RAPPORT DE RÉFÉRENCE DMARC

Analyse de l'Authentification des E-mails et de la Protection des Domaines

Avril 2026

10 833 Domaines Analysés

Entre 15+ secteurs aux Pays-Bas, en Allemagne, en Belgique et en France

Commandé par

GUARDIAN 360°

Schouwburgplein 30-34
3012 CL Rotterdam, Pays-Bas

RÉSUMÉ EXÉCUTIF

Ce rapport présente les résultats d'une évaluation DMARC (Domain-based Message Authentication, Reporting & Conformance) à grande échelle menée dans **10 833 domaines uniques** associés à des organisations de l'écosystème Guardian360. L'analyse a été effectuée par DMARC Advisor B.V. en avril 2026.

Le constat principal est alarmant : **77,6 % de tous les domaines analysés ne sont pas entièrement protégés contre l'usurpation d'identité par e-mail.** Cela signifie que pour la grande majorité des organisations, les cybercriminels peuvent envoyer des e-mails qui semblent provenir d'adresses e-mail légitimes, permettant l'hameçonnage, la compromission d'e-mails professionnels (BEC) et l'usurpation de marque à grande échelle.

Seuls 22,4 % des domaines ont implémenté une politique p=reject, qui est le seul niveau de politique DMARC qui prévient activement les e-mails usurpés d'atteindre les destinataires. Les domaines restants sont distribués entre la protection partielle (p=quarantine, 22,1 %), le mode suivi uniquement (p=none, 29,7 %) et aucune configuration DMARC (25,8 %).

L'analyse couvre les organisations dans plus de 15 secteurs et quatre marchés primaires : les Pays-Bas, l'Allemagne, la Belgique et la France. Des différences importantes dans l'adoption de DMARC ont été constatées entre les secteurs, le Finance et la Sécurité de l'Information étant en tête, tandis que le Transport et le Commerce de détail sont considérablement à la traîne.

PRINCIPAUX RÉSULTATS

- **77,6 %** des domaines ne sont pas entièrement protégés contre l'usurpation d'identité par e-mail
- **55,5 %** n'ont pas d'enregistrement DMARC u ont une politique p=none (risque élevé à maximal)
- **2 797 domaines** (25,8 %) n'ont pas d'enregistrement DMARC, face à un risque de sécurité maximal et à des problèmes de livraison d'e-mails
- **30,5 %** des domaines avec DMARC n'ont pas de rapport RUA, opérant à l'aveugle sans surveillance
- **Finance (35,7 %)** et **Sécurité de l'Information (34,6 %)** sont en tête de l'adoption p=reject
- **Transport (15,3 %)** et **Juridique (16,7 %)** ont les taux de protection les plus bas

COMPRENDRE DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) est un protocole d'authentification d'e-mail qui protège les organisations contre l'usurpation d'identité par e-mail et les attaques par hameçonnage. Il s'appuie sur deux mécanismes existants : SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail).

Une politique DMARC indique aux serveurs de courrier électronique récepteurs ce qu'ils doivent faire lorsqu'ils rencontrent un e-mail qui échoue les vérifications d'authentification. Il y a trois niveaux de politique :

Politique	Risque de Sécurité	Ce qui se Passe	Impact
p=reject	BAS	Les e-mails usurpés sont rejetés (retournés)	Protection complète. Les attaquants ne peuvent pas envoyer d'e-mails depuis votre domaine.
p=quarantine	MOYEN	Les e-mails usurpés vont au dossier spam/indésirables	Protection partielle. Les destinataires peuvent encore trouver et faire confiance à des e-mails usurpés dans le spam.
p=none	ÉLEVÉ	Les e-mails usurpés sont livrés normalement	Aucune protection. Suivi uniquement. Les attaquants peuvent usurper librement votre domaine.
Pas de DMARC	MAXIMAL	Aucune instruction pour les serveurs de réception	Aucune protection et aucune visibilité. Cause également des problèmes de livraison d'e-mails avec les grands fournisseurs.

