PERIMETRY RESEARCH

Baromètre de la sécurité des domaines .fr

Les domaines .fr actifs sont-ils bien protégés ? Mesures passives d'un échantillon aléatoire des domaines des données ouvertes du registre du .fr, par âge, fournisseur de messagerie et type de site, comparées aux organismes publics.

Édition de novembre 2026

17 820
domaines actifs mesurés

11,7 %
appliquent DMARC (quarantine ou reject)

3 %
ont A ou B

Perimetry Cloud
perimetry.cloud · Publiée le 14 novembre 2026

À propos de ce rapport

Perimetry Research publie des études sur la façon dont les organisations protègent leurs sites et leur messagerie, mesurée avec les mêmes contrôles passifs que Perimetry Cloud. Cette édition porte sur un échantillon aléatoire de 20 000 domaines tirés parmi les 4 633 263 domaines .fr des données ouvertes de l'Afnic, le registre du .fr ; 17 820 d'entre eux sont actifs. Le registre ne dit pas qui détient la plupart des domaines .fr, et beaucoup appartiennent à des particuliers : ce rapport ne nomme aucun domaine, et chaque chiffre est une moyenne.

Sommaire

01 Synthèse 3

02 Principaux constats 4

03 Notes 5

04 Contrôle par contrôle 6

05 Selon l'âge du domaine 8

06 Selon le fournisseur de messagerie 9

07 Selon le type de site 10

08 Comparaison avec les organismes publics 11

09 Recommandations 12

10 Méthodologie 13

11 À propos de Perimetry 15

01

Synthèse

17 820	32	11,7 %	3 %
domaines actifs mesurés	note moyenne sur 100	appliquent DMARC (quarantine ou reject)	ont A ou B

Note moyenne des 17 820 domaines notés : 32 sur 100 ; médiane 33.

1. 71,6 % des domaines notés ont un enregistrement SPF strict et 38,6 % publient une politique DMARC, mais seulement 11,7 % l'appliquent. Pour les autres, un e-mail falsifié à leur nom (une fausse facture, un changement de RIB) est en général distribué.
2. Côté sites : 59,1 % des domaines qui ont un site à eux ont un certificat valide et 53,4 % renvoient les visiteurs de HTTP vers HTTPS ; 17,3 % utilisent HSTS d'au moins six mois et 14,1 % envoient les en-têtes de protection de base.
3. 25,9 % des domaines sont signés avec DNSSEC ; 1,2 % publient un enregistrement CAA.
4. Les domaines récents font mieux : 37 sur 100 en moyenne pour ceux enregistrés il y a moins de deux ans, 27 pour ceux enregistrés il y a plus de dix ans.
5. Le fournisseur de messagerie compte : les domaines dont la messagerie est chez Google Workspace ont en moyenne 39, chez Microsoft 365 37, chez OVHcloud 29.
6. Au total, 32 sur 100 sur neuf contrôles ; les communes françaises ont en moyenne 47 sur dix.

02

Principaux constats

Ce qu'utilisent les domaines actifs

Fournisseur de messagerie



Microsoft 365 5,1 % Google Workspace 3,8 % OVHcloud 32 %
Autre fournisseur de messagerie 45,5 % Pas de serveur de messagerie (pas de MX) 13,7 %

Site web



WordPress 17 % Un créateur de sites (Wix, Shopify, Squarespace, Webflow, Jimdo) 4,4 %
Un autre type de site 60,5 % Pas de site à lui (messagerie seule, ou renvoi vers un autre domaine) 18,1 %

Messagerie : DMARC rarement appliqué

71,6 % des domaines notés ont un enregistrement SPF strict et 38,6 % publient une politique DMARC, mais seulement 11,7 % l'appliquent. Pour les autres, un e-mail falsifié à leur nom (une fausse facture, un changement de RIB) est en général distribué.

Les sites

Côté sites : 59,1 % des domaines qui ont un site à eux ont un certificat valide et 53,4 % renvoient les visiteurs de HTTP vers HTTPS ; 17,3 % utilisent HSTS d'au moins six mois et 14,1 % envoient les en-têtes de protection de base.

