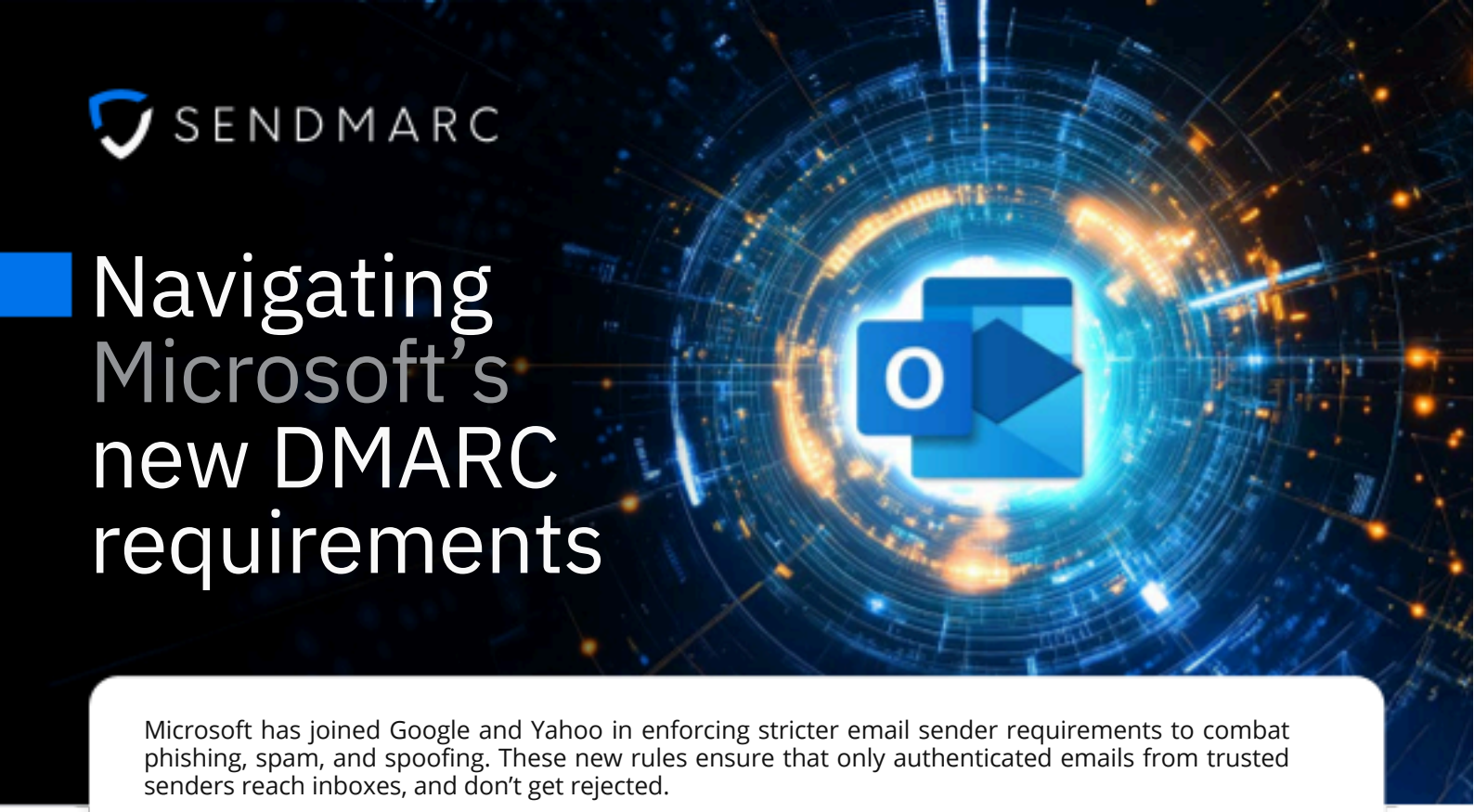
SENDMARC

Navigating Microsoft's new DMARC requirements



Microsoft has joined Google and Yahoo in enforcing stricter email sender requirements to combat phishing, spam, and spoofing. These new rules ensure that only authenticated emails from trusted senders reach inboxes, and don't get rejected.

Starting May 5, 2025, Microsoft will begin rejecting emails from high-volume senders (sending 5 000+ messages/day) that don't meet the new requirements.

What's changing?

Mandatory requirements for bulk email senders:

Authenticate allemailswith SPF, DKIM & DMARC

Emailssent to Microsoftdomains like outlook.com, hotmail.com, and msn.com require authentication using SPF, DKIM, and a DMARC policy of at least p=none*.

Watch this short video for more information.

*While this ensures compliance, it won't protect your business from cyberattacks.

Check your domain

Start your DMARC journey.
Contact us today.

Why it matters

Non-compliance = email rejection

Starting May 5,2025,if your emails don't meet the authentication requirements, Microsoft will reject them — even if they're legitimate.

Protect your domain from spoofing

SPF,DKIM,and DMARChelp prevent attackers from impersonating your business.

Gain visibility with DMARC reports

Monitor how yourdomain is being used (or abused) worldwide with insight-rich DMARC reports.

trinITy

In partnership with: SENDMARC

Compliance timeline

May 5, 2025
Microsoft begins rejecting unauthenticated emails from high-volume senders. All senders should act now to avoid disruption.

Ongoing
Microsoft will actively monitor compliance, reputation, and user complaints — enforcement is expected to intensify over time.

Microsoft's additional email hygiene recommendations to boost quality and trust

- Use valid 'From' addresses that can receive replies
- Provide easy unsubscribe links
- Keep email lists clean by removing invalid addresses
- Avoid misleading subject lines and headers
- Ensure recipients have opted in to receive your emails

> Outlook has stated that it "reserves the right to take negative action, including filtering or blocking, against non-compliant senders, especially for critical breaches of authentication or hygiene."

Let the Sendmarc platform handle it

NavigatingSPF, DKIM,andDMARC doesn't have to be complicated. The Sendmarc platform simplifies setup, improves security, and ensures compliance - fast.

Contact us to get started.

trinTy

In partnership with: SENDMARC