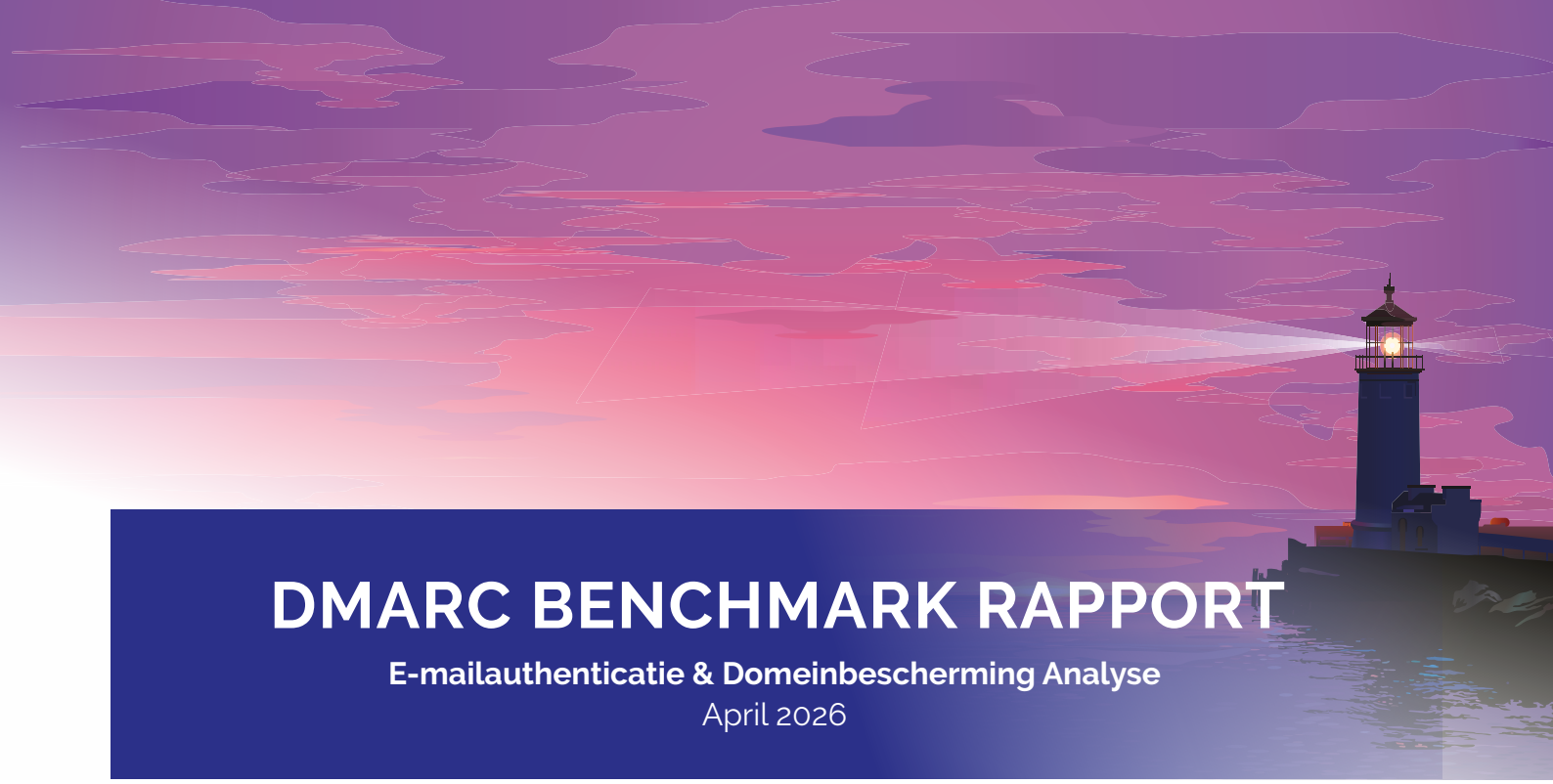


DMARC BENCHMARK RAPPORT

E-mailauthenticatie & Domeinbescherming Analyse

April 2026

10.833 domeinen geanalyseerd

In meer dan 15 branches in Nederland, Duitsland, België en Frankrijk

In opdracht van:

GUARDIAN 360°

Schouwburgplein 30-34
3012 CL Rotterdam - Nederland

SAMENVATTING

Dit rapport presenteert de bevindingen van een grootschalig DMARC (Domain-based Message Authentication, Reporting & Conformance) onderzoek dat is uitgevoerd op 10.833 unieke domeinen die zijn gekoppeld aan organisaties in het Guardian360 ecosysteem. Het onderzoek is uitgevoerd door DMARC Advisor B.V. in april 2026.

