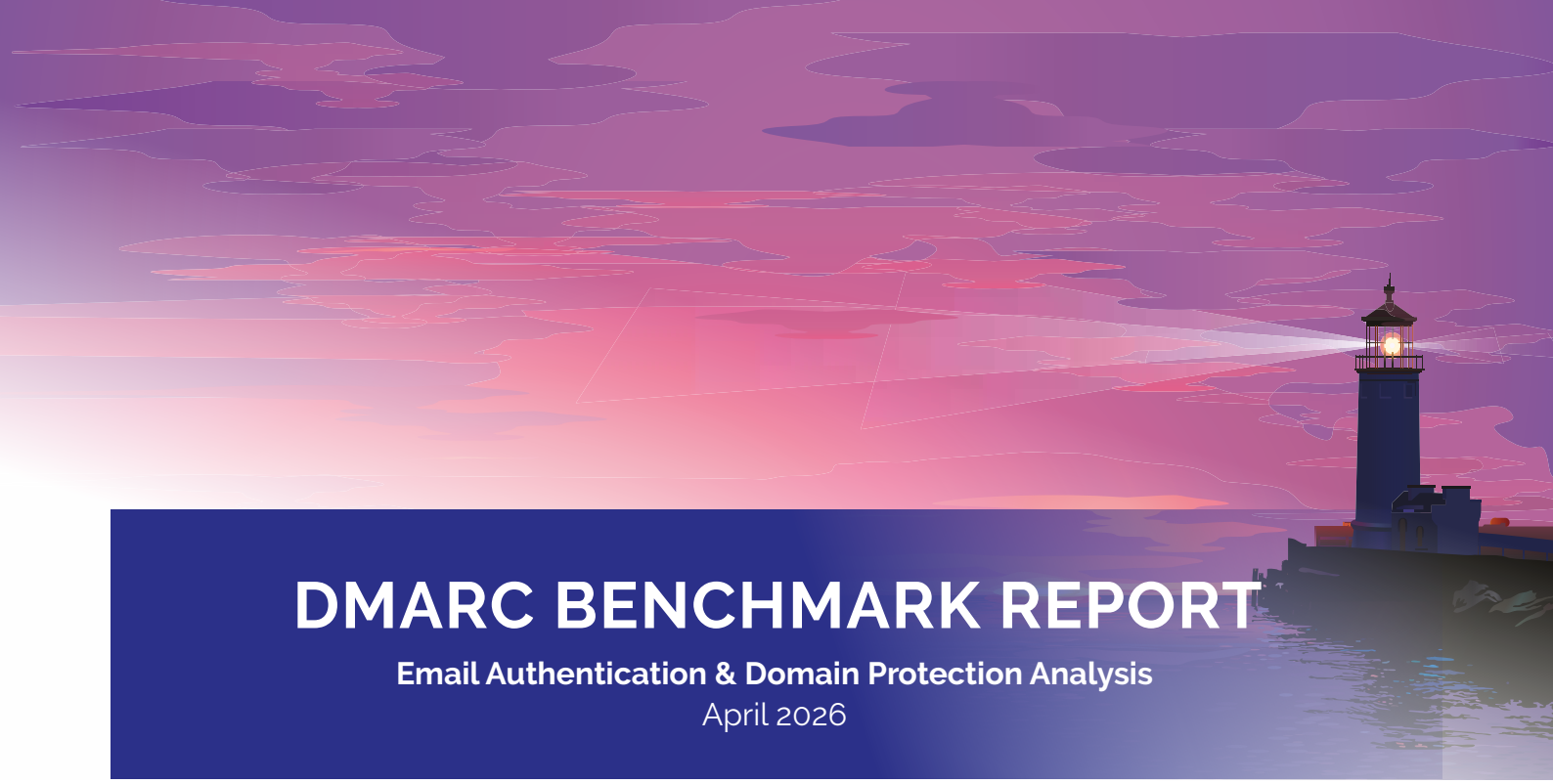


DMARC BENCHMARK REPORT

Email Authentication & Domain Protection Analysis

April 2026

10,833 Domains Analysed

Across 15+ Industries in the Netherlands, Germany, Belgium & France

Commissioned by:

GUARDIAN 360°

Schouwburgplein 30-34
3012 CL Rotterdam - The Netherlands

EXECUTIVE SUMMARY

This report presents the findings of a large-scale DMARC (Domain-based Message Authentication, Reporting & Conformance) assessment conducted across 10,833 unique domains associated with organisations in the Guardian360 ecosystem. The scan was performed by DMARC Advisor B.V. in April 2026.