Important : Depuis 2024, les grands fournisseurs de courrier électronique (Google, Microsoft, Yahoo) ont renforcé leurs exigences en matière de livraison d'e-mails. Les organisations qui envoient plus de 5 000 e-mails par semaine sans au moins un enregistrement DMARC basique (p=none) risquent que leurs e-mails légitimes soient rejetés ou filtrés, impactant directement la communication professionnelle et l'efficacité du marketing.

RÉSULTATS GLOBAUX

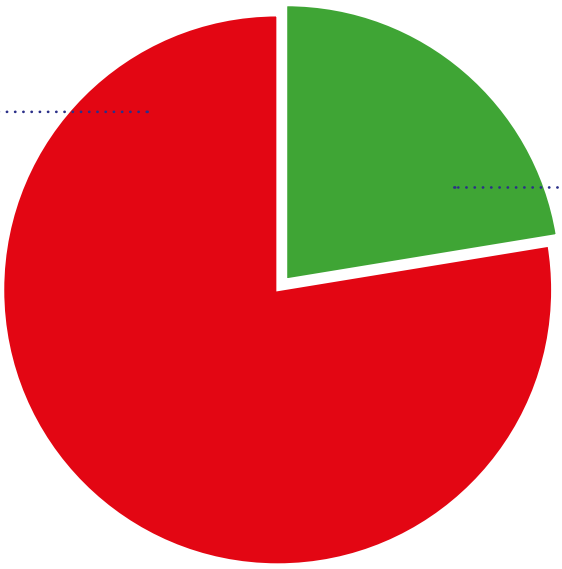
L'analyse DMARC a examiné 10 833 domaines uniques. Le tableau suivant montre la distribution entre les quatre catégories de politique DMARC :

Politique DMARC	Domaines	Pourcentage	Risque de Sécurité	Risque d'E-mail
p=reject	2 432	22,4 %	Bas	Bas
p=quarantine	2 391	22,1 %	Moyen	Bas
p=none	3 213	29,7 %	Élevé	Moyen
Kein DMARC record	2 797	25,8 %	Maximal	Élevé
GESAMT	10 833	100 %		

77,6%

NON ENTIÈREMENT PROTÉGÉ

8 401 Domaines



22,4%

PROTÉGÉ

2 432 Domaines

Pour les 8 401 domaines sans protection complète, les conséquences sont tangibles : les cybercriminels peuvent envoyer des e-mails qui semblent provenir des adresses e-mail légitimes de ces organisations. Pour les 2 797 domaines sans enregistrement DMARC, le risque est aggravé par les problèmes potentiels de livraison d'e-mails, car les grands fournisseurs demandent de plus en plus la conformité DMARC.

ANALYSE PAR SECTEUR

L'adoption de DMARC varie considérablement entre les secteurs. Le tableau ci-dessous montre la distribution de la politique DMARC pour chaque secteur, triée par pourcentage de domaines avec p=reject (entièrement protégés). La colonne « Risque Élevé » représente le pourcentage combiné de domaines avec p=none ou sans enregistrement DMARC, qui sont les plus vulnérables aux attaques d'usurpation d'e-mail.

Secteur	n	p=reject	p=quar.	p=none	Pas DMARC	Risque Élevé
Sécurité de l'Information	179	34,6%	36,3%	15,6%	13,4%	**29,1%**
Finance	381	35,7%	23,9%	28,6%	11,8%	**40,4%**
Gouvernement	401	32,4%	19,5%	6,5%	41,6%	**48,1%**
Logement	58	27,6%	41,4%	29,3%	1,7%	**31,0%**
Régie des eaux	8	37,5%	50,0%	12,5%	0,0%	**12,5%**
Santé	369	27,4%	24,1%	27,9%	20,6%	**48,5%**
Éducation	215	27,0%	25,6%	31,6%	15,8%	**47,4%**
Logiciels & 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%**
Conseil	294	25,5%	21,8%	32,7%	20,1%	**52,7%**
Construction	69	26,1%	24,6%	31,9%	17,4%	**49,3%**
Hébergement	60	21,7%	28,3%	36,7%	13,3%	**50,0%**
Commerce de détail	133	23,3%	15,0%	40,6%	21,1%	**61,7%**
Transport	59	15,3%	20,3%	37,3%	27,1%	**64,4%**
Juridique	24	16,7%	29,2%	33,3%	20,8%	**54,2%**

