GUARDIAN360

*in samenwerking met DMARC Advisor*

# E-mailsecurity-benchmark

## DMARC-bescherming bij Managed Service Providers in de DACH-regio

Duitsland · Oostenrijk · Zwitserland | 1.311 aanbieders gescand

NETWERKEVENT

**Netwerkevent grensoverschrijdende cybersecurity voor MSP's en IT-systeemhuizen**

TopGolf Oberhausen · 2 september 2026

---

Data-analyse door DMARC Advisor | Rapport door Guardian360 · Juli 2026 · benchmarkgegevens verzameld op 8 juli 2026

Georganiseerd door de Nederlandse overheid & InnovationQuarter, met Passguard, SecuMailer, SecureMe2, DMARC Advisor en Guardian360.

# Managementsamenvatting

E-mail is nog altijd het belangrijkste kanaal waarlangs organisaties worden aangevallen. DMARC (Domain-based Message Authentication, Reporting and Conformance) is de meest effectieve maatregel om te voorkomen dat criminelen e-mail versturen uit naam van een organisatie. Toch blijft de toepassing op *handhavend* niveau opvallend laag, zelfs bij de bedrijven die hun brood verdienen met security.

Deze benchmark is opgesteld voor het netwerkevent grensoverschrijdende cybersecurity voor MSP's en IT-systeemhuizen (TopGolf Oberhausen, 2 september 2026). **DMARC Advisor** analyseerde de publieke DMARC-configuratie van **1.311 Managed Service Providers (MSP's)** in Duitsland, Oostenrijk en Zwitserland, en **Guardian360** stelde op basis van die bevindingen dit rapport op. Met een strikte definitie waarbij alleen een beleid van **p=reject** als beschermd geldt, zijn de resultaten ontnuchterend.

**74,5%**

van de MSP's in DACH is NIET beschermd tegen e-mailspoofing

Slechts **25,5%** van de gescande MSP's handhaaft DMARC met p=reject. De overige driekwart publiceert ofwel helemaal geen DMARC-record, ofwel voert een beleid (p=none of p=quarantine) waarbij vervalste e-mail de ontvanger toch bereikt, in de inbox of in de spammap die de meeste gebruikers actief controleren. Omdat MSP's e-mail en IT beheren voor duizenden onderliggende klanten, is een onbeschermd MSP-domein niet alleen een risico voor de aanbieder zelf, maar ook een geloofwaardige aanvalsroute naar zijn hele klantenbestand.

## Belangrijkste bevindingen in één oogopslag

- **Slechts 1 op de 4 is beschermd.** 334 van de 1.311 MSP's (25,5%) handhaven p=reject. De grootste groep, 398 aanbieders (30,4%), blijft op p=quarantine hangen, dat spoofing niet tegenhoudt.
- **Bijna 1 op de 5 heeft helemaal geen DMARC-record.** 257 aanbieders (19,6%) publiceren geen enkel DMARC-record en laten hun domein volledig open voor imitatie.
- **Opvallend consistent over de grenzen heen.** De bescherming ligt op 27,7% in Zwitserland, 25,2% in Duitsland en 22,4% in Oostenrijk. Dit is een structureel, geen nationaal probleem.
- **Grootte helpt nauwelijks.** Grote en enterprise-MSP's zijn maar marginaal beter beschermd dan eenmanszaken. Zelfs in het best presterende segment is minder dan een derde beschermd.
- **De specialistenparadox.** MSP's die expliciet cybersecurity- of email-securitydiensten verkopen (26,4% beschermd) presteren nauwelijks beter dan het gemiddelde en beschermen hun eigen domein in bijna drie op de vier gevallen niet.
- **Rapportage is een blinde vlek.** 42,0% van de MSP's heeft helemaal geen DMARC-aggregatierapportage (RUA) geconfigureerd en heeft dus geen enkel zicht op wie er e-mail verstuurt in hun naam.

# Reikwijdte, methode en definities

De benchmark is gebaseerd op een externe, niet-intrusieve scan van openbaar beschikbare DNS-records. Er is geen toegang tot systemen geweest en er zijn geen gegevens verzameld buiten openbare DMARC- en DNS-informatie. De dataset omvat **1.311 MSP's** in de DACH-regio: 1.006 in Duitsland, 220 in Zwitserland en 85 in Oostenrijk. Voor elk domein is het gepubliceerde DMARC-record opgehaald, het handhavingsbeleid geclassificeerd en gecontroleerd of aggregatierapportage (rua) aanwezig is.