De voornaamste bevinding is alarmerend: **77,6% van alle geanalyseerde domeinen zijn niet volledig beschermd tegen e-mailspoofing.** Dit betekent dat cybercriminelen voor het overgrote deel van de organisaties e-mails kunnen verzenden die lijken afkomstig te zijn van legitieme bedrijfsadressen, waardoor phishing, business email compromise (BEC) en merkplundering op grote schaal mogelijk zijn.

Slechts 22,4% van de domeinen heeft een **p=reject** beleid geïmplementeerd, wat het enige DMARC beleidsniveau is dat actief voorkómt dat vervalste e-mails ontvangers bereiken. De resterende domeinen zijn verdeeld over gedeeltelijke bescherming (p=quarantine, 22,1%), alleen-monitoring mode (p=none, 29,7%) en helemaal geen DMARC configuratie (25,8%).

De analyse omvat organisaties in meer dan 15 branches en vier primaire markten: Nederland, Duitsland, België en Frankrijk. Er zijn aanzienlijke verschillen in DMARC adoptie tussen sectoren gevonden, waarbij Financiën en Informatiebeveiliging leiden en Transport en Detailhandel aanzienlijk achterlopen.

BELANGRIJKSTE BEVINDINGEN IN ÉÉN OOGOPSLAG

- **77,6%** van de domeinen is niet volledig beschermd tegen e-mailspoofing.
- **55,5%** hebben ofwel geen DMARC record ofwel een p=none beleid (hoog tot maximaal risico).
- **2.797 domeinen** (25,8%) hebben helemaal geen DMARC record, wat maximaal beveiligingsrisico en e-mailbezorgingsproblemen meebrengt.
- **30,5%** van de domeinen met DMARC mist RUA rapportage, zonder inzicht in wat er gebeurt.
- **Financiën (35,7%)** en **Informatiebeveiliging (34,6%)** leiden in p=reject adoptie.
- **Transport (15,3%)** en **Juridisch (16,7%)** hebben de laagste beveiligingsgraad.

DMARC BEGRIJPEN

DMARC (Domain-based Message Authentication, Reporting & Conformance) is een e-mailauthenticatieprotocol dat organisaties beschermt tegen e-mailspoofing en phishing-aanvallen. Het bouwt voort op twee bestaande mechanismen: SPF (Sender Policy Framework) en DKIM (DomainKeys Identified Mail).

Een DMARC beleid geeft ontvangende mailservers instructies wat te doen wanneer zij een e-mail tegenkomen die niet aan authenticatiechecks voldoet. Er zijn drie beleidsniveaus:

Beleid	Beveiligingsrisico	Wat gebeurt er	Gevolg
p=reject	LAAG	Vervalste e-mails worden geweigerd (teruggestuurd)	Volledige bescherming. Aanvallers kunnen geen e-mails van uw domein verzenden.
p=quarantine	GEMIDDELD	Vervalste e-mails gaan naar spam/junk folder	Gedeeltelijke bescherming. Ontvangers kunnen vervalste e-mails in spam nog steeds vinden en vertrouwen.
p=none	HOOG	Vervalste e-mails worden normaal bezorgd	Geen bescherming. Alleen monitoring. Aanvallers kunnen uw domein vrijelijk vervalsen.
Geen DMARC	MAXIMAAL	Geen instructies voor ontvangende servers	Nul bescherming en nul zichtbaarheid. Ook veroorzaakt e-mailbezorgingspro-blemen bij grote providers.