DNS

25,9 % des domaines sont signés avec DNSSEC ; 1,2 % publient un enregistrement CAA.

Les domaines anciens sont à la traîne

Les domaines récents font mieux : 37 sur 100 en moyenne pour ceux enregistrés il y a moins de deux ans, 27 pour ceux enregistrés il y a plus de dix ans.

Le fournisseur de messagerie

Le fournisseur de messagerie compte : les domaines dont la messagerie est chez Google Workspace ont en moyenne 39, chez Microsoft 365 37, chez OVHcloud 29.

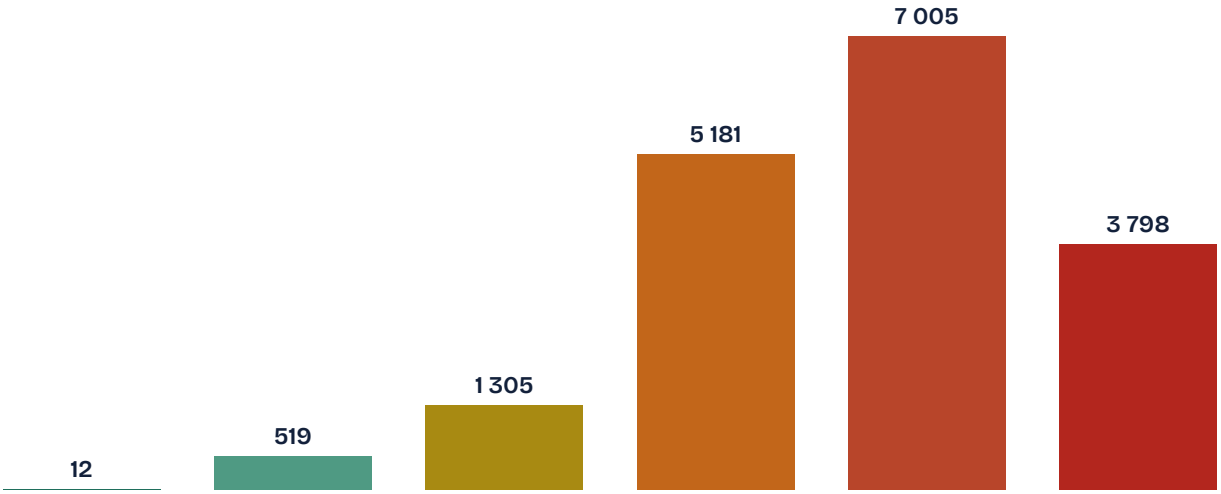
Comparaison avec les communes

Au total, 32 sur 100 sur neuf contrôles ; les communes françaises ont en moyenne 47 sur dix.

03

Notes

Chaque domaine actif reçoit une note : la part des neuf contrôles qu'il réussit, parmi ceux qui le concernent (la note de nos études des organismes publics, sans le contrôle de l'adresse de contact, qu'un domaine seul ne donne pas). A à partir de 90, B de 75, C de 60, D de 40, E de 20, F en dessous.

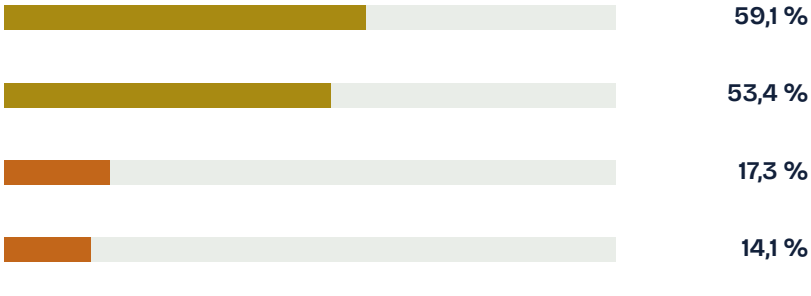


04

Contrôle par contrôle

Part des domaines notés qui réussissent chaque contrôle, parmi ceux qu'il concerne. Les contrôles du site ne concernent que les domaines qui ont un site à eux.