The headline finding is alarming: **77.6% of all analysed domains are not fully protected against email spoofing.** This means that for the vast majority of organisations, cybercriminals can send emails that appear to originate from legitimate corporate addresses, enabling phishing, business email compromise (BEC), and brand impersonation at scale.

Only 22.4% of domains have implemented a **p=reject** policy, which is the only DMARC policy level that actively prevents spoofed emails from reaching recipients. The remaining domains are distributed across partial protection (p=quarantine, 22.1%), monitoring-only mode (p=none, 29.7%), and no DMARC configuration at all (25.8%).

The analysis covers organisations across 15+ industries and four primary markets: the Netherlands, Germany, Belgium, and France. Significant differences in DMARC adoption were found between sectors, with Finance and Information Security leading, while Transport and Retail lag considerably behind.

KEY FINDINGS AT A GLANCE

- **77.6%** of domains are not fully protected against email spoofing
- **55.5%** have either no DMARC record or a p=none policy (high to maximum risk)
- **2,797 domains** (25.8%) have no DMARC record at all, facing maximum security risk and email deliverability issues
- **30.5%** of domains with DMARC lack RUA reporting, flying blind without monitoring
- **Finance (35.7%)** and **Information Security (34.6%)** lead in p=reject adoption
- **Transport (15.3%)** and **Legal (16.7%)** have the lowest protection rates

UNDERSTANDING DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication protocol that protects organisations against email spoofing and phishing attacks. It builds on two existing mechanisms: SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).

A DMARC policy tells receiving email servers what to do when they encounter an email that fails authentication checks. There are three policy levels:

Policy	Security Risk	What Happens	Impact
p=reject	LOW	Spoofed emails are rejected (bounced)	Full protection. Attackers cannot send emails from your domain.
p=quarantine	MEDIUM	Spoofed emails go to spam/junk folder	Partial protection. Recipients may still find and trust spoofed emails in spam.
p=none	HIGH	Spoofed emails are delivered normally	No protection. Monitoring only. Attackers can freely spoof your domain.
No DMARC	MAXIMUM	No instructions for receiving servers	Zero protection and zero visibility. Also causes email deliverability problems with major providers.

Important: Since 2024, major email providers (Google, Microsoft, Yahoo) have tightened their requirements for email delivery. Organisations sending more than 5,000 emails per week without at least a basic DMARC record (p=none) risk having their legitimate emails rejected or filtered, directly impacting business communication and marketing effectiveness.

OVERALL RESULTS

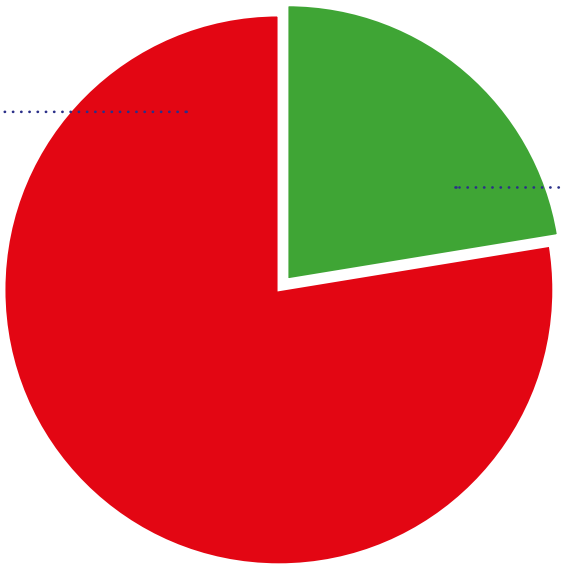
The DMARC scan assessed 10,833 unique domains. The following table shows the distribution across the four DMARC policy categories:

DMARC policy	Domains	Percentage	Security Risk	E-mail Risk
p=reject	2,432	22.4%	Low	Low
p=quarantine	2,391	22.1%	Medium	Low
p=none	3,213	29.7%	High	Medium
No DMARC record	2,797	25.8%	Maximum	High
TOTAL	10,833	100%		

77.6%

NOT FULLY PROTECTED

8,401 domains



22.4%

PROTECTED

2,432 domains

For the 8,401 domains without full protection, the consequences are tangible: cybercriminals can send emails that appear to come from these organisations' legitimate email addresses. For the 2,797 domains with no DMARC record at all, the risk is compounded by potential email deliverability issues, as major providers increasingly require DMARC compliance.