## Over dit rapport en het event

Dit rapport verschijnt in het kader van het netwerkevent **grensoverschrijdende cybersecurity voor MSP's en IT-systeemhuizen**, dat op 2 september 2026 plaatsvindt bij TopGolf Oberhausen. Het event wordt georganiseerd door de Nederlandse overheid (haar diplomatieke netwerk in Duitsland) samen met regionale ontwikkelingsmaatschappij InnovationQuarter, en brengt Duitse MSP's samen met vijf Nederlandse cybersecuritybedrijven: Passguard, SecuMailer, SecureMe2, DMARC Advisor en Guardian360. De data-analyse achter deze benchmark is uitgevoerd door **DMARC Advisor**; het rapport is opgesteld door **Guardian360**. Omdat het event vooral MSP's uit Nordrhein-Westfalen samenbrengt, zijn de regionale bevindingen voor NRW (zie de focus verderop) bijzonder relevant voor het publiek.

## Hoe we bescherming classificeren

Volgens de met DMARC Advisor afgestemde classificatie wordt elk domein teruggebracht tot een binaire uitkomst: **Beschermd** of **Niet beschermd**. De logica is bewust streng, want alles onder volledige handhaving laat een vervalst bericht nog steeds de ontvanger bereiken.

| Status | Criterium | Wat het betekent |
|---|---|---|
| **Beschermd** | alleen p=reject | Het domein is volledig beschermd. Vervalste e-mail wordt vóór aflevering direct geweigerd. |
| **Niet beschermd** | p=quarantine | Vervalste e-mail wordt niet geblokkeerd, maar naar de spam-/ongewenstmap geleid, waar 76-86% van de gebruikers naar 'verdwenen' e-mail zoekt. |
| **Niet beschermd** | p=none | Alleen monitoring. Er vindt geen handhaving of blokkering plaats; spoofing slaagt. |
| **Niet beschermd** | Geen DMARC-record | Geen record gepubliceerd. Het domein staat volledig open voor imitatie. |

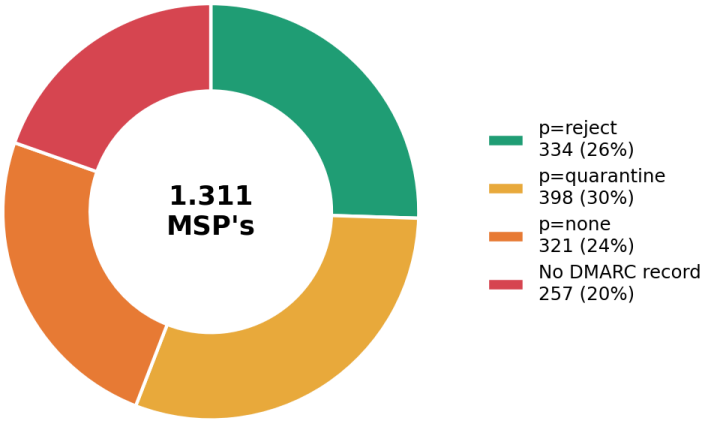
De redenering is eenvoudig: bij 'Geen DMARC', p=none *en* p=quarantine bereikt een vervalste e-mail nog steeds de ontvanger. Omdat de gemiddelde gebruiker zijn spammap actief controleert op legitieme post, blijft hij zeer kwetsbaar. Alleen p=reject verwijdert het bericht voordat het schade kan aanrichten. Daarom rekenen we p=quarantine, de grootste groep in deze dataset, niet als beschermd.

> *Opmerking over p=reject: organisaties moeten nooit direct naar p=reject overstappen. Monitor eerst de RUA-rapporten, bevestig dat elke legitieme afzender correct authenticeert en scherp daarna pas het beleid aan. Te vroeg handhaven kan legitieme zakelijke e-mail blokkeren.*

# Het totaalbeeld

Over alle 1.311 MSP's zijn de vier DMARC-toestanden vrijwel gelijk verdeeld, waarbij p=quarantine, een beleid dat een vals gevoel van veiligheid geeft, de meest voorkomende configuratie is.

