GUARDIAN360

en partenariat avec DMARC Advisor

Benchmark de sécurité e-mail

Protection DMARC chez les Managed Service Providers de la région DACH

Allemagne · Autriche · Suisse | 1 311 prestataires analysés

ÉVÉNEMENT DE NETWORKING

Événement « Cybersécurité transfrontalière » pour les MSP et intégrateurs IT

TopGolf Oberhausen · 2 septembre 2026

Analyse des données par DMARC Advisor | Rapport par Guardian360 · Juillet 2026 · données du benchmark collectées le 8 juillet 2026

Organisé par le gouvernement néerlandais & InnovationQuarter, avec Passguard, SecuMailer, SecureMe2, DMARC Advisor et Guardian360.

Résumé

L'e-mail reste le premier canal par lequel les organisations sont attaquées. DMARC (Domain-based Message Authentication, Reporting and Conformance) est la mesure la plus efficace pour empêcher des criminels d'envoyer des e-mails au nom d'une organisation. Pourtant, son adoption à un niveau *contraignant* demeure étonnamment faible, y compris parmi les entreprises dont la sécurité est le métier.

Ce benchmark a été préparé pour l'événement de networking « Cybersécurité transfrontalière » destiné aux MSP et intégrateurs IT (TopGolf Oberhausen, 2 septembre 2026). **DMARC Advisor** a analysé la configuration DMARC publique de **1 311 Managed Service Providers (MSP)** en Allemagne, en Autriche et en Suisse, et **Guardian360** a rédigé le présent rapport à partir de ces résultats. En appliquant une définition stricte où seule une politique **p=reject** est considérée comme protégée, les résultats sont préoccupants.

74,5 %

des MSP en DACH ne sont PAS protégés contre l'usurpation d'e-mail

Seuls **25,5 %** des MSP analysés appliquent DMARC avec p=reject. Les trois quarts restants ne publient aucun enregistrement DMARC, ou appliquent une politique (p=none ou p=quarantine) qui laisse malgré tout un e-mail usurpé atteindre le destinataire, dans la boîte de réception ou dans le dossier spam que la plupart des utilisateurs consultent activement. Comme les MSP gèrent la messagerie et l'informatique de milliers de clients en aval, un domaine de MSP non protégé n'est pas seulement un risque pour le prestataire lui-même, mais aussi une voie d'attaque crédible vers l'ensemble de sa base de clients.

Principaux résultats en un coup d'œil

- **Seul 1 sur 4 est protégé.** 334 des 1 311 MSP (25,5 %) appliquent p=reject. Le groupe le plus important, 398 prestataires (30,4 %), reste en p=quarantine, qui n'arrête pas l'usurpation.
- **Près d'1 sur 5 n'a aucun enregistrement DMARC.** 257 prestataires (19,6 %) ne publient aucun enregistrement DMARC, laissant leur domaine totalement exposé à l'usurpation.
- **Remarquablement homogène d'un pays à l'autre.** La protection s'établit à 27,7 % en Suisse, 25,2 % en Allemagne et 22,4 % en Autriche. Il s'agit d'un écart structurel, non national.
- **La taille n'aide guère.** Les grands MSP et ceux de type entreprise ne sont que légèrement mieux protégés que les structures individuelles. Même dans la meilleure tranche de taille, moins d'un tiers est protégé.
- **Le paradoxe des spécialistes.** Les MSP qui vendent explicitement des services de cybersécurité ou de sécurité e-mail (26,4 % protégés) dépassent à peine la moyenne générale et ne protègent pas leur propre domaine dans près de trois cas sur quatre.
- **Le reporting est un angle mort.** 42,0 % des MSP n'ont aucun reporting agrégé DMARC (RUA) configuré et n'ont donc aucune visibilité sur qui envoie des e-mails en leur nom.

