A Guide to Evaluating Security & Spam Solutions

For Office 365 Outlook

sendio®

Contents

Introduction

Microsoft Office 365 is increasingly popular with organizations happy to be freed from managing a continually mutating zoo of desktop and mobile office systems. Although companies rely on multiple solutions within Microsoft Office 365, email may, arguably, be the most used with more than 121 average emails sent and received per day by each user. As a result, email security has become indispensable for the productive use of Office 365 (and, of course, to the personal productivity of anyone in business.)

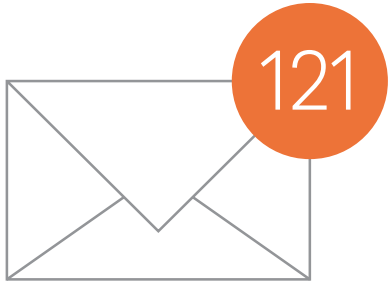
Microsoft recognizes this fact and has included a range of email security features in Office 365 Exchange. However, those features are entirely conventional ones, in an environment where conventional, at the enterprise level, is no longer adequate.

Conventional email security can be likened to urban water "systems" of 150 years ago. Residents were expected to dig wells or go to the river to get water for their personal use. Those who used and drank that water were wise to filter, boil, or use another method to counter the harmful things this water might contain. To dispose of wastewater, including both sewage and storm runoff, they dug ditches.

Modern enterprise-level email security must be more like the plumbing of a 21st-century city than water systems of 150 years ago. Today, urbanites have sophisticated water systems that are equipped to handle a growing population and conveniently deliver clean water to a resident's faucets. They're systems that have been carefully built and engineered so that the resident need not worry about extra precautions to ensure his or her water is safe.

With Office 365 Exchange, unfortunately, further precautions are in order. There's a growing population of cyberthreats that cannot be handled with conventional security systems likened to water systems of 150 years ago. Office 365 email is a necessity like water to life for some organizations, which means that adequately protecting a vital communication tool with added security and spam solutions is critical to business success. In this guide, we offer a comprehensive look at the existing security measures in Outlook, examine where it fails IT, and provide expertise on selecting the right solution for your organization.

Although companies rely on multiple solutions within Microsoft Office 365, email may, arguably, be the most used with more than 121 average emails sent and received per day by each user.



Office 365 and Exchange Online

Office 365 is a cloud-based shared office environment based on widely used Microsoft office productivity applications, such as Word for word processing, Excel for spreadsheets, and Power-Point for presentations. Each user only needs a compatible machine, or mobile device, with Internet access. Networking and storage can also be done through the cloud. Microsoft handles software maintenance for the applications. The advantages to an enterprise, in terms of simplified management, are significant.

Of course, when discussing email security, we are focusing on the Exchange Online component of Office 365. Basically, Exchange Online is the cloudbased version of Exchange Server. The latter has been the traditional email server for offices using Microsoft Office, running locally on the enterprise's network, with Outlook as the traditional email client for individual users. With Office 365, all the features of Exchange Server are available through Exchange Online, plus features available only in the cloud, such as globally redundant servers for disaster recovery, uptime backed by service-level agreements, and backups to the cloud. Maintenance is through a Web interface. All the advantages involving the productivity applications of Office 365 also apply to Exchange Online, with patching and updating being handled automatically by Microsoft. (Hybrid environments, involving both hosted and on-premises servers, are also possible.)

Exchange Security Features

Office 365, through its Exchange Online component, offers conventional anti-spam protection, plus anti-malware (i.e., viruses and spyware) protection. It also offers a number of email-related security features, of interest to certain organizations, which do not directly protect against spam and malware.

To prevent incoming spam, Exchange offers spam filters and connection filtering. Spam filters examine the contents of incoming email for the characteristics, or signature features, of spam. End users and administrators can be alerted when email has been diverted as suspected spam so that they can check for false positives.

Connection filters enable the administrator to allow or block all email from specific IP addresses. Basically, the administrator has to manually compose a white list (the mail from which is allowed through) and a black list (the mail from which is blocked), although Microsoft will optionally supply a default white list. If an incoming message is blocked by a connection filter, the recipient receives no notification. With connection filters, administrators must constantly be on the lookout for potentially dangerous IP addresses.

Newsletters and sales offers constitute a troublesome gray area for Exchange Online and conventional email security, because they often enter the recipient's inbox and become mixed with legitimate, important email. Sent by automated systems, they are frequently a time-wasting nuisance even if their contents are not malicious. These items may pass both a spam filter and a connection filter, depending on the nature of their contents and the sender's IP address. But if they are successfully blocked, this can also be a problem, as a specific user may want to receive a specific machine-sent item.