**Verdeling van DMARC-beleid onder MSP's in de DACH-regio**



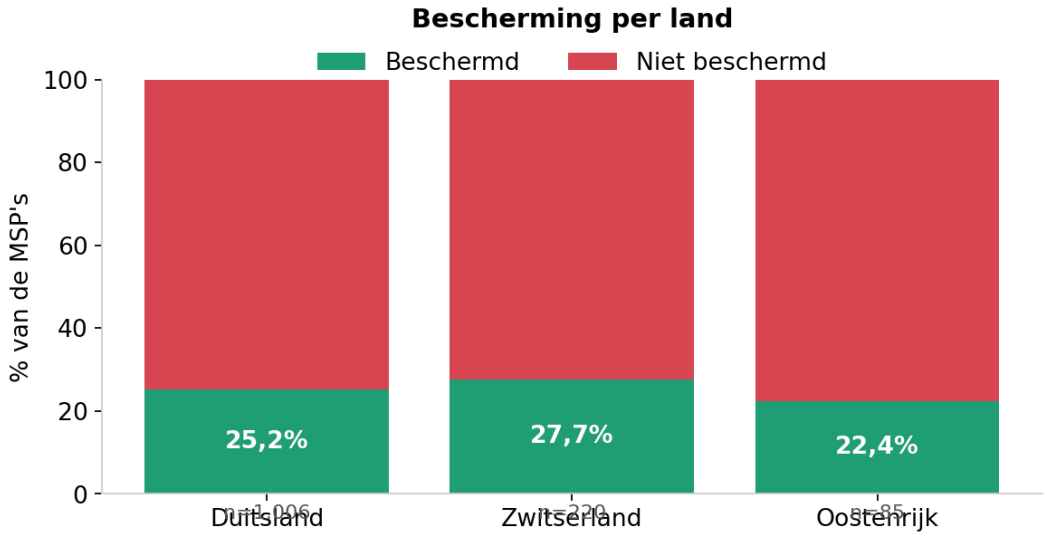

| DMARC-beleid | MSP's | Aandeel | Beschermd? |
|---|---|---|---|
| **p=reject** | 334 | 25,5% | Beschermd |
| **p=quarantine** | 398 | 30,4% | Niet beschermd |
| **p=none** | 321 | 24,5% | Niet beschermd |
| **Geen DMARC-record** | 257 | 19,6% | Niet beschermd |
| **Totaal gescand** | 1.311 | 100% | - |

**Slechts 1 op de 4 MSP's in DACH is beschermd tegen spoofing (p=reject)**


Teruggebracht tot de binaire kern die telt, is **977 van de 1.311 gescande aanbieders (74,5%) niet beschermd** tegen het versturen van e-mail uit hun naam. Voor een sector waarvan de hele belofte berust op het zijn van een vertrouwd, veilig verlengstuk van de IT van klanten, is dat een aanzienlijk risico.

# Analyse per land

Je zou betekenisvolle verschillen tussen de drie markten verwachten. In de praktijk is het beeld opvallend uniform: de bescherming loopt slechts van 22,4% tot 27,7%. Het probleem is structureel in het hele Duitstalige gebied en niet specifiek voor één land.



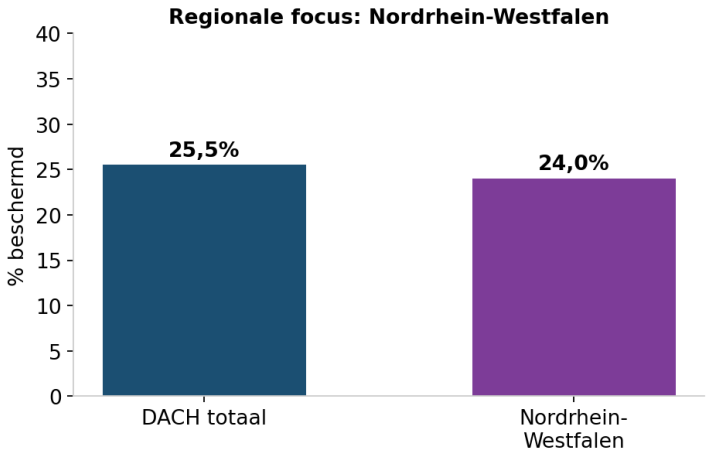

| Land | MSP's | p=reject | quarantine | p=none | Geen record | % beschermd |
|---|---|---|---|---|---|---|
| **Duitsland** | 1.006 | 254 | 296 | 243 | 212 | 25,2% |
| **Zwitserland** | 220 | 61 | 74 | 52 | 33 | 27,7% |
| **Oostenrijk** | 85 | 19 | 28 | 26 | 12 | 22,4% |