Périmètre, méthode et définitions

Le benchmark repose sur une analyse externe et non intrusive d'enregistrements DNS publics. Aucun système n'a été consulté et aucune donnée au-delà des informations DMARC et DNS publiques n'a été collectée. L'ensemble comprend **1 311 MSP** de la région DACH : 1 006 en Allemagne, 220 en Suisse et 85 en Autriche. Pour chaque domaine, l'enregistrement DMARC publié a été récupéré, la politique d'application classée et la présence d'un reporting agrégé (rua) vérifiée.

À propos de ce rapport et de l'événement

Ce rapport paraît dans le cadre de l'événement de networking **« Cybersécurité transfrontalière » pour les MSP et intégrateurs IT**, organisé le 2 septembre 2026 au TopGolf Oberhausen. L'événement est organisé par le gouvernement néerlandais (son réseau diplomatique en Allemagne) avec l'agence régionale de développement InnovationQuarter, et réunit des MSP allemands et cinq entreprises néerlandaises de cybersécurité : Passguard, SecuMailer, SecureMe2, DMARC Advisor et Guardian360. L'analyse des données de ce benchmark a été réalisée par **DMARC Advisor** ; le rapport a été rédigé par **Guardian360**. Comme l'événement réunit surtout des MSP de Rhénanie-du-Nord-Westphalie, les résultats régionaux pour la NRW (voir le focus plus loin) sont particulièrement pertinents pour le public.

Comment nous classons la protection

Selon la classification convenue avec DMARC Advisor, chaque domaine est ramené à un résultat binaire : **Protégé** ou **Non protégé**. La logique est volontairement stricte, car tout ce qui est en deçà d'une application complète laisse un message usurpé atteindre le destinataire.

Statut	Critère	Signification
Protégé	p=reject uniquement	Le domaine est entièrement protégé. Les e-mails usurpés sont rejetés avant leur remise.
Non protégé	p=quarantine	Les e-mails usurpés ne sont pas bloqués mais dirigés vers les spams/indésirables, où 76-86 % des utilisateurs cherchent leurs e-mails « perdus ».
Non protégé	p=none	Surveillance uniquement. Aucune application ni blocage ; l'usurpation réussit.
Non protégé	Aucun enregistrement DMARC	Aucun enregistrement publié. Le domaine est totalement exposé à l'usurpation.

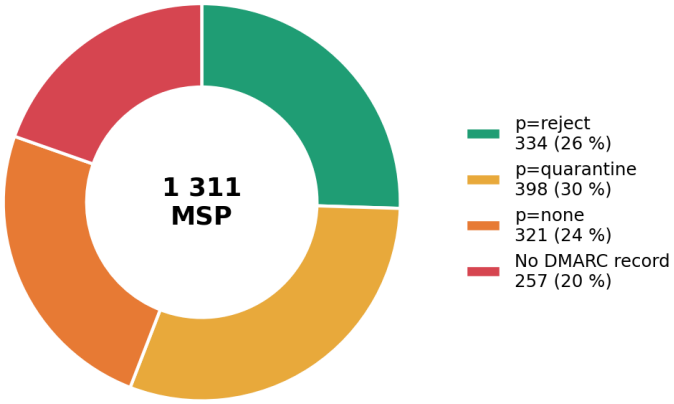
Le raisonnement est simple : avec « Aucun DMARC », p=none *et* p=quarantine, un e-mail usurpé parvient tout de même au destinataire. Comme l'utilisateur moyen consulte activement son dossier spam à la recherche de courriers légitimes, il reste très vulnérable. Seul p=reject supprime le message avant qu'il ne nuise. C'est pourquoi nous ne comptons pas p=quarantine, le groupe le plus important de cet ensemble, comme protégé.

> *Remarque sur p=reject : une organisation ne doit jamais passer directement à p=reject. Surveillez d'abord les rapports RUA, vérifiez que chaque expéditeur légitime s'authentifie correctement, puis durcissez la politique. Une application prématurée peut bloquer des e-mails professionnels légitimes.*

Le tableau d'ensemble

Sur l'ensemble des 1 311 MSP, les quatre états DMARC se répartissent presque également, p=quarantine, une politique qui procure un faux sentiment de sécurité, étant la configuration la plus fréquente.

