EASYDMARC

EasyDMARC 2025
DMARC Adoption Report

Table of Contents

Foreword

At EasyDMARC, our objective is clear: to help organizations secure their digital communications and build trust in every email sent. As enterprises move from awareness to action in email security, DMARC has become a foundational solution for protecting organizations against the growing threats of phishing, spoofing, and impersonation.

The EasyDMARC 2025 DMARC Adoption Report reveals both encouraging progress and significant gaps. Our research shows more organizations are starting their DMARC journey, driven by new requirements from major mailbox providers, government regulations, and industry standards like PCI DSS. But starting isn't the same as securing.

The real concern lies in the widening gap between DMARC adoption and effective enforcement. While valid records are on the rise, the majority remain stuck at the monitoring-only (p=none) state that offers zero protection. Even more concerning, misconfigurations and a lack of reporting persist, leaving organizations vulnerable and blind to attacks.

At EasyDMARC, we believe that every organization, regardless of size or technical expertise, deserves the tools, support, and knowledge to implement DMARC correctly and confidently. That's why we offer a platform that simplifies enforcement, provides free training through our EasyDMARC Academy, and works closely with partners around the world to raise the standard for email security.

I invite you to explore the findings in this report. Use the insights to evaluate your current posture, identify gaps, and take the next steps toward meaningful, measurable protection. Because in a world where email remains the number one attack vector, the stakes are simply too high to stop halfway.

Gerasim Hovhannisyan
CEO, EasyDMARC

> At EasyDMARC, our objective is clear: to help organizations secure their digital communications and build trust in every email sent.
>
> GERASIM HOVHANNISYAN, CEO

Most domains still lack proper DMARC enforcement and reporting.

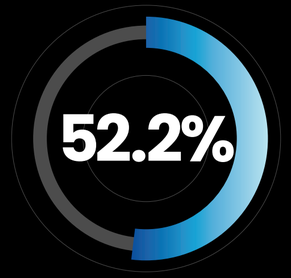
Executive Summary

Email continues to be the primary attack vector for cybercriminals, with phishing and spoofing attacks causing serious harm to organizations of all sizes. DMARC (Domain-based Message Authentication, Reporting, and Conformance) remains the industry's most effective defense against these threats, helping to prevent unauthorized use of domains.

EasyDMARC's 2025 research analyzed the **top 1.8 million domains globally**, ranked by visitor traffic, to assess the current state of DMARC adoption. While there's encouraging growth, especially following new requirements from major email providers and regulatory mandates, a significant gap remains between implementation and protection. Most domains still lack proper enforcement and reporting. Without moving beyond basic implementation, organizations remain vulnerable, not only to impersonation attacks but also to email deliverability issues. As mailbox providers increasingly enforce authentication standards, misconfigured or weak DMARC policies can disrupt outbound email flow, causing legitimate emails to be delayed, rejected, or flagged as suspicious.

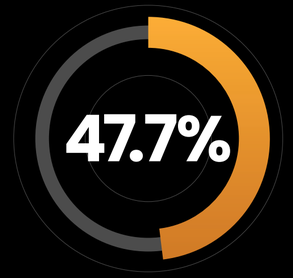
This report examines the current state of DMARC adoption, uncovers where domains are falling short, and provides actionable insights for organizations looking to strengthen their email security posture. Supported by targeted research across Fortune-ranked companies, high-risk geographies, and surveyed IT professionals, **the findings confirm a global trend: enforcement is lagging behind awareness.** To close this gap, DMARC must evolve from a passive compliance measure into an actively managed layer of defense.

Key Findings at a Glance



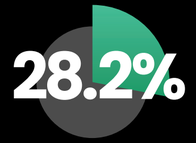
of the top 1.8 million domains have no DMARC record at all

(improved from 70.9% in 2023)



have a valid DMARC record, up from 29.1% in 2023

Of those with valid records:



use p=none (monitoring only), up from 16.1% in 2023

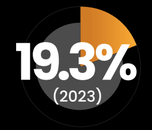
use p=quarantine (gradual enforcement), increased slightly from 6.6% in 2023

use p=reject (full enforcement), up from 6.4% in 2023

RUA reporting[1] is present on

28% of the top 1.8 million domains,

an increase of just under 10 percentage points when compared to 2023



Just

7.7% of domains

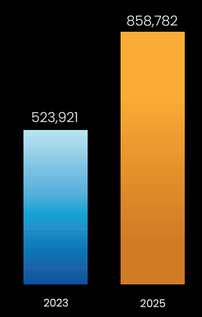
are correctly configured according to DMARC best practices (p=reject with RUA), a slight increase from 5.2% in 2023

1 RUA reporting provides domain owners with regular aggregate reports in XML format, summarizing how their emails are authenticated and processed by receiving mail servers. It offers visibility into potential spoofing or delivery issues.

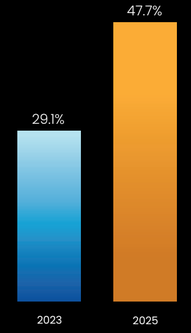
The State of DMARC Today

1. DMARC Adoption Is Rising- But Still Not Enough

There has been a measurable improvement in DMARC adoption since 2023:



Number of Domains With Valid DMARC Records



Percentage of Top 1.8M Domains with Valid DMARC Records

DMARC adoption among the top 1.8 million domains increased from 29.1% to 47.7% (an 18.6 percentage point increase), representing a substantial 63.9% growth in domains with valid DMARC records.[2] This indicates a mounting awareness of the need for email authentication. A major driver of this growth is the shift in sender policies by major email providers. Google and Yahoo began requiring DMARC implementation as of February 2024 to enhance email security and deliverability. This momentum is expected to continue with Microsoft's updated standards, which took effect on May 5th, 2025.