Zwitserland leidt nipt met **27,7%**, gevolgd door Duitsland (**25,2%**) en Oostenrijk (**22,4%**). Oostenrijk heeft ook het hoogste aandeel aanbieders dat blijft steken op p=none (alleen monitoring), wat erop wijst dat een aantal organisaties wel aan DMARC is begonnen maar het nooit heeft afgerond.

# Regionale focus: Nordrhein-Westfalen

Als dichtstbevolkte deelstaat en dichtste MSP-markt van Duitsland is Nordrhein-Westfalen (NRW) apart geanalyseerd. Met **221 aanbieders** volgt NRW het DACH-gemiddelde vrijwel exact, wat bevestigt dat de handhavingskloof zelfs in een volwassen, competitieve regionale markt blijft bestaan.

Deze regio is hier bijzonder relevant: het netwerkevent vindt plaats in Oberhausen, in het hart van NRW, en het publiek bestaat grotendeels uit MSP's en IT-systeemhuizen uit de regio. De onderstaande cijfers beschrijven dus de directe peer group van de meeste aanwezigen, en een eerlijke maatstaf waaraan ieder zijn eigen domein kan afmeten.




| Kengetal | Nordrhein-Westfalen | DACH totaal |
|---|---|---|
| **Geanalyseerde MSP's** | 221 | 1.311 |
| **p=reject (beschermd)** | 53 (24,0%) | 334 (25,5%) |
| **p=quarantine** | 67 | 398 |
| **p=none** | 55 | 321 |
| **Geen DMARC-record** | 46 | 257 |
| **Niet beschermd** | 168 (76,0%) | 977 (74,5%) |

In NRW is 76,0% van de MSP's niet beschermd, vrijwel identiek aan de 74,5% van de hele regio. De grootste groep is opnieuw p=quarantine.

## Bescherming per deelstaat

Binnen Duitsland variëren de beschermingsgraden sterker op deelstaatniveau, al is voorzichtigheid geboden bij kleine steekproeven in de minst bevolkte deelstaten. De grotere MSP-markten liggen dicht rond het landelijk gemiddelde.

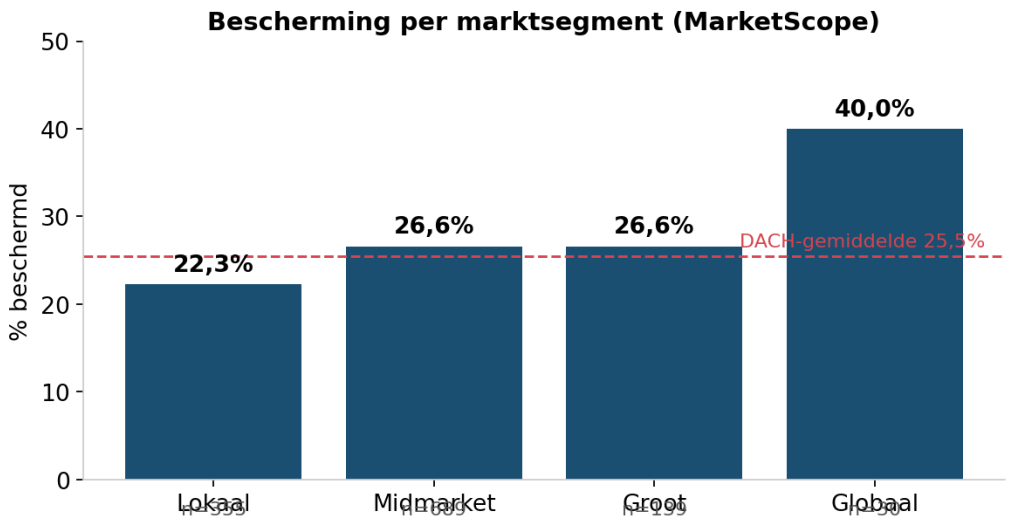
| Deelstaat | MSP's | Beschermd | % beschermd |
|---|---|---|---|
| **Nordrhein-Westfalen** | 221 | 53 | 24,0% |
| **Bayern** | 194 | 54 | 27,8% |
| **Baden-Württemberg** | 141 | 30 | 21,3% |
| **Hessen** | 96 | 22 | 22,9% |
| **Niedersachsen** | 66 | 17 | 25,8% |
| **Berlin** | 57 | 14 | 24,6% |
| **Hamburg** | 53 | 12 | 22,6% |
| **Rheinland-Pfalz** | 44 | 13 | 29,5% |
| **Schleswig-Holstein** | 36 | 6 | 16,7% |

