The Essential Guide to

Protecting Your Office 365 Investment with Robust Email Security

appriver

Table of Contents

Introduction

If your business has made the investment in Office 365 from Microsoft, congratulations—you likely have already benefited from this wise decision. And if you are considering adopting this powerful suite of cloud-based productivity and management services, you will quickly realize the many advantages it delivers you, your team members, and your entire organization.

Office 365 is rapidly becoming the worldwide standard for business communication and collaboration. In October 2017, Microsoft reported that Office 365 had 120 million monthly active users, and that number is expected to continue growing.[1] In an increasingly mobile and remote workforce, Office 365 offers versatility with minimal infrastructure and at a low cost. It is surpassing Hosted Exchange as the solution of choice, especially for companies with on-premises servers that are looking for an easy path to the cloud.

A major attraction of Office 365 is its comprehensive email capabilities, giving businesses simple yet robust features as well as plenty of storage. However, a major concern with this email solution is security. Some of the worst data breaches and system infections in digital history occurred through email; plus, with Office 365 based in the cloud, organizations might be hesitant to trust such a bold structural move.

> In an increasingly mobile and remote workforce, Office 365 offers versatility with minimal infrastructure and at a low cost.

An investment in Office 365 is just that—an investment, not only in the solution, but also in your business, because if a problem occurs with the suite, ultimately, your bottom line will suffer. This guide will examine the issues Office 365 users face with security, then detail how to protect your investment from evolving email and cyber threats.

Email Security and Office 365

Office 365 is an excellent service for businesses to deliver productivity tools to their employees and manage documents, email, calendars, data, and more. The competitive advantages Office 365 offer include:

- Cloud-based environment
- Simpler management of company assets
- Consolidated interface
- Empowerment of employees to work from anywhere, on any device
- Security features to protect company data

The Microsoft name gives Office 365 plenty of pedigree to back up its advanced functionality, but from a security standpoint, the solution isn't 100 percent reliable or secure. These shortcomings can be especially troublesome for organizations that rely heavily on the email features of Office 365. Although the basic layer of security isn't substandard, it is still just a single layer. Some key gaps exist, primarily in these two areas:

Weak filtering: Office 365's default email filtering leaves too many gaps for spam, malware, and phishing to sneak in. Settings can be customized, but that takes time and can interfere with the application's functionality and productivity.

No point-to-point encryption: In Office 365, emails are encrypted only when they reach the server, thus leaving them exposed while they are in transit.

Many IT professionals want the peace of mind with email security they had when they managed servers on premises. Unfortunately, Office 365 isn't quite there, thus requiring organizations to supplement their security measures in order to take advantage of all the suite has to offer.

Office 365 is an excellent service for businesses to deliver productivity tools to their employees and manage documents, email, calendars, data, and more.

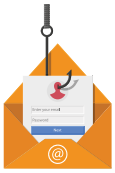
Common Email Security Threats

Office 365 email users can be vulnerable if steps—which might include purchasing third-party software from a reputable provider—aren't taken to overcome archiving and data protection issues. The threats detailed here are the most common (and, often, the most damaging) and need measures beyond what standard Office 365 subscriptions provide:

Ransomware

Ransomware is simply nasty. In this cyberattack, the bad guys infect an organization's systems with a malicious application that encrypts data and essentially prevents users from accessing the system. Then, the attackers demand payment to unlock the systems and let you use your computers again. Even if the payment is met, there's no guarantee the systems will be released, and if they are, data may be lost.

Ransomware attacks are on the rise and are becoming incredibly expensive for small and mid-sized businesses (SMBs)—in 2016, victims paid the bad guys $301 million dollars to unlock their computers.[2] Unless organizations have sufficient backup capabilities to restore their systems without paying the ransom, they are in for an expensive and potentially resource-draining fix. The best defense against ransomware is to not open emails and attachments containing the malicious software—or to prevent those messages from ever landing in inboxes in the first place.



Malware and phishing

Besides ransomware, many other types of malware can infect computers and systems via email. Viruses, worms, Trojan horses, spyware, and other destructive applications can steal data, interfere with business operations, and otherwise wreak havoc with your systems.