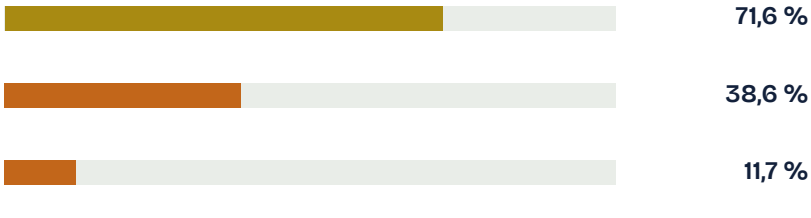
Site web



DNS



E-mail



Les neuf contrôles	
Site web · Certificat HTTPS valide	Le site répond en HTTPS avec un certificat en cours de validité, émis pour son nom et reconnu par les navigateurs.
Site web · HTTP renvoie vers HTTPS	Quelqu'un qui tape l'adresse arrive sur le site chiffré, et non sur une page que n'importe qui sur le réseau peut lire ou modifier.
Site web · HSTS d'au moins six mois	Les navigateurs retiennent qu'il faut utiliser HTTPS : la première requête non chiffrée ne peut pas être détournée.
Site web · En-têtes de protection de base	X-Content-Type-Options: nosniff, et une protection contre l'affichage du site dans le cadre d'un autre site (X-Frame-Options ou frame-ancestors dans la CSP).
DNS · DNSSEC	Les réponses DNS du domaine sont signées : on ne peut pas faire croire à un résolveur que son site ou sa messagerie sont ailleurs.
DNS · Enregistrement CAA	Le domaine désigne les autorités de certification autorisées à émettre des certificats à son nom.

Les neuf contrôles	
E-mail · SPF strict	Le domaine liste les serveurs autorisés à envoyer son courrier et demande de rejeter ou de signaler les autres (-all ou ~all).
E-mail · Enregistrement DMARC	Le domaine publie une politique DMARC, la norme qui relie SPF et DKIM à l'expéditeur affiché.
E-mail · DMARC appliqué	La politique est quarantine ou reject : un message falsifié au nom du domaine, une fausse facture envoyée à un client par exemple, part en indésirables ou est refusé, au lieu d'être distribué.

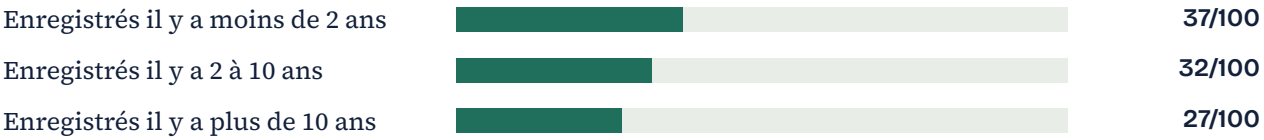
05

Selon l’âge du domaine

D’après la date de création du fichier du registre.

Groupe	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
Enregistrés il y a moins de 2 ans	5 705	37	4,3 %	12,9 %	33
Enregistrés il y a 2 à 10 ans	7 704	32	2,5 %	11 %	33
Enregistrés il y a plus de 10 ans	4 411	27	2,2 %	11,1 %	22

