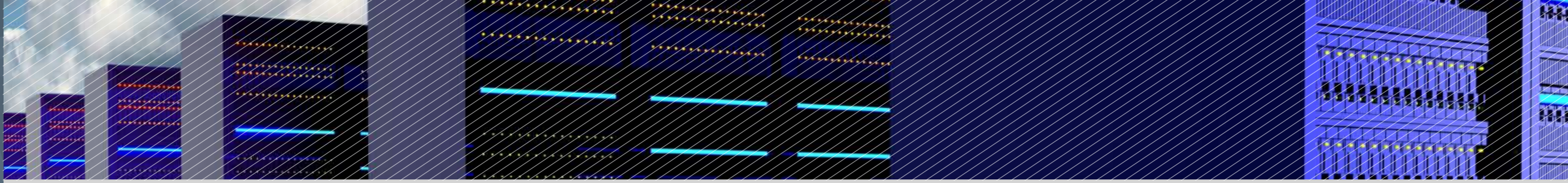
PLANNING FOR OFFICE 365 GAPS

mimecast®



There is a major shift happening right now in the world of enterprise technology.

Many businesses are trading in their focus and investment in on-premises technology for the cloud, a move that brings virtually limitless data scalability, storage and accessibility – at a lower cost and with reduced complexity.

It is estimated that **worldwide spending on public cloud services** will grow at a 19% CAGR from nearly $70 billion in 2015 to more than $141 billion in 2019.

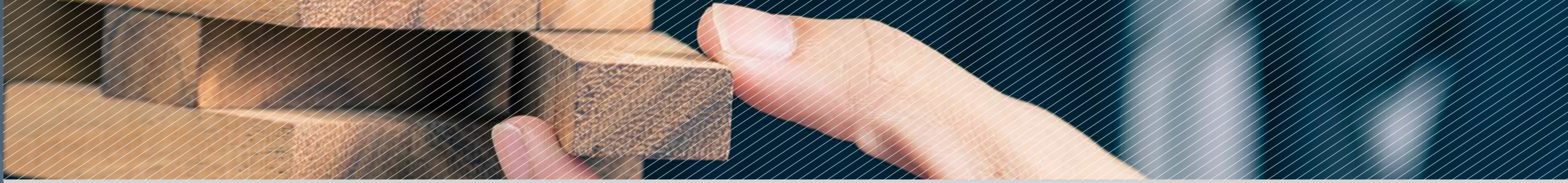
If you're a longtime Microsoft user, the logical first step in making the journey from on-premises to the cloud is to move your email to Office 365. You aren't alone. Office 365 is Microsoft's **fastest-growing business**, ever. According to Gartner, **78 percent** of IT decision makers indicated that they are currently using or planning to use Office 365 software and services in the next six months.

Quick Facts

Office 365 has more than **85 million** corporate users.

Office 365 adds **50,000** new organizations a month – this growth occurred for 28 straight months.

Office 365 has been named **"the most used cloud service"** among **4,000** cloud applications.



So, what’s the issue?

If Office 365 is the cloud email management service of choice for a growing majority of businesses, it must be pretty flawless and risk-free, right? On the surface, it seems to check all the right boxes: resilient architecture, ease-of-use, decent security features, to name a few. However, what isn’t as obvious is the potentially risky new relationship you enter into when you become an Office 365 customer. The reality is, you become fully reliant on a single vendor for security, data assurance and email continuity.

HAVE A PLAN FOR CYBER RESILIENCE

Security threats, like phishing, ransomware and impersonation attacks, are leading to unprecedented financial and data loss, as well as dramatically impacting productivity.

The only way to protect your organization is to implement a cyber resilience strategy that delivers protection of users, data and operations from the risks resulting from technology failure, human error or malicious intent. What's worse? These risks only increase as more organizations migrate to Office 365, making it a higher-value target.

What's an organization to do? The answer is still move to Office 365, but do so wisely. Make sure you have a cyber resilience strategy to address diverse security threats; robust continuity options to solve for unplanned downtime so employees can keep working during an outage; and the ability to recover lost or corrupted data after an attack.

Three Office 365 Risks to Consider:

Ignoring the pitfalls that come with relying on a single vendor increases your risk profile and potential for disaster. With the right planning, cyber resilience strategy and third-party cloud services, you can make the move to Office 365 with confidence.

