That Insecure Feeling About Office 365 Email Security and Resilience

Third-party solutions are key to realizing the benefits of Office 365 without the inherent risks

Table of Contents

If you are among the IT professionals feeling a little uneasy about relying solely on the email security provided by Microsoft in Office 365™, you are not alone. Various research shows ongoing security concerns about email security in Office 365. What IT teams want is the same sense of security they had when they were managing email servers on-premises.

Here's the good news: there are effective, complementary third-party solutions that can not only mirror the kind of layered security built for on-premises solutions, but also ensure uninterrupted access to Office 365 email, even if it crashes.

Surveys show grave concerns over email security

First, consider the "burden of proof" that makes an undeniable case for the email security gaps inherent in Office 365. In a global survey of 600 IT professionals, nearly half characterized themselves as "highly concerned" about email security gaps in Office 365.[1] Not surprisingly, 91% of respondents said their organizations will seek out third-party solutions to bolster the built-in security in Office 365.

Additionally, an Email Security Risk Assessment conducted this year by Mimecast re-examined some more than 40 million emails that had been OK'd by various security solutions including Office 365.[2] Of those, more than 19,000 were found to be "dangerous file types," infected with malicious malware attachments or cleverly disguised impersonation attacks.

1 Research from Vanson Bourne, compiled by Mimecast, 2017

2 "The Mimecast Email Security Risk Assessment," Mimecast, May 2017

mimecast®

TechTarget® | Custom Media

Microsoft Office 365 email security gaps

There are numerous security gaps in Office 365 and many are not insignificant. Most notably, Office 365 is protected by a single security layer. This exposes users to multiple threats—especially since the wild popularity of Office 365 makes it a prime target for hackers and cybercriminals.

When it comes to archiving of emails, Office 365 suffers from an inability to locate, review and verify the completeness and accuracy of data stored within it. Data loss or damage could go undetected for extended periods of time. And Microsoft bears no responsibility for such data loss.

In terms of business continuity, Office 365 is far from bullet-proof. Its email service once went down for nine hours, slamming U.S. users during the last day of the month of June and the last day of the fiscal quarter (and fiscal year for some).[3] Users had to wait around for Microsoft to eventually fix the problem.

Differentiating among third-party solutions

The case for a comprehensive third-party email security solution for Office 365 is a solid one. But like anything else in the IT world, third-party email security solutions for Office 365 are not created equal. One significant difference is that is some are developed for the cloud from day one while others are an outgrowth of solutions developed initially for on-premises use. In the latter case, the vendor will essentially leverage virtual machine technology to send the solution to a cloud platform, such as Amazon Web Services™ or another provider. When this happens, users can find themselves running out of resources, often when they most need them.

3 "Microsoft fixes Exchange Online outage after almost 9 hours," Computerworld, June 24, 2014

If you're considering a solution that comes with gauges and dials indicating when you are running low on system resources or it needs sizing for your environment, it likely was developed for on-premises use.

The importance of being multi-tenant

A cloud-native solution is one that is truly multi-tenant. Solutions that are not multi-tenant often come with fewer network benefits than cloud-native solutions, which offer far more visibility into the kinds of threats that a broad range of users face in real time at any point in time. That means patches, fixes and notifications can be delivered quickly, before problems arise.

With solutions that are not multi-tenant, each customer environment must be maintained, often meaning it may not be on the latest version. Updates may require downtime and may not instantly reflect the latest protection and features that are constantly applied to multi-tenant software-as-a-service (SaaS) solutions.

Finally, some third-party products have been built over time by acquiring different pieces of the solution. IT leaders are much better off considering a solution built organically over time, rather than one that has been rehabilitated module by module. This often results in little to no integration between them and administrators having to use multiple screens for management.

Or, consider a solution developed organically, with archiving and security directly built in together. A user can click on a current email in the inbox or on an email that's five years old and in both cases get the same real-time threat protection against potentially malicious URLs embedded in the emails. In the case of the solution fused overtime, the archived emails could potentially be exposed to malicious links even if the inbox is temporarily locked down in an attack.

Conclusion

If your current email security doesn't fit your risk profile, consider a third-party solution to provide what Office 365 clearly does not. Choose carefully among the many such solutions out there, guided by the experiences of organizations and IT professionals that have already made the move to bolster your resilience.

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.

Case studies

Here's a brief look at what two companies have done to boost email security and resilience within the context of their Office 365 email environments.

Manufacturer adds critical layers of email security to Office 365

Hydradyne, a Fort Worth, Texas-based manufacturer and distributor of industrial motion control products, made the move from an on-premises version of Exchange Server to Office 365 in 2014. As IT Director Mike O'Neil recalls, Hydradyne didn't feel it was wise or prudent to put all its email security eggs in one basket, namely Microsoft.

O'Neil's department supports some 450 email users scattered throughout the Southeast U.S. in 32 locations. For such a highly distributed and decentralized organization, email is mission-critical. In fact, it was several email outages the company suffered with its on-premises Exchange Server solution that got O'Neil thinking about complementary email security solutions.

The process of syncing up the solution with the Office 365 environment was done in a matter of minutes.

So, along with the switch to the cloud-based Office 365, Hydradyne opted for a third-party security solution that immediately gave IT administrators highly granular controls for protecting email far beyond the capabilities of Office 365 alone.[4] Moreover, the process of syncing up the solution with the Office 365 environment was done in a matter of minutes.

Today, Hydradyne receives integrated email security and continuity services from the third-party solution, with continuity serving as a backup to ensure a consistent flow of email. Hydradyne also gets real-time dynamic analysis of all clicked URLs to head off spear-phishing attacks.

Flooring giant simplifies email archiving and retrieval

Although it has more than 20,000 employees, global flooring manufacturer Mohawk Industries has only three IT workers dedicated to supporting and managing email. Its aging archiving platform took as many as seven days to complete a weekly backup, meaning the company finished one backup and then immediately began the next. Worst still, the backups often failed while consuming enormous amounts of storage.

The company reduced internal storage space by 25% while eliminating the need for internal backups.

This was an untenable situation as the company starting receiving more frequent requests from the IT email team for a full day or more. Meanwhile, Mohawk had serious concerns about continuity, given its mission-critical reliance on email communications.

All things considered, Mohawk decided to leverage a SaaS solution, choosing a complete package of email security and email archiving, with litigation search capabilities.[5] The IT staff and users found the solution very easy to use and migrate, as well as compatible with existing applications. Today, most litigation requests can be filled in less than an hour—10 times faster than previously. The company also retired more than a dozen email servers, reducing internal storage space by 25% while eliminating the need for internal backups.

4 "Hydradyne Hydraulics Secures Office 365 Email with Mimecast," Mimecast case study, 2017

5 "Mohawk Industries Uses Mimecast to Simplify Email Archiving/Retrieval and Ensure an Effective AS/AV Strategy," Mimecast case study, 2017