OBSERVATIONS CLÉS PAR SECTEUR

Leaders

Sécurité de l'Information et **Finance** mènent l'adoption de DMARC avec les taux p=reject les plus élevés (34,6 % et 35,7 % respectivement) et l'exposition au risque la plus faible. La Sécurité de l'Information se distingue avec seulement 29,1 % dans la catégorie à risque élevé. Ces secteurs traitent des données particulièrement sensibles, ce qui entraîne probablement une sensibilisation plus forte à la sécurité des e-mails. Cependant, même ici, la majorité des domaines restent insuffisamment protégés.

Milieu du Classement

Gouvernement présente une image polarisée : un taux p=reject relativement élevé (32,4 %) mais aussi un taux très élevé sans DMARC (41,6 %). Cela suggère que tandis que de nombreux organismes gouvernementaux ont agi, un grand groupe n'a pas commencé. **Les MSP (Managed Service Providers)** montrent une adoption moyenne (25,0 % reject) mais représentent le plus grand groupe en volume (3 212 domaines). Compte tenu de leur rôle dans la gestion de l'informatique pour d'autres organisations, leur propre position DMARC a une importance disproportionnée.

Retardataires

Transport (64,4 % risque élevé) et **Commerce de détail (61,7 % risque élevé)** sont les secteurs les plus exposés. Ces industries interagissent souvent avec les consommateurs par e-mail (notifications d'expédition, reçus, promotions), ce qui en fait des cibles privilégiées pour les attaques d'usurpation. Juridique (54,2 % risque élevé) est également préoccupant compte tenu de la sensibilité et de la confiance inhérentes aux communications juridiques.

ANALYSE GÉOGRAPHIQUE

L'analyse a couvert des domaines provenant principalement de quatre pays : les Pays-Bas, l'Allemagne, la Belgique et la France. Voici comment l'adoption de DMARC se compare entre les régions :

Pays	Domaines	p=reject	p=quarantine	p=none	Pas DMARC
Pays-Bas	4 702	25,9%	24,8%	30,3%	18,9%
Allemagne	3 003	22,7%	20,0%	27,1%	30,2%
Belgique	411	22,6%	29,4%	34,3%	13,6%
France	75	38,7%	29,3%	13,3%	18,7%

Les Pays-Bas sont en tête de l'adoption de DMARC parmi les marchés du Benelux et de la DACH (25,9 % p=reject) et ont le taux le plus bas de domaines sans enregistrement DMARC (18,9 %). Cela peut refléter la promotion active par le gouvernement néerlandais des normes de sécurité des e-mails.

L'Allemagne a le taux le plus élevé de domaines sans enregistrement DMARC (30,2 %), suggérant des lacunes de sensibilisation plus larges malgré un environnement réglementaire en cybersécurité solide.

La Belgique montre l'adoption de quarantine la plus élevée (29,4 %), indiquant que de nombreuses organisations belges ont commencé à implémenter DMARC mais n'ont pas encore procédé à l'application complète.

La France montre l'adoption p=reject la plus forte dans ce benchmark (38,7 %), bien que la taille de l'échantillon soit plus petite (75 domaines). Les organisations françaises ont également le taux p=none le plus bas (13,3 %), suggérant que lorsque les organisations françaises implémentent DMARC, elles ont tendance à passer plus décisivement à l'application. Ceci est notable dans le contexte de l'accent réglementaire fort de la France sur la cybersécurité via l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et de la position proactive du pays sur la transposition de NIS2.

SURVEILLANCE ET RAPPORTS DMARC

Un aspect souvent négligé de la mise en œuvre DMARC est la configuration du RUA (Reporting URI for Aggregate reports). RUA permet aux organisations de recevoir des rapports sur les résultats d'authentification des e-mails, fournissant une visibilité sur qui envoie des e-mails en leur nom et si des tentatives d'usurpation se produisent.