Répartition des politiques DMARC chez les MSP de la région DACH



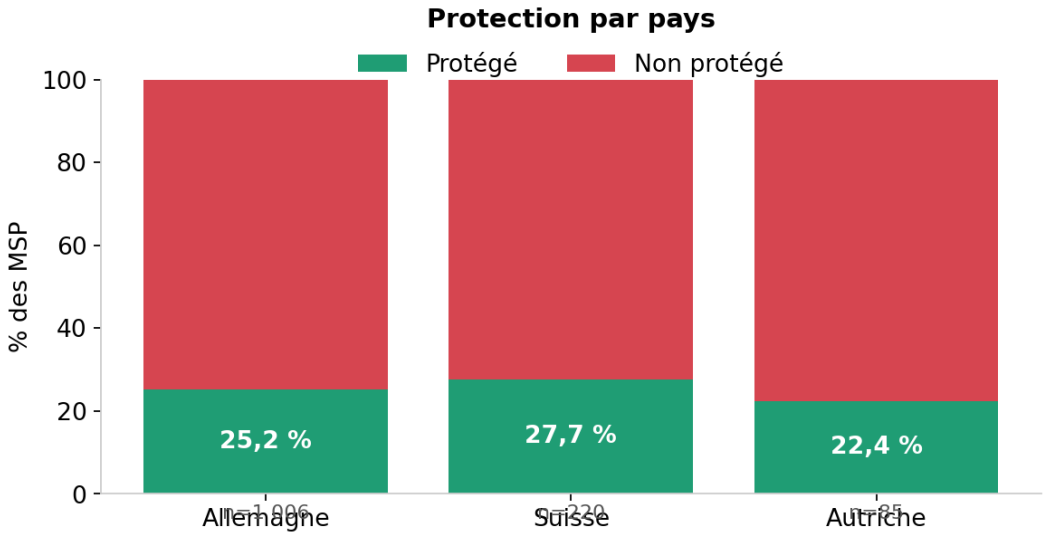
Politique DMARC	MSP	Part	Protégé ?
p=reject	334	25,5 %	Protégé
p=quarantine	398	30,4 %	Non protégé
p=none	321	24,5 %	Non protégé
Aucun enregistrement DMARC	257	19,6 %	Non protégé
Total analysé	1 311	100 %	-

Seul 1 MSP sur 4 en DACH est protégé contre l'usurpation (p=reject)

Réduit à la question binaire essentielle, **977 des 1 311 prestataires analysés (74,5 %) ne sont pas protégés** contre l'envoi d'e-mails en leur nom. Pour un secteur dont toute la proposition repose sur le fait d'être une extension fiable et sûre de l'IT de ses clients, c'est une exposition considérable.

Analyse par pays

On pourrait s'attendre à des différences marquées entre les trois marchés. En pratique, le tableau est remarquablement uniforme : la protection ne varie que de 22,4 % à 27,7 %. Le problème est structurel dans toute la région germanophone et non propre à un pays.



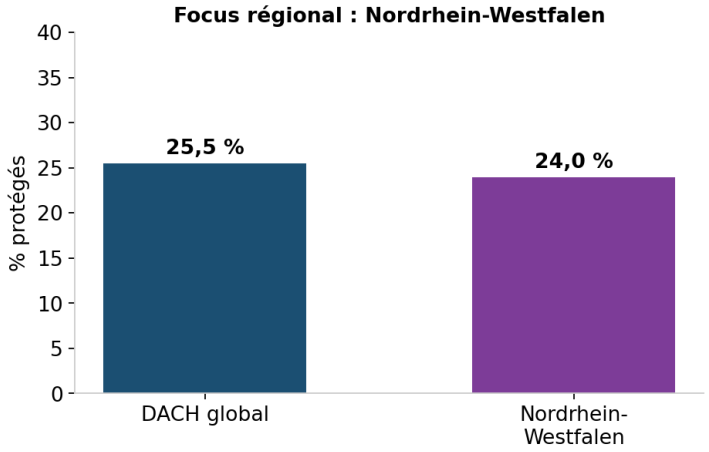
Pays	MSP	p=reject	quarantine	p=none	Aucun enr.	% protégés
Allemagne	1 006	254	296	243	212	25,2 %
Suisse	220	61	74	52	33	27,7 %
Autriche	85	19	28	26	12	22,4 %