To prevent incoming spam, Exchange offers spam filters and connection filtering.

Phishing, meanwhile, is assuredly malicious. Phishing, of course, is the use of targeted spam to trick the recipients into doing something advantageous to the spammer, such as sending money or revealing information. Phishing messages typically incorporate detailed information about the recipients so that they'll be lulled into thinking they're dealing with someone who has legitimate ties to their organization. Exchange Online has no filter designed to spot phishing scams. Users must rely on general filtering. If a phishing email does get through, the first line of defense becomes the security expertise of the recipient, which is often minimal.

Malware, of course, refers to software that can infect a machine (i.e., viruses) and software that can gather personal information (i.e., spyware). As a hosted service, with the resources of the cloud at its disposal, Exchange Online uses multiple scanning engines to examine email for malware. Detection rules can be updated every two hours, and partial rules can be applied even when full details about a new threat are lacking. Definitions used by the scanning engines are updated hourly. Unfortunately, hackers, in recent years especially, have moved beyond malware, making it a much smaller part of an attack strategy and, in many instances, the least concerning threat.

Other Conventional Features

Other useful security features that Exchange Online offers include data loss prevention, e-discovery, journaling, audit reports, rights management, and message encryption. While they involve security and email, and may be of great value to specific organizations, they fall more under the heading of regulatory compliance than the suppression of spam and email threat protection. A breakdown of each can be found to the right:

E-discovery lets a compliance officer search archived mailboxes of Exchange users across the enterprise, examine the results, and preserve them in separate archives.

- **Data loss prevention** is aimed at data breaches caused by insiders sending information to outsiders. Using content analysis, emails can be filtered for sensitive information and the attachment of restricted files, as identified by the administrator. Email users can be told they're about to violate a policy before they click Send.
- **E-discovery** lets a compliance officer search archived mailboxes of Exchange users across the enterprise, examine the results, and preserve them in separate archives.
- **Journaling** is the recording of all communications connected with certain business tasks, for regulatory and compliance purposes. It is more targeted than archiving.
- **Auditing** features track all changes made to the enterprise's mail server configuration and track all access to mailboxes by persons other than their owners.
- **Information rights management** allows the administrator to control who can access, forward, print, or copy any sensitive data contained within or attached to an email, protecting things like sales reports and personnel files.
- **Message encryption** with Office 365 works with recipients on any mail service, as the messages are viewed through decrypting Web portals.

Conventional vs. **Modern** Security

The previously discussed email security features of Exchange Online are entirely conventional. By conventional standards, they are comprehensive. Certainly, having these features is vastly preferable to having no protection at all. But users of Exchange Online and its protection features report that spam, malware, and unwanted newsletters and sales offers continue to get through at uncomfortable rates. This is not surprising. To return to our plumbing analogy, the conventional approach is based on the old concept of drawing water from the well, or the river, and doing something to it to prevent illness from drinking water.

For someone who has never experienced modern plum ing, treating the water on the fly seems like the logical course of action. If the contents of the water keep changing, the answer is to put more effort into treating it. However, for someone who has become accustomed to modern plumbing, all that effort may seem like an irrelevant diversion from what ought to be done: building a system with a controlled source of water that reliably delivers something that's safe to drink.

Fortunately, setting up Internet plumbing to preserve the cybernetic health of your enterprise does not require massive civil engineering projects. Basically, you'd want to employ two sets of technologies that do two things: challenge the legitimacy of each sender and their server and IP's reputation. As many IT professionals have discovered, it is possible, using a hosted service, to add such methods to an existing Office 365 environment to ensure email arriving through Exchange Online safeguards with modern levels of security protection.

Modern Methods

Modern methods involve challenge response technologies for assured security, augmented by other technologies, because, frankly, assured security is not entirely a good thing you don't want to be cut off from the rest of the world.

Challenge-Response

The first modern method, involving challenge–response technology, ensures that all mail reaching the inbox is from a legitimate human being, one actually interested in having a conversation with the recipient. To ensure the sender is a legitimate human trying to have a conversation, that sender is sent an email that he or she must respond to—and that response requires a click verification that only humans can make. (Basically, the sender has to answer a question that would stump a machine.)

After passing the test, that sender's messages are always sent straight to the recipient's inbox in the future.