Métrique	Nombre	Pourcentage	Risque
DMARC avec RUA (surveillance active)	5 588	69,5%	Géré
DMARC sans RUA (aucune surveillance)	2 448	30,5%	Aveugle

Adoption RUA par niveau de politique :

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

D'une préoccupation particulière sont les **561 domaines avec p=reject mais sans RUA et 592 domaines avec p=quarantine mais sans RUA**. Ces organisations ont appliqué des politiques DMARC mais n'ont pas de visibilité pour savoir si leurs propres e-mails légitimes sont bloqués en raison de mauvaises configurations. Sans surveillance, elles risquent de perdre silencieusement des communications e-mail essentielles à l'entreprise.

IMPACT COMMERCIAL ET ÉVALUATION DES RISQUES

Risques de Sécurité

Pour les 8 401 domaines sans application p=reject, les vecteurs d'attaque suivants restent viables :

- **Usurpation d'e-mail :** Les attaquants peuvent envoyer des e-mails qui semblent provenir d'adresses e-mail légitimes, ciblant les clients, les employés et les partenaires.
- **Compromission d'E-mail Professionnel (BEC) :** La fraude au PDG, la manipulation de factures et les attaques par redirection de paiement exploitent tous des adresses d'expéditeur usurpées.
- **Usurpation de Marque :** Les campagnes d'hameçonnage qui abusent de votre domaine endommagent la confiance des clients et la réputation de la marque.
- **Attaques de la Chaîne d'Approvisionnement :** Usurper le domaine d'un fournisseur de confiance peut être utilisé pour infiltrer les réseaux des partenaires.

Risques de Livraison d'E-mail

Depuis 2024, Google, Microsoft et Yahoo exigent que les expéditeurs en masse (>5 000 e-mails/semaine) aient au minimum un enregistrement DMARC avec p=none. Pour les 2 797 domaines sans enregistrement DMARC, les e-mails légitimes peuvent être rejetés ou filtrés par ces fournisseurs, impactant directement la communication professionnelle, les campagnes de marketing et les e-mails transactionnels (factures, confirmations, notifications).

Pourquoi l'Examen Périodique de DMARC est Essentiel

La mise en œuvre de DMARC n'est pas une activité ponctuelle. L'infrastructure d'e-mail est dynamique : les organisations adoptent régulièrement de nouveaux outils pour le marketing, la CRM, le support client, la facturation et la communication interne. Chaque nouvel outil qui envoie des e-mails en votre nom doit être correctement authentifié via SPF et DKIM. Sans examen périodique, ces changements introduisent une dérive de configuration qui peut compromettre même une politique DMARC bien configurée.

Les causes courantes de dérive de configuration DMARC incluent :

- **Nouveaux services d'envoi d'e-mail :** Ajouter une plateforme de marketing, un outil de recrutement RH, un système de facturation ou une assistance qui envoie des e-mails depuis votre domaine. Chacun nécessite des mises à jour SPF/DKIM souvent oubliées.
- **Changements SPF du côté du fournisseur :** Les fournisseurs tiers peuvent mettre à jour leurs propres enregistrements SPF ou ajouter de nouvelles inclusions DNS. Parce que SPF évalue toutes les recherches imbriquées (avec un maximum de 10), les changements des fournisseurs peuvent pousser silencieusement votre domaine au-delà de la limite de recherche, causant des échecs d'authentification.
- **Rotation de clé DKIM :** Les clés DKIM doivent être régulièrement rotatées pour la sécurité. Si les enregistrements DNS ne sont pas mis à jour en conséquence, la validation DKIM échouera.
- **Migrations d'infrastructure :** Le passage à une nouvelle plateforme d'e-mail, un fournisseur cloud ou un nouvel environnement informatique introduit souvent des lacunes dans la configuration d'authentification.
- **Paysage des menaces en évolution :** Les attaquants adaptent continuellement leurs techniques. La surveillance des rapports DMARC aide à détecter les nouvelles tentatives d'usurpation ciblant votre domaine, permettant une position de sécurité proactive.

Le risque de ***ne pas*** examiner DMARC périodiquement est double : les e-mails professionnels légitimes peuvent être silencieusement rejetés (impactant les revenus et la communication des clients), tandis qu'au même moment, de nouvelles lacunes de protection peuvent émerger que les attaquants peuvent exploiter. La surveillance continue via les rapports agrégés DMARC (RUA) est le moyen le plus efficace de détecter ces problèmes avant qu'ils n'aient un impact commercial.