La Suisse est en tête de peu avec **27,7 %**, devant l'Allemagne (**25,2 %**) et l'Autriche (**22,4 %**). L'Autriche présente aussi la plus forte proportion de prestataires bloqués en p=none (surveillance seule), ce qui suggère que plusieurs organisations ont entamé la démarche DMARC sans jamais l'achever.

Focus régional : Rhénanie-du-Nord-Westphalie

Land le plus peuplé et marché MSP le plus dense d'Allemagne, la Rhénanie-du-Nord-Westphalie (NRW) a été analysée séparément. Avec **221 prestataires**, la NRW suit presque exactement la moyenne DACH, confirmant que l'écart d'application persiste même sur un marché régional mature et concurrentiel.

Cette région est ici particulièrement pertinente : l'événement se tient à Oberhausen, au cœur de la NRW, et son public se compose en grande partie de MSP et d'intégrateurs IT de la région. Les chiffres ci-dessous décrivent donc le groupe de pairs immédiat de la plupart des participants, et un étalon équitable pour mesurer son propre domaine.



Indicateur	Rhénanie-du-N.-W.	DACH global
MSP analysés	221	1 311
p=reject (protégés)	53 (24,0 %)	334 (25,5 %)
p=quarantine	67	398
p=none	55	321
Aucun enregistrement DMARC	46	257
Non protégés	168 (76,0 %)	977 (74,5 %)

En NRW, 76,0 % des MSP ne sont pas protégés, quasi identique aux 74,5 % de l'ensemble de la région. Le groupe le plus important reste p=quarantine.

Protection par Land allemand

En Allemagne, les taux de protection varient davantage au niveau des Länder, mais les faibles effectifs des Länder les moins peuplés incitent à la prudence. Les marchés MSP les plus importants se regroupent étroitement autour de la moyenne nationale.

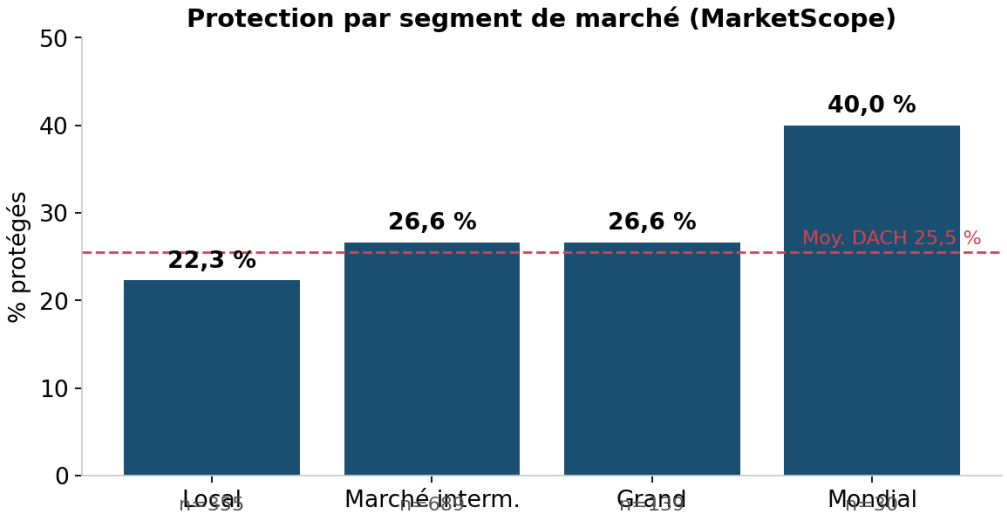
Land	MSP	Protégés	% protégés
Nordrhein-Westfalen	221	53	24,0 %
Bayern	194	54	27,8 %
Baden-Württemberg	141	30	21,3 %
Hessen	96	22	22,9 %
Niedersachsen	66	17	25,8 %
Berlin	57	14	24,6 %
Hamburg	53	12	22,6 %
Rheinland-Pfalz	44	13	29,5 %
Schleswig-Holstein	36	6	16,7 %