> *Deelstaten met minder dan 30 MSP's zijn weggelaten omwille van statistische betrouwbaarheid.*

# Analyse per bedrijfstype en -grootte

## Per marktsegment

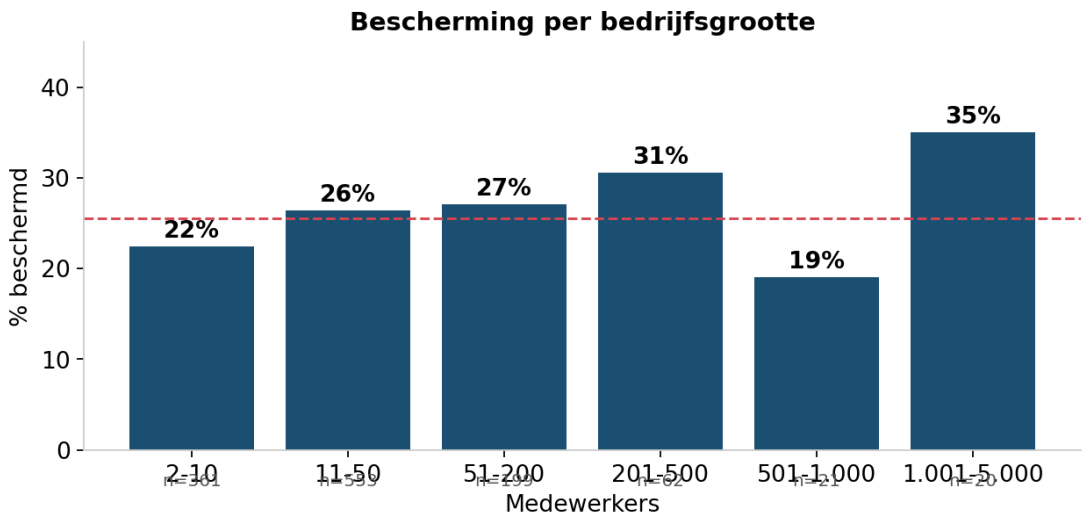
Wanneer we MSP's classificeren naar de markt die ze primair bedienen (MarketScope), blijkt dat alleen de kleine groep wereldwijd opererende aanbieders het gemiddelde betekenisvol overtreft. Lokale aanbieders, de grootste groep die het mkb bedient, zijn het slechtst beschermd.




| Marktsegment | MSP's | % beschermd |
|---|---|---|
| **Lokaal** | 355 | 22,3% |
| **Midmarket** | 689 | 26,6% |
| **Groot** | 139 | 26,6% |
| **Globaal** | 30 | 40,0% |