INDUSTRY ANALYSIS

DMARC adoption varies significantly across industries. The table below shows the DMARC policy distribution for each sector, sorted by the percentage of domains with p=reject (fully protected). The "High Risk" column represents the combined percentage of domains with either p=none or no DMARC record, which are the most vulnerable to email spoofing attacks.

Industry	n	p=reject	p=quar.	p=none	No DMARC	High Risk
Information Security	179	34.6%	36.3%	15.6%	13.4%	**29.1%**
Finance	381	35.7%	23.9%	28.6%	11.8%	**40.4%**
Government	401	32.4%	19.5%	6.5%	41.6%	**48.1%**
Housing	58	27.6%	41.4%	29.3%	1.7%	**31.0%**
Water Boards	8	37.5%	50.0%	12.5%	0.0%	**12.5%**
Health	369	27.4%	24.1%	27.9%	20.6%	**48.5%**
Education	215	27.0%	25.6%	31.6%	15.8%	**47.4%**
Software & SaaS	210	25.2%	32.4%	29.5%	12.9%	**42.4%**
MSP	3,212	25.0%	24.1%	25.8%	25.1%	**50.9%**
Consulting	294	25.5%	21.8%	32.7%	20.1%	**52.7%**
Construction	69	26.1%	24.6%	31.9%	17.4%	**49.3%**
Hosting	60	21.7%	28.3%	36.7%	13.3%	**50.0%**
Retail	133	23.3%	15.0%	40.6%	21.1%	**61.7%**
Transport	59	15.3%	20.3%	37.3%	27.1%	**64.4%**
Legal	24	16.7%	29.2%	33.3%	20.8%	**54.2%**

KEY INDUSTRY OBSERVATIONS

Leaders

Information Security and **Finance** lead DMARC adoption with the highest p=reject rates (34.6% and 35.7% respectively) and the lowest high-risk exposure. Information Security stands out with only 29.1% in the high-risk category. These sectors handle particularly sensitive data, which likely drives stronger email security awareness. However, even here, the majority of domains remain insufficiently protected.

Middle of the Pack

Government shows a polarised picture: a relatively high p=reject rate (32.4%) but also a very high "No DMARC" rate (41.6%). This suggests that while many government bodies have acted, a large group has not started at all.

MSPs (Managed Service Providers) show average adoption (25.0% reject) but represent the largest group by volume (3,212 domains). Given their role in managing IT for other organisations, their own DMARC posture has outsized significance.

Laggards

Transport (64.4% high risk) and **Retail (61.7% high risk)** are the most exposed sectors. These industries often interact with consumers via email (shipment notifications, receipts, promotions), making them prime targets for spoofing attacks. Legal (54.2% high risk) is also concerning given the sensitivity and trust inherent in legal communications.

GEOGRAPHIC ANALYSIS

The scan covered domains primarily from four countries: the Netherlands, Germany, Belgium, and France. Here is how DMARC adoption compares across regions:

Country	Domains	p=reject	p=quarantine	p=none	No DMARC
Netherlands	4,702	25.9%	24.8%	30.3%	18.9%
Germany	3,003	22.7%	20.0%	27.1%	30.2%
Belgium	411	22.6%	29.4%	34.3%	13.6%
France	75	38.7%	29.3%	13.3%	18.7%

The Netherlands leads in DMARC adoption among the Benelux and DACH markets (25.9% p=reject) and has the lowest rate of domains with no DMARC record (18.9%). This may reflect the Dutch government's active promotion of email security standards.

Germany has the highest rate of domains with no DMARC record (30.2%), suggesting broader awareness gaps despite a strong cybersecurity regulatory environment.

Belgium shows the highest quarantine adoption (29.4%), indicating many Belgian organisations have started implementing DMARC but have not yet moved to full enforcement.

France shows the strongest p=reject adoption in this benchmark (38.7%), though the sample size is smaller (75 domains). French organisations also have the lowest p=none rate (13.3%), suggesting that when French organisations implement DMARC, they tend to move more decisively to enforcement. This is notable in the context of France's strong regulatory focus on cybersecurity through ANSSI (Agence nationale de la sécurité des systèmes d'information) and the country's proactive stance on NIS2 transposition.

DMARC MONITORING & REPORTING

An often-overlooked aspect of DMARC implementation is the configuration of RUA (Reporting URI for Aggregate reports). RUA enables organisations to receive reports about email authentication results, providing visibility into who is sending email on their behalf and whether spoofing attempts are occurring.