First, you need to consider – and plan for – the following three problems:

SECURITY

1

THE PROBLEM:

Cyberattacks Can Cripple Your Business and Cost You Millions

Cyberattacks are on the rise, and they are only getting more targeted, sophisticated and damaging. They can cost your organization millions of dollars, cripple employee productivity, result in downtime, and compromise data.

A multitenant environment, like Office 365, can lead to more risk. Mailboxes are always under attack but because there are so many customers that use and rely on the service, attackers will be drawn to it. The same single-vendor security protection for all Office 365 customers means a single lock to pick, increasing each organization's risk exposure and vulnerability to cyberattacks.

THE SOLUTION:

Layered Cloud Security

Think back to when you were on-premises. You likely had multiple layers of protection – why would you forgo this practice when moving your mailbox to the cloud? You didn't rely solely on Microsoft to protect you then, so why would you now that you're in the cloud? Use an additional third-party complimentary cloud service to help defend against advanced cyber threats.

TOP OFFICE 365 Security Gaps

1 New email security threats emerge daily, and one solution that often relies on static lists, won't catch them all.

2 Office 365, protected by a single security layer on a single domain, could expose you to further threats.

3 Sufficient security protection for ever-evolving threats is not addressed by the default Office 365 offering.

ARCHIVING

THE PROBLEM:

Mistaking Data Redundancy for a Data Archive

Office 365 is a real-time data environment, and trusting it with all your email data is risky. Although Microsoft stores multiple copies of data, remember, they all reside in the same architecture and platform, causing a single-point-of-failure. If data is lost, most solutions like Office 365, Salesforce and Workday aren't responsible. They can't control your administrators so you need to plan accordingly.

THE SOLUTION:

Independent Archive

You can't rely on Microsoft alone to keep an independent, verifiable copy of your data. And, without the right backup plan in place, your data could be lost or corrupted due to human error, malicious intent, technology failure or cyberattack. Only by layering in a third-party cloud archive can you provide the best possible protection for your data.

TOP OFFICE 365 Data Protection Gaps

1. An inability to independently locate, review or verify the completeness and accuracy of data stored within Office 365.
2. Data loss or damage caused by technology failure or human error could go undetected for extended periods of time.
3. Malicious or unauthorized access (stolen credentials) to Office 365 could result in data loss or damage.

CONTINUITY

THE PROBLEM:

Email Uptime is Essential for Productivity

Corporate email is dependent on Office 365, so what happens when it goes down? **It does**, and will continue to have outages or delays that can seriously impact productivity. Office 365 is a complex system with many components that must work together.

THE SOLUTION:

Email Continuity in the Cloud

Now that you're in the cloud, you're completely reliant on a single platform with no secondary service in the event of an outage. The only way to ensure business continuity for your messaging platform is to layer in a third-party complimentary cloud solution that covers your email gateway and authentication.

TOP OFFICE 365 Continuity Gaps

1 Risk of significant and long-term regional outage due to technical issues or maintenance related to Office 365.

2 Azure Active Directory is a common approach to authenticate many Office 365 users. However, should Azure go offline, users are no longer able to authenticate, and in turn, access their email.

3 Various aspects of Office 365 go offline on a regular basis. And, while this may not be your live email feed, having long periods of downtime for administration or archive access can expose your business to risk.

Plan your risk management strategy - don’t just hope your email and data is protected in the cloud.

Ignoring the gaps that come with relying on a single vendor dramatically increases your risk profile and potential for disaster. It doesn’t have to be this way. With proper cyber resilience planning and the right third-party cloud services, you can reduce your security, business continuity and data integrity risk, and make the move to Office 365 with confidence.

THE HOPE CLUB	THE PLAN CLUB
Hopefully, nothing will go wrong.	I know something will go wrong.
Risk management is Microsoft’s responsibility.	It’s my business, so risk management is my responsibility.
It’s OK to act after disaster strikes.	I predict failure and prepare before an incident occurs.
It’s OK to only have a “Plan A.”	I have a “Plan B.”
Management budget is not a priority.	Management budget is a must – I understand the potential cost of not taking action.
Cloud best practices are different from on-prem.	Cloud best practices are the same as on-site.
Other companies might have a risk management strategy, but I don’t need one.	Other companies have a risk management strategy, so I might be at a disadvantage without one.
I trust Microsoft when it says I don’t need another environment.	I use an additional third-party cloud service to mitigate the risks of a single environment.

Learn how Mimecast makes Office 365 safer for business.

Mimecast (NASDAQ:MIME) makes business email and data safer for thousands of cu stomers and 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.

www.mimecast.com | © 2017 Mimecast