Remedying the Email Security Gaps in Microsoft Office 365

Proof that a great cloud platform still needs a great third-party security solution

Table of Contents

If you have made the move to Microsoft Office 365™ or imminently plan to, you are in good company. In a recent global poll of 600 IT decision-makers, 94% of respondents said they are either currently using Office 365 or are planning to do so, with 58% already using it. About 70% of email users in organizations that have moved to Office 365 are using it for their email activities.[1] In doing so, they'll reap the cloud benefits of ubiquitous data access and overall agility, as well as the ability to shift certain capital expenses to operational expenses.

That's the good news. The bad news is that in moving email to this versatile cloud environment, organizations may well be exposing themselves to a wide range of security risks, data loss, and business continuity issues. And, more bad news: They may be doing this unknowingly, susceptible to the belief that Office 365 has the highest level of built-in email security available. Plus, the incredible popularity of Office 365 around the world makes it an attack target of high value to hackers and cyber thieves. An infamous bank robber from the early 20th century Willie Sutton once said he robbed banks because, "that's where the money is." Likewise, today's hackers pick targets where the most users and data reside.

[1] Research conducted by Vanson Bourne, commissioned by Mimecast, 2017

Office 365 email security: Unsafe at any speed

Research shows this confidence in the built-in email security of Office 365 is misguided, which is particularly important for both IT and business executives to understand, given today's hyper-dynamic threat environment. The biggest and most destructive security breaches in the past several years were initiated by email phishing and other email-enabled attacks. In fact, the industry-sponsored **Anti-Phishing Working Group** found that the total number of phishing attacks increased dramatically in 2016—by 65% compared with 2015.[2]

In the Vanson Bourne survey cited in the opening paragraph, conducted by Vanson Bourne and sponsored by Mimecast, 88% of respondents said email is critical to their organization.[3] But nearly half of all respondents said they are highly concerned about email management gaps related to data privacy in Office 365, and a full 91% will use third-party solutions to augment Office 365 capabilities, including security. Nearly three-fourths of all respondents said their organizations still need to build additional security protections around Office 365 email use.

Research points to the obvious

Other research builds an even starker case for the use of third-party tools and solutions to strengthen the email security defenses delivered with Office 365. Earlier this year, Mimecast launched its **Email Security Risk Assessment** (ESRA) tool to test the effectiveness of incumbent email security.[4] Using the ESRA tool Mimecast re-inspected emails—more than 26 million of them—that had been "inspected" by incumbent security systems, including Office 365. The following results are provocative, to say the least:

- Of the more than 26 million emails inspected (and previously by the incumbent security), 2 million were quarantined and 1.5 million outright rejected as spam.
- 6,681 "dangerous file types" were flagged and snared.
- 1,628 malware attachments were caught.
- 1,697 impersonation attacks were caught.
- In all, more than 13% of the emails that had been passed on by the incumbent email security defenses were "bad" or "likely bad" emails.

The bottom line: while many organizations believe their current email defenses are up to the task of protecting data in today's threat environment, they are in fact not. This research blows a large hole in the many vague claims and representations of email security often made by incumbent email providers. There are many reasons why IT and business leaders should be concerned about such gaps in Office 365 email security.

Email resilience

First, there is the email security issue itself. Risks abound in a multi-tenant environment such as Office 365, not the least of which is the same security protection for all customers. With new email threats emerging daily, a single security solution just won't catch all of them, as the research demonstrates. There are just too many pathways offering hackers a way in, including phishing, but also spear-heading, ransomware and denial-of-service attacks.

[2] "Phishing Activity Trends Report, 4th Quarter 2016," APWG, Feb. 23, 2017

[3] 3 Ibid. footnote 1

[4] "The Mimecast Email Security Risk Assessment," Mimecast, 2017

Archiving and data protection

Then there is the challenge of data preservation or archiving. Trusting a real-time data environment with all of an organization's data is risky. Microsoft does store multiple copies of data, but they all reside on the same architecture and platform, resulting in a single point of failure. Other data protection gaps include an inability to independently locate, review or verify the accuracy of data stored within Office 365. And actual data loss caused by technical failure or human error could go undetected for a long time. By the way, if data is lost or damaged as a result of any of these gaps, it is gone and Microsoft cannot get it back. It is up to the customer to find some other way of mitigating these risks.

