud-based solution is the high level of redundancy and, therefore, availability of services. Rightly so, it's also one of the requirements businesses like yours look for when even considering a cloud-based solution.

And the more critical the solution to the business, the more scrutiny put on availability.

No system provides 100% uptime. That's why we live in the world of three, four, five, or even six 9's of availability, each one getting us closer to being up all the time, but still leaving room for the possibility that a system may not be up and running for some period of time.

So, how does Exchange Online stack up when it comes to availability?

The Hype

While there's no hype here, it's important to point out that Microsoft's uptime SLA is measured monthly, guaranteeing a 99.9% uptime (which equates to a little less than 44 minutes of downtime a month) and is a reasonable service level.

But even so, is three 9's of availability enough?

The Reality

Large or small, most businesses simply cannot be without email. Given the existence of Exchange Online outages (take the 8 hour outage in June of 2014 for example) where customers experienced everything from email delays to no access at all, it's understandable to see why some companies are unwilling to move to Exchange Online without a solid business continuity plan for email in place.

The reality is, simply put, it can happen, it has happened, and will likely happen again.

Regardless of whether Microsoft is able to meet their uptime SLA or not, availability should always be a concern, even when a solution is in the cloud. An outage doesn't just present a risk to the organization; it lies much closer to home. The IT pro that made the decision to go to Exchange Online may find their job at risk in the event of an outage – especially if there's no continuity plan.

Your on-premises disaster recovery infrastructure and business continuity plan cannot be replicated by Microsoft.

Your on-premises disaster recovery infrastructure and business continuity plan cannot be replicated by Microsoft, or any other cloud vendor alone for that matter. One vendor alone, with a common architecture and platform, cannot address downtime risk and becomes a single point of failure. Remember you've given up control with Exchange Online for the simplicity, ease of use, and all those other benefits covered at the beginning of this paper. The only way to mitigate the risk of Exchange Online downtime is to consider adding a third party solution where employees can continue sending and receiving email during a Microsoft outage, and, in a perfect world, in such a way they don't even know there's an outage.

Keep in mind that employees are never as technical as you, so the solution you choose should provide as continuous an experience within Outlook as possible. Alternatives for users accessing email from other applications (e.g. via web access or mobile) should all work to reduce user impact and confusion, while keeping the cost of support and ownership low.

Conclusion

Like any good strategic IT thinker, you've been weighing the pros and cons of Exchange Online. The move from servers, support, capital expenditures, and days of your time, to the effortlessness of simply creating a mailbox and you're done should have everyone up and down the IT food chain paying attention.

But by moving one of the most critical and central parts of your corporate communications outside of the corporate walls and into the

It's critical to the success of your move to Exchange Online to choose a cloud-based solution to meet the need here.

cloud, you create risk - security risk, data integrity risk, and the risk of a service outage.

The goal is to mitigate these risks by first understanding them better, and, when possible, addressing them yourself by doing with Exchange Online what you've always done when it comes to Exchange – finding an integrated solution to close up the gaps. Just as you've historically chosen solutions to augment on-premises Exchange, it's critical to the success of your move to Exchange Online to choose a cloud-based solution to meet the need here – ideally one that addresses multiple risk factors – as you don't want multiple cloud point solutions. By doing so you'll create the reality that Exchange in the cloud can deliver on the benefits of reducing complexity while still providing the critical security, archiving and continuity your business demands. ■

With nearly 20 years of enterprise IT experience, Nick Cavalancia is an accomplished consultant, speaker, trainer, writer, and columnist and has achieved certifications including MCSE, MCT, MCNE and MCNI. He has authored, co-authored and contributed to over a dozen books on Windows, Active Directory, Exchange and other Microsoft technologies. He has spoken at conferences such as the Microsoft Exchange Conference, TechEd, Exchange Connections, and on countless webinars and at tradeshows around the world.