Metric	Count	Percentage	Risk
DMARC with RUA (monitoring active)	5,588	69.5%	Managed
DMARC without RUA (no monitoring)	2,448	30.5%	Blind

RUA adoption by policy level:

- **p=reject:** 76.9% have RUA configured
- **p=quarantine:** 75.2% have RUA configured
- **p=none:** 59.7% have RUA configured

Of particular concern are the **561 domains with p=reject but no RUA and 592 domains with p=quarantine but no RUA.** These organisations have enforced DMARC policies but have no visibility into whether their own legitimate emails are being blocked due to misconfigurations. Without monitoring, they risk silently losing business-critical email communication.

BUSINESS IMPACT & RISK ASSESSMENT

Security Risks

For the 8,401 domains without p=reject enforcement, the following attack vectors remain viable:

- Email Spoofing: Attackers can send emails that appear to come from legitimate company addresses, targeting customers, employees, and partners.
- Business Email Compromise (BEC): CEO fraud, invoice manipulation, and payment redirection attacks all leverage spoofed sender addresses.
- Brand Impersonation: Phishing campaigns that abuse your domain damage customer trust and brand reputation.
- Supply Chain Attacks: Spoofing a trusted supplier's domain can be used to infiltrate partner networks.

Email Deliverability Risks

Since 2024, Google, Microsoft, and Yahoo require bulk senders (>5,000 emails/week) to have at minimum a DMARC record with p=none. For the 2,797 domains with no DMARC record, legitimate emails may be rejected or filtered by these providers, directly impacting business communication, marketing campaigns, and transactional emails (invoices, confirmations, notifications).

Why Periodic DMARC Review is Essential

DMARC implementation is not a one-time activity. Email infrastructure is dynamic: organisations regularly adopt new tools for marketing, CRM, customer support, billing, and internal communication. Each new tool that sends email on behalf of your domain must be properly authenticated via SPF and DKIM. Without periodic review, these changes introduce configuration drift that can undermine even a well-configured DMARC policy..

Common causes of DMARC configuration drift include:

- **New email-sending services:** Adding a marketing platform, HR recruiting tool, billing system, or helpdesk that sends email from your domain. Each requires SPF DKIM updates that are often overlooked.
- **Vendor-side SPF changes:** Third-party vendors may update their own SPF records or add new DNS includes. Because SPF evaluates all nested lookups (with a maximum of 10), vendor changes can silently push your domain over the lookup limit, causing authentication failures.
- **DKIM key rotation:** DKIM keys should be rotated periodically for security. If DNS records are not updated accordingly, DKIM validation will fail.
- **Infrastructure migrations:** Moving to a new email platform, cloud provider, or IT environment often introduces gaps in authentication configuration.
- **Evolving threat landscape:** Attackers continuously adapt their techniques. Monitoring DMARC reports helps detect new spoofing attempts targeting your domain, enabling a proactive security posture.

The risk of ***not*** reviewing DMARC periodically is twofold: legitimate business emails may be silently rejected (impacting revenue and customer communication), while at the same time new gaps in protection may emerge that attackers can exploit. Continuous monitoring through DMARC aggregate (RUA) reports is the most effective way to catch these issues before they have business impact.

Compliance & Regulatory Frameworks

Email authentication and DMARC are increasingly referenced in major regulatory frameworks and security standards. Organisations that neglect DMARC not only face direct security and deliverability risks, but may also find themselves falling short of regulatory expectations:

NIS2 Directive (EU)

The EU's **NIS2 Directive** (Network and Information Security Directive 2) significantly expands the scope of cybersecurity requirements for organisations across Europe. NIS2 emphasises supply chain security, cyber hygiene, and risk management practices. The absence of a DMARC policy with enforcement (p=reject) could weaken compliance with multiple NIS2 requirements, as email spoofing remains one of the most common initial attack vectors in supply chain compromises. Most "essential" entities face a compliance audit deadline of **June 30, 2026**. Implementing and maintaining DMARC with monitoring is a concrete, auditable measure that demonstrates proactive risk management.

ISO 27001

ISO 27001 is the international standard for information security management systems (ISMS). While ISO 27001 does not prescribe specific technologies, its risk-based approach requires organisations to identify and mitigate information security risks. Email spoofing and phishing represent significant risks that DMARC directly addresses. Annex A controls related to communications security (A.13), system acquisition and development (A.14), and supplier relationships (A.15) all have relevance to email authentication. Organisations pursuing or maintaining ISO 27001 certification should include DMARC enforcement in their control set as a demonstrable measure against email-based threats.