Belangrijk: Sinds 2024 hebben grote e-mailproviders (Google, Microsoft, Yahoo) hun vereisten voor e-mailbezorging aangescherpt. Organisaties die meer dan 5.000 e-mails per week verzenden zonder tenminste een basis DMARC record (p=none) lopen het risico dat hun legitieme e-mails worden geweigerd of gefilterd, wat direct gevolgen heeft voor bedrijfscommunicatie en marketing-effectiviteit.

ALGEHELE RESULTATEN

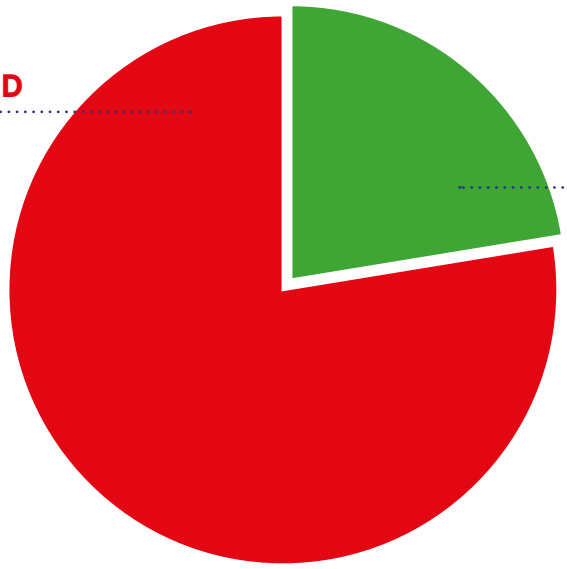
Het DMARC onderzoek evalueerde 10.833 unieke domeinen. De volgende tabel toont de verdeling over de vier DMARC beleidscategorieën:

DMARC beleid	Domeinen	Percentage	Beveiligingsrisico	E-mailrisico
p=reject	2.432	22,4%	Laag	Laag
p=quarantine	2.391	22,1%	Gemiddeld	Laag
p=none	3.213	29,7%	Hoog	Gemiddeld
Geen DMARC record	2.797	25,8%	Maximaal	Hoog
TOTAAL	10.833	100%		

77,6%

NIET VOLLEDIG BESCHERMD

8.401 domeinen



22,4%

BESCHERMD

2.432 domeinen

Voor de 8.401 domeinen zonder volledige bescherming zijn de gevolgen tastbaar: cybercriminelen kunnen e-mails verzenden die lijken afkomstig te zijn van de legitieme e-mailadressen van deze organisaties. Voor de 2.797 domeinen zonder DMARC record helemaal is het risico nog groter vanwege mogelijke e-mailbezorgingsproblemen, omdat grote providers steeds vaker DMARC conformiteit vereisen.

BRANCHE-ANALYSE

DMARC adoptie varieert aanzienlijk tussen branches. De tabel hieronder toont de DMARC beleidsverdeling per sector, gesorteerd op percentage domeinen met p=reject (volledig beschermd). De "Hoog risico" kolom geeft het gecombineerde percentage domeinen met p=none of geen DMARC record aan, wat het meest kwetsbaar is voor e-mailspoofing aanvallen.

Branche	n	p=reject	p=quar.	p=none	Geen DMARC	Hoog risico
Informatiebeveiliging	179	34,6%	36,3%	15,6%	13,4%	**29,1%**
Financiën	381	35,7%	23,9%	28,6%	11,8%	**40,4%**
Overheid	401	32,4%	19,5%	6,5%	41,6%	**48,1%**
Woningbouw	58	27,6%	41,4%	29,3%	1,7%	**31,0%**
Waterschappen	8	37,5%	50,0%	12,5%	0,0%	**12,5%**
Gezondheidszorg	369	27,4%	24,1%	27,9%	20,6%	**48,5%**
Onderwijs	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%**
Advies	294	25,5%	21,8%	32,7%	20,1%	**52,7%**
Bouw	69	26,1%	24,6%	31,9%	17,4%	**49,3%**
Hosting	60	21,7%	28,3%	36,7%	13,3%	**50,0%**
Detailhandel	133	23,3%	15,0%	40,6%	21,1%	**61,7%**
Transport	59	15,3%	20,3%	37,3%	27,1%	**64,4%**
Juridisch	24	16,7%	29,2%	33,3%	20,8%	**54,2%**

BELANGRIJKSTE BRANCHE-OBSERVATIES

Koppelingen

Informatiebeveiliging en Financiën leiden DMARC adoptie met de hoogste p=reject percentages (34,6% en 35,7%) en de laagste blootstelling voor hoog risico. Informatiebeveiliging springt eruit met slechts 29,1% in de hoogrisicocategorie. Deze sectoren verwerken bijzonder gevoelige gegevens, wat waarschijnlijk sterker bewustzijn over e-mailbeveiliging stimuleert. Maar ook hier blijft de meerderheid van de domeinen onvoldoende beschermd.

