

Unspam Releases DMARC Monitoring That Shows When It Is Safe to Enforce

It names the services sending as a domain and checks when its policy can safely move to p=reject, for \$6 per domain per month with the first domain included.

NEW YORK, NY, UNITED STATES, September 24, 2026 /EINPresswire.com/ -- Unspam

“

A lot of teams publish DMARC at p=none and leave it there for years. We built DMARC Monitoring to say plainly when the evidence is good enough to turn enforcement on.”

Andrian Valeanu, founder of Unspam

(unspam.email), the email deliverability platform, has released [DMARC Monitoring](#) for customers on its Custom plan. The service collects the aggregate reports that Gmail, Outlook, Yahoo and other mailbox providers send about a domain, shows which services send mail as that domain, and tells the owner when the policy can move from monitoring only (p=none) to enforcement (p=quarantine or p=reject) without blocking legitimate mail.

Mailbox providers have spent two years turning DMARC from advice into a requirement. Google and Yahoo began enforcing sender rules that include DMARC in February

2024, Microsoft followed for high-volume senders to Outlook.com in May 2025, and Gmail stepped up enforcement in November 2025 with temporary and permanent rejections of non-compliant bulk mail. In May 2026 the IETF made DMARC a Proposed Standard for the first time, as RFC 9989.

Adoption still lags. In Unspam's [Email Deliverability Benchmark](#), which covers checks run through the platform in the 12 months to September 24, 2026, 49 percent of senders had not implemented DMARC. The benchmark reflects senders who test with Unspam, so it skews toward teams already diagnosing a deliverability problem.

"A lot of teams publish DMARC at p=none and leave it there for years," said Andrian Valeanu, founder of Unspam. "The reports arrive as zipped XML full of IP addresses, and nobody can tell the billing system from someone forging the domain. We built DMARC Monitoring to answer that, and to say plainly when the evidence is good enough to turn enforcement on."

DMARC Monitoring groups reporting IP addresses into named sending sources and labels each one as an email service provider, the domain's own infrastructure, a forwarder or suspected spoofing. Each source is marked compliant, partially failing, failing or unauthorized, and opening

it explains why its mail fails and how to fix it. For every domain, a policy readiness check says whether it can move to p=quarantine or p=reject and lists what stands in the way: too few days of data, compliance below the threshold, a failing source, or traffic nobody has reviewed.

Agencies and multi-brand teams can add up to 500 domains to one account and compare compliance, alignment and policy across all of them in a single list. A summary email arrives every Monday covering the past week across all domains.

Setup is one DNS record. If a domain already publishes DMARC, Unspam adds its reporting address to the existing record, leaving the policy and any other report recipients as they are. Verification runs automatically, and mailbox providers usually send the first reports 24 to 48 hours later.

Developers can run the service through a REST API with eight endpoints, from registering a domain to opening a single report. The same eight operations are tools on Unspam's MCP server, so a team can ask an AI assistant to add a domain or summarize who sent mail as it last week.

DMARC Monitoring costs \$6 per domain per month on the Custom plan, with the first domain included. For a one-off look at a single report, Unspam's free [DMARC report analyzer](#) remains available. Details are at unspam.email/dmarc-monitoring.

About Unspam

Unspam is an email deliverability platform for marketers, founders, agencies and product teams. Its spam tests score a message on authentication, content, blacklists and HTML before it is sent, and inbox placement tests show whether each copy reached the inbox, the Promotions tab or spam at Gmail, Outlook, Yahoo and other providers. Email previews render a message in more than 50 real clients and devices in light and dark mode, and AI eye-tracking heatmaps predict where readers look first. DMARC monitoring collects a domain's aggregate reports to show who sends mail on its behalf, and an AI assistant reads every result and explains what to fix. Tests can run on a schedule or through the REST API and MCP server. Unspam also offers free SPF, DKIM, DMARC, BIMI and blacklist checkers, and hands-on help from its deliverability consultants.

Andrian Valeanu

Andrian Valeanu

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

[TikTok](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/944912171>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.