Moyenne



DMARC appliqué



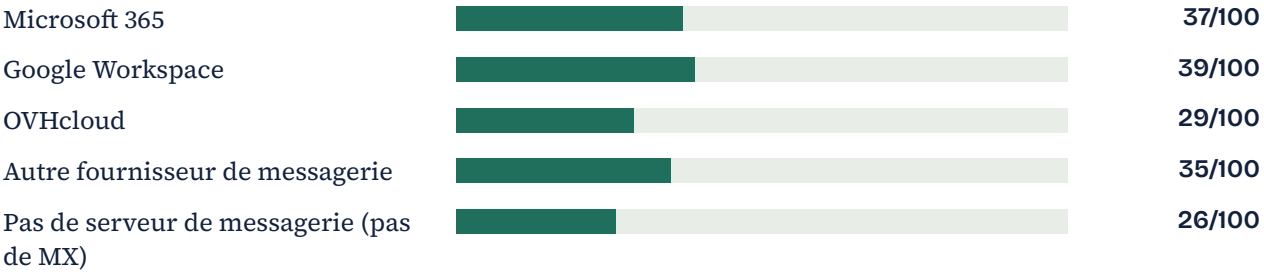
06

Selon le fournisseur de messagerie

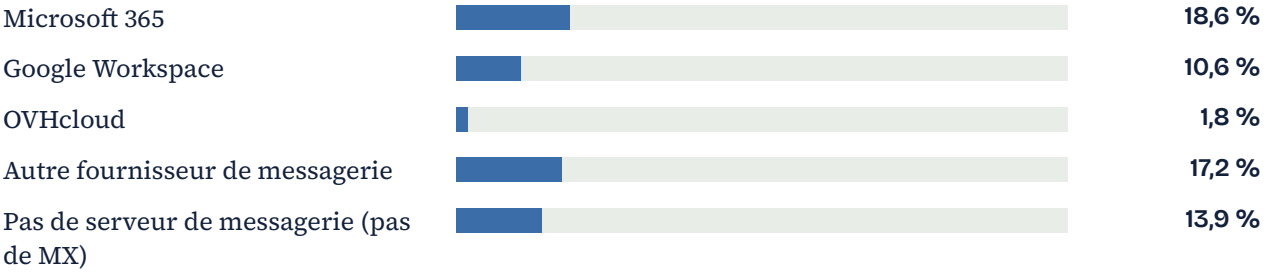
D'après le nom des serveurs de messagerie (MX) du domaine. OVHcloud installe par défaut ses serveurs de messagerie sur une grande partie des domaines enregistrés chez lui : son groupe mêle des messageries en service et des réglages laissés tels quels.

Groupe	Part	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
Microsoft 365	5,1 %	903	37	4,9 %	18,6 %	33
Google Workspace	3,8 %	679	39	4,3 %	10,6 %	40
OVHcloud	32 %	5 696	29	1,2 %	1,8 %	22
Autre fournisseur de messagerie	45,5 %	8 108	35	3,5 %	17,2 %	33
Pas de serveur de messagerie (pas de MX)	13,7 %	2 434	26	4,4 %	13,9 %	22

Moyenne



DMARC appliqué



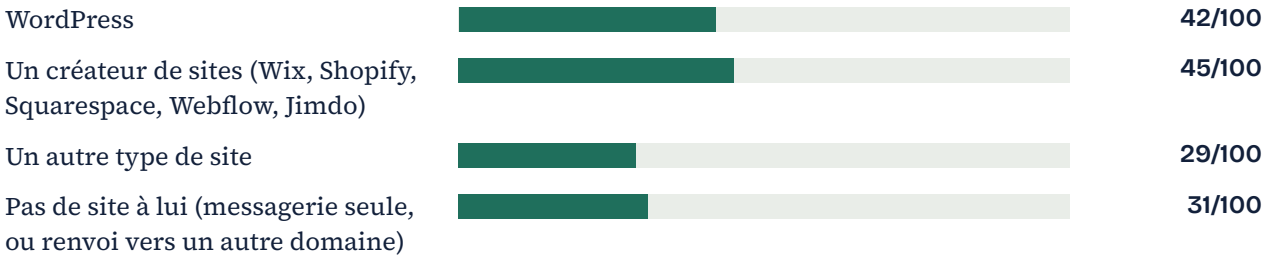
07

Selon le type de site

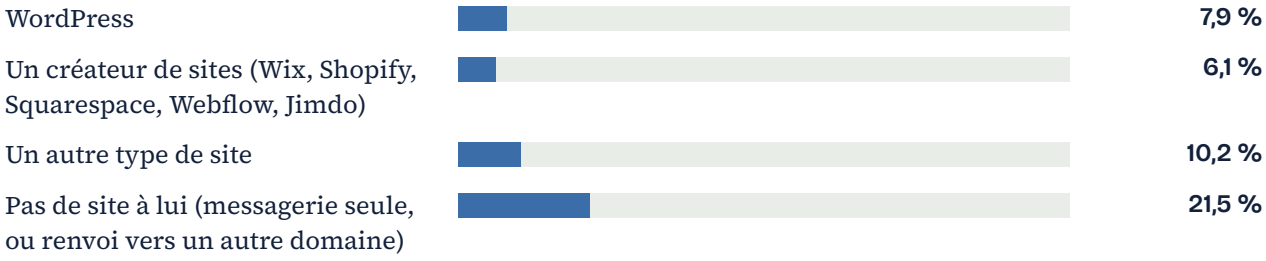
D’après la page d’accueil. Un domaine sans site à lui (messagerie seule, ou site qui renvoie vers un autre domaine) est noté sur son DNS et sa messagerie seulement.