Phishing differs in that a delivered email attempts to lure the user into doing something the cyberattacker wants, from clicking on a link to filling out a form to providing passwords. Once phishing emails reach an inbox, your last defense is the user not falling for it, but these emails have become so sophisticated and realistic that even the smartest employees might accidentally click something. The better defensive strategy is to employ software that filters out phishing emails and malware.

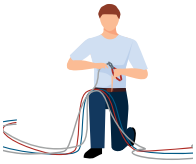
Archiving and data protection

Just because an email is free of malicious intent doesn't mean that risk is eliminated. Information contained within messages might be sensitive or proprietary, contain personal or financial details, and so on—anything that can be potentially damaging to the organization if it's lost or stolen. These emails must be securely protected and archived so that access is limited to authorized users and accounts.

When email goes down for whatever reason, business can grind to a halt.

Email downtime

Many organizations heavily rely on email to communicate with customers, partners, vendors, and employees. So when email goes down for whatever reason, business can grind to a halt. Moreover, data, in the form of emails sent to you or ones you tried sending before the downtime, can be bounced back or lost. Without some sort of continuity solution that lets you use email during downtime, you will be stuck waiting—and every minute lost is money lost.



Human error

Amid all the ransomware, malware, phishing emails, and other digital threats, one contributing factor is often overlooked: human error. A 2018 report from IBM discovered that people inadvertently contribute to nearly 70 percent of all data breaches.[3] Users are still opening suspicious emails, clicking on bad links, downloading unknown attachments, and replying to messages they shouldn't be replying to. Smart governance and user training can help, but ultimately, human error is a challenge that will never be truly eliminated, thus making other security measures all the more vital when someone inevitably clicks something they shouldn't.

How a Third-Party Solution Can Help

Email security threats can't be dismissed by SMBs as "something that won't happen to us." The threats are real, and smaller businesses are often considered easy pickings because they don't usually devote as many resources toward security as larger organizations do. A 2017 report by the Ponemon Institute found that 61 percent of SMB respondents were targeted by a cyberattack in the preceding year.[4] A robust third-party solution can supplement Office 365's basic security features and provide first-class protection for your email. Here are some key things to look for in a third-party solution:

Email filtering

Strong email filtering automatically shores up the gaps in Office 365. Benefits of this comprehensive feature include greater admin control over access, easy rules for implementation, and less clutter from known malware sources and other unwanted senders. The best solutions employ at least four antivirus engines that are continually updated, and offer a way to handle bulk email.

Web filtering

If an email with a bad link finds its way through despite all other security measures, web filtering—which Office 365 does not offer in its security features—can prevent it from infecting your network. Seek a third-party solution that offers dynamic DNS and content/category web filtering that protects against a wide range of malicious applications and monitors outgoing traffic, all without slowing down the network.

The best platforms include an e-signature option, which provides even more security for confidential communications.