On the regulatory front, more governments are now encouraging or requiring DMARC as part of their cybersecurity frameworks. Industry-specific standards like PCI DSS v4.0.1 have also accelerated adoption, particularly in the payments sector, where stricter email security measures became compulsory in March 2025 to safeguard cardholder data. The broader compliance landscape is changing quickly, with growing emphasis on domain-based email authentication.

While increased adoption is encouraging, implementation doesn't equal protection. Without moving to enforcement, domains remain vulnerable to impersonation. Email-based phishing and spoofing are still among the most damaging and costly attack vectors globally. Additionally, failing to meet modern email authentication expectations can lead to reduced inbox placement and lower engagement due to poor sender reputation.

2 To assess changes in DMARC adoption and enforcement between 2023 and 2025, we used domain data sourced from the Tranco List, which aggregates rankings from multiple providers including CrUX, Majestic, Cisco Umbrella, and Radar. From the most recent Tranco dataset, we extracted the top 4 million domains and cross-referenced them with a historical dataset of 30 million domains queried in 2023.

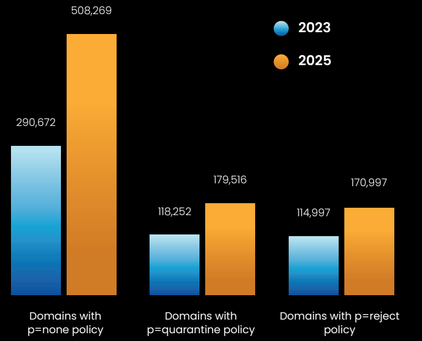
This comparison yielded a matched set of 1,804,632 domains present in both years, enabling a consistent, high-confidence analysis of DMARC status changes over time. We performed DNS lookups on this subset to retrieve current DMARC records and compare enforcement levels, reporting configurations, and policy trends. Additional queries were conducted to isolate key domain segments, including Fortune 500, Fortune 2000, Inc. 5000, and domains ending in .com and .org. These filtered datasets allowed for targeted analysis of high-profile organizations and common top-level domains within the broader study.

The State of DMARC Today

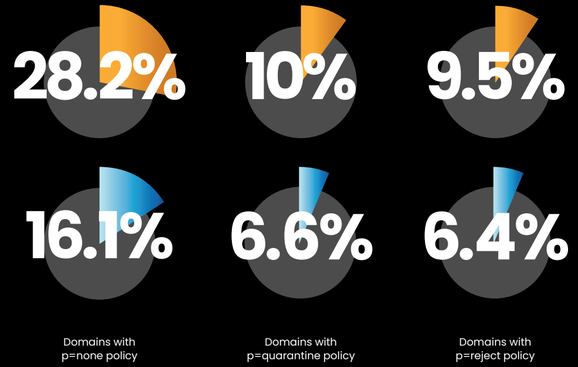
2. Enforcement Policies Are Slipping

Among domains with valid DMARC records, most are still in the early phases of adoption:

Domains with Valid DMARC Records



Percentage of Top 1.8M Domains with RUA Tags



From 2023 to 2025, there was a significant three-quarter increase (74.9%) in the number of domains using a p=none DMARC monitoring policy. However, the number of domains on enforcement policies (p=quarantine or p=reject) grew by only 50.3%, with a percentage point increase of just 6.5%.

Consequently, a DMARC policy of p=none remains the most common configuration, used by more domains than quarantine and reject combined. This suggests that many organizations rushed to adopt DMARC as a tickbox for compliance, rather than actual protection.

This gap highlights a trend: more companies are publishing DMARC records, but fewer are taking the next step to actually protect their domains. Over 80% of the top 1.8 million domains lack any form of DMARC protection, leaving them vulnerable to attacks and spoofing. While starting with a p=none DMARC policy is a good first step, staying there indefinitely offers no security.

› Back to Contents

The State of DMARC Today

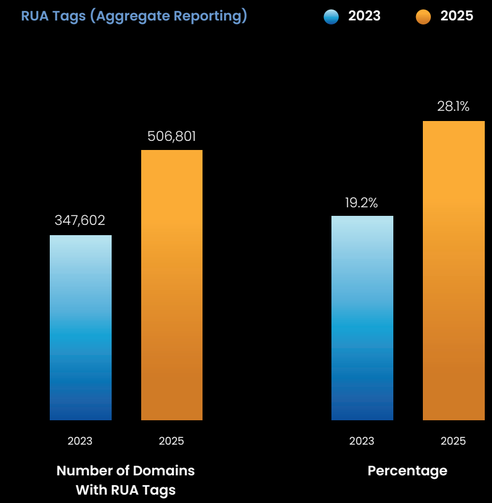
3. Reporting Remains a Blind Spot

DMARC reporting, specifically aggregate reports (RUA), provides crucial visibility into your email traffic and potential threats. RUA tags, embedded within your DMARC record, are the mechanism that instructs receiving mail servers to send these aggregate reports, detailing who is sending emails on your behalf, authentication failures, and the effectiveness of your DMARC configuration. Despite the essential insights these reports provide, they remain significantly underutilized.

Visibility through RUA reports also helps organizations troubleshoot outbound email issues, such as failed messages or unexpected sender sources.

Our data shows that only 28.1% of the top 1.8 million domains in 2025 are set up for aggregate reporting, meaning just under 40% of domains with a DMARC policy have no feedback loop. So, while RUA tag usage increased by 8.8 percentage points from 2023, effective monitoring and improvement remain hindered.

This reflects a critical gap in understanding: DMARC without reports is like flying blind. No matter your DMARC enforcement level, without aggregate reports, organizations lack visibility into authentication failures and their outbound email flow, making it challenging to identify and rectify issues promptly.



4. Misconfigurations Undermine Progress

Not all DMARC records are created equal. Even among those that appear to have a policy in place, many DMARC records have:

- Syntax errors
- Missing or misconfigured tags (especially RUA and RUF)
- Inconsistent alignment with SPF and DKIM
- Lack of monitoring despite being at enforcement

Misconfigurations erode trust and leave domains vulnerable to abuse, sometimes even causing false confidence in protection that doesn't exist. Organizations that move too fast without proper configuration or visibility put themselves at serious risk.