> *Les Länder comptant moins de 30 MSP sont omis pour des raisons de fiabilité statistique.*

Analyse par type et taille d'entreprise

Par segment de marché

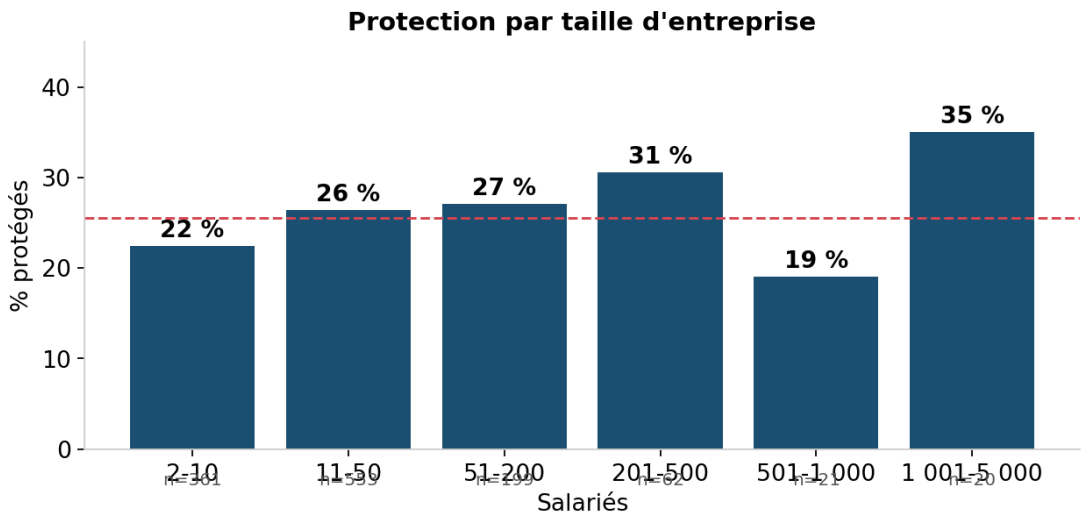
En classant les MSP selon le marché qu'ils servent principalement (MarketScope), on constate que seul le petit groupe de prestataires opérant à l'échelle mondiale dépasse nettement la moyenne. Les prestataires locaux, le groupe le plus nombreux servant les PME, sont les moins protégés.



Segment de marché	MSP	% protégés
Local	355	22,3 %
Marché interm.	689	26,6 %
Grand	139	26,6 %
Mondial	30	40,0 %

Par taille d'entreprise

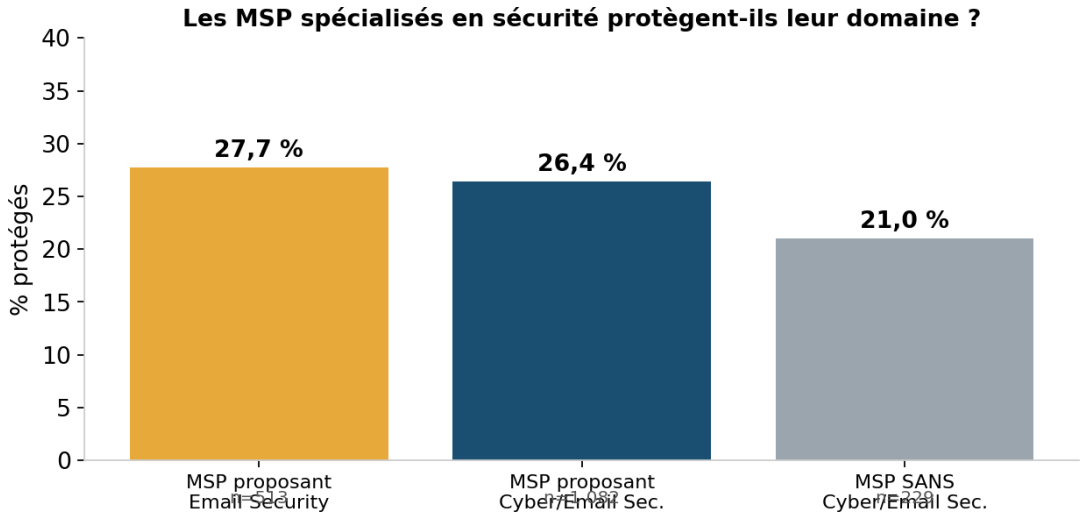
L'intuition selon laquelle les prestataires plus grands et mieux dotés sont mieux protégés ne se vérifie que faiblement. La protection augmente modestement avec la taille dans les tranches intermédiaires, mais même les meilleures tranches laissent environ deux tiers des prestataires exposés, et les plus grandes catégories sont irrégulières en raison de faibles effectifs.



