Trustwave®

Outlining the Benefits of Trustwave MailMarshal with Microsoft 365 Email

The numbers associated with email as a cyberattack vector are eye-opening to say the least:

- 90% of data breaches occur due to email-based phishing[1]
- 83% of organizations suffered a successful phishing attack in 2021, up from 57% in 2020[2]
- $43 billion in exposed losses due to business email compromise (BEC) from July 2016 to December 2021[3]
- A 65% increase in identified global exposed losses from BEC between July 2019 and December 2021[4]

Couple that with the fact that some 60% of organizations using Microsoft 365 say they have suffered a credential compromise[5] and you have definite cause for concern if you're employing Microsoft's cloud-based email solution (or anyone else's, for that matter).

Email security demands a layered approach

It should be clear from such stats that the tools Microsoft offers to secure its cloud email accounts are not enough. Just as with every other aspect of security, it takes a layered approach to properly secure email systems.

When it comes to Microsoft 365, layered security is exactly what Trustwave Mail Marshal provides, in two distinct ways.

First, MailMarshal provides layered security on its own with multiple approaches to email security, not only protecting against spam, phishing, malware, ransomware and zero-day attacks, but also data loss prevention, anti-virus, encryption, blended threats, and more. Second, MailMarshal complements the security tools Microsoft offers, providing an additional layer of protection.

Simply put, when it comes to providing email security, MailMarshal and Microsoft 365 are better together. Let us count the ways.

Granular control of email traffic

Most companies use rules-based policies to manage internal email, such as to block users from sending out sensitive intellectual property, customer data and the like. Often these policies are critical in terms of compliance with industry regulations around privacy and security.

Additionally, many companies use email as an interface between applications and systems – helpdesk systems, ticketing applications, databases, printers, and more – to automatically send email messages.

Cloud-based email systems such as Microsoft 365 have little to no capability to manage such internal email traffic.

MailMarshal provides granular control of internal email, including more than 130 built-in policies for email management. Users can manage policies and compliance through a single portal. So, even when migrating to Microsoft 365, you can retain control over internal email policies and rules that may be critical to compliance and everyday workflow.

Research-driven, proactive approach

Keeping up with cyber threats requires deep research into the latest tools, techniques and threat vectors perpetrators are seeking to exploit. Most any decent secure email gateway (SEG) can detect a known virus or malware for which a signature is readily available. But detecting newer threats – including zero-day threats for which no signature has yet been developed – requires a more thorough approach.

The Trustwave SpiderLabs Security Research Team consists of more than 50 cyber security experts who are continually on the hunt for new threats. They maintain the Trustwave Global Threat Database, which holds billions of records about cyber threats, malware and vulnerabilities from around the world, including malicious URLs, IP addresses, file hashes and the like.

This research is critical in enabling MailMarshal (and other Trustwave security tools) to identify threats that others simply can't. It enables MailMarshal to take a proactive approach to security, identifying patterns that indicate a new threat – a crucial capability in detecting zero-day threats.

Insight into blended threats

SpiderLabs research is also at the heart of MailMarshal's ability to identify blended threats, which use multiple vectors in an attempt to compromise information. Typical examples include a personal, targeted email message that includes a website link that leads to malicious code or attempts to extract personal information.

The MailMarshal Blended Threat Module provides a real-time defense against blended threats. It includes a Link Validator that ensures links are legitimate before completing the connection to the target site, while blocking requests to malicious sites.

Improved protection against common threats

While Microsoft 365 does detect spam and malware (malspam), success rates are far superior with the addition of MailMarshal. What's more, suspicious emails detected by Microsoft 365 are not quarantined from end users as they are with solutions like the Trustwave Link Validator.

But combining the proprietary defense filters in Trustwave MailMarshal with the built-in security protections in Microsoft 365 delivers unprecedented detection.

In tests Trustwave conducted with tens of thousands of emails, the results were clear: the combination of MailMarshal and Microsoft 365 caught 100% of phishing and malware threats, 99.4% of spam, and 99.3% of BEC attempts (see chart below).

	Samples	MailMarshal		Microsoft 365		Combined	
	Total	Missed	Detection Rate	Missed	Detection Rate	Missed	Detection Rate
Malware	9.705	0	100.00%	7	99.93%	0	100.00%
Phishing	11.248	17	99.85%	14	99.88%	0	100.00%
Spam	21,732	49	99.77%	154	99.29%	17	99.94%
BEC	1,001	9	99.10%	43	95.70%	7	99.30%

Track record of success

The simple fact is MailMarshal has a track record of success over the past 25 years, including:

- A 99.99% Malware and exploit capture rate
- Zero clients reported ransomware infection or major incidents
- < 0.001% spam false positives

Rather than relying on Microsoft 365 alone, take a layered approach to email security. Join those who have dramatically improved their security posture and take advantage of the deep security expertise built into MailMarshal.

To learn more, check out our **webinar on the value of layered security** or visit the **MailMarshal page**. You're also welcome to **request a demo** or **sign up for a free trial**.

[1] **"2021 Cyber security threat trends,"** Cisco.

[2] **"22 very bad stats on the growth of phishing, ransomware,"** VentureBeat, Feb. 22, 2022, quoting **Proofpoint 2022 State of the Phish** report.

[3, 4] **"Business Email Compromise: The $43 Billion Scam,"** FBI Public Service Announcement, May 4, 2022

[5] **"Cybersecurity threats facing enterprise email accounts,"** SecurityMagazine.com, April 21, 2022.

Trustwave®

www.trustwave.com