Groupe	Part	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
WordPress	17 %	3 030	42	2,6 %	7,9 %	44
Un créateur de sites (Wix, Shopify, Squarespace, Webflow, Jimdo)	4,4 %	782	45	4,3 %	6,1 %	44
Un autre type de site	60,5 %	10 790	29	2,1 %	10,2 %	22
Pas de site à lui (messagerie seule, ou renvoi vers un autre domaine)	18,1 %	3 218	31	5,9 %	21,5 %	20

Moyenne



DMARC appliqué



08

Comparaison avec les organismes publics

Les mêmes contrôles que nos études des communes, des collectivités et des établissements d'enseignement supérieur français (dernières éditions) : part des organismes notés qui réussissent chacun. Leurs moyennes comptent dix contrôles pour les communes et les collectivités, neuf pour l'enseignement supérieur et les domaines .fr.

	Communes	Collectivités	Enseignement supérieur	Domaines .fr
Note moyenne	47	60	64	32
Certificat HTTPS valide	93,4 %	98,7 %	100 %	59,1 %
HTTP renvoie vers HTTPS	86,4 %	90,9 %	95,2 %	53,4 %
HSTS d'au moins six mois	28,3 %	38,8 %	46,1 %	17,3 %
En-têtes de protection de base	26,1 %	40,7 %	57,5 %	14,1 %
DNSSEC	22,1 %	25,9 %	12,7 %	25,9 %
Enregistrement CAA	2,8 %	2,6 %	41 %	1,2 %
SPF strict	85,9 %	97,1 %	93 %	71,6 %
Enregistrement DMARC	45,2 %	77,8 %	86,9 %	38,6 %
DMARC appliqué	19,2 %	32,8 %	45,4 %	11,7 %

09

Recommandations

1 Appliquer DMARC

Publier une politique DMARC ne suffit pas : lire ses rapports quelques semaines, recenser chaque service qui envoie en votre nom (facturation, lettre d'information, boutique en ligne), puis passer à quarantine et reject. C'est ce qui empêche un e-mail falsifié à votre nom d'arriver chez vos clients.

2 Rediriger vers HTTPS et activer HSTS

Chaque visite doit arriver sur le site chiffré ; HSTS le fait retenir aux navigateurs. La plupart des hébergeurs et des créateurs de sites proposent les deux dans un réglage.

3 Signer son domaine avec DNSSEC et ajouter un enregistrement CAA

La plupart des bureaux d'enregistrement proposent DNSSEC, souvent en un clic. Un enregistrement CAA désigne les autorités autorisées à émettre vos certificats.

4 Revoir les anciens réglages

Plus un domaine est ancien, plus sa note est basse : des enregistrements faits il y a des années (un ancien fournisseur de messagerie dans le SPF, un site que plus personne ne met à jour) sont rarement revus.

5 Surveiller dans la durée

Les certificats expirent, les prestataires changent, des enregistrements se perdent lors d'une migration. Un contrôle régulier le voit avant vos clients.

10

Méthodologie

Des contrôles passifs uniquement

Nous lisons ce que n'importe quel visiteur ou serveur de messagerie peut voir : les enregistrements DNS publics, l'enregistrement du domaine (RDAP), le certificat TLS, une requête sur la page d'accueil en HTTP (sa redirection est lue, pas suivie), et la page d'accueil en HTTPS (en suivant ses redirections, comme un navigateur). Rien d'autre n'est demandé au site. Quand un domaine publie une politique MTA-STS, son fichier de politique est lu aussi, comme le font les serveurs de messagerie.

Pas de balayage de ports, pas de recherche de sous-domaines, pas de tentative de connexion, pas de formulaire, pas de test de vulnérabilité. Le robot est lent exprès et répartit ses requêtes sur plusieurs heures.