Organizations that move too fast without proper configuration or visibility put themselves at serious risk.

5. Comprehensive Protection is Very Rare

When we look at domains that meet the gold standard, p=reject with RUA reporting, we find:

- **137,812 domains** meet the criteria
- That's only **16% of valid DMARC records**
- And just **7.7%** of all top 1.8 million domains

This number has only slightly increased from 92,782 domains (5.2%) in 2023, highlighting that while adoption is improving, comprehensive protection is still the exception.

DMARC isn't just a technical best practice; it's a business-critical safeguard:

- Phishing and BEC attacks are still on the rise and increasingly sophisticated
- Reputation damage from spoofed emails can be lasting and severe
- Compliance obligations (PCI DSS v4.0.1, NIS2, Google, and Yahoo sender rules) are quickly shifting from recommendations to mandatory requirements

If your domain isn't protected, you're not just at risk; you are non-compliant.

The Adoption–Enforcement Gap

Despite growing awareness, regulatory mandates, and new email provider requirements pushing organizations to adopt DMARC, meaningful enforcement remains a rare achievement. EasyDMARC's 2025 research shows that while 47.7% of the top 1.8 million domains now have valid DMARC records, which is a notable improvement from 29.1% in 2023, only 7.7% are correctly configured according to DMARC best practices, by combining a p=reject policy with RUA reporting.

A key reason lies in how many organizations, and the email service providers that support them, approach DMARC implementation. In the rush to meet minimum compliance standards, most domains default to p=none, often without reporting mechanisms like RUA tags. This checkbox-style compliance creates the illusion of security without the actual enforcement or visibility needed to protect against spoofing and phishing attacks.

This trend defeats DMARC's core purpose: to block unauthorized use of a domain and enhance email deliverability. When DMARC is implemented without reporting, organizations are essentially "flying blind," unable to see who is sending email on their behalf or whether those emails are passing authentication checks. Worse still, enforcement without reporting creates operational blind spots, where legitimate emails might be blocked silently, damaging deliverability and trust.

Deliverability is a growing concern, with top email providers increasingly using DMARC status to determine inbox placement, especially since Google and Yahoo's 2024 requirements. Without a valid or properly enforced DMARC policy, even legitimate emails may be flagged or sent to spam folders, eroding communication with customers and partners.

EasyDMARC's 2025 research shows that 47.7% of the top 1.8 million domains now have valid DMARC records.

Additionally, duplicate records, syntax errors, and misconfigurations are all too common, even among domains that appear to have enforcement policies. These technical issues often go unnoticed without proper monitoring, weakening email defenses and leaving brands exposed to impersonation attacks.

Simply put, the majority of organizations are starting the DMARC journey, but too few are seeing it through. And even for those that reach the destination – full enforcement with aggregate reporting – the journey doesn't really end. Ongoing monitoring is essential to keep protections strong and ensure only legitimate emails get through. Without it, most of the world's most visible domains remain vulnerable to one of the oldest and most effective cyberattack methods.

Our Recommendations

- **Move beyond p=none –** DMARC adoption must go further than p=none. Organizations should progress to enforcement-level policies (p=quarantine or p=reject) after monitoring, testing, and record validation. Without enforcement, domains remain exposed to spoofing and phishing.
- **Make aggregate reporting the default –** RUA reporting is essential for visibility into domain abuse and email delivery health. Every DMARC record should include an RUA tag, enabling organizations to monitor authentication failures and fine-tune configurations continuously.
- **Fix misconfigurations before they create risk –** Syntax errors, missing tags, and SPF DKIM alignment issues are widespread and costly. DMARC should be configured carefully, reviewed regularly, and tested in stages to ensure both protection and deliverability.
- **Define DMARC as a lifecycle, not a launching point –** Publishing a DMARC record is the beginning, not the end. Ongoing monitoring, enforcement tuning, and reporting analysis must become standard practice to keep domains secure, compliant, and trusted.

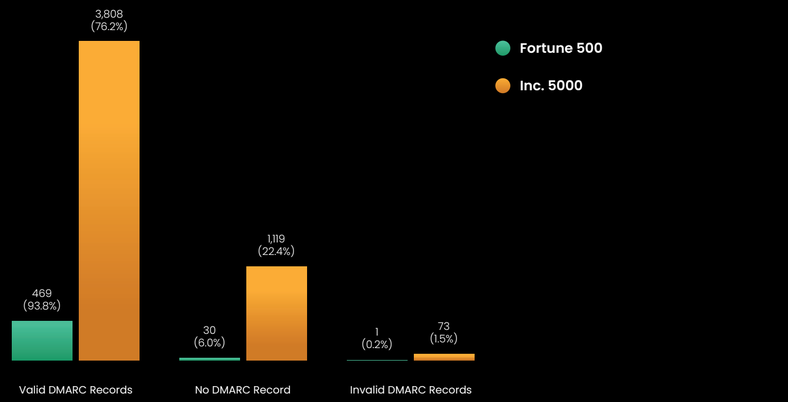
› Back to Contents

DMARC Adoption Across Fortune 500 and Inc. 5000

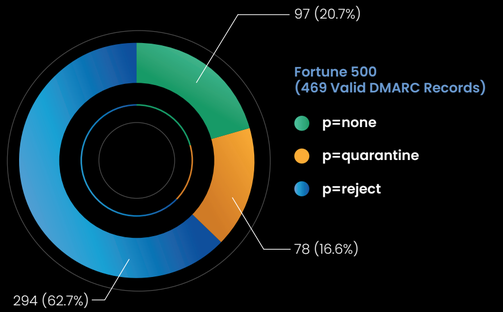
While our analysis of the DMARC policies of the top 1.8 million domains offers a comprehensive view of DMARC adoption across various industries, it is equally important to zoom in on how this varies among specific segments of the business landscape. To this end, we examined the DMARC policies of the Fortune 500 and Inc. 5000 companies and noted how organizational size and resources influence DMARC maturity.