This technology, by itself, can serve as an analogy for a 21st-century drinking-water system, because its sources of content are assuredly safe. There, however, the analogy weakens, because you really don't want to cut yourself off from the outside world, and that's what you're doing if you accept mail only from a fixed list of senders. For this, other security technologies come into play. The user, depending on administrative restrictions, still has access to all of his or her emails, albeit with precautions.

To that end, emails from unverified senders still reach the recipient's failed-sender archive—after being filtered to counter spam and malware using other modern technologies. These modern technologies include:

- Sender reputation tracking
- IP reputation tracking
- Silver-listing through deferrals
- Industry-standard anti-spoofing methods

Each of these technologies offers a different line of protection. Below is a breakdown of how each works, which will help you understand the importance of these added lines of defense to Exchange:

IP Reputation Tracking

As the term indicates, IP reputation tracking works by giving IP addresses that spew spam a lower reputation score on a number scale (based on the volume and consistency of spam from the IP address from day to day), and email from these IP addresses can be proactively held for IT administrator review. IP reputation tracking is best done by a hosted service that can perform global monitoring— emails, after all, can come from anywhere on the Internet.

Silver-Listing Through Deferrals

Silver-listing through deferrals is a way to defeat spam by short-circuiting typical mass-emailing software. Deferred email is email that is sent back without either delivering it or rejecting it (451 deferral code in the email standards), usually because of a technical problem at the receiving end. A legitimate email server will resend the message a few minutes later. Spam software will not react to a deferred message and, as a result, will not resend it. Consequently, such spam is automatically stopped without ever accepting the email message. If the deferred message is later resent, the sender is assumed to be legitimate and is added to the silver list pass list. That sender's messages (based on its sending IP address) are allowed through. But a silver list is not a white list—each sender is tested every 30 days with a deferral to make sure it is behaving like a legitimate mail server.

Spam software will not react to a deferred message and, as a result, will not resend it.

Anti-Spoofing

Spoofing involves email that pretends to be from someone other than the spammer who sent it. Spoofing is essential to successful spamming and phishing; however, there are industry-standard techniques that can be used to block spoofed messages: Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM).

Entries for individual domains within the distributed Domain Name System specify which IP addresses are allowed to send emails for that domain. With SPF, a recipient can check to see if the sending computer was authorized by the domain that the message purportedly came from. If not, the email is considered spoofed and can be blocked automatically.

DKIM looks at the contents of the message when deciding if the message is spoofed. The sending software adds a DKIM signature field to the message that includes a hash of the message—i.e., a value derived by algorithmically processing the message itself. If the recipient can decode the hash using the sender's public key (available from the Internet), the recipient can be assured that the message is from the stated sender.

The recipient can also be sure that the message was not altered in transit. DKIM is used by major mail services to block spoofed messages from one service to another. Using all these technologies in combination will achieve the best results. Anti-virus scanning is still prudent as well, and a hosted service can continually update its library of spam and malwares ignatures.

Other **Desirable** Features

In this day and age, when user interface design has become a science, flexible but undemanding administration tools are not an option. The tools should work across multiple domains, if necessary.

Less visible, but also not optional, is a hardened software kernel that will be opaque to any hacker who penetrates that far. Industry-standard operating systems may be open books to hackers, but an in-house rewrite of, say, Linux, that's stripped of nonessential features, will be more like an office safe. Of course, it takes effort to build that safe.

Meanwhile, there are more threats to a mail system than spam and malware, such as the storms and broken plumbing that generate power outages and wreck hardware. Any top-tier email system must include continuity features so that an office can recover from the inevitable outage. A hosted system, for instance, can just as easily store copies of delivered messages for set periods to allow them to be recovered if they ended up being lost by the recipients. In addition, with a host system, the email server is automatically off site, which is an important factor in disaster recovery.

Automatic encryption of email in transit (regardless of whether or not the user encrypted it as well) is also a desirable feature that many organizations seek in providers.

ABOUT SENDIO

The modern security and spam features that we've laid out describe a unique approach offered by Sendio. With hosted features, Sendio protection can be added to Office 365 immediately, painlessly, and without any hardware investment. Email security concerns will immediately become a thing of the past. With Sendio protection, it's possible to realize the promise of a truly unplugged office that Office 365 offers. Without that protection, you may simply inherit the problems that beset your legacy environment. If you're ready to experience Office 365 the way it ought to be, **request a demo** to see Sendio in action today.

(949) 274-4375 | www.sendio.com

sendio®