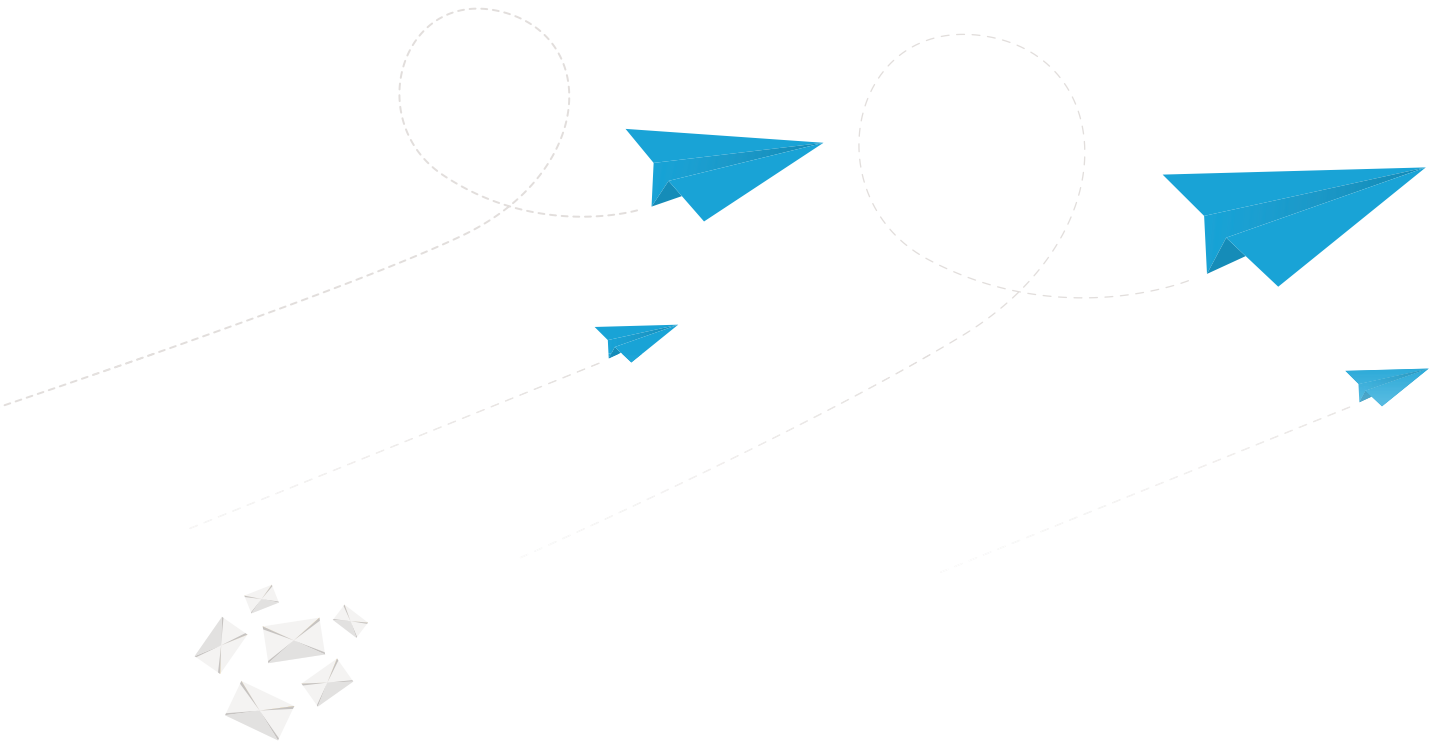
Advanced point-to-point encryption

As already stated, Office 365 encrypts emails only when they arrive at the server. Quality third-party email security solutions encrypt the entire journey, thus allowing secure recipient experiences on any device. Some solutions may even offer a “send secure” option that keeps the encrypted message in the server and sends the recipient instructions to access the message in a secure portal, thus ensuring infected emails are never sent nor received. Also, the best platforms include an e-signature option, which provides even more security for confidential communications while reducing costs and turnaround times.

Archiving

Email has come a long way since a few decades ago when it was just a new way to send messages to people. Today's businesses rely on email for privileged and/or confidential information, to send and receive contracts and affidavits, to exchange proprietary and strategic information, and more use cases beyond simple communication. Therefore, losing this important data because of server or user error is simply unacceptable in today's business world. Moreover, when you have thousands—or even hundreds of thousands—of emails, finding the one you need can be a challenge, particularly if a coworker is the person searching for it.

Archiving solutions that work with Office 365 store emails and records off-site, thus allowing for easy retrieval if and when needed. The best platforms comply with a host of government and industry regulations (such as HIPAA, SOX, and NASD), provide full audit trails and reports, and employ dual encryption to ensure privacy, confidentiality, and non-disclosure.



Email continuity software

If your email servers go down for any reason, sending or receiving messages will obviously be impossible. Email continuity software (which, ideally, won't require any installation on-site) allows you to use Outlook as if your servers were still up and running. Key emails are never lost, and customers will never get a confidence-eroding error message that their emails were undeliverable.

Email continuity software (which, ideally, won't require any installation on-site) allows you to use Outlook as if your servers were still up and running.