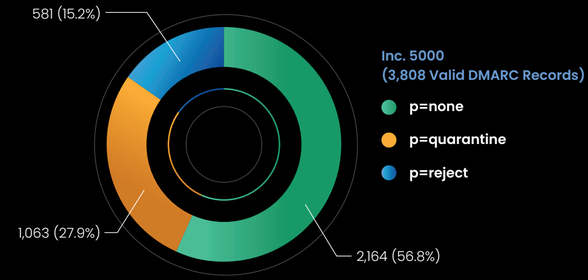
Out of the Fortune 500, 469 (93.8%) have valid DMARC records in place, with only 6% lacking any DMARC configuration. In contrast, the Inc. 5000 companies show a lower overall adoption rate, with 3,808 (76.2%) valid DMARC records and 22.4% with no DMARC at all.

DMARC Record Status of Fortune 500 and Inc. 5000 Companies



DMARC Policies of Fortune 500 and Inc. 5000 Companies





Examining policy enforcement reveals a stark contrast in security posture between the two groups. Among Fortune 500 companies with valid DMARC records, 62.7% enforce the strictest policy (p=reject), while only 15.2% of Inc. 5000 companies have reached this level. Conversely, a high proportion of Inc. 5000 companies remain on the permissive p=none policy (56.8%), indicative of passive monitoring without active protection.

When combined, enforcement policies (p=quarantine + p=reject) cover 79.3% of Fortune 500 companies with DMARC, equating to 74.4% of all Fortune 500 firms. For the Inc. 5000, enforcement policies are present in only 43.2% of companies with DMARC, representing 32.9% of the total Inc. 5000.

Monitoring through aggregate reporting (RUA) is nearly universal among Fortune 500 companies, with 97.9% including RUA tags in their DMARC records. By comparison, only 67.4% of Inc. 5000 companies with DMARC utilize RUA, suggesting less visibility and feedback on email flows. While the Inc. 5000 lag behind the Fortune 500 in both enforcement and reporting maturity, their overall DMARC adoption and protection levels still outperform those of the top 1.8 million domains, where only 47.7% have valid records and less than 20% are at enforcement.

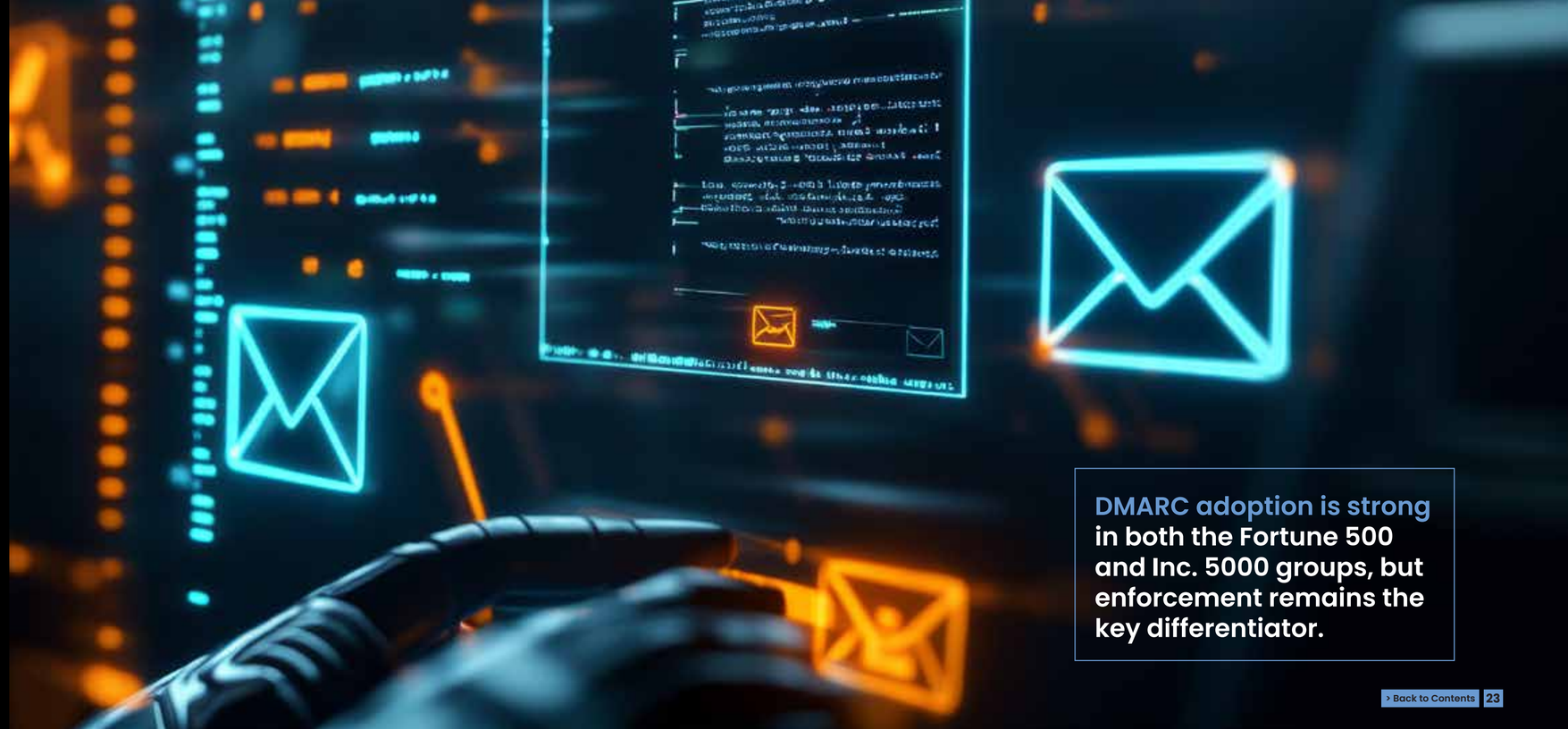
Adoption ≠ Enforcement

DMARC adoption is strong in both the Fortune 500 and Inc. 5000 groups, but enforcement remains the key differentiator. Nearly three-quarters of Fortune 500 companies enforce DMARC with quarantine or reject policies, while most Inc. 5000 companies rely on monitoring-only (p=none), leaving them vulnerable to phishing and spoofing attacks.

Although DMARC reporting (RUA) is widely used, especially among Fortune 500 firms, it does not always translate to protective enforcement, revealing a maturity gap, particularly in mid-market organizations. The large disparity in strict policy adoption between the two groups (p=reject: 62.7% vs. 15.2%) underscores the need for policy hardening within the Inc. 5000 to close this security divide.

Our Recommendations

- **Raise awareness –** Industry stakeholders must educate organizations on the risks associated with p=none policies and promote gradual policy escalation from p=none to p=quarantine to p=reject.
- **Promote enforcement –** Email service providers and industry bodies should advocate for default DMARC configurations favoring stronger enforcement to better protect email ecosystems.
- **Prioritize reporting –** Universal adoption of RUA tags is critical to maintain visibility into email authentication status and identify potential threats proactively.



DMARC adoption is strong in both the Fortune 500 and Inc. 5000 groups, but enforcement remains the key differentiator.

DMARC Enforcement at the National Level

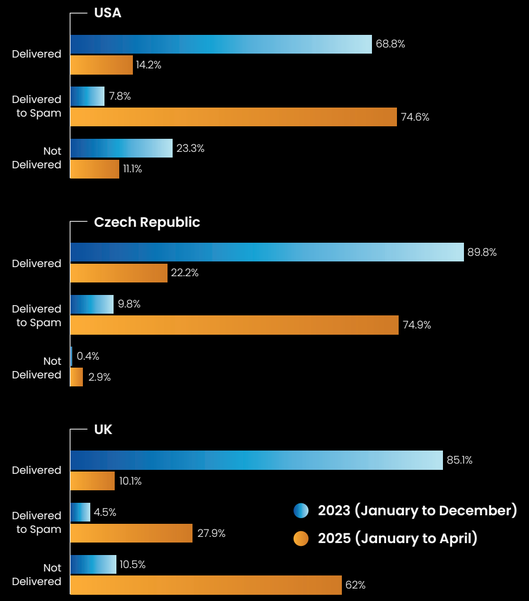
While organizational size influences DMARC posture, national policy is an equally powerful driver of email security outcomes. To examine this, we analyzed phishing data from 2023 and 2025 across seven countries with varying levels of DMARC enforcement. These countries were selected not only due to high phishing activity across our customer base but also to represent a range of enforcement maturity, from strict mandates to minimal or voluntary guidance.[3]

The findings reveal a consistent trend: where governments require enforcement-level DMARC (p=quarantine or p=reject), phishing emails are far more likely to be blocked or flagged as suspicious. In contrast, countries without strong policies saw little improvement, with many phishing attempts still landing directly in inboxes. The delivery status of these messages – accepted, sent to spam, or rejected – offers a clear snapshot of how national-level policy impacts real-world email threat exposure.

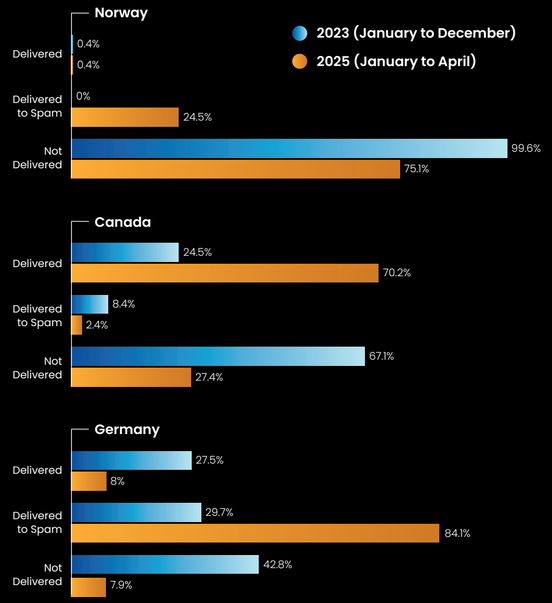
3 This section draws on proprietary aggregate DMARC data collected through EasyDMARC's platform, based on DMARC aggregate reports from global mailbox providers. The analysis covers metadata only – such as sender domains, policy dispositions, and reporting IPs – and does not include any email content. We analyzed over 278 million emails from 2023 and more than 115 million emails from January to April 2025 across seven countries. These countries were selected to reflect varying levels of DMARC policy enforcement, providing a comparative view of how national-level mandates influence real-world phishing exposure.

Delivery Status of Phishing Attack Emails

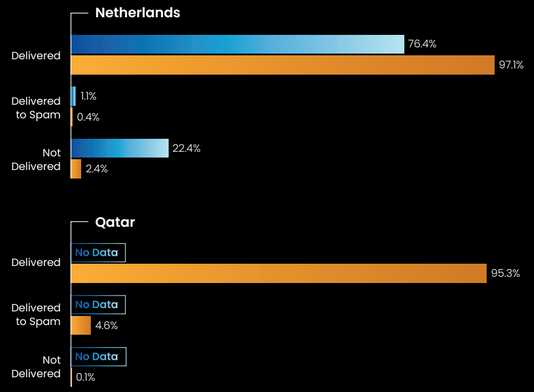
Countries with Strong Enforcement Mandates



Countries with Partial or Recommended Policies



Countries with Minimal Enforcement Activity



Our 2023 data reflects a full-year analysis, while our 2025 data covers January through April. Percentages represent the distribution of phishing email outcomes and are suitable for comparing relative DMARC policy effectiveness across countries.

Countries with Strong Enforcement Mandates

Countries with strict DMARC mandates – such as the United States, the Czech Republic, and the United Kingdom – demonstrated the most significant declines in phishing attacks that bypass authentication. In 2023, more than two-thirds of phishing messages originating from the US came from domains using a p=none policy. By 2025, that number dropped sharply to just 14.2%, with the majority of attempts filtered into quarantine or outright rejected.

Similar shifts were observed in the Czech Republic, where the p=none policies dropped from 89.8% to 22.2%, and the UK, which reduced its p=none footprint from 85.1% to 10.1%, while doubling its reject rate. These improvements closely align with government mandates requiring federal or public-sector domains to implement and enforce DMARC with policies of p=quarantine or p=reject.

Countries with Partial or Recommended Policies

In contrast, countries with only soft recommendations or phased mandates showed more mixed results. Norway entered the period with strong DMARC protections already in place – 99.6% of phishing messages in 2023 were rejected. By 2025, the country retained the same enforcement rate, although some traffic shifted into quarantine. Canada followed a moderate trajectory, holding steady at 70.2% at p=reject and 24.5% at p=none, reflecting progress tied to a phased public-sector DMARC rollout. Germany's pattern, however, was more unusual: while p=reject policy usage dropped from 42.6% to just 7.9%, p=quarantine usage surged to 84.1%. This likely indicates a preference for softer enforcement among German organizations, despite increasing awareness.

Countries with Minimal Enforcement Activity

Meanwhile, the Netherlands and Qatar illustrate the risks of minimal or unenforced DMARC policies. In both countries, nearly all phishing attacks landed directly in primary inboxes in 2023 and 2025. The Netherlands, despite a government "comply or explain" recommendation, saw its p=none rate rise from 76.5% to 97.1%. Qatar's figures show no meaningful adoption of DMARC protections.

The data is clear: countries with mandated DMARC enforcement consistently reduce exposure to phishing. Where guidance alone exists, progress is slower and often uneven. And where no policy exists, or existing guidance lacks accountability, attackers exploit the gap.

The data is clear: countries with mandated DMARC enforcement consistently reduce exposure to phishing.

Our Recommendations

- **Mandate enforcement-level DMARC policies –** Governments should require DMARC policies set to p=quarantine or p=reject. Legal mandates, supported by compliance mechanisms, are the most effective path to adoption.
- **Implement phased timelines –** New mandates should include structured rollouts with deadlines for transitioning from p=none to enforcement. This approach addresses deliverability concerns while maintaining forward progress.
- **Elevate guidance to regulation –** Countries like Germany and Norway should elevate DMARC from "recommended" to "required." Non-binding guidance results in uneven adoption and ongoing exposure.
- **Take action in lagging regions –** Lagging regions like the Netherlands and Qatar urgently need clear DMARC mandates. Despite guidance, adoption in the Netherlands has declined due to a lack of enforcement. Qatar remains almost entirely on p=none, with no national stance.
- **Lead by government example –** Mandating DMARC for public-sector domains, as seen in the US and Czech Republic, significantly reduces risk and drives private-sector alignment. Government action sets a powerful precedent.
- **Promote public-private collaboration –** Governments should support adoption with technical resources, awareness campaigns, and partnerships, especially in critical sectors like healthcare, education, and finance.

DMARC Awareness and Adoption Inside Organizations

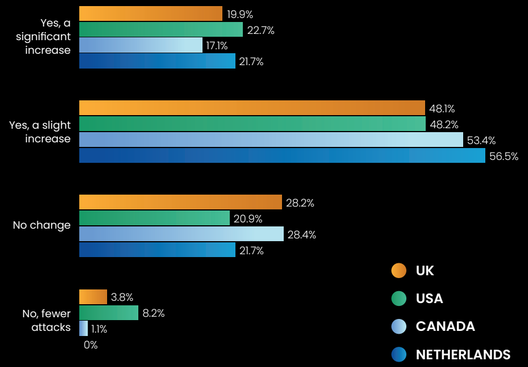
While national DMARC policies clearly shape the broader phishing landscape, individual organizational practices play a critical role in translating these mandates into effective email security. To deepen this understanding, EasyDMARC conducted a comprehensive survey of 980 IT professionals across four key countries – the UK, the US, Canada, and the Netherlands – focusing on corporate DMARC adoption, enforcement, and phishing attacks.[4]

The survey reveals a near-universal perception of rising phishing threats: across all regions, the majority of respondents report at least a slight increase in phishing and spoofing incidents over the past year. The US notably leads with 22.7% of organizations observing a significant rise, reflecting the intense threat environment faced by many enterprises.

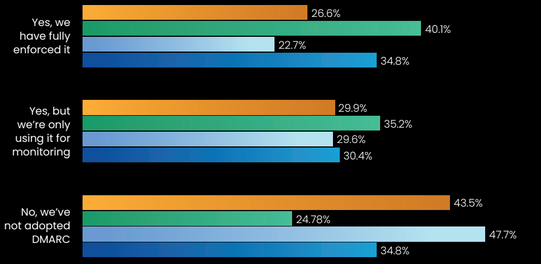
Despite widespread recognition of the threat, DMARC adoption varies considerably by country. US organizations show the strongest commitment to enforcement, with 40.1% fully enforcing DMARC policies and more than three-quarters adopting DMARC in some form. This seems to confirm the data from our EasyDMARC customer base in the US.

4 These findings were from an independent survey of 980 IT decision-makers across the UK, US, Canada, and the Netherlands in Q2 2025. Respondents came from a wide range of industries, and held roles across IT infrastructure, cybersecurity, operations, compliance, and senior leadership roles.

Has your organization experienced a rise in phishing or spoofing attacks in the last 12 months?

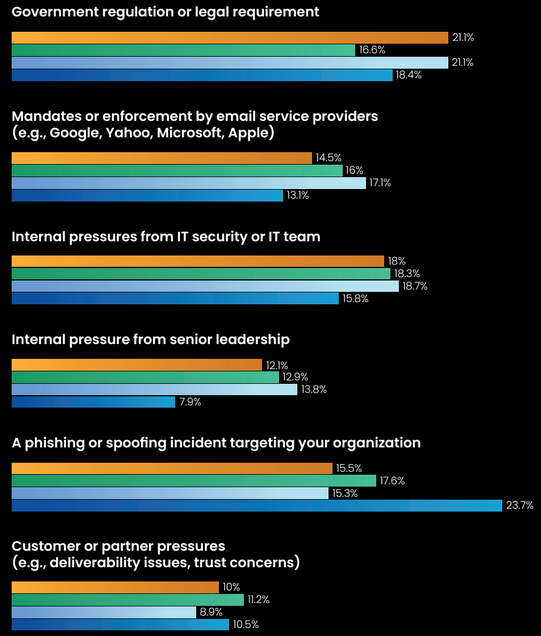


Has your organization adopted DMARC?



Government mandates emerge as a critical driver of enforcement motivation, particularly in the UK and Canada, where regulatory frameworks and legal requirements are top incentives. However, the data suggest that mandates alone are not enough without complementary internal pressures from IT security teams and reactionary measures following phishing incidents, factors that are more prominent in the US context. Mandates by major email service providers also exert influence, signaling the growing role these platforms play in enforcing stronger email security standards.

What would most motivate your organization to fully enforce DMARC (select all that apply)?

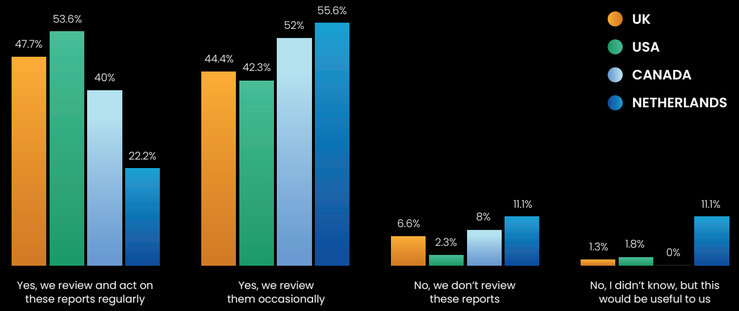


Awareness and active use of DMARC's reporting capabilities, which are essential for ongoing domain protection, are highest in the US, where over three-quarters of respondents understand and engage with aggregate reports. This contrasts with more moderate familiarity and usage levels in the UK and Canada, indicating further opportunities for education and process integration.

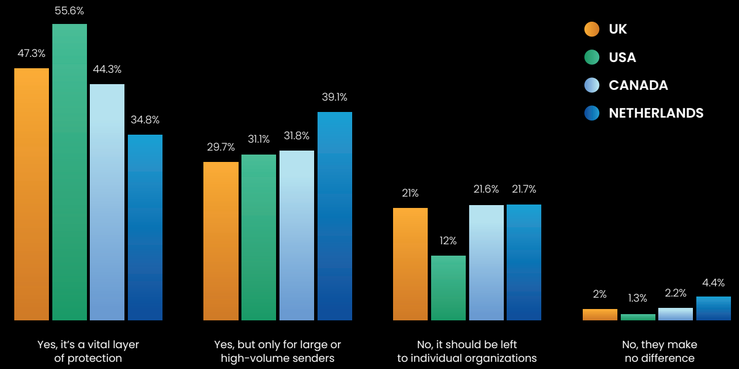
Are you aware DMARC provides aggregate reports on domain spoofing?

	UNITED KINGDOM	USA	CANADA	NETHERLANDS
Yes	55.9%	75.3%	54.4%	60%
No	27.4%	17.3%	32.6%	13.3%
Not sure	16.7%	7.5%	13%	26.7%

Do you review your aggregate reports?



Do you think major email providers like Google, Yahoo, Microsoft, and Apple should go further by requiring full DMARC enforcement (i.e. p=reject DMARC policy), rather than just DMARC adoption or implementation?



Finally, support for enhanced enforcement requirements by major providers is strong across all surveyed countries, with the US again leading in backing firm p=reject policies as a vital security layer. This consensus highlights a growing recognition that industry-wide standards and enforcement mechanisms are key to countering increasingly sophisticated phishing threats.

Our Recommendations

- **Strengthen internal ownership –** IT and security teams should take the lead in advancing DMARC from monitoring to enforcement. While external mandates help, internal prioritization is essential to closing the protection gap.
- **Promote reporting literacy –** IT departments must increase awareness of and actively use aggregate (RUA) reports. Monitoring authentication performance is vital for effective policy management and long-term success.
- **Align external and internal drivers –** Regulatory bodies, email providers, and organizational leadership must work together to create aligned, sustained pressure for enforcement. True protection requires more than publishing a record; it demands follow-through.

What the Data Tells Us

The EasyDMARC 2025 DMARC Adoption Report presents a multi-dimensional view of global DMARC deployment – from large-scale domain telemetry and organizational benchmarks to customer patterns and market perceptions. Together, these findings reveal a persistent gap between adoption and protection, highlighting the complex realities of email authentication in practice.

At the macro level, analysis of the top 1.8 million domains shows progress: DMARC adoption has increased from 29.1% in 2023 to 47.7% in 2025. Yet only 7.7% of domains meet DMARC best practices by combining full enforcement (p=reject) with aggregate reporting. P=none remains the most common policy, and misconfigurations, lack of reporting, and syntactic errors continue to undermine effectiveness.

This theme carries through in our more focused analyses. Our customer data from seven high-risk countries shows that national policy is a powerful influence. Countries with strict mandates – such as the US, Czech Republic, and the UK – saw significant reductions in phishing messages delivered from unauthenticated sources. In contrast, low-enforcement countries like the Netherlands and Qatar saw phishing exposure remain high or worsen. DMARC policy at the national level clearly shapes outcomes at scale.

DMARC adoption has increased from 29.1% in 2023 to 47.7% in 2025.

When comparing Fortune 500 and Inc. 5000 companies, the same pattern emerges. While DMARC adoption is relatively high across both groups, enforcement is the differentiator. Nearly three-quarters of Fortune 500 companies enforce DMARC with p=quarantine or p=reject, compared to just one-third of Inc. 5000 companies. Smaller organizations appear more likely to stop at monitoring, limiting the protocol's protective value.

Lastly, our survey of 980 professionals across the US, UK, Canada, and the Netherlands reveals that awareness of DMARC is rising, but understanding and operational execution remain uneven.

Many respondents expect phishing threats to increase, and most agree that major mailbox providers should go further in enforcing DMARC. However, a substantial number of organizations still lack reporting visibility, and enforcement rates lag behind intent, particularly in countries without clear mandates.

The survey also reveals that enforcement is not just a technical barrier; it's an organizational and ecosystem-wide challenge. Respondents widely acknowledged the importance of DMARC, but many cited internal blockers such as a lack of leadership support, competing priorities, and limited visibility into reporting data. This underscores that meaningful enforcement depends on more than just publishing a record; it requires sustained attention, resources, and cross-functional ownership.

To close the gap, stronger DMARC enforcement must be driven collectively. Email service providers must play a critical role in setting baseline expectations, governments must establish and enforce national standards, and internal IT and security teams must translate both into operational practice. Without alignment across these three fronts, even the best technical controls will remain inconsistently applied, and their protective potential will not be fully achieved.

One crucial point emerges – adoption alone doesn't equal security. Closing the adoption–enforcement gap is essential to safeguarding trust, deliverability, and resilience in the email ecosystem.

› Back to Contents

How to Get DMARC Right: A Phased Approach

Whether you're responding to new compliance demands or strengthening your overall security posture, effective DMARC implementation requires a structured, deliberate approach.

Start with Monitoring

Begin by publishing a p=none policy and enabling aggregate reporting (RUA). This allows you to build visibility into your email ecosystem without disrupting mail flow, providing the foundation for informed decisions.

Move to Enforcement

As your domain's email sources are authenticated and aligned, begin shifting to p=quarantine, followed by p=reject. Full protection requires consistent SPF, DKIM, and DMARC alignment, backed by a reject policy to stop unauthorized use.

Review Regularly

Threats change, email infrastructures evolve, and new services are added. Regularly reviewing your DMARC posture helps maintain strong protection, support deliverability, and meet growing compliance expectations.

Analyze and Adjust

Use a platform like EasyDMARC to interpret reporting data, identify legitimate sending sources, and resolve any configuration or alignment issues. This step ensures you're ready to move toward enforcement with confidence.

Maintain Visibility

Aggregate reporting remains essential even after enforcement. Keeping RUA in place ensures ongoing insight into authentication failures, new senders, and potential abuse. DMARC is not a one-time task; it needs oversight to remain effective.

What EasyDMARC Is Doing to Drive DMARC Adoption and Enforcement

At EasyDMARC, we believe DMARC should be more than a compliance checkbox; it should be a strategic pillar of your email security posture. That's why we've built a robust platform and support ecosystem to help organizations not only adopt DMARC, but reach and maintain enforcement with full visibility.

To help drive broader DMARC adoption and enforcement, EasyDMARC provides practical support for both individuals and organizations. Our EasyDMARC Academy offers free video-based courses designed to build foundational knowledge of DMARC, even for those without a technical background. With five million cybersecurity positions unfilled globally, we see education as a critical piece of the puzzle in closing the gap and improving global email security.

Conclusion: Progress Is Real – but Protection Still Falls Short

Our 2025 research shows real progress in DMARC adoption, but also reveals a widening gap between adoption and protection.

External pressure from tech providers and regulators is prompting organizations to begin their DMARC journey, yet far too many stop short of enforcement or overlook critical reporting elements. As a result, most domains are still at risk and remain vulnerable to email-based threats.

EasyDMARC's 2025 research reveals a critical gap: despite growing DMARC adoption, most domains are still vulnerable to email threats. This is because enforcement rates show insufficient progress, reporting is underused, and misconfigurations are common. Understanding these challenges and following best practices are essential to protect your brand, enhance security, and ensure compliance.

EasyDMARC's 2025 findings also highlight a deeper truth: stronger enforcement doesn't hinge on technology alone - it requires aligned action. National policy must set the tone, major email service providers must reinforce standards, and IT and security teams must prioritize operational follow-through. Without shared responsibility across this ecosystem, DMARC's full protective value will remain untapped. DMARC isn't just a checkbox for compliance; it's a tool that, when properly configured and monitored, protects your brand, your customers, and your email deliverability. EasyDMARC's findings highlight the importance of moving beyond the basics and building a strategy that closes the gap between adoption and actual security.

To stay ahead, organizations need to treat DMARC as an evolving process, and not a one-time setup. Progress comes from consistent monitoring, considered enforcement, and adapting as threats change. That's how organizations can turn DMARC from a technical protocol into a business asset, protecting brands, customers, and the trust that connects them.

To stay ahead, organizations need to treat DMARC as an evolving process, and not a one-time setup.

Join 175,000+ domains worldwide secured with us

web: easydmarc.com
academy.easydmarc.com

email: sales@easydmarc.com

+1-888-563-5277

+31-970-1028-0670

+44-204577-2894

+65-3125-1760

EASYDMARC