La leçon est inconfortable mais claire : l'application de DMARC n'est pas avant tout un problème de moyens. Des prestataires de toutes tailles ne parviennent pas à combler une lacune dont la correction est gratuite et relève précisément de leur propre expertise.

Le paradoxe des spécialistes

L'angle sans doute le plus révélateur compare les MSP selon ce qu'ils vendent. Si un groupe devait avoir sa propre maison en ordre, ce sont les prestataires qui commercialisent explicitement des services de **cybersécurité** et de **sécurité e-mail**.

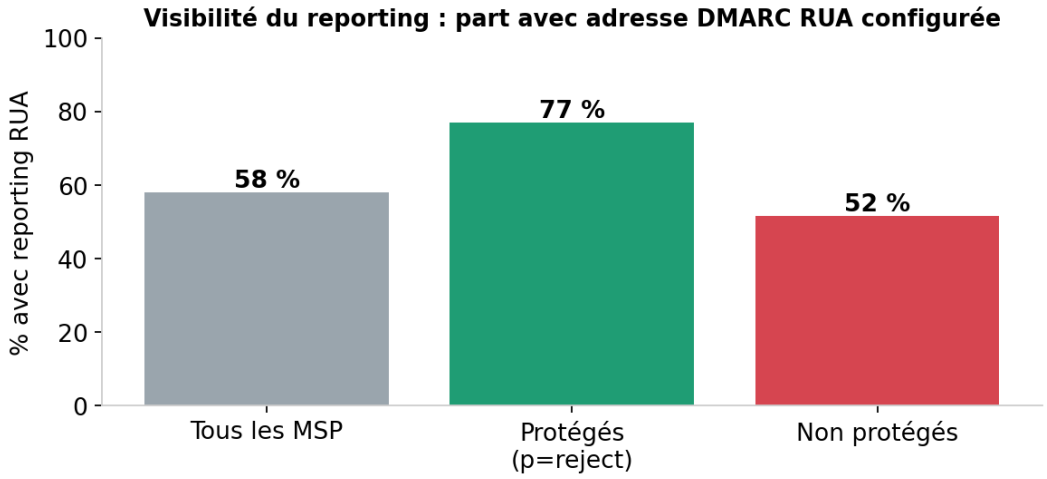


Groupe	MSP	% protégés
MSP proposant Email Security	513	27,7 %
MSP proposant Cyber/Email Security	1 082	26,4 %
MSP proposant ni l'un ni l'autre	229	21,0 %

Les spécialistes de la sécurité se protègent un peu plus souvent, mais l'écart est marginal : **26,4 % contre 21 %**. En clair, environ **trois MSP sur quatre qui vendent de la sécurité e-mail ne peuvent pas démontrer que leur propre domaine est protégé contre l'usurpation.** Pour des clients et partenaires potentiels, c'est une question de due diligence simple et légitime.