## Per bedrijfsgrootte

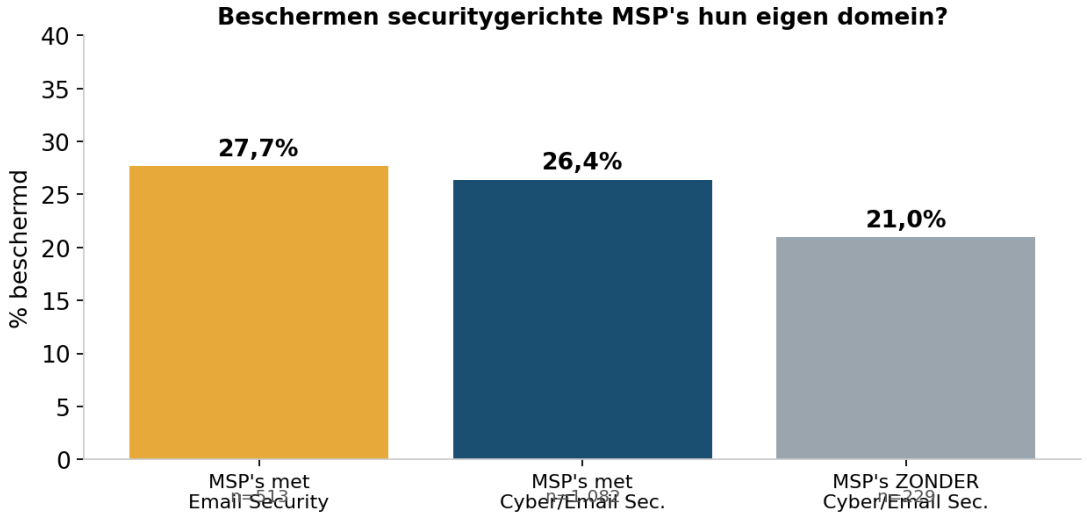
De aanname dat grotere, beter uitgeruste aanbieders beter beschermd zijn, houdt maar zwak stand. De bescherming loopt in het middensegment licht op met de grootte, maar zelfs de best presterende klassen laten ongeveer twee derde van de aanbieders onbeschermd, en de allergrootste categorieën zijn door kleine aantallen inconsistent.




De conclusie is ongemakkelijk maar duidelijk: DMARC-handhaving is in de eerste plaats geen kwestie van middelen. Aanbieders van elke omvang slagen er niet in een kloof te dichten die gratis te verhelpen is en precies binnen hun eigen expertise ligt.

# De specialistenparadox

Misschien wel de meest veelzeggende doorsnede van de data vergelijkt MSP's op basis van wat ze verkopen. Als één groep de eigen zaken op orde zou moeten hebben, zijn het de aanbieders die klanten expliciet **cybersecurity**- en **email-security**-diensten aanbieden.

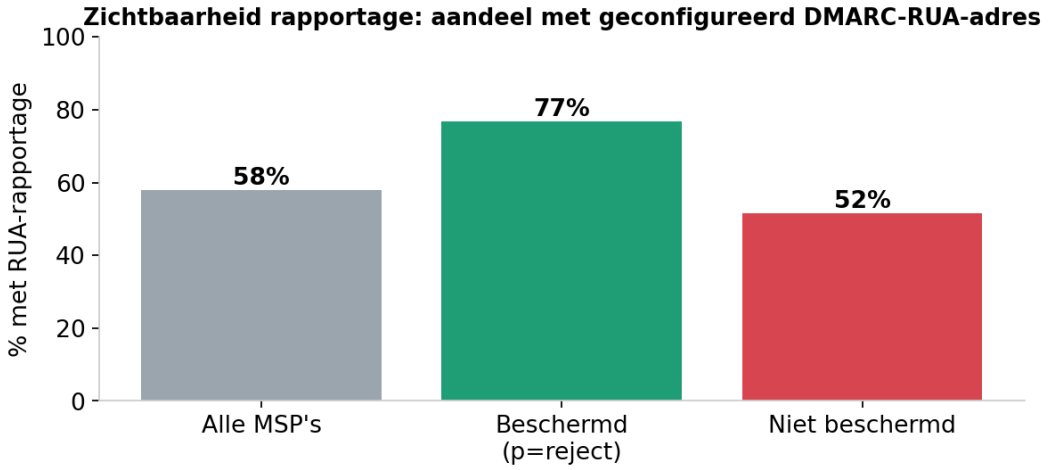



| Groep | MSP's | % beschermd |
|---|---|---|
| **MSP's met Email Security** | 513 | 27,7% |
| **MSP's met Cyber-/Email Security** | 1.082 | 26,4% |
| **MSP's zonder beide** | 229 | 21,0% |

Securityspecialisten beschermen zichzelf iets vaker, maar het verschil is marginaal: **26,4% tegenover 21%**. Kort gezegd: ongeveer **drie op de vier MSP's die email security verkopen, kunnen niet aantonen dat hun eigen domein beschermd is tegen spoofing.** Voor potentiële klanten en partners is dit een eenvoudige en eerlijke due-diligencevraag.

