Quick Answer: Is Microsoft's Email Security Capability Good Enough?

Published 16 September 2022 - ID G00764669 - 5 min read

By Ravisha Chugh, Franz Hinner

Microsoft has continuously improved its email security capabilities, yet there are gaps. Security and risk management leaders must understand the strengths and weaknesses of Microsoft's email security capabilities to determine whether it can meet business requirements.

Quick Answer

Are Microsoft's email security capabilities good enough?

- Microsoft's email security capabilities vary according to the type of license your organization holds.
- With the rise of business email compromise (BEC)-type phishing, no secure email gateway (SEG) is 100% effective in blocking all the attacks.This requires organizations to assess the native capabilities of Microsoft and further augment with a third-party solution if needed.

More Detail

Microsoft's Capabilities Depend on the License

Microsoft has two offerings for inbound email filtering: Exchange Online Protection (EOP) and Microsoft Defender for Office 365 (MDO). MDO is further available in two editions: MDO Plan 1 (P1) and MDO Plan 2 (P2). Each edition offers different sets of capabilities.

Figure 1 illustrates the features available with each of the products, in Microsoft's terminology.

Figure 1: Microsoft's Email Security Product Capabilities

Microsoft's Email Security Products

Source: Gartner
721153_C

Gartner

EOP is the basic functionality included with all plans, and is a cloud-based anti-spam and signature-based anti-malware service. It is available for both on-premises Exchange and Exchange Online. It provides basic anti-spam protection in the form of IP connection checks and simple email content scanning. Antivirus protection uses multiple primarily signature-based anti-malware engines, one of which is Microsoft Defender for Endpoint.

In addition, EOP also includes a feature called Zero-Hour Auto Purge (ZAP), which can remove a malicious email after it has been delivered to a user's inbox. Such a feature is highly beneficial if an email were to be weaponized after being delivered, as ZAP can identify it and directly move it to quarantine without notifying the user. This feature is not available with on-premises Exchange infrastructure

By default, EOP scans all inbound and outbound emails, but you can also get additional features such as internal protection and data loss prevention (DLP). Email security requires more than the basic protection provided by EOP, and Gartner client inquiry data reveals that EOP does not meet the requirements for most of our clients. Therefore, it is highly recommended not to use the basic EOP as your only email security solution.

To get the more-advanced inbound email security capabilities, Microsoft offers MDO. Following are the three core features included with MDO P1:

- Safe Links provides URL rewriting for Exchange, SharePoint, OneDrive, Office Client and Teams Chat/Channel.
- Safe Attachments provides sandboxing features for Exchange, SharePoint, OneDrive and Teams.

- Anti-phishing protection provides some protection for BEC and other social engineering phishing attacks.

MDO P2 adds additional capabilities to Plan one. Three of the biggest benefits of P2 are:

- Security awareness training
- Automated investigation and response to automatically resolve user-submitted suspected malicious messages
- Threat Explorer and Threat Tracker to improve visibility into local attack patterns and techniques combined with threat intelligence

Security awareness training includes simulation and training capabilities.It also includes a rich catalog of training modules for which Microsoft partners with Terranova Security. Currently, MDO P2 features are also available for a free 90-day trial that allows organizations to try features of MDO before finally opting for it. However, your experience will vary here, depending on whether you are utilizing a secure email gateway or native Microsoft capabilities.

For example, organizations using MDO P2 with SEG can only operate it in audit mode, whereas Microsoft customers can also use it in block mode. One of the biggest advantages of MDO is its integration into the Microsoft Security Response Center. It offers an integrated extended detection and response (XDR) capability that unifies incident response across Microsoft Defender for Endpoint, Azure AD and MDO. It provides automated playbooks that can perform automated tasks that cut across these three major security products. For example, an incident responder can initiate an Exchange search and remove from inboxes all emails related to the current investigation.

MDO provides all the capabilities expected of an email security product and is a decent solution that is a good competitor of other SEGs. Gartner client inquiry data indicates a significant improvement in client satisfaction with MDO over time. However, some clients still report a level of dissatisfaction related to BEC protection. For most organizations, we assess MDO protection as good enough.

However, we expect that more-demanding Gartner clients will consider supplementing Microsoft's native capabilities with third-party integrated cloud email security (ICES) solutions. These solutions focus on the capability gaps of Microsoft and are generally deployed via API-based solutions or the ICES solution's routed solution between Exchange and the mailbox. In some cases, the lack of effectiveness is due to mail routing rules bypassing the protection capabilities or incorrect settings, such as mailbox intelligence not being turned on or an anti-phishing configuration set to the lowest level.

Organizations can use Microsoft's preset security policies service to fix the poor default configuration of EOP/MDO. In many cases, this will help increase the detection level and possibly

lead to not having to augment MDO.When migrating to MDO, security and risk management leaders must carefully evaluate these rules.

Augment MDO With a Third-Party Solution If It Is Not Sufficient

While MDO is sufficient for most organizations, no solution is perfect. Due to the rise in business email compromises, account takeovers and the increasing sophistication of modern phishing attacks, highly security-conscious organizations will likely want to augment MDO with another solution to improve overall anti-phishing effectiveness. The good news is that there is a plethora of ICES solutions that are designed to complement MDO and easy to trial via API integration.

ICES solutions (see Market Guide for Email Security) use API access or connectors to analyze email content after MDO, but either before or concurrently with delivery to the inbox, without the need to change the MX record. Most of these solutions use machine-learning-based detection, natural language processing (NLP), image analysis, computer vision technology and behavior analysis to detect phishing attacks. They are often very quick and easy to deploy, as they don't require changes to the email flow at the gateway level.

However, there can be latency issues with API-based solutions that could result in a malicious email being delivered to a user's inbox before a final verdict from these solutions. Thus, organizations can leverage the anti-spam, anti-malware and other capabilities from Microsoft, and then use the capabilities of these API-based products for protection against advanced attacks that bypass Microsoft.

Recommended by the Authors

Market Guide for Email Security

Protecting Against Business Email Compromise Phishing

Tool: Vendor Identification for Email Security

5 Components for Securing Microsoft 365

Evidence

Email Security Services (ESS): Enterprise 2022 Q2, SE Labs.

Exchange Online Protection Overview, Microsoft.

Microsoft Defender for Office 365 Security Overview, Microsoft.