Midden van het veld

Overheid toont een gepolariseerd beeld: een relatief hoog p=reject percentage (32,4%) maar ook een zeer hoog "Geen DMARC" percentage (41,6%). Dit suggereert dat veel overheidsorganisaties actie hebben ondernomen, maar een grote groep nog niet is begonnen. **MSP's (Managed Service Providers)** tonen gemiddelde adoptie (25,0% reject) maar vertegenwoordigen de grootste groep op volume (3.212 domeinen). Gezien hun rol in IT-beheer voor andere organisaties is hun eigen DMARC positie van extra groot belang.

Achterblijvers

Transport (64,4% hoog risico) en **Detailhandel (61,7% hoog risico)** zijn de meest blootgestelde sectoren. Deze branches communiceren vaak met consumenten via e-mail (verzendberichten, bonnen, promotiemails), waardoor zij prime targets voor spoofing aanvallen zijn. Juridisch (54,2% hoog risico) is ook zorgwekkend gezien de gevoeligheid en vertrouwen inherent aan juridische communicatie.

GEOGRAFISCHE ANALYSE

Het onderzoek dekte domeinen af van voornamelijk vier landen: Nederland, Duitsland, België en Frankrijk. Dit toont hoe DMARC adoptie tussen regio's verschilt:

Land	Domeinen	p=reject	p=quarantine	p=none	Geen DMARC
Nederland	4.702	25,9%	24,8%	30,3%	18,9%
Duitsland	3.003	22,7%	20,0%	27,1%	30,2%
België	411	22,6%	29,4%	34,3%	13,6%
Frankrijk	75	38,7%	29,3%	13,3%	18,7%

Nederland leidt in DMARC adoptie onder Benelux en DACH markten (25,9% p=reject) en heeft het laagste percentage domeinen zonder DMARC record (18,9%). Dit kan het gevolg zijn van de actieve promotie van e-mailbeveiligingsnormen door de Nederlandse overheid.

Duitsland heeft het hoogste percentage domeinen zonder DMARC record (30,2%), wat wijst op bredere bewustijnsgaten ondanks een sterke cyberbeveiliging regelgeving. België toont de hoogste quarantine adoptie (29,4%), wat aangeeft dat veel Belgische organisaties met DMARC zijn begonnen maar nog niet naar volledige handhaving zijn overgegaan.

Frankrijk toont de sterkste p=reject adoptie in deze benchmark (38,7%), hoewel de steekproef kleiner is (75 domeinen). Franse organisaties hebben ook het laagste p=none percentage (13,3%), wat suggereert dat wanneer Franse organisaties DMARC implementeren, zij sneller naar handhaving gaan. Dit is opmerkelijk gezien Frankriks sterke regelgevingsfocus op cyberbeveiliging via ANSSI (Agence nationale de la sécurité des systèmes d'information) en het proactieve standpunt van het land op NIS2 transpositie.

DMARC MONITORING EN RAPPORTAGE

Een vaak over het hoofd gezien aspect van DMARC implementatie is de configuratie van RUA (Reporting URI for Aggregate reports). RUA stelt organisaties in staat om rapporten te ontvangen over e-mailauthenticatieresultaten, wat zicht biedt op wie e-mail namens hen verzendt en of spoofing pogingen voorkomen.