# Rapportage en zichtbaarheid (RUA)

Een DMARC-beleid is maar het halve verhaal. Het aggregatierapportageadres (rua) geeft een organisatie inzicht in wie er e-mail verstuurt uit haar naam, welke legitieme diensten geauthenticeerd moeten worden en waar spoofingpogingen vandaan komen. Zonder dit vliegt een organisatie blind en kan zij niet veilig naar p=reject doorgroeien.




| Groep | % met geconfigureerde RUA-rapportage |
|---|---|
| **Alle MSP's** | 58,0% |
| **Beschermd (p=reject)** | 76,9% |
| **Niet beschermd** | 51,5% |

42,0% van alle MSP's heeft helemaal geen rapportage geconfigureerd. Rapportage correleert sterk met handhaving: 76,9% van de beschermde aanbieders verzamelt RUA-data, tegenover slechts 51,5% van de onbeschermde, precies de volgorde die een gezonde DMARC-uitrol volgt: rapportage aanzetten, leren, dan handhaven.

> *Belangrijke nuance: een externe scan kan bevestigen dat er een rua-adres bestaat, maar niet of de rapporten daadwerkelijk worden gelezen. Als rapporten naar een interne mailbox worden gestuurd, komen ze binnen als ruwe XML, die tijdrovend en foutgevoelig te interpreteren is en vaak ongelezen wordt gearchiveerd. Duidelijk eigenaarschap van het DMARC-protocol, idealiter met geautomatiseerde rapportverwerking, is essentieel.*

# Wat dit betekent en wat te doen

De kernboodschap van deze benchmark is niet dat DMARC moeilijk is. Het is dat een maatregel die gratis, goed gedocumenteerd en direct binnen de expertise van elke MSP ligt, door driekwart van de sector onvoltooid wordt gelaten. Voor MSP's is de inzet nog groter: een onbeschermd aanbiederdomein is een kant-en-klaar sjabloon voor aanvallers om zich richting de eigen klanten voor te doen als een vertrouwde leverancier.

## Voor MSP's

- **Publiceer vandaag nog een DMARC-record als u er geen heeft.** Begin met p=none en een rapportageadres zodat u zonder risico zicht krijgt.
- **Blijf niet steken op p=quarantine.** Het is de meest voorkomende configuratie in deze dataset en beschermt u niet. Zie het als tussenstation, niet als eindbestemming.
- **Lees uw RUA-rapporten.** Gebruik ze om elke legitieme afzender te identificeren en te authenticeren, en ga vervolgens gericht over naar p=reject.
- **Praktiseer wat u verkoopt.** Als u email- of cybersecurity aanbiedt, is een beschermd domein het minimale geloofwaardige bewijs.

## Voor klanten en partners

- **Stel de vraag.** "Staat uw primaire domein op DMARC p=reject, en monitort u RUA?" is een eerlijke, onthullende due-diligencevraag aan elke aanbieder.
- **Controleer ook uw eigen situatie.** Dezelfde strikte toets geldt voor de domeinen van uw eigen organisatie.

## Hoe Guardian360 en DMARC Advisor helpen

Guardian360 en DMARC Advisor helpen organisaties veilig van geen bescherming naar volledige handhaving te komen: doorlopend scannen en monitoren, geautomatiseerde interpretatie van RUA-rapporten en deskundige begeleiding tot p=reject zonder legitieme e-mail te verstoren. Beide nemen samen met Passguard, SecuMailer en SecureMe2 deel aan het netwerkevent grensoverschrijdende cybersecurity. Het doel van deze benchmark is niet aan de schandpaal nagelen, maar een onzichtbaar risico zichtbaar maken en de sector, en de MSP's in de zaal, helpen een kloof te dichten die ze bij uitstek kunnen dichten.

---

**Over deze benchmark.** Data-analyse door DMARC Advisor; rapport opgesteld door Guardian360. Gebaseerd op een externe, niet-intrusieve scan van openbare DNS-/DMARC-records van 1.311 DACH-MSP's, gegevens verzameld op 8 juli 2026. Opgesteld voor het netwerkevent grensoverschrijdende cybersecurity voor MSP's en IT-systeemhuizen (TopGolf Oberhausen, 2 september 2026), georganiseerd door de Nederlandse overheid en InnovationQuarter, met deelnemende bedrijven Passguard, SecuMailer, SecureMe2, DMARC Advisor en Guardian360. Percentages zijn afgerond op één decimaal. Een domein geldt alleen als beschermd wanneer het DMARC-beleid p=reject is. 