Cadres de Conformité et Réglementaires

L'authentification des e-mails et DMARC sont de plus en plus référencés dans les grands cadres réglementaires et les normes de sécurité. Les organisations qui négligent DMARC ne font pas seulement face à des risques directs de sécurité et de livraison, mais peuvent également se trouver en deçà des attentes réglementaires :

Directive NIS2 (UE)

La Directive NIS2 (Network and Information Security Directive 2) de l'UE élargit considérablement le champ des exigences de cybersécurité pour les organisations dans toute l'Europe. NIS2 met l'accent sur la sécurité de la chaîne d'approvisionnement, l'hygiène de la cybernétique et les pratiques de gestion des risques. L'absence d'une politique DMARC avec application (p=reject) pourrait affaiblir la conformité avec plusieurs exigences de NIS2, car l'usurpation d'e-mail reste l'un des vecteurs d'attaque initiaux les plus courants dans les compromissions de la chaîne d'approvisionnement. La plupart des entités « essentielles » font face à une date limite d'audit de conformité de 30 juin 2026. L'implémentation et la maintenance de DMARC avec surveillance est une mesure concrète et auditable qui démontre une gestion des risques proactive.

ISO 27001

ISO 27001 est la norme internationale pour les systèmes de gestion de la sécurité de l'information (ISMS). Bien qu'ISO 27001 ne prescrive pas de technologies spécifiques, son approche basée sur les risques exige que les organisations identifient et atténuent les risques de sécurité de l'information. L'usurpation d'e-mail et l'hameçonnage représentent des risques importants que DMARC aborde directement. Les contrôles de l'annexe A liés à la sécurité des communications (A.13), l'acquisition et le développement des systèmes (A.14) et les relations avec les fournisseurs (A.15) ont tous une pertinence pour l'authentification des e-mails. Les organisations poursuivant ou maintenant la certification ISO 27001 devraient inclure l'application de DMARC dans leur ensemble de contrôles comme une mesure démontrable contre les menaces basées sur les e-mails.

NEN 7510 (Santé, Pays-Bas)

NEN 7510 est la norme néerlandaise pour la sécurité de l'information dans le secteur de la santé, étroitement liée à ISO 27001 mais spécifiquement adaptée au secteur de la santé. La législation néerlandaise exige que les prestataires de soins de santé se conforment à NEN 7510 lors de l'utilisation de systèmes d'information de santé et de systèmes d'échange électronique. Compte tenu que les organisations de santé communiquent fréquemment des données sensibles des patients et des informations de rendez-vous par e-mail, l'application de DMARC est une mesure technique critique pour prévenir l'usurpation d'identité des domaines de santé. Avec 48,5 % des domaines du secteur de la santé dans la catégorie à risque élevé dans notre benchmark, il y a une marge de manœuvre considérable pour l'amélioration. La bonne implémentation de DMARC soutient la conformité avec NEN 7510 en sauvegardant l'intégrité et l'authenticité des communications e-mail.

Dans tous ces cadres, le fil conducteur est clair : l'authentification des e-mails via DMARC n'est plus facultative mais de plus en plus attendue comme une mesure de sécurité de base. Les organisations devraient traiter l'application de DMARC non pas comme un projet autonome mais comme faisant partie de leur gestion continue de la sécurité de l'information, avec des examens périodiques intégrés dans leurs cycles de conformité.

RECOMMANDATIONS

Sur la base des résultats de ce rapport, nous recommandons aux organisations de prendre les mesures suivantes selon leur statut DMARC actuel :

Pour les Domaines Sans Enregistrement DMARC (2 797 domaines)

1. **Implémentez un enregistrement DMARC immédiatement,** en commençant par p=none pour commencer à collecter les données d'authentification sans impacter le flux d'e-mail.
2. **Incluez une adresse RUA** pour recevoir des rapports agrégés DMARC et obtenir une visibilité sur les résultats d'authentification des e-mails.
3. **Vérifiez les configurations SPF et DKIM** pour vous assurer que toutes les sources d'e-mail légitimes sont correctement authentifiées.