Metriek	Aantal	Percentage	Risico
DMARC met RUA (monitoring actief)	5.588	69,5%	Beheerd
DMARC zonder RUA (geen monitoring)	2.448	30,5%	Blind

RUA adoptie per beleidsniveau:

- **p=reject:** 76,9% heeft RUA geconfigureerd
- **p=quarantine:** 75,2% heeft RUA geconfigureerd
- **p=none:** 59,7% heeft RUA geconfigureerd

Van bijzonder belang zijn de **561 domeinen met p=reject maar zonder RUA en 592 domeinen met p=quarantine maar zonder RUA.** Deze organisaties hebben DMARC beleidsregels afgedwongen maar hebben geen zicht op of hun eigen legitieme e-mails worden geblokkeerd vanwege misconfiguraties. Zonder monitoring riskeren zij stilzwijgend zakelijk-kritieke e-mailcommunicatie te verliezen.

BEDRIJFSIMPACT EN RISICOBEOORDELING

Beveiligingsrisico's

Voor de 8.401 domeinen zonder p=reject handhaving blijven de volgende aanvalsvectoren levensvatbaar:

- E-mailspoofing: Aanvallers kunnen e-mails verzenden die lijken afkomstig te zijn van legitieme bedrijfsadressen en gericht zijn op klanten, werknemers en partners.
- Business Email Compromise (BEC): CEO-fraude, factuurmanipulatie en betalingsomleiding aanvallen maken allemaal gebruik van vervalste verzenderadressen.
- Merkplundering: Phishing-campagnes die uw domein misbruiken beschadigen klantvertrouwen en merkreputatie.
- Supply chain aanvallen: Het vervalsen van een vertrouwde leverancierdomein kan gebruikt worden om partnernetwerken te infiltreren.

E-mailbezorgings risico's

Sinds 2024 vereisen Google, Microsoft en Yahoo dat bulk verzenders (>5.000 e-mails/week) op zijn minst een DMARC record met p=none hebben. Voor de 2.797 domeinen zonder DMARC record kunnen legitieme e-mails door deze providers worden geweigerd of gefilterd, wat direct gevolgen heeft voor bedrijfscommunicatie, marketingcampagnes en transactionele e-mails (facturen, bevestigingen, meldingen).

Waarom periodieke DMARC-controle essentieel is

DMARC implementatie is geen eenmalige activiteit. E-mailinfrastructuur is dynamisch: organisaties nemen regelmatig nieuwe tools aan voor marketing, CRM, klantenondersteuning, facturering en interne communicatie. Elk nieuw tool dat e-mail namens uw domein verzendt, moet correct worden geverifieerd via SPF en DKIM. Zonder periodieke controle introduceren deze wijzigingen configuratiedrift die zelfs een goed geconfigureerd DMARC beleid kan ondermijnen.

Veelvoorkomende oorzaken van DMARC configuratiedrift zijn:

- **Nieuwe e-mailverzendservices:** Het toevoegen van een marketingplatform, HR recruiting tool, facturatiesysteem of helpdesk die e-mail van uw domein verzendt. Elk vereist SPF/DKIM updates die vaak over het hoofd worden gezien.
- **Leverancier-zijde SPF wijzigingen:** Derde partijen kunnen hun eigen SPF records bijwerken of nieuwe DNS includes toevoegen. Omdat SPF alle geneste lookups evalueert (met een maximum van 10), kunnen leverancier wijzigingen uw domein stilzwijgend over de lookup limiet duwen, waardoor authenticatiefouten ontstaan.
- **DKIM sleutel rotatie:** DKIM sleutels moeten periodiek roteren voor beveiliging. Als DNS records niet dienovereenkomstig worden bijgewerkt, zal DKIM validatie mislukken.
- **Infrastructuurmigraties:** Het verplaatsen naar een nieuw e-mailplatform, cloudprovider of IT-omgeving leidt vaak tot hiaten in authenticatieconfiguratie.
- **Evoluering van bedreigingslandschap:** Aanvallers passen hun technieken voortdurend aan. Het monitoren van DMARC rapporten helpt nieuwe spoofing pogingen die op uw domein gericht zijn te detecteren, wat een proactief beveiligingsposture mogelijk maakt.

