Publication date:
31 Jul 2025
Author(s):
Rik Turner, Chief Analyst, Cybersecurity

On the Radar: EasyDMARC offers authentication, security, and deliverability for corporate email

Summary

Catalyst

EasyDMARC delivers a platform enabling organizations that own an email domain to deploy protection for it based on the Domain-based Message Authentication, Reporting, and Conformance (DMARC) authentication protocol.

Omdia view

Email was already established as a core part of businesses' internal and external communications long before the COVID-19 pandemic turbocharged digital transformation projects. The pandemic further increased organizations' reliance on digital channels to interact with employees, partners, and customers.

However, this reliance also creates fertile ground for cyberattacks, and it is no coincidence that phishing remains a central pillar of attack methodologies. The advent of generative artificial intelligence (GenAI) has actually increased the attraction of phishing for threat actors, making it so much easier to craft and iterate convincing emails to mount an attack.

DMARC is designed to address the challenge of spoofed domains, bolstering recipients' confidence that the emails they open and respond to are genuine. It also reduces organizations' exposure to third parties taking their name in vain for nefarious purposes. EasyDMARC's approach of offering an easy-to-use platform to enable DMARC bodes well for its progress in this still nascent market.

Why put EasyDMARC on your radar?

The vendor's name underscores its commitment to simplifying the deployment of a DMARC-compliant infrastructure for email security. EasyDMARC's automated management of DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and DMARC records reduces the complexity and time required for setup and ongoing maintenance. The EasySender service is an enhancement that complements the flagship EasyDMARC platform, and it should make the vendor attractive to an even wider swathe of potential customers.

Market context

Since the internet took off as a vehicle for business in the 1990s, email has been a cornerstone of business communications. Other messaging methods have certainly come along in the meantime, from the Short Message Service (SMS) on mobile phones to instant messaging (IM) platforms such as WhatsApp and its more business-friendly cousins such as Microsoft Teams. While these methods offer a more real-time experience, they have yet to dethrone email for internal and external business communications, particularly those that include attachments or links with additional information.

As a result of its success and resulting ubiquity in business life, email is also a primary vector for cyberattacks. Phishing, in which recipients are duped into clicking on malicious links or opening malware-laden attachments, is an almost permanent component in most attacks. A favorite way to craft a phishing email is to make it look like it comes from a legitimate sender. Since the late 1990s, the technical community has sought to address the security shortcomings of the Simple Mail Transfer Protocol (SMTP) that underpins most email communications.

SPF for sender verification

The first fruits of their labor came in the form of the SPF standard, a public version of which debuted in 2003. SPF verifies the sender of an email, thereby addressing a functional gap in SMTP that allows any computer to send emails pretending to be from another address.

SPF went through various iterations and improvements (including different names that its initials stood for). In 2014, the Internet Engineering Task Force (IETF) published it as a proposed standard, namely RFC 7208.

DKIM adds digital signatures

However, other issues with SMTP remained. For instance, since everything is in plain text, there was no real protection for the message itself, so anyone could hijack the information flow and change the communication (man-in-the-middle attack). Furthermore, with businesses increasingly sharing servers and services in the cloud, SPF might show a false positive if used alone.

For this reason, the next evolution in email security standards was DomainKeys Identified Mail (DKIM), which verifies email messages using a digital signature and an encryption key, ensuring email messages cannot be altered or faked. First published by the IETF as a proposed standard (RFC 4871) in 2007, DKIM brought together two projects, namely DomainKeys from Yahoo and Identified Internet Mail from Cisco. It is now an official IETF standard called RFC 6376.

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Enter DMARC

The logical next step was a standard combining the approaches of both SPF and DKIM, which is DMARC. This standard was first proposed in January 2012 and was the subject of the IETF's informational RFC 7489 in March 2015.

DMARC is designed to help domain owners prevent email spoofing and phishing attacks by verifying the sender's identity. It builds on both SPF and DKIM, unifying the two into a common framework that enables domain owners to advise how they want email from their domain to be handled if it fails authorization, including actions such as rejecting or quarantining the message. DMARC also enables reporting on email authentication activity.

Since the publication of RFC 7489, the story has been one of DMARC gradually gaining steam. A significant moment occurred in February 2024, when both Google and Yahoo made it mandatory for bulk senders (i.e., those who send more than 5,000 emails to Gmail or Yahoo addresses within a 24-hour period). Microsoft has since joined the fray, with a similar requirement for bulk senders from May 2025. Many countries have made DMARC implementation mandatory or recommended for government organizations, including the US, the UK, Norway, Australia, the Netherlands, Denmark, and (most recently) New Zealand.

DMARC adoption improves, but configuration lags

Despite all its promise and the nudges from Google and Yahoo, DMARC has not been universally adopted. The reasons for this are several and varied. One significant issue is the complexity of DMARC, particularly for organizations with many domains and third-party vendors. Meanwhile, smaller companies may simply lack the resources for implementation and monitoring. And many organizations are hesitant to enforce certain DMARC policies, such as quarantining or rejection, due to concerns about potentially blocking legitimate emails.