Business continuity

Finally, there is the issue of business continuity. While Office 365 is an excellent service, it is not 100% reliable. In fact, its email service went down for nine hours in June 2016 and similarly the year before, slamming U.S. users during the last day of the month and quarter (and fiscal year for some).[5] All users could do was wait around for Microsoft to fix the problem.

What to look for in a third-party solution

Clearly, a comprehensive third-party solution should be a high priority for every organization committed to Office 365 and email security. But what should this solution look like? What should be the key features and functions?

Consider the three issues outlined above, starting with **email security**. A solution addressing the Office 365 security gaps should look back on when your organization handled email on premises, meaning you had multiple layers of protection. Why forego that when you have moved to the cloud with Office 365? Instead, consider a third-party complementary cloud service as a booster shot for greater email security.

To overcome the **archiving and data protection** gaps, don't rely on Microsoft alone to keep a verifiable copy of your data. Instead, layer in a third-party cloud archive with a comprehensive backup plan to protect against data loss regardless of the source, be it human error, technology failure or cyberattack.

And again, to ensure **business continuity**—because you never know when Office 365 email might go down—layer in a third-party complementary cloud solution that blankets your email gateway as well as authentication.

Look for the following attributes and features in a third-party Office 365 email security solution:

- Consider only a comprehensive solution that the vendor built over time or in-house, rather than one that grew via acquisition. The latter solution may be fraught with integration issues when deployed, adding to IT complexity instead of reducing it.
- Similarly, there are benefits to a solution that is 100% cloud native, meaning it was created from the outset as a cloud solution and grown and improved the same way.
- For ease of use, focus on solutions that administrators can manage and manipulate through a so-called single pane of glass, meaning one management console.
- Make sure the vendor has a proven track record for supporting its solution and ease of deployment.

[5] See Office 365 on Downdetector.com.

Case study: Clover Industries

Several organizations and businesses have successfully navigated their way to highly satisfactory, reliable third-party solutions for enhancing Office 365 email security.

At 116 years old, Clover Industries is one of the most recognized and trusted brand names in South Africa. The branded food and beverage distributor and retailer has some 2,100 email users, with email forming a critical piece of Clover's complex supply chain. Server infrastructure manager Louis van der Walt says losing email service would be "catastrophic," so the company needed a solution to ensure that would not happen.

Clover decided to go with Office 365 for email, but being a public company in South Africa, it was required to first undertake a full risk assessment. With that assessment, Clover felt it needed the same kind of multi-layered email security it had provided itself when email was managed on premises.

The solution that Clover settled on, in this case Mimecast, now buffers all of the company's 80,000 emails per day from spam, weaponized attachments and potentially malicious URLs.[6] Management is via a single centralized console. And, the solution has allowed Clover to drop mailbox size limits, which has supported greater productivity.

Comprehensive solutions to the many email security gaps inherent in Office 365 are available for literally any size organization in any industry or vertical segment. They may be the only thing offering business and IT managers true peace of mind about email data security.

> *"It's a perfect fit: Mimecast, as a single provider, enables a multilayered approach to security, archiving and disaster recovery. Clover now gets all that without building massive storage arrays and cumbersome, expensive systems on premises."*
>
> *– Louis van der Walt*
> *Server Infrastructure*
> *Manager*

About Mimecast

Mimecast Limited (NASDAQ:MIME) makes business email and data safer for more than 26,400 customers 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 in a single, fully-integrated subscription service.

[6] "Mimecast and Microsoft: A Perfect Fit for Clover Industries," Mimecast case study, 2017