NEN 7510 (Healthcare, Netherlands)

NEN 7510 is the Dutch standard for information security in healthcare, closely related to ISO 27001 but specifically tailored to the healthcare sector. Dutch legislation requires healthcare providers to comply with NEN 7510 when using healthcare information systems and electronic exchange systems. Given that healthcare organisations frequently communicate sensitive patient data and appointment information via email, DMARC enforcement is a critical technical measure to prevent spoofing of healthcare domains. With 48.5% of health sector domains in the high-risk category in our benchmark, there is substantial room for improvement. Proper DMARC implementation supports NEN 7510 compliance by safeguarding the integrity and authenticity of email communications.

Across all these frameworks, the common thread is clear: email authentication through DMARC is no longer optional but increasingly expected as a baseline security measure. Organisations should treat DMARC enforcement not as a standalone project but as part of their ongoing information security management, with periodic reviews built into their compliance cycles.

RECOMMENDATIONS

Based on the findings in this report, we recommend organisations take the following actions depending on their current DMARC status:

For Domains with No DMARC Record (2,797 domains)

1. **Implement a DMARC record immediately**, starting with p=none to begin collecting authentication data without impacting email flow.
2. **Include an RUA address** to receive aggregate DMARC reports and gain visibility into email authentication results.
3. **Verify SPF and DKIM configurations** to ensure all legitimate email sources are properly authenticated.

For Domains with p=none (3,213 domains)

1. **Analyse DMARC aggregate reports** to identify all legitimate email sources and address any authentication failures.
2. **Plan a migration path to p=quarantine and then p=reject.** Staying on p=none indefinitely provides no protection.
3. Consider engaging a DMARC management specialist to accelerate the transition to enforcement.

For Domains with p=quarantine (2,391 domains)

1. **Move to p=reject** once DMARC reports confirm all legitimate email sources pass authentication consistently.
2. Ensure RUA reporting is active (currently 24.8% of quarantine domains lack monitoring).

For Domains with p=reject (2,432 domains)

1. **Maintain active DMARC monitoring.** 23.1% of reject domains lack RUA reporting.
2. Regularly review DMARC reports to catch misconfigurations early, especially when adding new email-sending services or migrating infrastructure.

For All Organisations

- **Schedule periodic DMARC reviews** (at minimum quarterly) to detect configuration drift, new unauthorised senders, and changes in the threat landscape.
- **Integrate DMARC into your compliance programme** as a demonstrable control for NIS2, ISO 27001, and sector-specific standards such as NEN 7510.
- **Ensure supply chain awareness:** evaluate the DMARC posture of your key partners and suppliers as part of your third-party risk management process.

METHODOLOGY

This benchmark study was conducted using the following approach:

1. **Domain collection:** A deduplicated list of 10,833 unique domains was compiled from the Guardian360 platform, representing organisations across the Guardian360 partner and customer ecosystem.
2. **DMARC Scanning:** Each domain was scanned by DMARC Advisor B.V. to retrieve its current DMARC DNS record, extracting the policy (p= value), reporting addresses (RUA/RUF), and related configurations.
3. **Industry Classification:** Domains were matched to organisation records (85.7% match rate) to enable breakdown by industry, organisation type, and geography.
4. **Analysis Period:** The scan was conducted in April 2026. DMARC records are dynamic and can change at any time; this report reflects the state at the time of scanning.

OVER ONS

Guardian360

Guardian360 is a cybersecurity company based in Rotterdam, the Netherlands. Guardian360 provides continuous security monitoring, vulnerability assessment, and compliance services to organisations across Europe, both directly and through a network of Managed Service Provider (MSP) partners.

DMARC Advisor

DMARC Advisor B.V., based in Dordrecht, the Netherlands, specialises in email authentication and DMARC management. Their platform helps organisations implement and maintain DMARC, SPF, and DKIM to protect domains against email spoofing and improve email deliverability.

Need Help Improving Your DMARC Posture?

Guardian360 can help you assess your current email authentication status, implement DMARC with enforcement, and set up continuous monitoring to protect your domain against spoofing and ensure email deliverability.

Contact us:
support@guardian360.eu

GUARDIAN 360°
www.guardian360.eu

Disclaimer: This report is based on publicly available DNS records and data from the Guardian360 platform. DMARC records are dynamic and may have changed since the time of scanning. The industry classifications are based on CRM data and may not perfectly reflect each organisation's primary sector. This report is provided for informational purposes and does not constitute legal or compliance advice.