Trustwave®

Why Microsoft 365 Needs Additional Email Security

Email is among the top attack vectors used by cyber threat actors and their attacks are only increasing in effectiveness. At the same time, cloud-based email solutions – especially Microsoft 365 – are increasing in popularity, despite a significant hole: they lack sophisticated, comprehensive email security.

This may come as a surprise to Microsoft 365 users, who are told the offering comes with security built in, namely Exchange Online Protection (EOP). While that's true, EOP is far from all-encompassing.

EOP "lacks advanced anti-phishing and other threat protection capabilities," according to Gartner.[1] "With the rise of business email compromise (BEC)-type phishing, no secure email gateway (SEG) is 100% effective in blocking all attacks. This increase requires an additional email security solution for organizations with stringent email security needs."

Email: an attractive target

Arguably any organization has "stringent email security needs" given how frequently email is targeted in cyber-attacks, and the fact that the trend toward remote work has only increased reliance on email.

According to the 2022 Verizon Data Breach Investigations Report, email was the attack vector of choice in about one-third of all breaches. Those breaches led to actions including stolen credentials (about 40% of attacks), ransomware (25%) and phishing attacks (20%), among others.[2]

A study by Arlington Research found the situation is even worse for remote workers, especially for Microsoft 365 users. Of IT leaders who use Microsoft 365, more than two-thirds report an increase in data breaches due to remote work, versus just 32% of IT leaders who are not using Microsoft 365.[3]

Exchange Online Protection is not enough

That is not surprising given EOP is missing capabilities such as SMTP policy management, which means a loss of control over internal email business processes and policies. It also lacks proper protection against threats like ransomware, malware, phishing, BEC, and spam.

EOP relies on static signatures to detect phishing and malware attacks. While that's a start, it does not protect organizations against zero-day attacks for which no signatures exist. Nor does it help in instances when a user falls victim to a phishing attack by clicking on a malicious link or attachment.

To gain such capabilities organizations need to take Gartner's advice and adopt an additional layer of email security, which is in keeping with an overall layered, "defense in depth" approach to security.

To learn what full-fledged email security should look like, check out the **Trustwave MailMarshal Suite** – with a 20-year record of no major reported client incident. Then **schedule a demo** or **try it for free**.

1 "**Determine If Email Security in Office 365 Meets Your Organization's Needs**," by Ravisha Chugh and Mark Harris, Gartner, Oct. 23, 2020.

2 "**2022 Verizon Data Breach Investigations Report**," Verizon Business, May 2022.

3 "**An Alarming 85% of Organizations Using Microsoft 365 Have Suffered Email Data Breaches, Research by Egress Reveals**," Business Wire, May 11, 2021.

www.trustwave.com

MM365_1222