Le robot

Il se présente comme PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). Si vous gérez un site qu'il a visité et préférez qu'il ne le fasse plus, écrivez à hello@perimetry.cloud : nous retirerons le domaine des prochaines éditions.

L'étude des domaines .fr actifs

Population étudiée : les domaines .fr des données ouvertes de l'Afnic, le registre du .fr (fichier A, « Noms de domaine en .fr », Licence Ouverte), encore enregistrés, en .fr simple (pas asso.fr, com.fr ni semblables) et non internationalisés. Le fichier ne donne le type de titulaire que pour très peu de domaines, les données des titulaires étant protégées : les quelques domaines indiqués comme détenus par une personne physique, ou par un titulaire hors de France, sont écartés ; tous les autres sont gardés. L'édition de novembre 2026 part du fichier de septembre 2026 : 4 633 263 domaines retenus.

Un échantillon aléatoire de 20 000 d'entre eux est mesuré, tiré de nouveau à l'identique à partir de la graine de l'édition. Avec un échantillon de cette taille, une part mesurée sur l'ensemble est à environ un point près de la part parmi tous les domaines retenus (confiance de 95 %) ; pour un groupe, la marge grandit à mesure que le groupe est petit.

Comme le titulaire est inconnu pour la plupart des domaines, l'étude ne peut pas distinguer le domaine d'une entreprise de celui d'une association ou d'un particulier. C'est pourquoi elle ne nomme jamais un domaine, pas même les bons élèves : elle ne publie que des moyennes.

Un domaine est inactif, compté et écarté, quand il n'existe pas dans le DNS ou n'a ni site en service ni serveur de messagerie : une page parking ou une page d'attente d'hébergeur n'est pas un site en service. Le site est lu sur le domaine lui-même, puis sur www quand le domaine lui-même n'a pas de site. Un domaine dont le site renvoie vers un autre domaine (un alias de l'adresse principale d'une marque, par exemple) est noté sur son DNS et sa messagerie seulement, son site étant celui d'un autre.

Les contrôles, la note et les lettres de l'étude des communes, sans le contrôle de l'adresse de contact, qu'un domaine seul ne donne pas : neuf contrôles, comme dans l'étude de l'enseignement supérieur. Un domaine doit avoir trois contrôles applicables pour être noté.

Groupes : par âge (d'après la date de création du fichier de l'Afnic), par fournisseur de messagerie (d'après le nom des serveurs de messagerie, MX, du domaine : Microsoft 365, Google Workspace, OVHcloud, un autre fournisseur, aucun) et par type de site (d'après la page d'accueil : WordPress, un créateur de sites, un autre type de site, pas de site à lui). OVHcloud installe par défaut ses serveurs de messagerie sur une grande partie des domaines enregistrés chez lui : son groupe mêle des messageries en service et des réglages laissés tels quels. Les bureaux d'enregistrement ne sont pas publiés.

Limites

Chaque édition est une photographie prise en quelques heures. L'annuaire peut être en retard ou erroné ; nous l'utilisons tel qu'il est publié. Les clés DKIM ne sont cherchées que sur les sélecteurs courants : elles ne sont donc pas notées. Un site derrière un service de protection peut répondre à un robot autrement qu'à un visiteur. Les serveurs de messagerie ne sont pas testés (STARTTLS demande le port 25, que l'infrastructure de l'étude ne peut pas joindre).

11

À propos de Perimetry

Perimetry est un outil libre qui audite l'extérieur d'un domaine comme n'importe qui sur Internet le voit : authentification des e-mails, DNS, certificats, serveurs de messagerie, sites. Perimetry Cloud en est la version hébergée, avec surveillance continue, alertes et rapports, pour les organisations et les agences qui s'en occupent.

Citer : Perimetry Research, Baromètre de la sécurité des domaines .fr, novembre 2026. https://perimetry.cloud/fr/research/fr-domains/

Vous pouvez réutiliser les chiffres de ce rapport avec un lien vers l'étude. Les données ouvertes de l'Afnic restent sous Licence Ouverte (source : Afnic, fichier A des domaines en .fr).

Contact : hello@perimetry.cloud

`https://perimetry.cloud/fr/research/fr-domains/`