Reporting et visibilité (RUA)

Une politique DMARC ne raconte que la moitié de l'histoire. L'adresse de reporting agrégé (rua) donne à une organisation la visibilité sur qui envoie des e-mails en son nom, quels services légitimes doivent être authentifiés et d'où proviennent les tentatives d'usurpation. Sans elle, une organisation avance à l'aveugle et ne peut pas progresser en toute sécurité vers p=reject.



Groupe	% avec reporting RUA configuré
Tous les MSP	58,0 %
Protégés (p=reject)	76,9 %
Non protégés	51,5 %

42,0 % de l'ensemble des MSP n'ont aucun reporting configuré. Le reporting est fortement corrélé à l'application : 76,9 % des prestataires protégés collectent des données RUA, contre seulement 51,5 % des non protégés, soit exactement la séquence d'un déploiement DMARC sain : activer le reporting, apprendre, puis appliquer.

> *Nuance importante : une analyse externe peut confirmer l'existence d'une adresse rua, mais pas si les rapports sont réellement lus. Livrés dans une boîte interne, les rapports arrivent en XML brut, long et source d'erreurs à interpréter, et sont souvent archivés sans être lus. Il est essentiel d'établir une responsabilité claire du protocole DMARC, idéalement avec un traitement automatisé des rapports.*

Ce que cela signifie et quoi faire

Le message clé de ce benchmark n'est pas que DMARC est difficile. C'est qu'une mesure gratuite, bien documentée et relevant directement de l'expertise de chaque MSP reste inachevée pour les trois quarts du secteur. Pour les MSP en particulier, l'enjeu est amplifié : un domaine de prestataire non protégé est un modèle tout prêt permettant à des attaquants de se faire passer, auprès de ses propres clients, pour un fournisseur de confiance.

Pour les MSP

- **Publiez dès aujourd'hui un enregistrement DMARC si vous n'en avez pas.** Commencez par p=none avec une adresse de reporting pour gagner en visibilité sans risque.
- **Ne vous arrêtez pas à p=quarantine.** C'est la configuration la plus courante de cet ensemble et elle ne vous protège pas. Considérez-la comme une étape, non une destination.
- **Lisez vos rapports RUA.** Utilisez-les pour identifier et authentifier chaque expéditeur légitime, puis passez délibérément à p=reject.
- **Appliquez ce que vous vendez.** Si vous proposez de la sécurité e-mail ou cyber, un domaine protégé est la preuve crédible minimale.

Pour les clients et partenaires

- **Posez la question.** « Votre domaine principal est-il en DMARC p=reject, et surveillez-vous les RUA ? » est une question de due diligence juste et révélatrice pour tout prestataire.
- **Vérifiez aussi votre propre posture.** Le même test strict s'applique aux domaines de votre organisation.

Comment Guardian360 et DMARC Advisor vous aident

Guardian360 et DMARC Advisor aident les organisations à passer en toute sécurité de l'absence de protection à une application complète : analyse et surveillance continues, interprétation automatisée des rapports RUA et accompagnement expert jusqu'à p=reject sans perturber les e-mails légitimes. Tous deux participent, aux côtés de Passguard, SecuMailer et SecureMe2, à l'événement de networking « Cybersécurité transfrontalière ». L'objectif de ce benchmark n'est pas de pointer du doigt, mais de rendre visible un risque invisible et d'aider le secteur, et les MSP présents, à combler une lacune qu'ils sont particulièrement bien placés pour combler.

À propos de ce benchmark. Analyse des données par DMARC Advisor ; rapport rédigé par Guardian360. Basé sur une analyse externe et non intrusive d'enregistrements DNS/DMARC publics de 1 311 MSP de la région DACH, données collectées le 8 juillet 2026. Préparé pour l'événement de networking « Cybersécurité transfrontalière » pour les MSP et intégrateurs IT (TopGolf Oberhausen, 2 septembre 2026), organisé par le gouvernement néerlandais et InnovationQuarter, avec les entreprises participantes Passguard, SecuMailer, SecureMe2, DMARC Advisor et Guardian360. Les pourcentages sont arrondis à une décimale. Un domaine n'est considéré comme protégé que si sa politique DMARC est p=reject.