EasyDMARC's own analysis of 1.8 million domains, carried out earlier in 2025, reveals progress in DMARC adoption, with valid records increasing from 29.1% in 2023 to 47.7% now—an increase of over 18 percentage points. Yet, enforcement still lags, as most domains remain at a "p=none" policy, which is a monitoring policy that tells recipient email servers to take no action on emails that fail DMARC authentication.

Such a stance offers no real protection against spoofing, and the gap is largely driven by a critical yet underestimated challenge: email sender configuration. Many Domain Name System (DNS) providers and email platforms automatically publish basic DMARC records with p=none but fail to guide users through the complex task of identifying, verifying, and aligning all legitimate sending sources—such as CRM systems, marketing platforms, and transactional email systems. Without proper SPF and DKIM alignment across these sources, organizations hesitate to enforce stronger policies due to the risk of breaking legitimate email flows.

As Google, Yahoo, and Microsoft tighten authentication requirements and compliance standards expand globally, moving beyond default configurations is essential. DMARC is not "set and forget"; real protection demands ongoing monitoring, clear visibility into sender behavior, proactive misalignment detection, and a path to confidently enforce p=quarantine or p=reject.

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Product/service overview

As its name suggests, EasyDMARC was created to address some, if not all, of the obstacles to the wider adoption of the DMARC standard. The vendor delivers its eponymous technology platform in software as a service (SaaS) mode. This means that an organization signs up to use it, with the first step being for the platform to suggest the most appropriate storage of the customer's records.

These include the SPF, DKIM, and DMARC records, as well as ones generated in accordance with the Brand Indicators for Message Identification (BIMI) specification. BIMI allows organizations to display their brand logo in recipients' inboxes alongside their authenticated emails. When a company is using a managed service provider (MSP) to deliver DMARC, it delegates these records to the provider.

Signing up to the platform gives an organization access to the platform's tools for generating, analyzing, and maintaining its records, as well as managing the various email authentication protocols and monitoring domain health. EasyDMARC provides what it calls "smart" dashboards, as well as simplified reporting systems designed to enable customers of all sizes to keep their email authentication on track, reduce the time they spend on troubleshooting, and increase operational efficiency.

An addition to the customer's DNS

DMARC relies on an organization's DNS to publish policies that inform receiving mail servers on how to treat emails claiming to be from its domain. As such, a TXT record must be added to the DNS zone of the domain, which is a comparatively simple process entailing a one-line insertion.

EasyDMARC also suggests a one-click setup to simplify DNS record updates, since manual DNS management is often error-prone and technically challenging. This approach helps users avoid misconfigurations and syntax issues in the DNS zone, making the enforcement process more reliable and user-friendly. It is worth noting that while the initial setup is straightforward enough, identifying all sending sources and configuring them correctly requires time and diligence.

EasySender

While the EasyDMARC platform remains the vendor's flagship product, in October 2023, it launched a second offering, namely EasySender, which it describes as an email deliverability platform. EasySender provides email verification, ridding email lists of problematic addresses and decreasing the incidence of hard bounce. It also offers inbox placement, giving insight into whether emails will reach the inbox or spam folder. It consists of two components:

- **Email Verification,** which removes problematic addresses from an organization's email lists to minimize the hard bounce. To do this, it addresses several issues, including the following:
  - Misspelled addresses
  - Disposable addresses
  - Domains lacking mail exchange (MX) records
  - Inactive or full mailboxes
  - Unavailable servers

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

  - Non-existent domain names

This part of the service is activated in one of three ways: a customer can cut and paste their email list into EasyDMARC's system, upload a list, or connect to the vendor's API when a real-time verification is required.

- **Inbox Placement,** which gives insight into how its emails will be received (i.e., whether they will land in the inbox or spam folder). This service uses the seed list testing method. A customer sends an email to EasyDMARC's list of internal email addresses from the most popular mailbox providers (like Google, Outlook, etc.). The vendor then reviews the addresses and detects where the sent emails landed. The customer can then send a copy of their actual email to the seed list (around 50 email addresses on various email providers) and see the number that arrived in test recipients' inboxes. Doing so provides insight into how many messages landed in spam and how many were not delivered at all.

Company information

Background

EasyDMARC was founded in 2018 by Gerasim Hovhannisyan and Avag Arakelyan, both early employees of PicsArt—an Armenia-born tech unicorn. With over a decade of experience in high load distributed systems and cybersecurity, they built EasyDMARC to help organizations simplify and scale email authentication. EasyDMARC has raised a total of $22.3m in funding across three rounds. Its most recent funding round was a $20m Series A round in September 2024, led by Radian Capital.

Current position

EasyDMARC boasts a customer base that operates over 175,000 domains across 130 countries, including a global network of 2,000-plus MSPs, resellers, and technology integrators. The vendor offers an enterprise-grade solution for large organizations. It cites names such as consumer electronics giant Panasonic, UK forex trading platform FXPro, US automotive exchange Auto Lenders, and the enterprise arm of telecom equipment provider Alcatel-Lucent as paying customers.