Het risico van ***geen*** periodieke DMARC controle is tweeledig: legitieme zakelijke e-mails kunnen stilzwijgend worden geweigerd (waardoor inkomsten en klantencommunicatie worden beïnvloed), terwijl tegelijkertijd nieuwe hiaten in bescherming kunnen ontstaan die aanvallers kunnen exploiteren. Continue monitoring via DMARC aggregate (RUA) rapporten is de meest effectieve manier om deze problemen op te sporen voordat zij bedrijfsimpact hebben.

Compliance & regelgevingsraamwerken

E-mailauthenticatie en DMARC worden steeds vaker genoemd in grote regelgevingsraamwerken en beveiligingsnormen. Organisaties die DMARC verwaarlozen, lopen niet alleen direct beveiligings- en bezorgingsrisico's, maar kunnen ook ontdekken dat zij niet aan regelgevingsverwachtingen voldoen:

NIS2 Richtlijn (EU)

De EU's **NIS2 Richtlijn** (Network and Information Security Directive 2) vergroot de reikwijdte van cyberveiligheidsvereisten voor organisaties in heel Europa aanzienlijk. NIS2 benadrukt supply chain beveiliging, cyberkunde en risico-

beheerpraktijken. De afwezigheid van een DMARC beleid met handhaving (p=reject) kan naleving van meerdere NIS2 vereisten verzwakken, aangezien e-mailspoofing een van de meest voorkomende initiële aanvalsvectoren in supply chain compromissen blijft. De meeste "essentiële" entiteiten hebben een compliance audit deadline van **30 juni 2026.** Het implementeren en onderhouden van DMARC met monitoring is een concrete, controleerbare maatregel die proactief risicobeheer aantoont.

ISO 27001

ISO 27001 is de internationale norm voor informatie-veiligheidsmanagementsystemen (ISMS). Hoewel ISO 27001 geen specifieke technologieën voorschrijft, vereist de op risico's gebaseerde benadering organisaties om informatieveiligheidsrisico's te identificeren en beperken. E-mailspoofing en phishing vertegenwoordigen aanzienlijke risico's die DMARC direct aanpakt. Annex A controles met betrekking tot communicatiebeveiliging (A.13), systeemaankoop en ontwikkeling (A.14) en leverancier-relaties (A.15) hebben allemaal relevantie voor e-mail-authenticatie. Organisaties die ISO 27001 certificering nastreven of handhaven, moeten DMARC handhaving in hun controleset opnemen als aantoonbare maatregel tegen e-mail gebaseerde dreigingen.

NEN 7510 (Gezondheidszorg, Nederland)

NEN 7510 is de Nederlandse norm voor informatie-beveiliging in de gezondheidszorg, nauw gerelateerd aan ISO 27001 maar specifiek afgestemd op de gezond-heidszorgsector. Nederlandse wetgeving vereist dat zorgaanbieders voldoen aan NEN 7510 bij het gebruik van gezondheidsinformatiesystemen en elektronische uitwisselingssystemen. Gezien zorgorganisaties regel-matig gevoelige patiëntgegevens en afsprakeinformatie via e-mail communiceren, is DMARC handhaving een kritische technische maatregel om vervalsung van gezondheidszorgdomeinen te voorkomen. Met 48,5% van de gezondheidszorgsectordomeinen in de hoogrisico-categorie in onze benchmark, is er aanzienlijk ruimte voor verbetering. Juiste DMARC implementatie ondersteunt NEN 7510 compliance door de integriteit en authenticiteit van e-mailcommunicatie te beschermen.

In al deze raamwerken is de algemene lijn duidelijk: e-mailauthenticatie via DMARC is niet langer optioneel maar steeds vaker verwacht als basisbeveiligingsmaat-regel. Organisaties moeten DMARC handhaving niet als een zelfstandig project beschouwen maar als onder-deel van hun lopend informatieveiligheidsbeheer, met periodieke controles ingebouwd in hun compliance cycli.

AANBEVELINGEN

Op basis van de bevindingen in dit rapport, bevelen wij organisaties aan de volgende acties te ondernemen afhankelijk van hun huidige DMARC status:

Voor domeinen zonder DMARC record (2.797 domeinen)

1. **Voer onmiddellijk een DMARC record in**, te beginnen met p=none om authenticatie-gegevens in te verzamelen zonder e-mailstroom te beïnvloeden.
2. **Voeg een RUA adres toe** om aggregate DMARC rapporten te ontvangen en zicht op e-mailauthenticatieresultaten te verkrijgen.
3. **Controleer SPF en DKIM configuraties** om ervoor te zorgen dat alle legitieme e-mailbronnen correct worden geverifieerd.