Pour les Domaines avec p=none (3 213 domaines)

1. **Analysez les rapports agrégés DMARC** pour identifier toutes les sources d'e-mail légitimes et résoudre les échecs d'authentification.
2. **Planifiez un chemin de migration vers p=quarantine puis p=reject.** Rester sur p=none indéfiniment ne fournit aucune protection.
3. Envisagez d'engager un spécialiste en gestion DMARC pour accélérer la transition vers l'application.

Pour les Domaines avec p=quarantine (2 391 domaines)

1. **Passez à p=reject** une fois que les rapports DMARC confirment que tous les sources d'e-mail légitimes réussissent l'authentification de manière cohérente.
2. Assurez-vous que la rapport RUA est active (actuellement 24,8 % des domaines en quarantine manquent de surveillance).

Pour les Domaines avec p=reject (2 432 domaines)

1. **Maintenez une surveillance DMARC active.** 23,1 % des domaines reject manquent de rapport RUA.
2. Examinez régulièrement les rapports DMARC pour détecter les mauvaises configurations rapidement, particulièrement lors de l'ajout de nouveaux services d'envoi d'e-mail ou la migration d'infrastructure.

Pour Toutes les Organisations

- **Planifiez des examens DMARC périodiques** (au minimum trimestriels) pour détecter la dérive de configuration, les nouveaux expéditeurs non autorisés et les changements dans le paysage des menaces.
- **Intégrez DMARC dans votre programme de conformité** comme un contrôle démontrable pour NIS2, ISO 27001 et les normes spécifiques à un secteur comme NEN 7510.
- **Assurer la sensibilisation de la chaîne d'approvisionnement** : évaluer la position DMARC de vos partenaires et fournisseurs clés dans le cadre de votre processus de gestion des risques tiers.

MÉTHODOLOGIE

Cette étude comparative a été menée selon l'approche suivante :

1. **Collecte de Domaines :** Une liste dédupliquée de 10 833 domaines uniques a été compilée à partir de la plateforme Guardian360, représentant des organisations dans l'écosystème partenaire et client de Guardian360.
2. **Analyse DMARC :** Chaque domaine a été analysé par DMARC Advisor B.V. pour récupérer son enregistrement DNS DMARC actuel, en extrayant la politique (valeur p=), les adresses de rapport (RUA/RUF) et les configurations associées.
3. **Classification Industrielle :** Les domaines ont été appariés avec les enregistrements d'organisations (taux d'appariement de 85,7 %) pour permettre la ventilation par secteur, type d'organisation et géographie.
4. **Période d'Analyse :** L'analyse a été menée en avril 2026. Les enregistrements DMARC sont dynamiques et peuvent changer à tout moment ; ce rapport reflète l'état au moment de l'analyse.

À PROPOS

Guardian360

Guardian360 est une entreprise de cybersécurité basée à Rotterdam, aux Pays-Bas. Guardian360 fournit une surveillance continue de la sécurité, une évaluation des vulnérabilités et des services de conformité aux organisations dans toute l'Europe, directement et par le biais d'un réseau de partenaires Managed Service Provider (MSP).

DMARC Advisor

DMARC Advisor B.V., basée à Dordrecht, aux Pays-Bas, se spécialise dans l'authentification d'e-mail et la gestion DMARC. Leur plateforme aide les organisations à mettre en œuvre et à maintenir DMARC, SPF et DKIM pour protéger les domaines contre l'usurpation d'e-mail et améliorer la livraison d'e-mails.

GUARDIAN 360°
www.guardian360.fr

Avis de non-responsabilité : Ce rapport est basé sur les enregistrements DNS publiquement disponibles et les données de la plateforme Guardian360. Les enregistrements DMARC sont dynamiques et peuvent avoir changé depuis le moment de l'analyse. Les classifications industrielles sont basées sur les données CRM et peuvent ne pas refléter parfaitement le secteur primaire de chaque organisation. Ce rapport est fourni à titre informatif et ne constitue pas un avis juridique ou de conformité.