The platform is a multi-tenant one, hence its success in cultivating the MSP channel. Given the importance of this route to market, EasyDMARC has also developed integrations with what it considers key technology vendors for MSPs, such as IT service management (ITSM) provider ConnectWise, business software marketplace Pax8, and professional services automation platform HaloPSA. EasyDMARC is also available on some of the leading marketplaces, such as those operated by Google and Microsoft.

The charging mechanism for EasyDMARC is an annual or three-year subscription, based on the number of domains protected by the platform as well as the volume of outbound emails the customer sends. For smaller companies, there is also a self-service package that can be acquired on a monthly subscription basis.

Future plans

Global expansion is a priority for the vendor, which will entail growing its regional expertise to support demand across the Asia & Oceania, European, and North American markets.

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

EasyDMARC has an active customer advocacy program, as evidenced on G2 and other review sites. This program helps the vendor ensure its products reflect the needs of the ever-evolving threat and business continuity landscape.

Given the growing importance of AI generally, as well as the fact that threat actors are leveraging it for malicious purposes, EasyDMARC is intensifying its use of AI to provide clarity on email senders, detect threat signals, and enhance reporting. It plans to use AI to detect phishing pattern URLs and uncover suspicious behavior.

The EasyDMARC Academy and Partner Program will continue to provide additional certifications and training to drive a greater understanding of DMARC and close the global skills gap.

Key facts

Table 1: Data sheet: EasyDMARC

Product/service name	EasyDMARC	**Product classification**	Email security
Version number	n/a	**Release date**	February 2018
Industries covered	Relevant for any company with an email domain, but particularly in finance, healthcare, education, retail, IT & services, network security, & public sector bodies	**Geographies covered**	North America, EMEA, and APAC
Relevant company sizes	All (enterprises to small and medium-sized businesses [SMBs], as well as service providers)	**Licensing options**	Subscription-based (monthly or annual) Multi-tenant licensing for MSPs Custom enterprise license for larger partners
URL	https://easydmarc.com https://academy.easydmarc.com/	**Routes to market**	Direct (via education and enablement programs, digital and event marketing); Channel (strategic partnerships and partner programs)
Company headquarters	Dover, Delaware, US	**Number of employees**	100+

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Source: Omdia

Analyst comment

EasyDMARC has faced two challenges in taking its technology to market. First is awareness of the DMARC standard, which is still surprisingly low in the enterprise market, despite the efforts of Google, Yahoo, and Microsoft to raise its profile. The vendor has engaged in considerable outbound activities to counter this issue, a notable example being its inclusion in a February 2025 *Forbes* article by cybersecurity journalist Davey Winder. This article addressed the rise in Gmail attack warnings and emphasized the importance of email authentication standards like DMARC. The vendor also conducts regular market and sector-specific surveys to highlight critical gaps and raise awareness among relevant institutions and stakeholders of DMARC and the security issues it addresses. EasyDMARC is actively present at global cybersecurity and MSP events, such as Black Hat and the RSA Conference.

Second is the complexity and cost of deploying a DMARC-compliant system. EasyDMARC has done a good job of addressing these issues by developing a platform, delivered in SaaS mode, and adopting a freemium model to promote the standard itself, bring users into its orbit, and enable the upsell opportunity. The fact that it now offers an email deliverability platform is clearly a positive development that should differentiate the vendor in the crowded email security space.

Omdia wonders what the barriers might be for some of the many players in email security to emulate EasyDMARC's approach to the DMARC issue. Although generally not as comprehensive as EasyDMARC's platform, several vendors have some form of DMARC offering in their portfolio. That said, EasyDMARC's focus on solving the two issues it faced in preaching the gospel of DMARC and enabling uptake might make it an attractive acquisition target for some of the larger competitors in this market.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Omdia Universe: Email Security, 2024 (December 2023)

"Proofpoint bolsters its AI expertise in email security with Tessian" (November 2023)

Content Security Gateway Appliances, Software, and SaaS 2Q23 (September 2023)

"Open Text puts outbound email security in the spotlight with its Zix buy" (December 2021)

Fundamentals of Inbound Email Security (August 2021)

"The value of outbound email security goes beyond highly regulated industries" (December 2020)

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Omdia Market Radar: Outbound Email Security (November 2020)

Fundamentals of Outbound Email Security (September 2020)

Davey Winder, "Critical Gmail Security Update—2.5 Billion Users Get Attack Protection," *Forbes* (February 5, 2025)

Gerasim Hovhannisyan, "Email Authentication Is A Must: Will DMARC Become Mandatory?" Forbes Technology Council

Author

Rik Turner, Chief Analyst, Cybersecurity

askananalyst@omdia.com

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com

© 2025 Omdia. All rights reserved. Unauthorized reproduction prohibited.