Voor domeinen met p=none (3.213 domeinen)

1. **Analyseer DMARC aggregate rapporten** om alle legitieme e-mailbronnen te identificeren en eventuele authenticatiefouten aan te pakken.
2. **Plan een migratiepad naar p=quarantine en vervolgens p=reject**. Indefinitief op p=none blijven biedt geen bescherming.
3. Overweeg een DMARC beheerspecialist in te schakelen om de overgang naar handhaving te versnellen.

Voor domeinen met p=quarantine (2.391 domeinen)

1. **Ga naar p=reject** zodra DMARC rapporten bevestigen dat alle legitieme e-mailbronnen consistent authenticatie doorstaan.
2. Zorg ervoor dat RUA rapportage actief is (momenteel mist 24,8% van quarantine domeinen monitoring).

Voor domeinen met p=reject (2.432 domeinen)

1. **Onderhoud actieve DMARC monitoring.** 23,1% van reject domeinen mist RUA rapportage.
2. Controleer regelmatig DMARC rapporten om misconfiguraties vroegtijdig op te vangen, vooral wanneer nieuwe e-mailverzendservices worden toegevoegd of infrastructuur wordt gemigreerd.

Voor alle organisaties

- **Plan periodieke DMARC controles in** (op zijn minst driemaandelijks) om configuratiedrift, nieuwe ongeautoriseerde verzenders en veranderingen in het bedreigingslandschap te detecteren.
- **Integreer DMARC in uw compliance programma** als een aantoonbare controle voor NIS2, ISO 27001 en sector-specifieke normen zoals NEN 7510.
- **Zorg voor supply chain bewustzijn:** evalueer de DMARC positie van uw sleutelpartners en leveranciers als onderdeel van uw risicobeheersing van derden.

METHODOLOGIE

Deze benchmark studie is uitgevoerd met de volgende aanpak:

1. **Domein verzameling:** Een gededupliceerde lijst van 10.833 unieke domeinen werd samengesteld uit het Guardian360 platform, representatief voor organisaties in het Guardian360 partner en klant ecosysteem.
2. **DMARC scanning:** Elk domein werd gescand door DMARC Advisor B.V. om zijn huidige DMARC DNS record op te halen, met extractie van het beleid (p= waarde), rapportageadressen (RUA/RUF) en gerelateerde configuraties.
3. **Branche classificatie:** Domeinen werden gematcht met organisatierecords (85,7% match percentage) om indeling per branche, organisatietype en geografie mogelijk te maken.
4. **Analyse periode:** De scan werd uitgevoerd in april 2026. DMARC records zijn dynamisch en kunnen op elk moment veranderen; dit rapport weerspiegelt de status op het moment van scanning.

OVER ONS

Guardian360

Guardian360 is een cyberveiligheidsbedrijf gebaseerd in Rotterdam, Nederland. Guardian360 biedt continue beveiligingsmonitoring, kwetsbaarheidsbeoordeling en compliance services aan organisaties in heel Europa, zowel direct als via een netwerk van Managed Service Provider (MSP) partners.

DMARC Advisor

DMARC Advisor B.V., gebaseerd in Dordrecht, Nederland, specialiseert zich in e-mailauthenticatie en DMARC beheer. Hun platform helpt organisaties DMARC, SPF en DKIM te implementeren en onderhouden om domeinen te beschermen tegen e-mailspoofing en e-mailbezorging te verbeteren.

GUARDIAN 360°
www.guardian360.nl

Disclaimer: Dit rapport is gebaseerd op openbaar beschikbare DNS records en gegevens van het Guardian360 platform. DMARC records zijn dynamisch en kunnen zijn veranderd sinds het moment van scanning. De branche classificaties zijn gebaseerd op CRM gegevens en weerspiegelen mogelijk niet perfect de primaire sector van elke organisatie. Dit rapport wordt verstrekt voor informatiedoeleinden en vormt geen juridisch of compliance advies.