What to Look for in a Provider

A comprehensive third-party email security solution must be a high priority for every organization—particularly SMBs—committed to Office 365 and protecting the communication and data flowing through the 365 framework. Microsoft offers an add-on security option, Advanced Threat Protection (ATP), but even that falls short in delivering the features necessary for fully safeguarding email. For true peace of mind, a third-party provider that delivers a cutting-edge, multi-layered solution including all the security features detailed in this e-book is your best bet.

Of course, not all providers are the same. You need the confidence that the software and the people behind the software will be there for you when required. Look for a third-party provider that:

- Has a proven track record working with a wide array of industries
- Offers a holistic, blended solution to cover every email security need and give much-needed peace of mind in today's active-threat environment
- Is easy to do business with and will work with you to ensure you're getting the most out of your Office 365 investment
- Has the support infrastructure (e.g., 24/7 support, help tickets, live chat) to always be there when you need help
- Ensures that a live, trained person—and an employee of the company instead of someone in an overseas call center—answers your call and is empowered to deliver the assistance you seek
- Brings years of excellence, both with its software and its service, to every client, big or small

In short, the third-party email security software you choose must be outstanding, but the people behind the software should be outstanding as well.

Conclusion

The threats businesses face with their email solutions are real and daunting. Office 365, which delivers the simplified-but-comprehensive framework many SMBs need, doesn't offer enough protection to address all the constantly evolving vulnerabilities and threats that loom over organizations trying to keep their networks secure. Robust solutions and top-of-the-line customer service from third-party providers present an answer for businesses looking to maximize their email security and enjoy peace of mind that their systems are protected from malware, ransomware, phishing, and other cyber attacks. AppRiver is such a provider that businesses can put their faith in.

The AppRiver Difference

Some of the things that set AppRiver apart include:

- Our award-winning Phenomenal Care® program, which delivers 24/7, white-glove experience to customers at no additional cost. This service gives our customers access to an extensive knowledge base, remote assistance, live chat support, phone and email support, and a portal with extensive self-service and subscription options. We also guarantee that when you call us, a live AppRiver employee who has undergone months of support training—and not someone in a call center—will assist you. There is simply nothing else like Phenomenal Care in the industry.

AppRiver is such a provider that businesses can put their faith in.

- Email encryption that provides true mailbox-to-mailbox security to keep confidential information safe and businesses compliant.
- Advanced email security anti-malware and anti-phishing protection that blocks 99 percent of unwanted messages.
- DNS-level and category/content web filtering.
- Email continuity software that disaster-proofs business email.
- Real-time network threat notification alerts.
- Weekly/monthly threat assessment reports, customized for your network.
- Compatibility with any email service.

About AppRiver

AppRiver works with more than 67,000 companies worldwide, providing cloud-based cybersecurity and productivity services to help meet IT needs. Contact us today at 866-223-4645 or sales@appriver.com, or visit our website, www.appriver.com, to learn more about how we can help your organization.

Free Trial

References

1. Foley, Mary Jo. "Microsoft Office 365 Now Has 120 Million Business Users." ZDNet, ZDNet, 26 Oct. 2017, www.zdnet.com/article/microsoft-office-365-now-has-120-million-business-users/.
2. "Businesses Paid $301M to Ransomware Hackers Last Year, New Datto Study Finds." About, Datto, 21 Sept. 2017, www.datto.com/news/datto-releases-global-state-of-the-channel-ransomware-report.
3. "IBM X-Force Report: Fewer Records Breached In 2017 As Cybercriminals Focused On Ransomware And Destructive Attacks." IBM News Room, 4 Apr. 2018, newsroom.ibm.com/2018-04-04-IBM-X-Force-Report-Fewer-Records-Breached-In-2017-As-Cybercriminals-Focused-On-Ransomware-And-Destructive-Attacks.
4. 201 7 State of Cybersecurity in Small & Medium - Sized Businesses (SMB). Ponemon Institute, Sept. 2017, csrps.com/Media/Default/2017%20Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf.